Verkehr

Überwachung

Foto: Shutterstock/chombosan

Wie Autohersteller unsere Daten sammeln

Nach den Wünschen von Politik und Grosskonzernen soll das Auto der Zukunft dem Fahrer jegliche Eigenverantwortung nehmen und automatisch von einem Bordcomputer gesteuert werden. Das Aufgeben der Verantwortung birgt jedoch grosse Risiken: Wer nicht selbst steuert, unterwirft sich sowohl der Überwachung als auch der Kontrolle anderer.

Der ADAC fand heraus, dass moderne Autos ihren Herstellern via Sim-Karte massenweise Daten senden. Die Untersuchung zeigte u.a., dass neben der Position des Fahrzeugs oder Zielen im Navigationssystem sogar Kontaktdaten der Handys von Insassen auf den Servern der Autohersteller landen.

Autohersteller können heute schon auf das einzelne Auto aus der Ferne zugreifen. Renault kann beispielsweise beim Elektroauto Zoé das Aufladen der Antriebsbatterie verhindern. Das zeigt, wie leicht den Fahrern schon jetzt die Souveränität über ihr Fahrzeug entzogen werden könnte.

Wie es scheint, werden in Zukunft Hersteller, Versicherer und höchstwahrscheinlich auch der Staat auf die eigentlich privaten Daten über die Position und das Verhalten des Fahrers zugreifen können. Garantieleistungen könnten verwehrt bzw. Versicherungsprämien erhöht werden, weil die Hersteller bzw. Versicherer Informationen über das risikoreiche Fahrverhalten des Automobilbesitzers erhalten. Sobald der Staat Zugriff auf diese Daten bekäme, bräuchte es keine Blitzer und Verkehrspolizisten mehr, denn jede Geschwindigkeitsüberschreitung könnte dann einfach digital bestraft werden, wie Justizminister Heiko Maas es sogar schon angedeutet hat.

Der nächste Schritt wäre dann das selbstfahrende Auto. Eine technische Utopie, mit der es anscheinend gar nicht schnell genug gehen kann. Die vorhandene Technologie, die eigentlich noch jahrzehntelange Forschungsarbeit bräuchte, um auszureifen, wird der Öffentlichkeit momentan im Eiltempo aufgedrückt, ohne dass man die Autofahrer je nach ihrer Meinung gefragt hätte.

Warum die Politik das selbstfahrende Auto kaum noch erwarten kann, lässt sich erahnen: Da die Freiheiten, die ein normales Auto bietet, den Regierenden ein Dorn im Auge sein könnten, könnte es jetzt schnellstmöglich darum gehen, eine Technologie zu entwickeln und unters Volk zu bringen, bei der letztlich der Staat am Steuer sitzt. Der Staat würde einfach einen Code benutzen, um sich in den Bordcomputer einzuklinken und könnte somit jederzeit die Kontrolle des Fahrzeugs übernehmen.

Laut einem Bericht des SRF hat der deutsche ADAC in einer aufwendigen Analyse vier Fahrzeug-Modelle von drei Automarken genauer untersucht: Einen Mercedes der B-Klasse, einen Renault Zoé sowie zwei Modelle von BMW, das Elektromobil i3 und den 320.

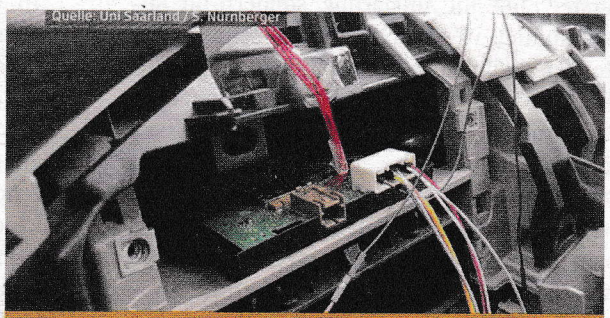
«Bei den vier Fahrzeugen, die wir untersucht haben, waren wir überrascht, welche Mengen an Daten erzeugt und übertragen werden und dass gegenüber dem Konsumenten keinerlei Details vermittelt werden», fasst Arnulf Thiemel gegenüber dem SRF die insgesamt zweijährige Untersuchung zusammen.

