Internationale Arbeitsgruppe
für den Datenschutz
in der Telekommunikation

# Vernetzte Fahrzeuge

*63. Sitzung, 9.-10. April 2018, Budapest, Ungarn*

## *Einleitung*

1. Im Jahr 2011 nahm die Arbeitsgruppe ein Arbeitspapier über die Sammlung von Ereignisdaten in Fahrzeugen (Event Data Recorder – EDR) an.[1] Seither hat sich die Verarbeitung von Fahrzeugdaten – einschließlich personenbezogener Daten – technologisch wesentlich weiter entwickelt, sowohl in Bezug auf die Verarbeitung in den Fahrzeugen selbst, als auch in Bezug auf die Übermittlung von Daten zwischen ihnen und die Verarbeitung außerhalb von ihnen. Vernetzte Fahrzeuge sind komplexe Systeme des Internets der Dinge (IoT) auf Rädern geworden, die aus vielen elektronischen Steuergeräten bestehen, die über ein bordeigenes Netz miteinander verbunden sind.

2. Heutzutage sind noch viele Fahrzeuge nicht nativ an das Internet angeschlossen. Es werden jedoch Technologien entwickelt und der Anwendung zugeführt, welche die Kommunikation über Vermittlungsstellen oder direkt zwischen Fahrzeugen oder Straßeninfrastrukturanlagen (z. B. Verkehrsschilder oder Sende-/Empfangs-Basisstationen) ohne das Eingreifen eines Netzbetreibers ermöglichen.

3. Die geplanten Anwendungen für vernetzte Fahrzeuge sind vielfältig und können wie folgt klassifiziert werden:[2]

    a. Mobilitätsmanagement: Funktionen, die es den Fahrern ermöglichen, einen Zielort schnell und kosteneffizient zu erreichen, indem sie rechtzeitig Informationen über potenziell gefährliche Umweltzustände (z. B. vereiste Straßen),

---

1 WGDPT Working Paper: Event Data Recorders (EDR) on Vehicles / Privacy and data protection issues for governments and manufacturers (Montreal (Canada) 4-5 April 2011), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2011/2011-WP-EDR_on_vehicles.pdf

2 PwC Strategy 2014. „In the fast lane. The bright future of connected cars“, https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

Verkehrsstaus oder Straßenbaumaßnahmen, die Verfügbarkeit von Parkplätzen oder Reparaturdiensten, die Optimierung des Kraftstoffverbrauchs oder Straßenbenutzungsgebühren erhalten.[3]

b. *Fahrzeugmanagement:* Funktionen, die den Fahrern helfen, die Betriebskosten zu senken und die Nutzung zu erleichtern, z. B. Mitteilungen über den Zustand des Fahrzeugs und Erinnerungen an anstehende Wartungsarbeiten, Transfer von Daten über die Nutzung des Fahrzeugs (z. B. an Reparaturdienste), kundenspezifische Versicherungen, bei denen die Prämien vom Fahrverhalten abhängen, Fernwirkverfahren (mit denen z. B. das Heizsystem eines Fahrzeugs aus der Ferne aktiviert werden kann) oder die Speicherung von Konfigurationsprofilen für Komfortfunktionen des Fahrzeugs (z. B. Sitzposition).

c. *Straßenverkehrssicherheit:* Funktionen, welche die Fahrer vor externen Gefahren warnen und interne Reaktionen des Fahrzeugs auf diese Gefahren ankündigen, z. B. Systeme für den Kollisionsschutz, Spurhaltesysteme, automatisierte Notrufe (*eCall*) oder Aufzeichnungsgeräte, welche Daten für die Crash-Untersuchung zur Verfügung stellen (Blackboxes).

d. *Unterhaltung:* Funktionen für die Information und die Unterhaltung von Fahrer und Mitreisenden, z. B. Schnittstellen für die Smartphone-Anbindung, die Bereitstellung eines WLAN, Musik-, Video-, Internet-, Social-Media-Dienste, Mobile-Office-Dienste oder die Anbindung an das Smart Home des Halters oder Fahrers.

e. *Fahrerunterstützung:* teilweise oder vollständig automatisierte Funktionen wie die operative Unterstützung des Fahrers oder die automatische Steuerung des Fahrzeugs bei starkem Verkehr, bei der Fahrt auf Autobahnen oder beim Parken.

f. *Funktionen für die Unterstützung des Wohlbefindens von Fahrern oder Mitreisenden:* Funktionen zur Überwachung der Fahrtüchtigkeit des Fahrers wie z. B. die Feststellung von Ermüdungszuständen oder die Bereitstellung von medizinischer Hilfe.

4. Da Fahrzeuge zunehmend mit dem Internet und anderen Fahrzeugen verbunden werden, werden immer mehr personenbezogene Daten durch die Fahrzeuge gesammelt, verarbeitet und Dritten zugänglich gemacht. Relevante Arten von Daten, die von den Sensoren des Fahrzeugs erfasst werden, können sich auf das Fahrerverhalten oder auf Informationen über andere Personen innerhalb oder außerhalb des Fahrzeugs beziehen. Diese Daten können durch die IT-Systeme des Fahrzeugs oder ggf. angeschlossene persönliche Geräte (wie z. B. Smartphones) verarbeitet werden.[4] Das Aufkommen autonomer Fahrzeuge wird zusätzliche Datenschutzprobleme aufwerfen, da ihre Funktionsweise die Erhebung und Nutzung

---

3 Bericht und Empfehlungen zu Mautsystemen – “Sofia Memorandum”. Sofia, Bulgarien, 12./13.03.2009, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2009/2009-Sofia_Memorandum-de.pdf

4 Infografik „Data and the connected car“. Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

erheblicher Datenmengen erfordert, von denen einige personenbezogene Daten sein werden.

