LANDTAG RHEINLAND-PFALZ
17. Wahlperiode

Drucksache 17/11044
zu Drucksache 17/10910
15. 01. 2020

Antwort

des Ministeriums des Innern und für Sport

auf die Kleine Anfrage der Abgeordneten Pia Schellhammer (BÜNDNIS 90/DIE GRÜNEN)
– Drucksache 17/10910 –

Datenverarbeitung und Künstliche Intelligenz in Fahrzeugen

Die **Kleine Anfrage – Drucksache 17/10910 –** vom 19. Dezember 2019 hat folgenden Wortlaut:

Die Digitalisierung sorgt auch in der Automobilindustrie für eine Vielzahl von Innovationen und Entwicklungen bis hin zum autonomen Fahren. Um Hindernisse zu umfahren oder die kürzeste Strecke zu berechnen, arbeiten Fahrassistenz- und Navigationssysteme mit Algorithmen. Künstliche Intelligenz spielt auch im modernen Auto eine wesentliche Rolle. Grundlage für diese Neuerungen ist immer das Erheben und Analysieren von Daten. Im vernetzten und internetfähigem Auto fallen daher erhebliche Datenmengen über Zustand, Bewegungen und Umgebung des Fahrzeugs an. Darüber hinaus werden teilweise sensible Daten über das Verhalten der Fahrenden erhoben.
Vor diesem Hintergrund frage ich die Landesregierung:

1. Welche Daten werden bei der Nutzung eines Fahrzeugs nach Kenntnis der Landesregierung gespeichert?
2. Zu welchen Zwecken werden nach Kenntnis der Landesregierung die aus dem Fahrzeug übermittelten Daten von der jeweiligen Stelle wie z. B. Versicherungen verarbeitet?
3. Wie schätzt die Landesregierung die Gefahr von Datenmissbrauch in internetfähigen Fahrzeugen ein?
4. Wie wird nach Kenntnis der Landesregierung der Datenschutz bei mit dem automatischen Notrufsystem Emergency Call (eCall) ausgerüsteten Automodellen gewährleistet?
5. Wie wird die Einhaltung von datenschutzrechtlichen Vorgaben bei Dienstfahrzeugen sichergestellt?
6. Wie wird gewährleistet, dass die Hoheit über gespeicherte oder verwendete Daten bei den Fahrzeugnutzer*innen bleiben?
7. Inwieweit verwendet die Polizei Daten aus internetfähigen Fahrzeugen (bitte aufschlüsseln nach Delikt und Zweckrichtung)?

Das **Ministerium des Innern und für Sport** hat die Kleine Anfrage namens der Landesregierung mit Schreiben vom 14. Januar 2020 wie folgt beantwortet:

Zu Frage 1:

Welche Daten im Fahrzeug anfallen und ob und wie lange diese gespeichert werden, wird nach Kenntnis der Landesregierung durch jeden Autohersteller unterschiedlich gehandhabt und unterscheidet sich zudem je nach Ausstattungsvariante und Modellreihe. Unterschieden wird grundsätzlich nach:

1. Betriebsdaten (z. B. aktuelle Geschwindigkeit). Diese werden spätestens beim Ausschalten des Fahrzeugs gelöscht, da sie dann ihren Zweck erfüllt haben.

2. Daten für Komfortfunktionen (z. B. automatische Abstandswahrung). Diese Daten werden i. d. R. ebenfalls nicht dauerhaft, sondern nur temporär im Fahrzeug gespeichert.

3. Fehler- und Wartungsdaten (z. B. überhöhte Motordrehzahl, Öffnen eines Cabrio-Dachs während der Fahrt). Diese Daten werden, je nach Kfz-Hersteller, i. d. R. langfristig gespeichert.

4. Unfalldaten (z. B. Zeitpunkt Airbag-Aktivierung). Diese Daten werden über das eCall-System (vgl. Antwort zu Frage 4) direkt an die Notfallzentrale gesendet und dort gespeichert, solange die Handhabung der Notfallsituation dies erforderlich macht.