«Da werden regelmässig ganze Datenpakete an den Hersteller geschickt, bei denen wir uns weder mit böswilligster noch mit gutwilligster Betrachtungsweise vorstellen können, was die Hersteller damit anfangen wollen», erklärt Thiemel.

Die Recherche des ADAC zeigt auch, dass sogar Kontaktdaten des Handys auf den Server des Autoherstellers geschickt werden.

In modernen Autos stecken bis zu 200 Sensoren. Diese erheben bei jedem Fahrkilometer unzählige Daten.

Foto: S 400 HYBRID (https://commons.wikimedia.org/wiki/File:Mercedes_C_200_Kompressor_Elegance_(W204)_front_20100603.jpg)



Via eingebauter Sim-Karte sendet das Auto über Mobilfunk automatisch ganze Datenpakete zum Hersteller. Dieser erfährt so vieles über Fahrzeug und Halter. Foto: SRF

...nd Entmündigung durch ...moderne Autos

...der welche Musik der Autofahrer abgespielt ...at. Diese Daten seien besonders problema...isch, weil sie Aufschluss über den Nutzer des ...utos geben würden, so Thiemel.

...Hersteller-Zugriff aus der Distanz

Äusserst brisant: Autohersteller können ...uch auf das individuelle Auto aus der Ferne ...ugreifen. Renault kann beispielsweise beim ...Elektroauto Zoé das Aufladen der Antriebs...batterie verhindern. «Der Fahrzeughersteller ...kann sogar den Antriebs-Akku abschalten. ...Und zwar dann, wenn Sie beispielsweise Ihre ...Leasinggebühr für den Akku nicht bezahlt ...haben», unterstreicht Arnulf Thiemel vom ...ADAC. So könnte Renault verhindern, dass ...das Auto wieder aufgeladen werden kann.

Renault schreibt hierzu an den SRF: «Die ...Unterbindung des Ladevorgangs eines Ren...ault Zoé per Mobilfunkverbindung ist bei ...Schweizer Renault Privatkunden noch nie ...eingesetzt worden.» Im extremen und un...wahrscheinlichen Fall sowie nach mehr...maliger Kontaktaufnahme mit dem Fahrer ...könne Renault den Ladevorgang unterbin...den. Das ändert jedoch nichts daran, dass die ...Technik zur Deaktivierung aus der Ferne be...reits voll funktionsfähig ist.

...ntransparente Autofirmen

Die vom ADAC untersuchten Automarken ...Renault, Mercedes und BMW behaupten alle, ...sie hielten sich an die Datenschutzbestim...mungen. Der Käufer stimme dem Daten-Aus...tausch beim Kauf zu und er würde an meh...reren Orten transparent darüber informiert. ...Eine Auflistung aller erhobenen Daten liefern ...die Hersteller nicht.

Eine Umfrage des SRF bei den zwölf Au...tomarken, die in der Schweiz am häufigsten ...verkauft werden, verlief sehr ernüchternd. ...Auch nach mehrmaligem Nachfragen schaff...ten es drei Anbieter nicht, klare Antworten zu ...liefern. Die simple Frage lautete: Welche Da...ten werden bei Ihrem meistverkauften Modell ...sowie bei Ihrem neusten Modell erhoben, ver...arbeitet, gespeichert und extern übermittelt?

Klar äussert sich Toyota: Man verbaue kei...ne SIM-Karten in den Autos. Eine Datenüber...mittlung sei somit ausgeschlossen. Und Opel liefert als einzige Marke eine nahezu vollständige Übersicht der gesammelten und gesendeten Daten inklusive Verwendungszweck.

Alle anderen Autobauer schreiben sinngemäss, dass ihnen Transparenz wichtig sei und sie nach geltenden Datenschutzrichtlinien handeln würden. Ausserdem würde die Käuferschaft dem Datenaustausch ausdrücklich zustimmen.