**Derzeitige und neu entstehende Interessenträger**

5. Telematikdaten und andere mit dem Fahrer zusammenhängende Daten können einer Reihe von Unternehmen – Fahrzeughersteller, Wartungsunternehmen, Vermietungs- und Car-Sharing-Unternehmen, Fahrzeugversicherungsunternehmen und Unterhaltungsanbieter – zur Verfügung stehen.

6. Außerdem hat sich eine Branche herausgebildet, die Telematikdienste für Fahrzeuge anbietet und in diesem Zuge auch personenbezogene Daten im Zusammenhang mit der Nutzung von Fahrzeugen verarbeitet.[5] Es sind neue Geschäftsmodelle entstanden, z. B. von Versicherungsgesellschaften entwickelte Modelle (z. B. „Pay as/how you drive“), die in hohem Maße von der Verarbeitung personenbezogener Daten der Fahrer abhängen.

7. Fuhrparkbetreiber, Leasinggesellschaften und Arbeitgeber, die ihren Mitarbeitern Fahrzeuge zur Verfügung stellen, sind ebenfalls an der Erhebung von personenbezogenen Daten beteiligt, die von vernetzten Fahrzeugen gewonnen werden (z.B. für die Zuweisung von Ressourcen, die Verfolgung von Fahrzeugen oder die Abrechnung von Dienstleistungen).

8. Schließlich werden große Datenmengen von Entwicklern autonomer Fahrzeuge (oder von Teilen davon) für die Gestaltung ihrer Produkte erhoben. Das Aufkommen autonomer Fahrzeuge wird zusätzliche Datenschutzprobleme aufwerfen, da ihre Funktionsweise die Sammlung und Nutzung erheblicher Datenmengen erfordert, von denen einige personenbezogene Daten sein werden.

9. Neue Akteure, insbesondere diejenigen aus der Internetindustrie, können ihre derzeitigen Vorgehensweisen bei der Speicherung und Verarbeitung personenbezogener Daten (insbesondere die Speicherung und Verarbeitung von Daten zu Zwecken, die nicht mit dem Hauptzweck der Datenerhebung zusammenhängen) auf die Automobilindustrie übertragen.[6]

---

5 Testimony and Statement for the Record of Khaliah Barnes, Associate Director and Administrative Law Counsel, EPIC. Hearing on “The Internet of Cars”, Joint Hearing Before the U.S. House of Representatives, Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Transportation and Public Assets, November 18, 2015, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf

6 So zielt beispielsweise die Open Automotive Alliance (OAA), eine globale Allianz großer Technologie- und Automobilunternehmen, auf die Nutzung der Android-Plattform in Automobilen, http://www.openautoalliance.net

**Zweck dieses Dokuments**

10. Dieses Dokument behandelt Datenschutzrisiken, die sich aus der Erhebung und Verarbeitung von Daten in unterschiedlichen Zusammenhängen und durch unterschiedliche Systeme ergeben:

    a. Vom Fahrzeug (einschließlich der im Fahrzeug eingebauten Informations- und Unterhaltungssysteme) gesammelte und verarbeitete Daten,

    b. Daten, die zwischen dem Fahrzeug und den angeschlossenen persönlichen Geräten ausgetauscht werden,

    c. Daten, die zwischen dem Fahrzeug und externen Stellen (z. B. Infrastrukturbetreibern, Fahrzeugherstellern, Versicherungen und Kfz-Werkstätten) ausgetauscht werden, und

    d. Daten, die an umliegende Fahrzeuge und Infrastruktureinrichtungen übertragen werden, um kooperative intelligente Verkehrssysteme (C-ITS) zu ermöglichen.[7]

11. Fahrzeughersteller erfassen und verarbeiten unter anderem Daten zur Konstruktion autonomer Fahrzeuge, bei denen es sich um einen bestimmten Typ eines vernetzten Fahrzeugs handelt. In diesem Dokument wird die Erhebung von Daten für und durch autonome Fahrzeuge erörtert, jedoch nicht die allgemeineren ethischen Fragen erörtert, die sich aus der Einführung autonomer Fahrzeuge ergeben. Darüber hinaus ist die Erfassung und Verarbeitung von Daten durch autonome Fahrzeuge und die damit verbundenen Einschränkungen, wie die Notwendigkeit der Echtzeitverarbeitung, nicht Gegenstand dieses Papiers.

12. Einige der in oder durch vernetzte Fahrzeuge gesammelten Daten werden zur Verbesserung der öffentlichen Sicherheit und zur Verringerung der Unfallzahlen verwendet. Beispielsweise kann eine Fahrzeug-zu-Fahrzeug-Kommunikation mit geringer Latenz helfen, schnell eine Reaktion des Fahrers auf einen sich entwickelnden Verkehrsunfall auszulösen. Diese Stellungnahme versucht nicht, einen Kompromiss zwischen dem Schutz der Privatsphäre und der öffentlichen Sicherheit zu finden, sondern gibt Empfehlungen zur Verbesserung des Schutzes der Privatsphäre bei bestehender Erlaubnis der Verwendung der Daten für die angegebenen Zwecke.

