3932/J XXVIII. GP

Eingelangt am 19.11.2025

ANFRAGE

der Abgeordneten Mag. Marie-Christine Giuliani-Sterrer, BA
an die Bundesministerin für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
betreffend **Gefahr für Datenschutz und nationale Sicherheit durch digitale Fahrzeuge**

Im Bereich der modernen Fahrzeuge und digitalen Endgeräte werden mittlerweile enorme Mengen an personenbezogenen Daten erfasst, ausgewertet und häufig ohne Wissen oder Zustimmung der Bürger weitergegeben. Die Hersteller integrieren standardmäßig Kameras, Mikrofone, Telematiksysteme, Sensoren und SIM-Karten in ihre Produkte. Dadurch entsteht ein ständiger Strom an hochsensiblen Informationen, der nicht selten direkt an ausländische Konzerne oder sogar an Behörden außerhalb der Europäischen Union übermittelt wird.

Am Beispiel chinesischer Hersteller wie Yutong[1], BYD[2], Huawei[3] oder der Social-Media-Plattform TikTok[4] werden die Risiken einer digitalen Überwachung, eines möglichen Missbrauchs sowie des Abflusses sensibler Daten ins Ausland in besonders drastischer Weise deutlich. In China gilt für Unternehmen sogar eine gesetzliche Verpflichtung, sämtliche Daten auf Anfrage an staatliche Stellen weiterzugeben.[5] Dies stellt nicht nur eine Gefährdung des Datenschutzes dar, sondern bedroht auch die nationale Souveränität Österreichs und der Europäischen Union insgesamt.

Gleichzeitig sind ähnliche Gefahren auch bei anderen internationalen Herstellern zu beobachten. US-Konzerne wie Tesla oder Apple betreiben eigene Datennetze, bei denen unklar bleibt, wohin die gesammelten Informationen tatsächlich weitergeleitet und zu welchem Zweck sie ausgewertet werden. Auch japanische und südkoreanische

1 https://www.focus.de/auto/elektroauto/spionieren-uns-chinesische-e-autos-aus-bus-leak-aus-norwegen-zeigt-sicherheitsrisiken_b24df506-a100-4050-8aa3-82e21f90e1bc.html (aufgerufen am 14.11.2025)
2 https://www.inside-politics.at/mit-oder-ohne-spion-behoerden-koennten-chinesische-autos-von-byd-kaufen-469/ (aufgerufen am 14.11.2025)
3 https://www.br.de/nachrichten/netzwelt/huawei-und-5g-einfallstor-fuer-china-spione-und-hacker,UBWgLIo (aufgerufen am 14.11.2025)
4 https://www.tagesschau.de/wirtschaft/unternehmen/tiktok-datenschutzverstoss-100.html (aufgerufen am 14.11.2025)
5 https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en (aufgerufen am 14.11.2025)

Unternehmen verfügen über Systeme, die den Zugriff auf persönliche Nutzerdaten ermöglichen.

Wie schwerwiegend das Problem tatsächlich ist, verdeutlicht die internationale Studie „Privacy Not Included“ der Mozilla Foundation aus dem Jahr 2023.[6] Sie analysierte 25 der weltweit größten Automarken und kam unter anderem zu folgenden alarmierenden Ergebnissen: 84% der untersuchten Marken teilen oder verkaufen persönliche Daten ihrer Kunden an Dritte. 56% der Hersteller geben personenbezogene Daten an Regierungen oder Strafverfolgungsbehörden weiter, zum Teil auch ohne Gerichtsbeschluss.

Noch gravierender ist, dass 92% der Automarken den Nutzern kaum oder gar keine effektive Kontrolle über die eigenen Daten einräumen. Damit sind die Bürger nicht nur in Österreich, sondern weltweit dem Risiko ausgesetzt, dass ihre Bewegungsdaten, Kommunikationsinhalte und persönlichen Präferenzen beliebig ausgewertet, übertragen oder sogar missbraucht werden können.