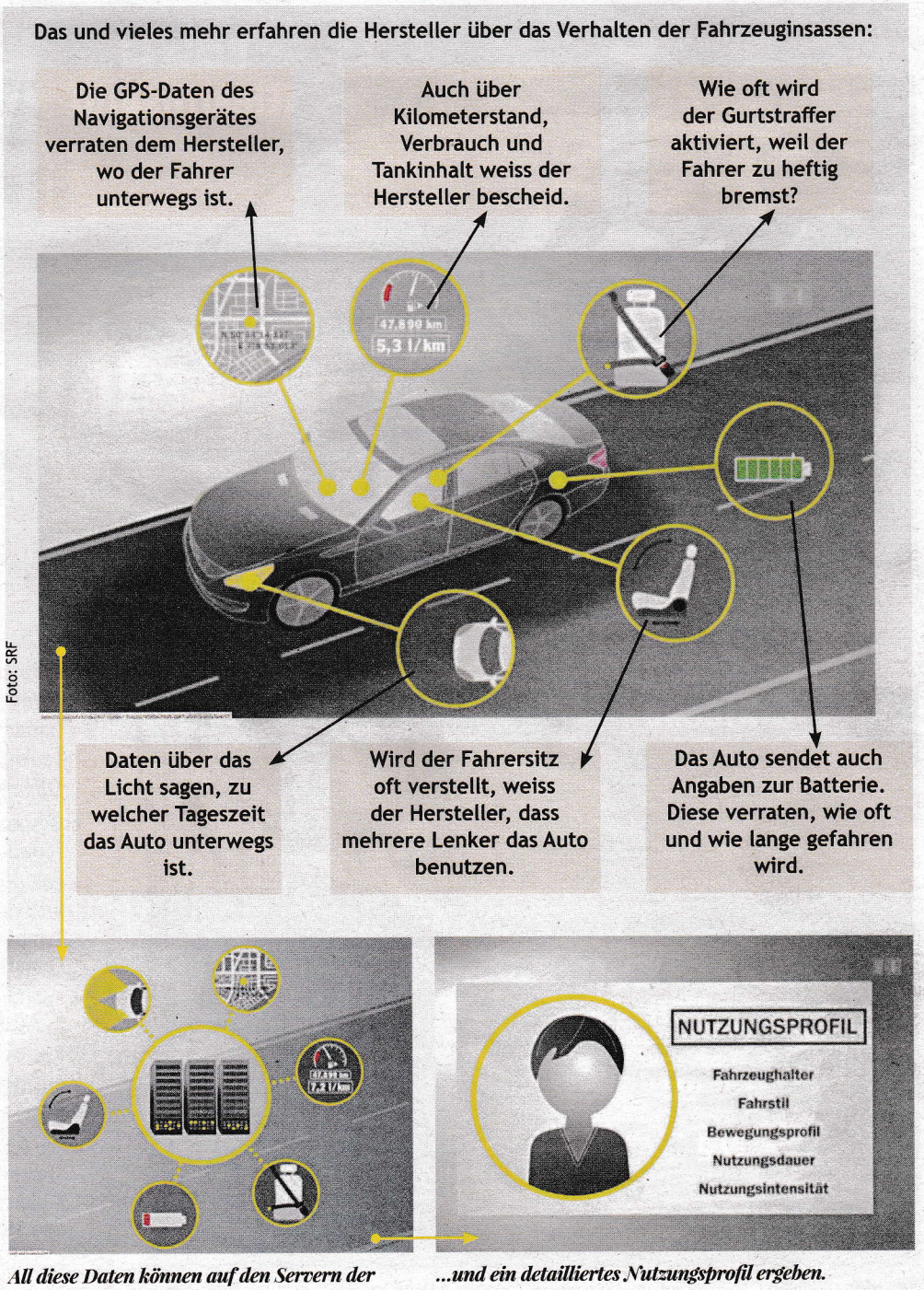


Foto: SRF

All diese Daten können auf den Servern der Fahrzeughersteller landen...

...und ein detailliertes Nutzungsprofil ergeben.