13. Arbeitgeber, die ihren Mitarbeitern Dienstwagen zur Verfügung stellen, könnten die Handlungen ihrer Mitarbeiter überwachen wollen (z. B. um die Sicherheit der Mitarbeiter, Waren oder Fahrzeuge zu gewährleisten, Ressourcen zuzuweisen, eine Dienstleistung zu verfolgen und abzurechnen oder die Arbeitszeit zu kontrollieren). Der Zugriff auf die Daten, die von den angeschlossenen Fahrzeugen in diesem Zusammenhang erzeugt werden, ist nicht Gegenstand dieses Papiers.

---

7 Kooperative intelligente Verkehrssysteme (C-ITS) verwenden Technologien, mit denen Straßenfahrzeuge mit anderen Fahrzeugen, Verkehrszeichen und Straßeninfrastrukturen sowie mit anderen Verkehrsteilnehmern kommunizieren können. Die Kommunikationsbeziehungen werden auch als Kommunikation von Fahrzeug zu Fahrzeug (V2V) oder zwischen Fahrzeug und Infrastruktur (V2I) bezeichnet.

## Betrachtete Datentypen

14. Verschiedene Arten von Daten können von vernetzten Fahrzeugen erfasst, generiert, übertragen, verarbeitet oder gespeichert werden. Einige dieser Daten, wie Besitzer-/Fahrerdaten, Identifikatoren (z. B. Fahrzeug-Identifikationsnummern, MAC-Adressen) oder Standortdaten können direkt einem bestimmten Gerät oder einer natürlichen Person zugeordnet werden. Darüber hinaus können erweiterte Funktionalitäten die Verarbeitung biometrischer Daten für die Authentifizierung des Fahrers (z. B. Sprach-, Fingerabdruck-, Video- und andere Authentifizierungsarten) oder seine Überwachung (z. B. Bildverarbeitung zur Ermüdungserkennung) ermöglichen.

15. Andere Daten sind indirekt mit dem Fahrer verknüpft, wie z. B. Telematikdaten (z. B. Geschwindigkeit oder Beschleunigung des Fahrzeugs, die Anwendung der Bremsen, die Sitzbelegung, erkannte Erschütterungen oder Aufprall) und Servicedaten. Sie können sich auf den Fahrer oder die Fahrgäste beziehen (z. B. Alkoholkonsum, Daten zum Fahrerverhalten, gehaltene oder benutzte Gegenstände, Identifikation von Fahrgastaktionen usw.). Einige dieser Daten sind als personenbezogene Daten zu klassifizieren.

## Bestehende und sich abzeichnende Vorschriften, Verpflichtungen und Empfehlungen

16. Vernetzte Fahrzeuge sind in den letzten zehn Jahren zu einem wichtigen Thema für die Regulierungsbehörden geworden, wobei in den letzten beiden Jahren ein deutlicher Anstieg zu verzeichnen war. Diese Regelungen und Initiativen ergänzen die bestehenden Datenschutzbestimmungen.

17. Die Entwicklung von vernetzten Fahrzeugen und insbesondere von kooperativen intelligenten Verkehrssystemen (Cooperative Intelligent Transportation Systems – C-ITS) wird sowohl von nationalen Regierungen als auch von supranationalen Akteuren gefördert:

    a. Im Jahr 2014 richtete die Europäische Kommission eine Plattform für die Einführung kooperativer intelligenter Verkehrssysteme in der Europäischen Union (die C-ITS-Plattform) ein, um technische Infrastrukturen und Standards für die Kommunikation unter Fahrzeugen sowie zwischen Fahrzeugen und straßenseitigen Elementen zu schaffen.[8]

    b. Im Jahr 2016 haben die Mitgliedstaaten und die Kommission die C-Roads-Plattform ins Leben gerufen, um die C-ITS-Einführungsaktivitäten zu verknüpfen, gemeinsam technische Spezifikationen zu entwickeln und auszutauschen und die Interoperabilität durch standortübergreifende Tests zu überprüfen.[9]

---

8 European Commission, Mobility and Transport, http://ec.europa.eu/transport/themes/its/c-its_en.htm

9 C-Roads, https://www.c-roads.eu/platform.html

Viele C-Roads-Pilotprojekte wurden initiiert, wie z. B. der "Nordic Way Coop", in dessen Rahmen eine Vorinstallation von C-ITS-Diensten in vier Ländern (Finnland, Schweden, Norwegen und Dänemark) getestet wird.

18. Im Januar 2016 haben die deutsche Konferenz der Datenschutz-Aufsichtsbehörden des Bundes und der Länder und der Verband der Automobilindustrie (VDA) eine gemeinsame Erklärung zu den Grundsätzen des Datenschutzes in vernetzten und nicht vernetzten Fahrzeugen veröffentlicht.[10]

19. Im Januar 2017 veröffentlichte die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eine Studie zur Cybersicherheit und Widerstandsfähigkeit von vernetzten Fahrzeugen, in der die in vernetzten Fahrzeugen vorhandenen sensiblen Güter sowie die entsprechenden Bedrohungen, die Risiken und Verfahren zu deren Minderung sowie mögliche Sicherheitsmaßnahmen aufgeführt sind.[11]

20. Im August 2017 veröffentlichte das Centre for Connected and Autonomous Vehicles des Vereinigten Königreichs einen Leitfaden, der die Grundsätze der Cybersicherheit für vernetzte und automatisierte Fahrzeuge darlegt, um das Bewusstsein für dieses Thema im Automobilsektor zu schärfen.[12]

21. Im September 2017 verabschiedete die Internationale Konferenz der Datenschutzbeauftragten eine Resolution zu vernetzten Fahrzeugen.[13]