Dass diese Gefahren längst Realität sind, zeigen auch aktuelle Vorfälle in Österreich: So wurden etwa Fälle bekannt, in denen bei Kunden einer Fahrzeugvermietung durch GPS-Überwachung und elektronische Fahrzeugkontrolle gravierend in deren Rechte und Sicherheit eingegriffen wurde.[7] Im Extremfall war das Fahrzeug, das über ein motorgestütztes Lenkungs- und Bremssystem verfügte, kaum noch zu lenken und zu bremsen gewesen.[8]

Aktuelle Berichte zeigen, dass im skandinavischen öffentlichen Busverkehr Fahrzeuge des chinesischen Herstellers Yutong von China aus jederzeit gestoppt und unbrauchbar gemacht werden können, einschließlich der elektronischen Türverriegelung.[1] Dies verdeutlicht die reale Gefahr einer fernsteuerbaren Beeinträchtigung kritischer Infrastruktur durch ausländische Anbieter. Die dänische Regierung leitet angesichts dieser Risiken eine Untersuchung ein. Im Gegensatz dazu beschränkt sich die österreichische Bundesregierung bislang auf Beschwichtigungen obwohl auch in Österreich Busse desselben Herstellers im Einsatz sind.

Das zeigt, dass die großflächige Vernetzung von Fahrzeugen, Telekommunikationssystemen und digitalen Anwendungen neue, bisher unterschätzte Gefahren für die öffentliche Sicherheit und die nationale Souveränität mit sich bringt. Experten warnen davor, dass die massenhafte Sammlung und Weiterleitung von Bewegungs-, Kommunikations- und Verhaltensdaten nicht nur für kommerzielle Zwecke, sondern gezielt von ausländischen Geheimdiensten und Terrornetzwerken ausgenutzt werden kann.

Im Zeitalter hybrider und subversiver Kriegsführung wird die digitale Kontrolle über Fahrzeuge, Infrastruktur und Kommunikation zunehmend zu einem Instrument der Einflussnahme und Destabilisierung. Angriffe auf vernetzte Systeme, das gezielte

---

6 https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ (aufgerufen am 14.11.2025)

7 https://konsument.at/avis-vernetzte-autos-datenschutzklausel-unzulaessig/65827 (aufgerufen am 14.11.2025)
https://www.kleinezeitung.at/kaernten/20177339/privates-unternehmen-kassiert-220-euro-fuer-zu-schnelles-fahren (aufgerufen am 14.11.2025)

8 https://www.krone.at/3898659 (aufgerufen am 14.11.2025)

Lahmlegen von Fahrzeugflotten oder die Auswertung sensibler Bewegungsprofile für Sabotageakte sind längst keine theoretischen Szenarien mehr, sondern stellen in Europa eine tägliche Realität dar. Gerade im Krisen- oder Kriegsfall kann die Fernsteuerung, Manipulation oder gezielte Abschaltung von Fahrzeugen und digitalen Diensten zu einer existenziellen Gefahr für Gesellschaft, Wirtschaft und staatliche Handlungsfähigkeit werden.

Die Bundesregierung hat bisher in Einzelfällen, wie beim Verbot der TikTok-App auf Diensthandys, auf die berechtigten Sorgen der Bevölkerung reagiert. Ein systematisches, transparentes und umfassendes Konzept zur Abwehr von Gefahren durch ausländische Hersteller fehlt aber bis heute. Der Schutz der Bürger, ihrer Privatsphäre und der nationalen Sicherheit darf jedoch nicht von Herkunft oder Bekanntheit des Herstellers abhängig gemacht werden.

Es bedarf Klarheit über die Prüf- und Zulassungskriterien, lückenlose Transparenz über den tatsächlichen Umgang mit den Daten der Bürger und eine aktive Aufklärung der Konsumenten über die bestehenden Risiken. Es darf nicht sein, dass österreichische Steuerzahler und Konsumenten unwissentlich zu Opfern globaler Datenkonzerne, fremder Geheimdienste oder terroristischer Netzwerke werden. Bürger und Staat müssen gleichermaßen vor digitalen Risiken geschützt werden, unabhängig davon, ob diese aus China, den USA oder anderen Staaten stammen.