BMW 320d

...93 (https://commons.wikimedia.org/wiki/File:BMW_320d_Touring_(F31)_%E2%80%93_Frontansicht,_11._Februar_2013,_D%C3%BCsseldorf.jpg) https://creativecommons.org/licenses/by-sa/3.0/de/deed.en

- Maximaldrehzahl des Motors mit jeweiligem Kilometerstand (erlaubt Rückschlüsse auf den Fahrstil)
- **Fahrstrecken**
- Dauer der Fahrt in den jeweiligen Modi des Automatikgetriebes (Rückschlüsse auf Fahrstil)
- Betriebsstunden der Fahrzeugbeleuchtung, getrennt nach Lichtquellen
- Zahl der Fahrersitz-Justierungen (erlaubt Rückschlüsse auf Anzahl Fahrer)
- Anzahl der eingelegten Medien ins CD-/DVD-Laufwerk
- Zahl der elektromotorischen Gurtstraffungen z.B. aufgrund starker Bremsmanöver (Erlaubt Rückschlüsse auf den Fahrstil)
- **Bei Anbindungen des Handys via Bluetooth Kontaktdaten (je nach Telefonmodell)**
- **Ins Navigations-System eingegebene Ziele**

BMW i3 (Elektroauto)

Foto: TTTNIS (https://commons.wikimedia.org/wiki/File:BMW_i3_01.jpg) https://creativecommons.org/publicdomain/zero/1.0/deed.en

- Detaillierte Daten der Antriebsbatterie (wie Ladezustand, Zelltemperatur usw.)
- Gewählter Fahrmodus (eco, eco plus, sport)
- Wie oft wurde der Ladestecker eingesteckt?
- Wie und wo wurde geladen, wie stark war die Antriebsbatterie entladen
- Kilometerstand bei Bedienvorgängen wie z.B. Laden
- Position der 16 zuvor benutzten Ladestationen
- **Rund 100 letzte Abstellpositionen des Fahrzeugs**
- **Telefonkontakte des Handys des Fahrers**
- **Abgespielte Musiktitel**

Mercedes-Benz B-Klasse

Foto: Matthias93 (https://commons.wikimedia.org/wiki/File:Mercedes_B-Klasse_Sportpaket_front.jpg) https://creativecommons.org/licenses/by-sa/3.0/deed.en

- **Etwa alle zwei Minuten werden die GPS-Position des Autos sowie Statusdaten an den Hersteller übertragen (unter anderem Kilometerstand, Verbrauch, Tankfüllung, Reifendruck sowie Füllstände von Kühlmittel, Wischwasser oder Bremsflüssigkeit)**
- Gespeichert wird die Anzahl der Gurtstraffungen (erlaubt Rückschlüsse auf den Fahrstil)
- Fehlerspeichereinträge werden teilweise mit Informationen über zu hohe Motordrehzahl oder -Temperatur abgelegt (erlaubt Rückschlüsse auf den Fahrstil)
- Fahrkilometer auf der Autobahn, ausserorts und in der Stadt werden getrennt gespeichert (erlaubt Rückschlüsse auf das Nutzungsprofil)
- Betriebsstunden der Fahrzeugbeleuchtung werden gespeichert
- Die letzten 100 Lade- und Entladezyklen der Starterbatterie werden mit Uhrzeit, Datum und Kilometerstand gespeichert. Daraus ergeben sich Fahr- und Standzeiten.

Renault Zoe (Elektroauto)

- **Aufladen der Antriebsbatterie kann von Renault via Mobilfunkverbindung jederzeit unterbunden werden. Der Autobauer kann also aus der Ferne auf das Auto zugreifen. Was wäre, wenn sich der Hersteller in der Zukunft das Recht herausnehmen würde, den Antriebsakku abzuschalten, z.B. bei nicht gezahlten Leasing-Gebühren?**
- Bei jeder Fahrt, spätestens nach jeweils 30 Minuten, wird ein Datenpaket (u.a. Fahrgestellnummer, div. Seriennummern, Datum, Uhrzeit, GPS-Position, Temperatur, Ladung und Zellspannung der Hochvolt-Antriebsbatterie) an Renault gesendet. Der Hersteller kann die Informationen jederzeit anfordern.