22. In den Vereinigten Staaten verabschiedete das US-Repräsentantenhaus im Jahr 2017 das Gesetz H.B. 3388, den Safely Ensuring Lives Future Development and Research in Vehicle Development (SELF DRIVE) Act zur Förderung von Tests, Entwicklung und Einsatz von hoch automatisierten Fahrzeugen, das Bestimmungen zum Datenschutz und zur Cybersicherheit enthält.[14] Die Federal Trade Commission veröffentlichte eine Einschätzung der Mitarbeiter der Behörde zu ihrem Workshop über vernetzte Fahrzeuge[15], der im Jahr 2017 stattfand, während die U.S. National Highway Traffic Safety Administration das Papier "Automated Dri-

---

10 Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), https://www.datenschutz-mv.de/static/DS/Dateien/Presse/2016/Erklaerung.pdf

11 Cyber Security and Resilience of smart cars, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

12 Principles of cyber security for connected and automated vehicles, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

13 Resolution on Data Protection in Automated and Connected Vehicles, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf

14 https://www.congress.gov/bill/115th-congress/house-bill/3388.

15 Staff Perspective Recaps Workshop Examining Privacy, Security Issues Related to Connected Cars, https://www.ftc.gov/news-events/press-releases/2018/01/staff-perspective-recaps-workshop-examining-privacy-security.

ving Systems 2.0: A Vision for Safety" veröffentlichte, das freiwillige Leitlinien enthält, die bewährte Verfahren fördern soll und der Betriebssicherheit Vorrang einräumt.[16]

23. Im Oktober 2017 verabschiedete die Artikel-29-Gruppe eine Stellungnahme zur Verarbeitung personenbezogener Daten im Rahmen von kooperativen intelligenten Verkehrssystemen.[17]

24. Ebenfalls im Oktober 2017 veröffentlichte die französische Datenschutzbehörde (CNIL) ein Compliance-Paket für vernetzte Fahrzeuge. Diese Leitlinien geben den Akteuren Hilfestellung bei der Integration des Datenschutzes durch Technikgestaltung und Voreinstellung in die Ausgestaltung der Fahrzeugsysteme mit dem Ziel, es den betroffenen natürlichen Personen zu erleichtern, ihre Daten wirksam zu kontrollieren.[18]

25. In einigen Rechtsordnungen ist die Möglichkeit für Fahrzeuge, sich an bestehende Telekommunikationsnetze anzuschließen, nun zwingend vorgeschrieben (z. B. müssen in der Europäischen Union Fahrzeuge, die nach dem März 2018 hergestellt werden, das sogenannte "eCall"-System enthalten).[19]

### *Datenschutzrisiken*

26. Die betroffenen Personen haben das Recht auf Datenschutz bei der Verarbeitung der sie betreffenden Daten innerhalb der im geltenden Recht vorgesehenen Grenzen. Dieses Recht ist unveräußerlich und nicht übertragbar. Die Diskussion über den Besitz von Fahrzeugdaten könnte die Verantwortlichen dazu verleiten, den Betroffenen ihre Rechte zu verweigern.[20,21]

---

16 https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf. Siehe auch NHTSA, Automated driving systems, https://www.nhtsa.gov/manufacturers/automated-driving-systems.

17 Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888.

18 Connected vehicles: a compliance package for a responsible use of data, https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

19 eCall ist eine europäische Initiative, die darauf abzielt, Autofahrern, die an einer Kollision beteiligt waren, überall in der Europäischen Union schnelle Hilfe zu leisten, https://de.wikipedia.org/wiki/ECall. Vgl. auch Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall system and amending Directive 2007/46/EC, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-10-29_eCall_EN.pdf

20 ACEA Position Paper Access to vehicle data for third-party services, http://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

21 Fair and Equal Access to Vehicles in a Digital Single Market Implementing the eCall mandate on the 'interoperable telematics platform' in line with the principles for fair competition and free consumer choice, https://www.figiefa.eu/wp-content/uploads/Manifesto-for-Fair-Access-to-the-Vehicle.pdf

Mangelnde Transparenz

27. Fahrzeugführer und Fahrgäste sind möglicherweise nicht ausreichend über die Verarbeitung von Daten im oder durch ein Fahrzeug informiert. Die Informationen werden möglicherweise nur an den Fahrzeughalter weitergegeben, der nicht notwendig der Fahrer des Fahrzeugs ist. Möglicherweise geschieht dies auch nicht rechtzeitig (d. h. vor dem Kauf, der Vermietung oder der Nutzung eines Fahrzeugs).

28. Sensorik (z. B. Abstandssensoren, Kameras) in Fahrzeugen wird möglicherweise nicht nur zur Beobachtung von Fahrern und Insassen im Fahrzeug, sondern auch zur Überwachung des Fahrzeugumfelds eingesetzt. Die Menschen in diesem Umfeld sind sich dieser Datenerhebung möglicherweise nicht bewusst, und es wird schwierig sein, sie zu informieren.

Unrechtmäßige Verarbeitung

29. Um personenbezogene Daten mit Hilfe von Fahrzeug-IT-Systemen zu verarbeiten, benötigt ein Verantwortlicher eine gesetzliche Grundlage. Je nach Zweck der Datenverarbeitung können verschiedene Rechtsgrundlagen (Einwilligung, Vertragserfüllung, berechtigtes Interesse, …) angewendet werden. Es besteht die Gefahr, dass die Verantwortlichen diese Anforderung nicht erfüllen und eine unrechtmäßige Verarbeitung vornehmen.