In diesem Zusammenhang richtet die unterfertigte Abgeordnete an die Bundesministerin für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz nachstehende

Anfrage

1. Welche Prüfmechanismen und Zulassungskriterien bestehen aktuell, um sicherzustellen, dass Kraftfahrzeuge und digitale Endgeräte ausländischer Hersteller keine datenschutzrechtlichen oder sicherheitsrelevanten Risiken für Bürger und Staat darstellen?
2. Inwieweit werden bei der Beschaffung von Fahrzeugen und digitalen Systemen für öffentliche Stellen gezielte Risikobewertungen hinsichtlich des Zugriffs ausländischer Konzerne, Geheimdienste oder Regierungen auf in Österreich erhobene Daten vorgenommen?
3. Wie viele Kraftfahrzeuge, die mit Telematiksystemen, integrierten SIM-Karten oder internetfähigen Sensoren ausgerüstet sind, wurden seit 2020 von öffentlichen Stellen angeschafft?
    a. Aus welchen Herstellungsländern kommen diese?
4. Welche Anforderungen stellt die Bundesregierung an Ausschreibungen und öffentliche Vergaben, um sicherzustellen, dass bei staatlichen Aufträgen nur Fahrzeuge und Systeme mit höchsten Datenschutz- und IT-Sicherheitsstandards beschafft werden?
5. Wie wird die laufende Überprüfung und bereits beschaffter Fahrzeuge und digitaler Systeme hinsichtlich möglicher Sicherheitslücken, Missbrauchsgefahren oder Manipulationsmöglichkeiten organisiert?
6. Gibt es technische oder rechtliche Mindeststandards, die ausländische Hersteller erfüllen müssen, um auf dem österreichischen Markt zugelassen zu werden?

   a. Wenn ja, welche?
   b. Wie wird die Einhaltung dieser Mindeststandards kontrolliert?
7. Welche Rolle spielen österreichische oder europäische Zulassungsstellen bei der Überprüfung der digitalen Komponenten, bevor ein Fahrzeugmodell für den Straßenverkehr zugelassen wird?
8. Welche Maßnahmen setzt die Bundesregierung, um zu verhindern, dass personenbezogene Daten aus Österreich durch ausländische Hersteller oder über deren Cloudsysteme ohne Wissen und Zustimmung der Betroffenen ins Ausland transferiert werden?
9. Welche Vorgaben bestehen für Anbieter von digitalen Diensten und Fahrzeugen, um einen Zugriff Dritter auf Fahrzeugdaten, Standortinformationen, Kommunikations- und Nutzungsdaten zu verhindern?
10. Inwieweit wird kontrolliert, ob Daten von österreichischen Nutzern, die durch ausländische Fahrzeughersteller oder App-Anbieter erhoben werden, tatsächlich ausschließlich innerhalb der EU gespeichert und verarbeitet werden?
11. Welche konkreten Erkenntnisse hat die Bundesregierung über den Datenabfluss nach China, in die USA oder andere Drittstaaten im Zusammenhang mit der Nutzung moderner Kraftfahrzeuge und Fahrzeug-Apps?
12. Welche Vereinbarungen bestehen mit internationalen Herstellern, um österreichischen Behörden im Anlassfall Zugang zu Daten oder technischen Schnittstellen von Fahrzeugen zu ermöglichen?
13. Wie stellt die Bundesregierung sicher, dass Bürger umfassend und transparent über die Datenerhebung, Datenverwendung und ihre Rechte durch Fahrzeughersteller und App-Anbieter informiert werden?
14. Wie viele Beschwerden oder Hinweise zu Datenschutzverletzungen im Zusammenhang mit digital vernetzten Fahrzeugen und Mobilitätsdienstleistungen sind seit 2020 bei österreichischen Behörden eingegangen?
15. Gibt es Überlegungen, die gesetzlichen Regelungen für digitale Produkte und Fahrzeuge zu verschärfen, um die nationale Souveränität im Bereich Datenschutz, IT-Sicherheit und kritische Infrastruktur zu stärken?
16. Welche Konsequenzen zieht die Bundesregierung, wenn ein Hersteller nachweislich gegen Datenschutzbestimmungen oder Sicherheitsauflagen verstößt?
17. Gibt es bereits Fälle, in denen Zulassungen entzogen oder Einschränkungen ausgesprochen wurden?
18. Gibt es Pläne, die Rolle und Ressourcen der Datenschutzbehörde im Bereich der Kontrolle ausländischer Digitalprodukte und Fahrzeuge auszubauen?
19. Wie wird geprüft, ob Funktionen zur Fernsteuerung, Abschaltung oder Überwachung von Fahrzeugen oder Endgeräten, etwa durch GPS-Blockierung oder digitale Zugangssperren, im Krisen- oder Kriegsfall eine Gefahr für Sicherheit und öffentliche Ordnung darstellen können?
20. Welche Kontrollen bestehen, um zu verhindern, dass über digitale Schnittstellen von Fahrzeugen Manipulationen, Sabotageakte oder unerlaubte Eingriffe vorgenommen werden?
21. Wie werden Betreiber von Fahrzeugflotten und Mobilitätsdienstleistern verpflichtet, ihre Kunden vor Missbrauch, Datenklau und Eingriffen durch Dritte zu schützen?
22. Wie bewertet die Regierung die Gefahr, dass durch die Verbreitung digital gesteuerter Fahrzeuge auch kritische Infrastruktur wie Rettungsdienste,