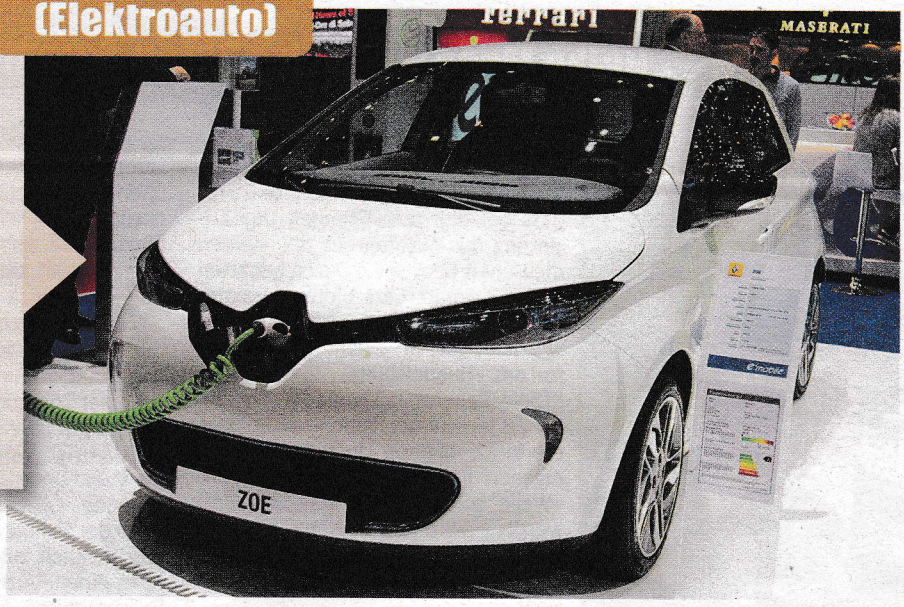
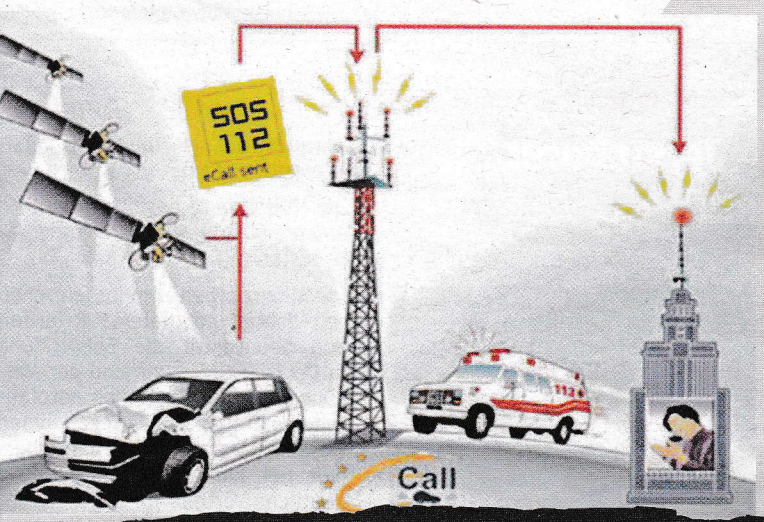


Foto: Clément Bucco-Lechat (https://commons.wikimedia.org/wiki/File:Geneva_MotorShow_2013_-_Renault_Zoe_charging.jpg) https://commons.wikimedia.org/wiki/User:Pleclown

srf.ch, Datenkrake Auto – Wie uns Autobauer ausspähen, 21.02.2017



Zwangseinführung des eCall-Notrufsystems: Lückenlose Überwachung des Autos ab 2018

Ab 2018 wird das automatische Notrufsystem eCall in allen neuen Pkw-Modellen in der EU zur Pflicht. Das EU-Parlament stimmte am 28.04.2015 abschliessend für das neue System, mit dem nach Schätzungen der EU-Kommission die Zahl der Unfalltoten um zehn Prozent verringert werden könnte.

Bei einem Unfall soll eCall automatisch den einheitlichen europäischen 112-Notruf auslösen. So sollen Helfer schneller zum Unfallort geführt werden – auch wenn der Fahrer bewusstlos ist. Die elementaren Bestandteile dieser ab 2018 für jeden Neuwagen verordneten Technologie sind ein GPS- und ein GSM-Modul zur Positionsbestimmung und für den Aufbau einer Daten- und Telefonverbindung.