Unerlaubte Weiterverwendung

30. Daten, die von Fahrzeugherstellern, Dienstleistern oder sonstigen Dritten erhoben wurden, können für Zwecke verwendet oder verkauft werden, für welche die betroffenen natürlichen Personen keine Einwilligung erteilt haben.

31. In kooperativen intelligenten Verkehrssystemen sind Nachrichten, die von Fahrzeug zu Fahrzeug oder von Fahrzeug zu Infrastruktureinrichtungen gesendet wer-den, zur Verbreitung an unbekannte Empfänger bestimmt und daher nicht gegen unbefugten Zugriff Dritter gesichert. Sie können von jedem, der sich im Bereich des Signals aufhält, abgefangen werden und zur Erstellung von Standortprofilen von Fahrzeugen und ihrer Fahrer verwendet werden.[22]

---

22 Es ist zu beachten, dass auch der Einsatz datenschutzfreundlicher Technologien – hier sich rasch verändernde Pseudonyme – nicht verhindern, dass Standortprofile erstellt werden, http://spectrum.ieee.org/cars-that-think/transportation/advanced-cars/researchers-prove-connected-cars-can-be-tracked

32. Die von den vernetzten Fahrzeugen gesammelten Daten könnten von Strafverfolgungsbehörden verwendet werden, um Geschwindigkeitsüberschreitungen oder andere Verstöße zu erkennen oder einzelne Verkehrsteilnehmer zu überwachen. Dies ist nur zulässig, wenn es gesetzlich ausdrücklich vorgesehen ist.[23]

Übermäßige Sammlung

33. Die zahlreichen Sensoren, die in vernetzten Fahrzeugen eingesetzt werden, bergen ein sehr hohes Risiko einer übermäßigen Datenerfassung im Vergleich zu dem, was zum Erreichen des Ziels notwendig ist. Dies ist insbesondere dann der Fall, wenn die Sensoren und die daran angeschlossenen IT-Systeme nicht nach datenschutzrechtlich gebotenen gestalterischen Gesichtspunkten wie der Durchsetzung der Zweckbestimmung und Datenminimierung ausgelegt sind.

34. Vernetzte Fahrzeuge bieten drahtlose Verbindungsmöglichkeiten, damit Fahrer und Passagiere Inhaltsdaten mit dem Fahrzeug teilen können. Dies kann dazu führen, dass übermäßig viele Daten von Telematik-Boxen, Smartphones und anderen persönlichen Geräten der Fahrgäste erfasst werden.

35. Die Entwicklung von autonomen Fahrzeugen, insbesondere der Einsatz von Algorithmen des maschinellen Lernens zur Optimierung von Funktionen für ihren Betrieb, kann eine große Menge an Daten erfordern, die über einen langen Zeitraum gesammelt werden.

Mangelnde Kontrolle

36. Es besteht das Risiko, dass die angebotenen Funktionalitäten und Optionen nicht ausreichen, um die Kontrolle auszuüben, die erforderlich ist, damit die Betroffenen von ihren Datenschutz- und Persönlichkeitsrechten Gebrauch machen können.

37. Im Laufe ihrer Lebensdauer können Fahrzeuge verschiedenen Eigentümern gehören, entweder weil sie verkauft werden oder weil ihr Leasingzeitraum endet. Darüber hinaus werden Fahrzeuge zunehmend nicht nur von Unternehmen, sondern auch von Privatpersonen mit Dritten geteilt oder vermietet. Dennoch ist es derzeit nicht möglich oder sehr schwierig, eine Sicherungskopie der im Fahrzeug gespeicherten Daten anzulegen und sie dann zu löschen. Damit besteht das Risiko, dass Daten über frühere Fahrzeuginsassen für nachfolgende Nutzer sichtbar sind.

38. Mietfahrzeuge, geleaste Fahrzeuge und Taxis (die nicht notwendigerweise im Besitz des Fahrers sind) sammeln wahrscheinlich Daten von Fahrern und Fahrgästen, die sich nicht auf den Eigentümer des Fahrzeugs beziehen. Dazu gehören

---

23 In der EU werden solche Daten als besondere Datenkategorien betrachtet. Die Verarbeitung solcher Daten ist verboten, es sei denn, eine der spezifischen Ausnahmen ist anwendbar (Art.9 der Datenschutz-Grundverordnung).

auch Arbeitnehmer, die ein von ihrem Arbeitgeber ausgestelltes Leasingfahrzeug nutzen. Unter diesen Umständen kann die Person, deren Daten erhoben werden, möglicherweise nicht gegen einzelne dieser Datenverarbeitungen Einspruch erheben. [24]

Unzureichende Sicherheit

39. Die Vielzahl von Funktionalitäten (z. B. für Unterhaltung und den Anschluss persönlicher Geräte wie Smartphones) und Schnittstellen (z. B. Web, USB, RFID, Wi-Fi) der angeschlossenen Fahrzeuge erhöht die Angriffsfläche und damit die Anzahl möglicher Schwachstellen, durch die persönliche Daten gefährdet werden können.

40. Im Gegensatz zu den meisten Geräten des „Internets der Dinge“ sind angeschlossene Fahrzeuge kritische Systeme, bei denen ein Sicherheitsvorfall das Leben der Nutzer und anderer Personen gefährden kann. Umso wichtiger ist es, dem Risiko entgegenzuwirken, dass Hacker versuchen, die Schwachstellen vernetzter Fahrzeuge auszunutzen.

