18447/J XXVII. GP

Eingelangt am 25.04.2024

ANFRAGE

des Abgeordneten Christian Hafenecker, MA
an den Bundesminister für Finanzen
betreffend **Gefährden datensammelnde Behördenfahrzeuge bald die nationale Sicherheit?**

Die zunehmende Digitalisierung schreitet auch im Bereich der Fahrzeuge rasch voran und macht aus Pkw und Co. „fahrende Datensammler“. So etwa im Falle des von der Europäischen Union verordneten „eCall-Systems“, welches mittels im Auto eingebauter Sensoren, einer GPS-Einheit zur Positionsbestimmung, einer eingebauten SIM-Karte und einer eingebauten Freisprecheinrichtung eine stetige Datenübermittlung nicht nur ermöglicht, sondern gesetzlich verordnet. In Notfällen sind dadurch Fahrzeugposition, Fahrtrichtung, Antriebsart, Anzahl der Personen im Fahrzeug sowie Fahrgestellnummer einsehbar und auslesbar. Diese Daten landen auf Servern und sind potenziellen Hackerangriffen, aber auch der illegalen Weitergabe ausgeliefert. Besonders brisant wird der Sachverhalt bei den seit einigen Jahren regelmäßig durchgeführten Softwareupdates, die mittlerweile von allen namhaften Autoherstellern auch ohne die aktive Zustimmung des Fahrzeugbesitzers aus der Ferne durchgeführt werden können.

Welche Gefahren hier lauern konnte eine Studie der „Mozilla Foundation“ aus dem Jahr 2023 aufzeigen.[1] Die Studienautoren schrieben dazu:

> *Jede Automarke, die wir uns angesehen haben, sammelt mehr personenbezogene Daten als nötig und verwendet diese Informationen für einen anderen Zweck als den Betrieb Ihres Fahrzeugs.*

Über Kameras und Sensoren, die auf Insassen und Umgebung gerichtet sind, sowie über gekoppelte Telefone und installierte Apps, werden Informationen erhalten, aus denen wiederum gigantische Datenprofile zu den Insassen der Pkw erstellt werden. Aus diesen lassen sich laut Studie Rückschlüsse auf Dinge wie Intelligenz, Fähigkeiten und Interessen der Fahrer ziehen. Die meisten (84 Prozent) der untersuchten Autohersteller geben an, dass sie persönliche Daten an Dritte weitergeben können – bei 19 von 25 Marken ist sogar von „Verkauf der Daten“ die Rede. Die Hälfte (56 Prozent) der Autobauer geben diese bei Anfragen auch an die Regierung oder Strafverfolgungsbehörden weiter.

[1] Studie entlarvt Autos als extreme Datensammler | AUTO MOTOR UND SPORT (auto-motor-und-sport.de)

Bedenklich ist auch, dass es laut der Untersuchung nur zwei Fahrzeugmarken (Renault und Dacia) gibt, die ihren Fahrern das Recht einräumen, persönliche Daten bei Bedarf zu löschen. Am schlechtesten schnitt die US-Automarke Tesla ab.

Nun hat der Bund just in einer Phase rund um die Diskussion von Sicherheitsbedenken bei der Nutzung von ausländischen Apps, wie TikTok, im öffentlichen Dienst bei einer aktuellen Ausschreibungen der Bundesbeschaffung GmbH (BBG) dem chinesischen Autobauer „BYD“ den Zuschlag für 640 neue Pkw erteilt.[2] Während man einerseits öffentlich Bediensteten im Sinne der „Informations- und Datensicherheit“ verbietet, auf Diensthandys TikTok zu installieren und zu nutzen[3], kauft man andererseits Fahrzeuge ausländischer Hersteller, die mit derselben und sogar noch umfassenderen Datensammel- und Überwachungstechnologie ausgestattet sind. Dabei führt die Implementierung von vernetzten Fahrzeugtechnologien, besonders unter Einbeziehung außereuropäischer Komponenten, zu erheblichen Sicherheitsrisiken. Weder die EU-Kommission noch die Bundesregierung, haben auf diese potenzielle Gefahr bisher adäquat reagiert.