5. Vom Insassen eingebrachte Daten (z. B. Navigationsziele). Gespeichert werden diese Daten in den manuellen Steuergeräten bis sie manuell gelöscht werden.

Solche Daten, die in einem vernetzten oder selbstfahrenden Fahrzeug anfallen, sind personenbezogen im Sinne der Europäischen Datenschutz-Grundverordnung, sobald diese mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen verknüpft

Druck: Landtag Rheinland-Pfalz, 30. Januar 2020

werden können und sich danach auf identifizierbare Personen (Halter/in, Fahrer/in) beziehen. Die Verarbeitung solcher personenbezogener Daten muss entweder auf der Einwilligung der/des Betroffenen oder auf einer gesetzlichen Regelung basieren.

Zu Frage 2:

Die aus dem Fahrzeug stammenden technischen Daten werden nach Kenntnis der Landesregierung von unterschiedlichen Stellen unter anderem dazu verarbeitet, Aussagen über das Fahrverhalten zu ermöglichen, das Unfallgeschehen zu rekonstruieren oder die Fahrfunktion technisch zu optimieren.

1. Seit dem Jahr 2014 existiert auf dem deutschen Markt bekanntlich ein Tarifmodell für eine Kfz-Versicherung, dessen Versicherungsprämie in Abhängigkeit zum Fahrverhalten bemessen wird („Pay as you drive“). Auf der Grundlage von aus technischen Daten erhobenen Score-Werten wird bei dieser sogenannte Telematik-Versicherung die zu zahlende Versicherungsprämie ermittelt. Die datenschutzrechtliche Legitimation dieser Verarbeitung personenbezogener Daten ergibt sich grundsätzlich aus dem zwischen beiden Parteien vereinbarten Vertrag und darf unter Beachtung der Datenschutzgrundsätze nur jene Datennutzung umfassen, die für die Erfüllung des vereinbarten Vertragszwecks (z. B. Telematik-Versicherung) erforderlich ist.
2. Durch das durch EU-Verordnung 2015/758 eingeführte eCall-System wird nach einem schweren Unfall automatisch ein Notruf an die europaweit einheitliche Rettungstelefonnummer 112 abgesetzt. Dadurch sollen Rettungskräfte schneller am Unfallort sein, um effizient Hilfe zu leisten. Laut Schätzungen der EU könnte hierdurch jährlich rund 2 500 Menschen das Leben gerettet werden.
3. In § 63 a Abs. 5 Straßenverkehrsgesetz (StVG) wurde bei der Nutzung von „Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion“ (autonomes Fahren) die Möglichkeit geregelt, Daten zur Unfallforschung in anonymisierter Form an Dritte zu übermitteln. In § 63 b StVG sind eine Reihe von Verordnungsermächtigungen zugunsten des Bundesministeriums für Verkehr und digitale Infrastruktur vorgesehen. Diese umfassen die technische Ausgestaltung, den Ort des Speichermediums sowie die Art und Weise der Speicherung, die Adressatin oder den Adressaten der Speicherpflicht nach § 63 a Abs. 3 StVG und die Maßnahmen, die zur Sicherung der gespeicherten Daten gegen unbefugten Zugriff bei Verkauf des Kraftfahrzeugs ergriffen werden müssen.
4. Bei „Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion“ müssen zudem die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben gem. § 63 a Abs. 1 Satz 1 StVG gespeichert werden, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt. Eine derartige Speicherung erfolgt auch, wenn die Fahrzeugführerin oder der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen, oder eine technische Störung des Systems auftritt. Ziel dieser Datenspeicherung ist es, nachvollziehbar festzuhalten, ob die Fahrzeugsteuerung durch das System oder die Fahrzeugführerin respektive den Fahrzeugführer erfolgt ist.