41. Personenbezogene Daten, die in Fahrzeugen und/oder an externen Standorten (z. B. bei Anbietern von Diensten des Cloud Computing) gespeichert sind, werden möglicherweise nicht ausreichend vor unbefugtem Zugriff geschützt. Beispielsweise muss ein Fahrzeug während der Wartung einem Techniker übergeben werden, der Zugang zu einigen technischen Daten des Fahrzeugs benötigt. Während der Techniker Zugriff auf die technischen Daten haben muss, könnte er seine Fähigkeiten missbrauchen, um auf alle im Fahrzeug gespeicherten Daten zuzugreifen. Darüber hinaus stellen Fahrzeugdaten einen Vermögenswert dar, der von Unternehmen, deren historisches Kerngeschäft nicht mit der Verarbeitung personenbezogener Daten zusammenhängt, möglicherweise nicht angemessen abgesichert wurde.

42. Fahrerassistenzfunktionen können angeschlossene Fahrzeuge zu Entscheidungen veranlassen, z. B. beim Spurwechsel oder beim Einsatz des Tempomaten. Im Falle einer Ungenauigkeit der Daten können solche Entscheidungen katastrophale Folgen für die Verkehrssicherheit haben.

43. Angeschlossene Fahrzeuge benötigen eine sehr geringe Latenz, um in Notfällen die zeitgerechte Reaktion des Fahrzeugs zu garantieren, z. B. wenn der Fahrer ein Fahrmanöver zur Vermeidung einer Kollision ausführt. Hacker könnten die Latenzzeit des Fahrsystems in schwerwiegender Weise beeinflussen, indem sie Systemstörungen ausnutzen und große Mengen an CPU-Ressourcen und Busbandbreite verbrauchen.

---

24 Connected Cars: What Happens To Our Data On Rental Cars? https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf

Mangelnde Rechenschaftspflicht

44. Fahrzeughersteller, Komponentenhersteller und Softwareentwickler können verschiedene Arten von Daten für unterschiedliche Zwecke sammeln. Einige können Datenverantwortliche sein, andere können als Auftragsverarbeiter agieren, und es besteht die Gefahr einer schlechten und/oder undurchsichtigen Rollenverteilung zwischen gemeinsam Verantwortlichen sowie zwischen Verantwortlichen und Auftragsverarbeitern.

45. Fahrzeugdaten werden oft nicht als personenbezogene Daten wahrgenommen, da es nicht möglich ist, diese Daten direkt mit der Identität der betroffenen Personen zu verknüpfen. Nicht alle von Fahrzeugen gesammelten oder ausgesendeten Daten sind personenbezogene Daten, aber zum Beispiel können Daten, die mit dem Standort der Fahrzeuge zu mehreren Zeitpunkten verknüpft sind, sehr oft auf eine bestimmte Person bezogen werden. Unternehmen, die Fahrzeugdaten verarbeiten, prüfen möglicherweise nicht ausreichend, ob sie personenbezogene Daten verarbeiten, mit dem Ergebnis, dass sie dies ggf. unter Verstoß gegen geltende Rechtsvorschriften tun.

***Empfehlungen***

Fahrzeug- und Gerätehersteller

46. Informationen über den Umfang, den Zweck, die für die Verarbeitung Verantwortlichen und die Rechte der betroffenen Personen sollten leicht zugänglich sein (z. B. über das Dashboard). Werden auch Informationen über Fahrgäste erfasst (z. B. durch Sensoren an Bord), sollten diese ebenfalls entsprechend informiert werden. Wenn zum Beispiel ein Fahrzeug immer auf ein Stichwort wartet, das eine akustische Datenerfassung auslöst, könnten die Fahrzeuge ein klares Signal an Bord haben (z. B. ein Licht), um die Fahrgäste darüber zu informieren, wenn diese Datenerfassung erfolgt. Um vollständig zu sein, sollten die Informationen für Fahrer und Fahrgäste die Rechte der betroffenen Personen (z. B. ihr Recht auf Zugang, ihr Recht auf Widerspruch, auf Widerruf der Einwilligung und auf Datenübertragbarkeit) in denjenigen Rechtsordnungen auflisten, in denen solche Rechte bestehen.

47. Die Fahrzeugsensorik sollte die Speicherung personenbezogener Daten von Personen, die sich außerhalb des Fahrzeugs befinden, vermeiden. Werden Daten gespeichert und nicht sofort nach der Echtzeitverarbeitung gelöscht, sollten zudem von Fahrzeugkameras gesammelte Gesichter und Fahrzeugkennzeichen als solche erkannt und dauerhaft verwischt werden.

48. Ein im Fahrzeug implementierter Profilmanager könnte die Präferenzen bekannter Fahrer speichern, um ihnen − und bis zu einem gewissen Grad auch häufigen Fahrgästen wie Familienmitgliedern − die Möglichkeit zu geben, ihre Privatsphäre-

Einstellungen zu setzen und zu speichern. Dies würde den Zeitaufwand für wiederholte Änderungen der Einstellungen erheblich vermindern.

49. Ein Teil der Funktionalitäten der vernetzten Fahrzeuge und der mit ihnen verbundenen Datenverarbeitungsvorgänge erfordert lediglich Verbindungen zwischen verschiedenen Komponenten oder Geräten an Bord des Fahrzeugs (einschließlich mit dem Fahrzeug verbundener Smartphones). Fahrzeug- und Geräteherstellern sollten die Kommunikation innerhalb des Fahrzeugs priorisieren und die Übertragung von Daten an entfernte Server vermeiden, wenn diese nicht unbedingt erforderlich ist.