Einerseits gibt es erhebliche Datenschutzbedenken, da die umfangreiche Datensammlung der Fahrzeuge potenziell die Privatsphäre der Nutzer gefährden kann. Andererseits besteht das Risiko der Industriespionage, da sensible Unternehmensinformationen, die in den Fahrzeugsystemen gespeichert sind, Ziel von Spionageaktivitäten werden könnten, was zu wirtschaftlichen Schäden führen kann. Zusätzlich erhöht die Möglichkeit der Fernsteuerung das Risiko von Sabotage und Manipulation der Fahrzeugfunktionalität, was sowohl die Sicherheit der Nutzer als auch die Effizienz der Fahrzeuge beeinträchtigen kann. Solche Manipulationen könnten auch zu Störungen in der kritischen Infrastruktur führen, insbesondere wenn Fahrzeuge in Schlüsselbereichen wie Logistik oder Notfallversorgung eingesetzt werden. Darüber hinaus stellen diese Sicherheitsrisiken eine direkte Gefahr für die öffentliche Sicherheit dar, da die potenzielle Manipulation von Fahrzeugen das Risiko von Unfällen und kriminellen Aktivitäten erhöht.

Durch den Einsatz von ausländischen Technologien im Bereich der öffentlichen Verwaltung, insbesondere von Netzwerkgeräten welche selbstständig mit dem Internet kommunizieren, wird die Integrität des österreichischen Sicherheitswesens daher stark gefährdet.

In Anbetracht dieser Risiken ist eine sorgfältige Überwachung und Anpassung der Sicherheitsprotokolle entscheidend, um den Schutz der Nutzer sowie der öffentlichen Sicherheit und Ordnung zu gewährleisten. Denn durch diese in den Fahrzeugen integrierte Technologien wird die Möglichkeit geschaffen, österreichische Behörden aktiv zu überwachen und Informationen direkt an ausländische Geheimdienste zu übermitteln.

Letztlich sei auch darauf hingewiesen, dass die zunehmende Abhängigkeit von außerhalb Europas importierten Technologien zu einem signifikanten Verlust der Wertschöpfung in Österreich führt, wobei zu bedenken ist, dass es durchaus

[2] Chinesischer Autobauer BYD liefert Behördenfahrzeuge - Wirtschaft - derStandard.at › Wirtschaft

[3] Österreich verbietet TikTok auf Diensthandys (futurezone.at)

leistungsfähige deutsche Alternativen gibt, die in Österreich produzieren und somit zur Sicherung heimischer Arbeitsplätze beitragen.

In diesem Zusammenhang stellt der unterfertigte Abgeordnete an den Bundesminister für Finanzen folgende

Anfrage

1. Wie viele Fahrzeuge außereuropäischer Hersteller sind im öffentlichen Dienst in Verwendung?
    a. Wie viele davon sind im Besitz des Bundes?
2. Wie wird die Einhaltung von Datenschutz- und Sicherheitsstandards bei der Beschaffung von Fahrzeugen für den öffentlichen Dienst gewährleistet?
    a. Gibt es spezifische Kriterien oder Zertifizierungen, die Hersteller erfüllen müssen, um als Lieferanten für den öffentlichen Dienst in Frage zu kommen?
    b. Wie werden diese Standards im Laufe der Nutzungsdauer der Fahrzeuge überprüft und aufrechterhalten?
3. Welche Sicherheitsvorkehrungen trifft der Bund in punkto illegale Datensammlung durch in Fahrzeugen der öffentlichen Verwaltung installierte Software- und Hardwaresysteme?
    a. Gibt es ein gesamtheitliches Sicherheitskonzept zu dieser Problematik?
4. Gibt es bei Fahrzeugen im öffentlichen Dienst eine Verschlüsselung der im Auto gespeicherten Daten?
    a. Wenn nein, warum nicht?
5. Was geschieht mit personenbezogenen Daten, die in Fahrzeugen des öffentlichen Dienstes durch den Fahrzeughersteller gesammelt werden?
    a. Wo werden diese Daten gesammelt und gespeichert?
    b. Hat der Bund Zugriff auf diese Daten?
    c. Werden diese Daten im Sinne der DSGVO behandelt?
    d. Werden diese Daten nach einer gewissen Zeit gelöscht, spätestens wenn das Fahrzeug den Besitzer/Benutzer wechselt?
    e. Haben öffentlich Bedienstete das Recht, personenbezogene Daten löschen zu lassen?
6. Wie will der Bund, respektive die Bundesregierung, eine mögliche Datenabwanderung, etwa an ausländische Regierungen und digitale Datenmakler, durch außereuropäische Fahrzeuge im öffentlichen Dienst verhindern?