Die eCall-Kritikerin Nadja Hirsch aus dem EU-Parlament erläuterte dem ARD-Magazin «Fakt» 2014, dass eCalls Überwachungsmöglichkeiten jedoch über Notrufe hinausgehen: «Die Kommission hat jetzt schon ganz klar gesagt, dass dieser Mechanismus auch genutzt werden kann, um gestohlene Autos zu finden. Das macht klar, dass die Sim-Karte jederzeit von aussen aktiviert werden kann, und das heisst natürlich: Wenn eben irgendjemand anderes – egal ob es ein Geheimdienst ist, eine Polizei, ein Steuerfahnder, dergleichen – dich finden will, wird er diesen Mechanismus dann aktivieren.»

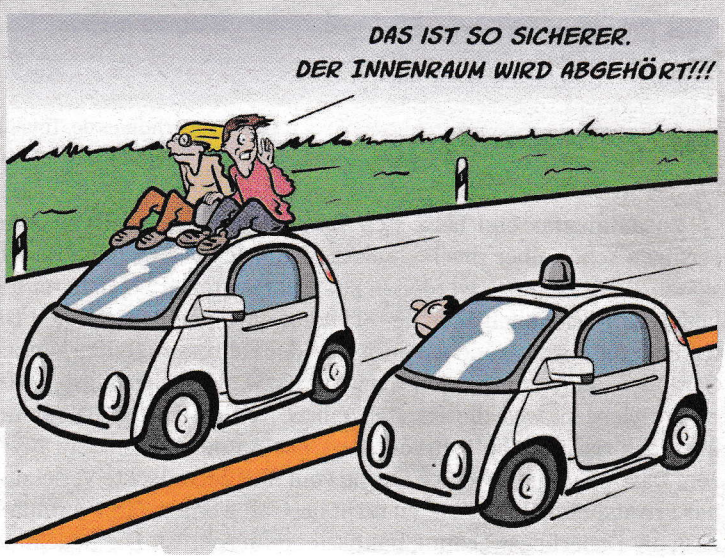
Die Mehrheit des EU-Parlaments stimmte gegen die Option, dass das System vom Fahrer deaktiviert werden könnte. «Der Verbraucher hat gar keine Wahl mehr. Er hat nicht die Wahl, ob es eingebaut wird oder nicht, und er hat auch nicht mehr die Wahl, ob dieses System, wenn es denn eingebaut ist, an – oder ausgeschaltet werden kann», kritisiert Hirsch.

Diese Verordnung ist symptomatisch für die Geisteshaltung der EU-Eliten und «Digitalisierer». Dem Verbraucher wird versprochen, es ginge um seine Sicherheit und deshalb müsste man ihn zu seinem Glück zwingen. Über die eigentlichen Wünsche des Verbrauchers wird achselzuckend hinweggesehen. Er hat nicht die Wahl zwischen mehr Freiheit oder mehr Sicherheit, seine Sicherheit wird ihm von oben aufgezwungen und perfide als «Modernisierung» verkauft.

Doch nach der antidemokratischen und destruktiven Politik (Grenzöffnung, Euro-Krise usw.) der letzten Jahre will man der EU nicht mehr so recht glauben, ihr läge die Sicherheit ihrer Bürger am Herzen. So schlussfolgert sogar die ARD: «Ebenso ging es mit der Abschaffung des Bankgeheimnisses. Zunächst sollten dadurch Terroristen gejagt werden, was erfolglos blieb. Drei Jahre später konnten die Finanzämter und Sozialbehörden auf die Kontodaten schauen, wovon massenweise Gebrauch gemacht wird. Sicherheit dient regelmässig als Türöffner.»

Die Abgeordnete Hirsch bemerkt abschliessend: «Wir merken sehr stark, dass [...] immer der Sicherheitsaspekt nach vorne geschoben wird, um die Freiheit der Menschen und auch die freie Entscheidung des Verbrauchers immer stärker einzuengen. Wir werden niemals hundertprozentige Sicherheit haben, aber was man hundertprozentig sagen kann, ist, dass die Freiheit immer stärker eingeschränkt wird.»