50. Fahrzeugsysteme, die für kritische Kernfunktionen der Steuerung des Fahrverhaltens erforderlich sind, sollten von Systemen isoliert werden, die optionale Funktionen wie Unterhaltung unterstützen, um sicherzustellen, dass das Fahrzeug weiterhin ordnungsgemäß funktioniert, wenn ein unkritisches System heruntergefahren wird oder sich unsachgemäß verhält.

51. Auch wenn keine spezifischen Rechtsvorschriften bestehen, sollte der Fahrer die Möglichkeit haben, die Erfassung bestimmter Arten von Daten vorübergehend oder dauerhaft zu unterbinden, sofern diese Daten für die kritischen Funktionen des Fahrzeugs (z. B. das Antriebssystem) nicht wesentlich sind.

52. Zusätzlich zur Konfiguration der Fahrzeugsysteme entsprechend der Prinzipien des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen sollten die Hersteller die Kontrolle der betroffenen Personen über ihre Daten während des gesamten Verarbeitungszeitraums erleichtern. Diese Kontrolle sollte sich insbesondere auf alle Einstellungen erstrecken, die Auswirkungen auf die Privatsphäre haben, und insbesondere

    a. die Möglichkeit, Einstellungen während der gesamten Bearbeitungszeit leicht zu ändern, insbesondere zum Zweck der Aktivierung oder Deaktivierung von Diensten, die auf der Grundlage der Zustimmung oder zur Erfüllung eines Vertrages erbracht werden (wie z. B. Pannenhilfe oder andere kommerzielle Angebote, die auf der Grundlage der Geolokalisierung personalisiert werden),

    b. gegebenenfalls die Möglichkeit, den Detaillierungsgrad der gesammelten Daten an den gewünschten Servicegrad anzupassen (z. B. durch Zugriff auf eine Landkarte ohne Geolokalisierung, wenn diese nicht geführt werden soll) und

    c. die Möglichkeit der einfachen Ausübung der Betroffenenrechte, einschließlich des Zugriffs und gegebenenfalls der Löschung personenbezogener Daten

    beinhalten.

53. Geolokalisierungsdaten geben besonderen Aufschluss über die Lebensgewohnheiten der Betroffenen. Die durchgeführten Fahrten sind insofern sehr charakteristisch, als sie es ermöglichen, den Arbeits- und Wohnort sowie die Interessenschwerpunkte des Fahrers, z. B. Freizeitbeschäftigungen, sowie eventuell Religionsausübung oder sexuelle Orientierung aus den besuchten Orten abzuleiten. Dementsprechend sollte der Diensteanbieter besonders darauf achten, keine

Standortdaten zu erheben, es sei denn, dies ist zum Zwecke der Verarbeitung unbedingt erforderlich.

54. Kooperative intelligente Verkehrssysteme (C-ITS) sollten die Übermittlung personenbezogener Daten auf die erforderlichen Empfänger beschränken. Beispielsweise sollten Daten, die nur im Rahmen der Fahrzeug-zu-Fahrzeug-Kommunikation nützlich sind, nicht von Infrastrukturbetreibern oder Fahrzeug- und Geräteherstellern erfasst und gespeichert werden, wenn dies nicht für einen eindeutig festgelegten Zweck geschieht.

55. Die persönlichen Daten eines Fahrzeugführers, Beifahrers oder Fahrzeughalters können von verschiedenen Teilen des Systems gespeichert werden, die jeweils unterschiedliche Funktionen unterstützen (z. B. im Telefonbuch des Fahrzeugs, im Soundsystem oder im Navigationssystem). Das Löschen persönlicher Daten aus dem Fahrzeug kann daher mehrere Operationen erfordern. Die Hersteller sollten die Funktionen zentralisieren, mit denen die Löschung personenbezogener Daten ermöglicht wird, um die Entfernung personenbezogener Daten aus Fahrzeugsystemen durch Fahrzeugwiederverkäufer und Fahrzeugvermieter zu vereinfachen.[25]

56. Wenn Fahrzeug- und Gerätehersteller als Datenverantwortliche tätig sind, die andere Parteien entweder als gemeinsame Verantwortliche einbeziehen oder als Auftragsverarbeiter beschäftigen (z. B. Anbieter von Mehrwertdiensten, Smartphone-Integration und Anwendungen), sollten sie ihre jeweiligen Rollen, Verantwortlichkeiten und Rechte in Bezug auf die Verarbeitung personenbezogener Daten eindeutig festlegen. Wenn der Dritte als Auftragsverarbeiter auftritt, sollten die Vereinbarungen vorsehen, dass er personenbezogene Daten nur gemäß den Anweisungen des für die Verarbeitung Verantwortlichen verarbeiten darf. Auch andere gesetzliche Bestimmungen, die die vertragsgemäße Verarbeitung personenbezogener Daten regeln, sollten gebührend berücksichtigt werden.

57. Fahrzeug- und Gerätehersteller sollten die Daten so schnell wie möglich nach Erfüllung der vorgegebenen Zwecke minimieren und aggregieren. Um risikobasierte Maßnahmen zum Schutz der Datensicherheit zu implementieren und die Folgen eines unberechtigten Zugriffs abzumildern, sollten zudem Pseudonymisierungstechniken eingesetzt werden.

58. Fahrzeug- und Gerätehersteller sowie Dienstleister dürfen die erhobenen Daten nicht zu einem Zweck verwenden, der mit dem ursprünglichen Zweck unvereinbar ist, nicht gesetzlich erlaubt ist oder für den die Betroffenen keine ausdrückliche, spezifische, informierte, eindeutige und freiwillig erteilte Einwilligung erteilt haben.