Zu Frage 3:

Die Mitglieder des Verbands der Autoindustrie (VDA) haben im Jahr 2014 „Datenschutzprinzipien für vernetzte Fahrzeuge“ formuliert, um die Anforderungen an den Schutz der zu verarbeitenden Daten zu gewährleisten. Zum Zweck der Informationssicherheit werden danach die sicherheitsrelevanten Systeme in der Fahrzeugelektronik von Navigations-, Telematik- und Infotainment-Anwendungen getrennt. Laut VDA schotten Gateways und Firewalls die sicherheitsrelevanten Bereiche im vernetzten Fahrzeug ab, Daten werden verschlüsselt und die Soft- und Hardwarearchitekturen der Fahrzeuge fortentwickelt. Durch diese Maßnahmen soll ein hohes technisches Sicherheitsniveau gewährleistet werden. Datenschutzrechtlich gilt auch hier jedenfalls der Grundsatz des „Privacy by Default“. Dieser bezeichnet die datenschutzfreundliche Grundeinstellung von Informations- und Kommunikationssystemen: Die Nutzerin oder der Nutzer muss darauf vertrauen können, dass die Herstellerfirma die Werkseinstellungen datenschutzfreundlich gestaltet. Das Prinzip „Privacy by Default“ führt dazu, dass die Nutzerin oder der Nutzer die Grundeinstellung des Systems nutzen kann und hierbei ohne Weiteres der Datenschutz gewährleistet wird. Neben den Grundeinstellungen im Rahmen des „Privacy by Default“ muss es der Nutzerin oder dem Nutzer möglich sein, die sie bzw. ihn betreffenden personenbezogenen Daten zu schützen, indem die Herstellerfirma entsprechende Möglichkeiten (z. B. Anonymisierung) zur Verfügung stellt.

Zu Frage 4:

Die EU-Verordnung 2015/758 regelt in Artikel 6 unter anderem, dass die verarbeiteten Daten ausschließlich für die Notfallsituation verwendet und nur an die verantwortliche Rettungsleitstelle übermittelt werden dürfen. Geregelt werden darüber hinaus die datensparsame Speicherung und Löschung des personenbezogenen Datensatzes, sobald dieser für die „Handhabung der Notfallsituation“ nicht mehr erforderlich ist. Da die stets zu verwendende, im Pkw fest installierte SIM-Karte sich erst dann in das vor Ort stärkste Mobilfunknetz unter der Notrufnummer 112 einbucht, wenn das Auto einen Unfall hatte, kann u. a. kein Bewegungsprofil erstellt werden.

Zu Frage 5:

Die Einhaltung der datenschutzrechtlichen Vorgaben rückt im Zuge der zunehmenden künstlichen Intelligenz im modernen Kraftfahrzeugbereich immer mehr in den behördlichen Fokus. Dies gilt insbesondere auch für Dienstfahrzeuge der Polizei Rheinland-Pfalz, weil die Erfassung und Verarbeitung der Daten unmittelbar die Sicherheitserwägungen der polizeilichen Tätigkeit betreffen. Um den Entwicklungen in diesem Bereich Rechnung zu tragen, enthalten aktuelle technische Leistungsbeschreibungen – die die Grundlage einer Fahrzeugausschreibung im Polizeibereich darstellen – Regelungen über den Umgang bzw. die Erhebung und Übertragung dieser Daten. Unter anderem wird gefordert, dass die Anforderungen des BSI IT-Grundschutzes durch