Quellen: epochtimes.de, eCall im Auto: Back to the future – die totale Überwachung, 29.04.2015
Youtube.com, E-Call wie die EU Autofahrer ausspionieren will, 08.04.2014



Heiko Maas warnt vor Daten-Sammelwut bei intelligenten Autos

Foto: Sandro Halank, Wikimedia Commons, CC-BY-SA 3.0

Ausgerechnet er? Bundesjustizminister Heiko Maas (SPD) mahnte 2015, dass bei der zunehmenden Digitalisierung des Autofahrens der Mensch die Hoheit über seine Daten behalten müsse. «Smart Cars bieten faszinierende Möglichkeiten», schrieb der SPD-Politiker in einem Gastbeitrag für das «Handelsblatt». Immer mehr Kfz-Versicherer böten Tarife an, bei denen jene einen Rabatt bekommen, die in die digitale Überwachung des eigenen Fahrverhaltens einwilligen. «Wenn solche Tarife zum Regelfall werden, wird die Freiheit des unkontrollierten Fahrens ein kostspieliger Luxus oder ganz unmöglich», so Maas.

Noch gehe es nur darum, Schadensfälle zu vermeiden, aber vorhandene Daten weckten stets Begehrlichkeiten. «Bewegungs- und Verhaltensprofile könnten erstellt werden, über die jeder Strafverfolger frohlocken würde», schreibt Maas und fügt hinzu: **«Mit der Datenübertragung in Echtzeit könnte der Fahrer vielleicht auch digital zur Einhaltung der Verkehrsregeln angehalten werden».** An die Industrie richtete Maas deshalb Forderungen zum Auto der Zukunft: Schon bei der Entwicklung müsse der Datenschutz berücksichtigt werden, Datenvermeidung und Datensparsamkeit müssten leitende Grundsätze sein. Ferner solle der Fahrer der Datensammlung ausdrücklich zustimmen. Auch müsse es einen «Aus-Knopf» geben: Dem Fahrer müsse es möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und zu stoppen. Fünftens solle jeder frei wählen können, welches Unternehmen Zugriff auf die Daten bekommt. Zudem solle Missbrauch und Manipulation verhindert werden. Schliesslich müssten jene Systeme, die für den Fahrer das «Denken» übernehmen, sicher sein.

Aus Maas' Mund, der nicht umsonst in Deutschland den Spitznamen «Überwachungsminister» weg hat, klingen diese eigentlich vernünftigen Aussagen wenig glaubwürdig. Handelt es sich dabei etwa um skrupellose Lügen, um dem Wahlvolk die Digitalisierung schmackhaft zu machen? Vor allem Maas' Szenario der digitalen Verkehrskontrolle bestätigt die Vorbehalte der Datenschützer gegen die Digitalisierung des Verkehrs.

Quelle: epochtimes.de, Maas warnt vor Daten-Sammelwut bei intelligenten Autos, 13.06.201

Totalüberwachung beim Autofahren – Versicherer berechnen Tarif nach Fahrstil

Mehrere Versicherer testen die Einführung sogenannter Telematik-Tarife. Das heisst, das Auto kommuniziert ohne das Wissen des Fahrers mit der Versicherung und speichert u.a. das Fahrverhalten. Dabei wird der Fahrstil, also beispielsweise das Beschleunigungs- und Bremsverhalten, eines Versicherten aufgezeichnet, übermittelt und ausgewertet. Die Idee dahinter: Wer vernünftiger fährt, soll weniger bezahlen.

Aus den Daten lassen sich exakte Verhaltens- und Bewegungsprofile des Fahrers erstellen. Viele Firmen haben daran grosses Interesse: der eigene Arbeitgeber, das Finanzamt, Versicherungen, Autowerkstätten, Fahrzeughersteller, Gesundheitsdienstleister. Vielleicht auch die Maut-Behörde und Geheimdienste.