Einsatzfahrzeuge und Energieversorgung im Ernstfall lahmgelegt oder manipuliert werden kann?

23. Welche rechtlichen oder technischen Hürden bestehen derzeit, um im Anlassfall die digitale Abschaltung oder Manipulation von Fahrzeugen durch ausländische Akteure nachzuweisen und zu verhindern?
24. Welche Rolle spielen ausländische Geheimdienste oder Terrornetzwerke nach Erkenntnis der Bundesregierung bei der gezielten Ausnutzung digitaler Schwachstellen in vernetzten Fahrzeugen, Mobilitätsdiensten und Kommunikationssystemen?
25. Gibt es Anhaltspunkte, dass ausländische Geheimdienste, terroristische Gruppen oder andere fremde Akteure in Österreich bereits versucht haben, über digitale Angriffe auf Fahrzeuge, Apps oder Flottenmanagementsysteme Informationen abzugreifen oder Sabotageakte zu begehen?
26. Wurden im Rahmen der nationalen Sicherheitsstrategie oder in der DSN konkrete Maßnahmen festgelegt, um die Risiken hybrider Kriegsführung im Bereich digitaler Mobilität und Infrastruktur abzuwehren?
    a. Wenn ja, welche?
27. Wie bewertet die Bundesregierung das Risiko, dass digitale Überwachung und Datenmissbrauch gezielt zur Erpressung, Diskreditierung oder zur Manipulation politischer Entscheidungsträger eingesetzt werden können?
28. Welche Kooperationsprojekte bestehen mit anderen EU-Mitgliedstaaten, um den Schutz der europäischen Bürger vor digitalen Risiken durch ausländische Fahrzeug- und Gerätehersteller zu verbessern?
29. Welche Rolle spielen europäische Institutionen, etwa die Europäische Agentur für Cybersicherheit (ENISA), bei der Entwicklung und Überwachung von Sicherheitsstandards für digital vernetzte Fahrzeuge?
30. Plant die Bundesregierung, internationale Erkenntnisse und Untersuchungen, wie jene aus Dänemark und Norwegen, künftig systematisch in nationale Risikoanalysen und Schutzmaßnahmen einfließen zu lassen?
    a. Wenn nein, warum nicht?