die Fahrzeuganbieter zwingend beachtet werden. Zudem befindet sich die bundesweit aktuell gültige Fassung der „Technischen Richtlinie Funkstreifenwagen“ derzeit durch das Polizeitechnische Institut (PTI) in Überarbeitung. Da die Themen Informations- und Datensicherheit auch in diesem Fahrzeugbereich eine wichtige Rolle spielen, werden diese in der neuen Richtlinie entsprechend berücksichtigt. Im Übrigen sind nach der jeweils gültigen Dienstkraftfahrzeugrichtlinie für jedes Fahrzeug des allgemeinen Dienstreiseverkehrs ein Fahrtenbuch und ein Kostenblatt zu führen (vgl. Ziffer 12 DKfzR vom 17. Dezember 2019 – MinBlatt Nr. 14 vom 30. Dezember 2019, Seite 404). Die in der Regel konventionell zu führenden Fahrtenbücher und Kostenblätter sind ständig unter Verschluss bzw. in gesicherten internen Systemen gespeichert, sodass auch die Datensicherheit gewährleistet wird. Die Daten aus dem jeweiligen Navigationssystem des Dienst-Kraftfahrzeugs werden bei der Rückgabe der Fahrzeuge gelöscht. Eine Telematik-Versicherung wird bei Dienst-Kraftfahrzeugen nicht genutzt (vgl. Antworten zu den Fragen 1 und 2).

Zu Frage 6:

Das Fahrzeug muss den gesetzlichen Bestimmungen entsprechen. Hierzu gehört auch die Berücksichtigung aller datenschutzrechtlichen Bestimmungen. Wer ein internetfähiges Fahrzeug erwirbt, entscheidet selbst, was mit seinen personenbezogenen Daten passiert und hat insbesondere die nach der Datenschutz-Grundverordnung garantierten Auskunfts- und Interventionsrechte. Da mithilfe der gewonnenen Daten Bewegungs-, Nutzungs- und Kommunikationsprofile erstellt werden könnten, ergibt sich eine Vielzahl attraktiver Verwendungsmöglichkeiten. Allerdings ist eine Verwendung der personenbezogenen Daten für andere Zwecke nach § 28 II Bundesdatenschutzgesetz und § 7 Abs. 1 Landesdatenschutzgesetz zu beurteilen. Danach ist die Verarbeitung personenbezogener Daten zu anderen Zwecken als zu demjenigen, zu dem die Daten erhoben wurden, nur auf wenige Ausnahmen beschränkt (z. B. Erforderlichkeit zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person).

Zu Frage 7:

Im Rahmen der präventiven oder auch repressiven Aufgabenwahrnehmung der Polizei RP können im Zusammenhang mit Fahrzeugen der neueren Generationen in Abhängigkeit vom Fahrzeugtyp und der Fahrzeugausstattung unterschiedlichste Daten relevant sein. Auf der Grundlage des konkreten Anlasses bzw. der jeweiligen rechtlichen Rahmenbedingungen sind in diesem Zusammenhang bislang insbesondere Daten von Belang, die bei der Nutzung von Navigationssystemen oder der Mobilfunktechnik anfallen. Das Landeskriminalamt und die Hochschule der Polizei Rheinland-Pfalz haben die Relevanz von Daten in bzw. aus Fahrzeugen frühzeitig erkannt und bereits vor längerer Zeit Arbeitsschwerpunkte im Bereich der Fahrzeugforensik als Teilbereich der digitalen Forensik gesetzt. Sobald im Rahmen von Strafverfahren zureichende tatsächliche Anhaltspunkte für den Anfangsverdacht einer verfolgbaren Straftat vorliegen, hat die Polizei den Sachverhalt nach § 163 Strafprozessordnung zu erforschen und die erforderlichen Maßnahmen zur weiteren Aufklärung und Beweissicherung zu treffen. Eingriffe in das Grundrecht der informationellen Selbstbestimmung aus Artikel 2 Abs. 1 Grundgesetz (GG) in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationsrechtlicher Systeme nach Artikel 1 Abs. 1 GG sowie ggfs. in das Telekommunikationsgeheimnis nach Artikel 10 Abs. 1 GG setzen allerdings das Vorliegen einer Eingriffsermächtigung voraus. Dies ist in jedem Ermittlungsverfahren im Einzelfall zu prüfen. Aufschlüsselungen zu Delikten und Zweckrichtungen sind mangels entsprechender statistischer Aufzeichnungen nicht möglich.

In Vertretung:
Nicole Steingaß
Staatssekretärin