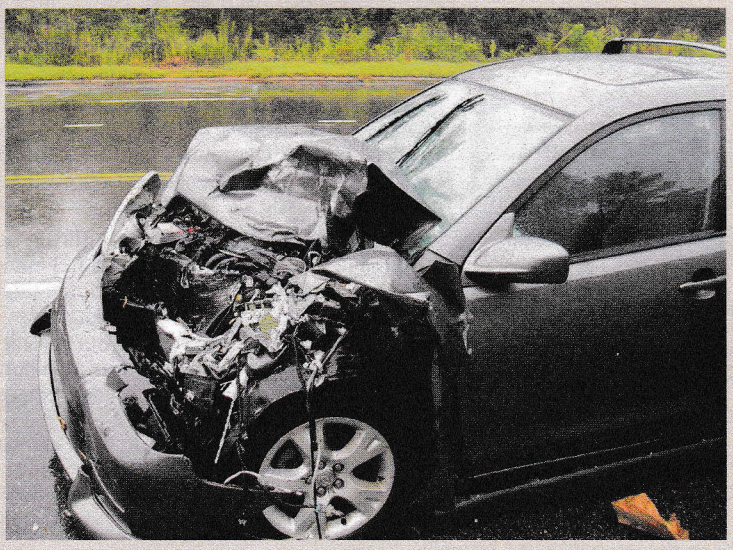


Foto: W. Robert Howell from Charlotte, NC, United States (https://commons.wikimedia.org/wiki/File:Car_Accident.jpg)

Konkret ist das von folgenden Versicherungen bekannt:

- Die HUK-Coburg bestätigt, dass sie entsprechende Aufzeichnungsgeräte testet.
- Die Allianz arbeitet in Italien schon seit Jahren mit Telematik-Tarifen und beobachtet die Entwicklung in Deutschland. «Wir sind der Meinung, dass die deutschen Autofahrer einen Telematik-Tarif annehmen werden, sofern er die Datensicherheit der Kunden sicherstellt und deutliche Vorteile für die Zielgruppe bringt», sagte Allianz-Vorstand Alexander Vollert.
- S-Direkt, die Sparkassen Direktversicherung (in Zusammenarbeit mit O2) lässt die Daten einer Auto-«Blackbox» von einem externen Dienstleister in einen Punktwert umrechnen, und sinkt dieser, bezahlt der Autofahrer weniger.
- Die Webseite Versicherungsbote.de nennt noch die VHV, Itzehoer sowie Axa, die im Herbst 2015 damit begonnen haben.

Quelle: epochtimes.de, Totalüberwachung beim Autofahren – Versicherer berechnen Tarif nach Fahrstil, 15.07.201

Zusammenfassend lässt sich feststellen: Viele moderne Autos verfügen schon über die Technik zur totalen Überwachung der Insassen. Wie es scheint, werden in Zukunft Hersteller, Versicherer und höchstwahrscheinlich auch der Staat auf die eigentlich privaten Daten über die Position und das Verhalten des Fahrers zugreifen können. Garantieleistungen könnten verwehrt bzw. Versicherungsprämien erhöht werden, weil die Hersteller bzw. Versicherer Informationen über das risikoreiche Fahrverhalten des Automobilbesitzers besitzen. Dass die Autohersteller für die vom SRF aufgedeckte Verletzung der Privatsphäre ihrer Kunden nicht bestraft werden, lässt vermuten, dass die Dauerüberwachung politisch erwünscht ist. Die Regeln des Strassenverkehrs ohne negative Konsequenzen zu brechen, könn mit diesen technischen Möglichkeiten bald nicht mehr möglich sei Sobald der Staat Zugriff auf diese Daten bekäme, bräuchte es kein Blitzer und Verkehrspolizisten mehr, denn jede Geschwindigkeits überschreitung könnte dann einfach digital bestraft werden, wie He ko Maas es sogar schon angedeutet hat. **Man muss kein Gegner von (Verkehrs-)Regeln sein, um zu erkennen, dass diese Art der Dauerüberwachung und des ständigen Zwangs zu fehlerlosem Verhalten charakteristisch für totalitäre Systeme ist, deren Bürger sie mehrheitlich zu politisch angepassten Drohnen entwickeln, die brav al Befehle der Regierung befolgen (siehe China).**