59. Für jede spätere Wiederverwendung von Daten, die von vernetzten Fahrzeugen erhoben wurden, die mit dem Hauptzweck unvereinbar ist, ist es notwendig, eine Einwilligung einzuholen und sicherzustellen, dass die Verwendung den Erwartungen der betroffenen Personen entspricht.

---

25 Personal Data in your car, https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf

60. Es ist jedoch zulässig, die Produkte von Datenverarbeitungsvorgängen, die anonymisierte Daten liefern, zu anderen Zwecken zu verarbeiten. Definitionsgemäß können anonymisierte Daten weder direkt noch indirekt mit einer natürlichen Person in Verbindung gebracht werden. Die Datenschutzgesetzgebung findet daher keine Anwendung.

Drittanbieter von Diensten und Anwendungen

61. Service- und Anwendungsanbieter sollten Datenschutzeinstellungen in ihre Produkte einschließen, um die Erfassung und Verwendung personenbezogener Daten zu begrenzen. Privatpersonen könnten – insbesondere im Kontext der Erbringung von Funktionen, die nicht zum Kern der Funktionalität des Fahrzeugs gehören – Wahlmöglichkeiten in Bezug auf die Erhebung und Verwendung auf sie bezogener Daten im Rahmen von bedarfsgesteuerten Mitteilungen angeboten werden, wenn sie mit einer Funktion oder Dienstleistung interagieren, welche die Erhebung und Verwendung personenbezogener Daten erfordert. Z. B. kann es eine Maßnahme des Datenschutzes durch Technikgestaltung darstellen, die Verarbeitung bestimmter Daten im Fahrzeug zu realisieren, um die Menge der Daten zu begrenzen, die außerhalb des Fahrzeugs verarbeitet werden. Diese Art der Implementierung könnte auch den Bandbreitenverbrauch reduzieren und die Datenverarbeitung beschleunigen.

62. Anwendungsanbieter und Drittanbieter verfügen möglicherweise nicht über Zugang zu allen Schnittstellen, die bereitstehen, um den Fahrzeugführer und Beifahrer über ihre Datenerfassung zu informieren. Sie sollten keine Daten sammeln oder verarbeiten, bis sie bestätigen können, dass der Fahrer und die Fahrgäste die Datenverarbeitung kennen und ihr zugestimmt haben oder dass sie eine andere legitime Grundlage für die Verarbeitung besitzen.

Normungsgremien

63. Es sollten Standards geschaffen werden, die es den für die Verarbeitung Verantwortlichen ermöglichen, ihren Sicherheitsverpflichtungen nachzukommen und insbesondere die Vertraulichkeit der gesammelten Daten zu gewährleisten. Im Zusammenhang mit vernetzten Fahrzeugen gilt das Erfordernis der Vertraulichkeit und Sicherheit sowohl für Daten, die innerhalb des Fahrzeugs erhoben und verarbeitet werden, als auch für Daten, die vom Fahrzeug aus versendet werden. Daher sollten strenge Datenschutz- und Sicherheitsstandards verfasst werden, die den Risiken der Datenverarbeitung gerecht werden.

64. Normen für die Verwirklichung kooperativer intelligenter Verkehrssysteme (C-ITS) sollten die Verbreitung von Informationen auf Fahrzeuge und Infrastruktureinrichtungen auf den Nahbereich des emittierenden Fahrzeugs beschränken.

65. Normen, die den Zugang zu Daten im Fahrzeug regeln, sollten die Einhaltung der geltenden Rechtsvorschriften erleichtern und es den Betroffenen ermöglichen, ihre Rechte effizient wahrzunehmen.[26]

Fahrer

66. Sobald sie ausreichend informiert sind, sollten die Fahrzeughalter ihrerseits andere Nutzer des Fahrzeugs über die Datenerhebungs- und Nutzungsrichtlinien und, wenn möglich, über die Optionen zur Wahl bestimmter Datenschutzeinstellungen informieren. Voraussetzung für die Information der anderen Insassen ist, dass der Fahrer selbst über diese Datenerhebungs- und Nutzungsrichtlinien unterrichtet ist.

Öffentliche Stellen

67. Die Behörden sollten die von den vernetzten Fahrzeugen gelieferten Daten hauptsächlich für Zwecke verwenden, denen die betroffenen Personen freiwillig zugestimmt haben oder die im öffentlichen Interesse liegen, oder um Aufgaben zu erfüllen, die in einem einschlägigen Gesetz festgelegt sind. Um einer Überdehnung der Verarbeitungszwecke entgegenzuwirken und die Akzeptanz von vernetzten Fahrzeugen zu vergrößern, sollten die Behörden diese Daten nur zur Anpassung der Infrastrukturen, zur Verbesserung der Straßenverkehrssicherheit und zur Verringerung der Verkehrsüberlastung verwenden.

68. Die Umnutzung von Fahrzeugdaten zu Überwachungszwecken oder zur Feststellung von Rechtsverstößen wie Geschwindigkeitsübertretungen muss eine klare Rechtsgrundlage haben.

Regulierungsbehörden

69. Die zuständigen Regulierungsbehörden sollten die Bereitstellung einer Funktion zur Löschung personenbezogener Daten (die vor dem Verkauf oder der nächsten Anmietung eines Fahrzeugs anzuwenden ist) vorschreiben.

70. Vernetzte Fahrzeuge, die komplexe Systeme sind, sollten vor ihrer Freigabe einer Datenschutz-Folgenabschätzung unterzogen werden. Diese Anforderung sollte durch einschlägige Gesetze, Verordnungen oder Richtlinien festgelegt werden.

---

26 Access to In-vehicle Data and Resources, https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf