DATEN SCHUTZ AGENTUR

Organisation Technik Compliance

DATENSCHUTZAGENTUR
Kirchberggasse 7/8, 1070 Wien

Parlament
Ausschuss für Konsumentenschutz
Dr.-Karl-Renner-Ring 3
1017 Wien

Stellungnahmen.Konsumentenschutzausschuss@parlament.gv.at

Wien, am 27.04.2019

Betreff: Stellungnahme zu den Anträgen 102/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes und 105/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes - insbesondere der Smart-Cars

Sehr geehrte Damen und Herren!

Bezugnehmend auf Ihr Schreiben vom 27.02.2019 bedanke ich mich für die freundliche Einladung zu den beiden oben genannten Anträgen Stellung zu nehmen.

Die nachfolgenden Ausführungen behandeln zuerst ausgewählte Aspekte des Internet der Dinge im Allgemeinen und gehen in weiterer Folge auf spezifische Fragestellungen des Internet der Dinge im Zusammenhang mit „Smart Cars“ ein.

Internet der Dinge

Einer der Grundgedanken des Internet der Dinge besteht in der Ausstattung von alltäglichen Gegenständen und Maschinen mit Funktionalitäten der Informationstechnologie. Diese Gegenstände und Maschinen sollen auf diese Weise Informationen über sich selbst und ihre Umwelt erfassen und zur Auswertung durch andere Systeme bereitstellen sowie bestimmte Aufgaben selbsttätig übernehmen.

In technischer Hinsicht kann dies durch unterschiedliche Technologien bewerkstelligt werden, wie etwa die Erfassung von Daten mittels Sensoren, die Speicherung, Bereitstellung und Übertragung von Daten mittels RFID-Etiketten (auch Funketiketten genannt), die Steuerung von Maschinen, die bisher über keine Datenverarbeitungskapazität verfügten, mit integrierten Computern sowie schließlich die

Anbindung derartiger Gegenstände an das Internet und Vernetzung mit umfangreichen Datenverarbeitungen in zentralen Rechenzentren sowie mit anderen Geräten des Internet der Dinge.

Entwickelt hat sich die Vision des Internet der Dinge aus den Konzepten des Ubiquitous Computing und der Ambient Intelligence, die bereits Ende der 1980er- / Anfang der 1990er-Jahre eine allgegenwärtige Datenverarbeitung und eine Einbettung derselben in die alltägliche Lebenswelt der Menschen propagierten.

Ein wesentlicher Ausgangspunkt der Überlegungen war die Feststellung, dass die tiefgreifendsten Technologien jene sind, die sich derartig in das tägliche Leben der Menschen einfügen, dass sie schließlich als selbstverständlich akzeptiert und nicht mehr bewusst wahrgenommen werden. Um einfach benutzbar zu sein, sollten Computer in einer Umgebung des Ubiquitous Computing jeweils für eine ganz spezielle Aufgabe zuständig sein und je nach Bedarf miteinander kommunizieren und zusammenarbeiten. Informationen sollen so jederzeit und überall abrufbar sein. Im Gegensatz zu herkömmlichen Laptops solle man aber nicht seinen persönlichen Computer mit sich herumtragen müssen. Vielmehr solle man jederzeit und selbstverständlich auf die in der Umgebung vorhanden Datenverarbeitungskapazitäten zugreifen können. (Weiser 1991)

Gegenstände und Maschinen, die diesem Ansatz folgen sind heutzutage bereits vielfach in unserer Lebensumwelt vorhanden. So versorgen beispielsweise Fahrgastinformationssysteme wartende Passagiere mit der Information, wann das nächste öffentliche Verkehrsmittel voraussichtlich an der Haltestelle eintreffen wird. Die für die Berechnung der Ankunftszeit erforderlichen Daten werden jedoch – von den Fahrgästen weitestgehend unbemerkt – auf Basis von Positionsdaten direkt im jeweiligen Verkehrsmittel erfasst und an das zentrale Flottenmanagementsystem des jeweiligen Verkehrsbetriebs weitergeleitet, das die erfassten Daten für die wartenden Passagiere aufbereitet und an der Haltestelle zur Verfügung stellt.

Ebenso kommen Sensornetzwerke zur Messung der Luftgüte, der Auslastung von Verkehrswegen und zur Messung zahlreicher anderer Sachverhalte zum Einsatz. Dies häufig ohne von der Allgemeinheit überhaupt wahrgenommen zu werden. KonsumentInnen nutzen lediglich die aus diesen Messungen resultierenden Informationen wie beispielsweise die voraussichtliche Reisezeitverzögerung auf gewissen Strecken.

Mit zunehmender Digitalisierung dringt diese Form der Datenverarbeitung jedoch auch in das unmittelbare persönliche Lebensumfeld von KonsumentInnen vor. Von der „intelligenten“ Zahnbürste über den „smarten“ Fernsehapparat bis zur vernetzten Glühbirne, die sich nahtlos in das „Smart Home“-

System des Haushalts eingliedert und die daraufhin durch den Benutzer ohne direkte Interaktion mit dem Lichtschalter ferngesteuert werden kann.

Gemeinsam ist diesen „intelligenten“ Anwendungen des Internet der Dinge, dass den KonsumentInnen regelmäßig nur die angenehmen und erwünschten Komfortfunktionen dieser Technologien offenbar werden. Die im Hintergrund stattfindende Datenverarbeitung und deren Funktionsweise bleiben oft – gemäß der oben genannten Vision des Ubiquitous Computing - im Verborgenen und sind für KonsumentInnen in der Regel nicht nachvollziehbar.

Je enger derartige Anwendungen jedoch mit natürlichen Personen in Kontakt kommen, umso wahrscheinlicher ist es, dass im Rahmen ihrer Ausführung personenbezogene Daten dieser Personen verarbeitet werden.

Unter personenbezogene Daten sind in diesem Zusammenhang (und gem. Art. 4 Z 1 Datenschutz-Grundverordnung; DSGVO) alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird dabei eine natürliche Person dann angesehen, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Im Zusammenhang mit Anwendungen des Internet der Dinge liegen personenbezogene Daten also auch dann vor, wenn diese Daten der betroffenen Person lediglich über eine Kennnummer, wie beispielsweise die IP-Adresse des privaten Internetanschlusses, oder andere Merkmale bzw. Merkmalskombinationen zugeordnet werden können. Dies ist – da es sich ja um internetbasierte Anwendungen handelt – regelmäßig der Fall, da sämtliche mit dem Internet verbundenen Geräte über permanente (z.B. MAC-Adresse der Netzwerkkarte) und temporäre (z.B. zugeordnete IP-Adresse) Identifikationskennzeichen verfügt.

Erschwerend kommt hinzu, dass sehr viele Anwendungen des Internet der Dinge die für die Erbringung ihrer Funktionen erforderlichen Datenverarbeitungen nicht lokal direkt im jeweiligen Gerät vornehmen, sondern stattdessen die erfassten Daten an ein Rechenzentrum des jeweiligen Geräteherstellers (bzw. „in die Cloud“) übermitteln. Dort werden die übermittelten Daten dann gespeichert, ausgewertet und die Berechnungsergebnisse an das vermeintlich intelligente Gerät zurückübermittelt um den KonsumentInnen zur Verfügung gestellt zu werden.

Wie bereits erwähnt erfolgen diese Abläufe häufig ohne Wissen und bewusste Einwilligung der KonsumentInnen, denen ja meist keinerlei Informationen über die Art und Funktionsweise der im Rahmen der jeweiligen Anwendung erfolgenden Datenverarbeitungen und –übermittlungen vorliegt.

Vor diesem Hintergrund ist der Feststellung jedenfalls zuzustimmen, „*dass das Internet der Dinge eine Realität erzeugt, die das Individuum nicht mehr kontrollieren kann.*“ (Antrag 102/A(E))

Illustriert sei dieser Sachverhalt am Beispiel handelsüblicher Staubsaug-Roboter, die sich bei KonsumentInnen zunehmender Beliebtheit erfreuen, da sie vollautomatisch die lästige Hausarbeit des Staubsaugens übernehmen.

Zahlreiche dieser Robotermodelle müssen zur Nutzung des vollständigen Funktionsumfanges über WLAN an das Internet angebunden werden. Erst dann steht den NutzerInnen die Möglichkeit zur Verfügung den Staubsaug-Roboter über eine Smartphone-App direkt vom Handy aus zu konfigurieren und zu steuern. Während der Roboter durch die zu reinigenden Räumlichkeiten fährt, erfasst er umfangreiche Daten über seine Umgebung zur Erstellung eines digitalen Grundrissplans der Räume und sämtlicher Gegenstände, die ihn auf seinem Weg durch die Wohnung an der Weiterfahrt hindern. Dieser Grundrissplan der Wohnung wird den NutzerInnen am Smartphone angezeigt und sie können in diesem Plan festlegen, welche Räume wann, wie häufig oder aber auch gar nicht gereinigt werden sollen. So weit, so praktisch.

Die Datenverarbeitung im Hintergrund dieser komfortablen Art der Wohnungsreinigung funktioniert in der Regel so, dass der Staubsaug-Roboter die durch seine Sensoren erfassten Daten über die zurückgelegten Wege, angetroffene Hindernisse, den Grad der Verschmutzung der Böden und ähnliche Parameter seiner Umgebung an ein Rechenzentrum des Herstellers übermittelt. In diesem Rechenzentrum werden diese Daten gespeichert und ausgewertet und die Auswertungsergebnisse – wie etwa der digitale Grundrissplan der eigenen Wohnung – den NutzerInnen über die Smartphone-App am Handy angezeigt. Haben NutzerInnen in der Regel den Eindruck, dass sie direkt über das Handy den Roboter steuern, erfolgt tatsächlich meist zuerst ein Datenaustausch mit dem Rechenzentrum des Herstellers und erst über diesen Umweg die Steuerung des Roboters.

Auf diese Art ist der Hersteller des Roboters stets über jedes Detail der Bodenreinigung in der Wohnung der NutzerInnen informiert und verfügt über Informationen zur geographischen Lage der Wohnung (diese kann über die IP-Adresse zumindest annäherungsweise festgestellt werden) über die Größe der Wohnung (und damit ansatzweise auch über die Vermögenssituation der NutzerInnen) über die Reinlichkeitsbedürfnisse der NutzerInnen, über Gegenstände, welche die Fahrt des Roboters behindern und ähnliches mehr. Je nach eingesetzter Steuerungstechnologie (Navigation mittels Laser-

Technologie oder mittels Kamerasystem und Bilderkennung) werden durch derartige Roboter auch Bilder der Wohnung erfasst. Ob diese auch an den Hersteller des Roboters übermittelt und von diesem weiterverarbeitet werden, ist in der Regel unklar.

Im Rahmen einer Studie zu vernetzten Automobilen des Instituts für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften wird diese Problematik verallgemeinernd folgendermaßen auf den Punkt gebracht: „*Was allen Digitalisierungsprozessen jedoch gemein ist, ist die Generierung von Daten über Menschen und Maschinen, bei allem, was sie tun. Diese Daten werden immer öfter gesammelt, gespeichert und für unterschiedliche Zwecke weiterverwendet. Diese Daten verraten viel über die Menschen, von denen sie kommen, meist ohne dass diesen klar ist, was alles über sie gewusst werden kann. Dadurch führen Digitalisierungsprozesse sehr häufig zu Privatsphäreproblemen.*“ (Krieger-Lamina 2016, S. 14)

Aus dem Blickwinkel des Konsumentenschutzes und des Schutzes der Grundrechte auf Datenschutz und Schutz der Privatsphäre sind dabei gleich mehrere Aspekte problematisch.

- **Mangelnde Information der KonsumentInnen:** Zum Zeitpunkt des Kaufs derartiger Geräte werden KonsumentInnen häufig keinerlei Informationen über die für den Betrieb des Geräts erforderliche Datenverarbeitung gegeben. Vielmehr ist es vielfach so, dass erst nach dem Kauf und im Rahmen der Inbetriebnahme bekannt wird, dass bestimmte – oder sogar alle – Funktionen des jeweiligen Geräts nur genutzt werden können, wenn die NutzerInnen zusätzlich ein Benutzerkonto beim Datenverarbeitungssystem des Herstellers anlegen mit dem dann die Smartphone-App sowie der Roboter verbunden werden. NutzerInnen, die dies nicht wollen, finden sich in einer Situation wieder in der ihnen die Nutzung des erworbenen Geräts nicht oder nur eingeschränkt möglich ist. Sind NutzerInnen jedoch bereit ein solches Benutzerkonto anzulegen, ist – abhängig vom jeweiligen Anbieter – die bereitgestellte Information über die vorgesehene Datenverarbeitung häufig nicht ausreichend, um eine klare Vorstellung davon zu vermitteln worauf man sich bei der Inbetriebnahme und Vernetzung des jeweiligen Geräts im Hinblick auf den Schutz der persönlichen Daten einlässt.
- **Datenübermittlung in Drittstaaten:** Abhängig davon, in welchem Land der Hersteller des jeweiligen Geräts bzw. der Anwendung seinen Sitz hat, erfolgt die Verarbeitung der personenbezogenen Daten der NutzerInnen gegebenenfalls in Drittstaaten außerhalb des Europäischen Wirtschaftsraums, die über kein angemessenes Datenschutzniveau verfügen. Mangels ausreichender Informationen über die Datenverarbeitung ist dies den NutzerInnen häufig nicht bekannt und verlassen sich diese – da sie das jeweilige Gerät ja innerhalb des Europäischen Wirtschaftsraums erworben haben – auf eine zuverlässige Durchsetzung des

europäischen Datenschutzrechts. Tatsächlich ist die DSGVO aufgrund des Marktortprinzips auch auf Anbieter in Drittstaaten anwendbar. Jedoch wird in der Praxis mangels Information über die stattfindende Datenverarbeitung auch die Durchsetzung des Datenschutzrechts häufig nicht stattfinden.

- **Unklare / mangelnde Rechtsgrundlage:** Die von den Herstellern in Anspruch genommene Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist mangels ausreichender Informationsbereitstellung häufig unklar. Mitunter wird im Rahmen der Registrierung eines Benutzerkontos eine Einwilligung zur Datenverarbeitung eingeholt. Diese dürfte jedoch mangels ausreichender Informationen über Zwecke, Datenarten, Übermittlungsempfänger, Speicherdauern und andere Aspekte der Datenverarbeitung häufig den Anforderungen der DSGVO nicht genügen. Hinsichtlich der Zweckbindung (vordergründig beispielsweise: Datenverarbeitung zur Durchführung der Wohnungsreinigung durch den Roboter) ist bemerkenswert, dass die Geschäftsmodelle der Hersteller meist nur die Entrichtung eines einmaligen Kaufpreises vorsehen. Dem gegenüber steht die Notwendigkeit für die Hersteller dauerhaft Datenverarbeitungskapazität zur Verfügung zu stellen, um den vollständigen Funktionsumfang des Gerätes auf Dauer aufrecht zu erhalten. Vor diesem Hintergrund liegt die Vermutung nahe, dass diese mitunter über viele Jahre hinweg zu erbringenden Leistungen zur Steuerung des Geräts nicht über den ursprünglichen Kaufpreis sondern auf andere Weise finanziert werden. Dies wäre beispielsweise durch Vermarktung der laufend durch die jeweiligen Geräte erhobenen personenbezogenen Daten möglich. Es wäre daher durchaus naheliegend, dass mit der Datenverarbeitung neben dem eigentlichen Verarbeitungszweck häufig auch noch andere Zwecke verfolgt werden.
- **Erschwernis der Ausübung der Betroffenenrechte:** Da KonsumentInnen häufig keine Kenntnis von der im Hintergrund stattfindenden Datenverarbeitung haben (und dies entsprechend den Gestaltungsprinzipien des Ubiquitous Computing auch nicht haben sollen) sind ihre Möglichkeiten zur Wahrnehmung ihrer durch die DSGVO verbrieften Betroffenenrechte (Recht auf Auskunft, Richtigstellung, Löschung, etc.) deutlich eingeschränkt. In der Wahrnehmung der KonsumentInnen kann im Beispiel des Staubsaug-Roboters leicht der Eindruck entstehen, dass das Smartphone ohne Zutun Dritter direkt mit dem Roboter kommuniziert. Entsprechend werden KonsumentInnen häufig keine Veranlassung sehen, sich mit Datenschutzfragen an den Hersteller des Geräts zu wenden.
- **Unklare Funktionsdauer:** Aufgrund der hohen Abhängigkeit von Internet-der-Dinge-Anwendungen und -Geräten von einer aufrechten Datenverbindung zum Rechenzentrum des jeweiligen Herstellers ergibt sich für KonsumentInnen auch die Situation, dass die tatsächliche Lebensdauer des erworbenen Produkts (z.B. des Staubsaug-Roboters) wesentlich von der

weiteren Existenz des Herstellers und dessen Aufrechterhaltung der Datenverarbeitung abhängig ist. Stellt dieser die Geschäftstätigkeit ein oder beendet aus anderen Gründen die Datenverarbeitung, werden mit einem Schlag sämtliche Geräte funktionsunfähig, deren zugrundeliegende Datenverarbeitung bisher im Rechenzentrum des Herstellers erfolgte. Auch wenn die Geräte selbst noch technisch einwandfrei sind, werden sie unverzüglich gebrauchsunfähig und können auch nicht mehr repariert werden, da die Datenverarbeitung des Rechenzentrums nicht angemessen ersetzt werden kann. Es ist zumindest zu bezweifeln, ob dieser Sachverhalt den KonsumentInnen bekannt ist, wenn sie so wie bisher einen herkömmlichen Staubsauger im Elektrofachmarkt oder Online-Shop einen „intelligenten" Staubsaug-Roboter erwerben.

Eine bemerkenswerte Kategorie von Anwendungen des Internet der Dinge sind sogenannte Assistenzsysteme wie beispielsweise „Amazon Alexa", „OK Google" oder „Apple Siri". Diese Anwendungen nehmen prinzipbedingt eine permanente akustische Raumüberwachung und Inhaltsanalyse des Gesagten vor, um festzustellen ob sie mit „Alexa", „OK Google" oder „Siri" angesprochen werden. Ob diese Analyse lokal am jeweiligen Gerät oder auf den Servern der Hersteller erfolgt ist für KonsumentInnen in der Praxis weitgehend unklar.

Bei Smartphones kommt es vor, dass diese Systeme bereits werkseitig aktiviert sind und Benutzern deren Existenz, Funktionsweise und Datenschutz-Implikationen nicht bekannt sind. Potentiell ist den Herstellern bzw. Betreibern dieser Dienste somit jegliche Unterhaltung, die in der Nähe derartiger Geräte geführt wird, inhaltlich zugänglich. Eine vertrauliche Unterhaltung ist ohne genaue Kenntnis der Konfiguration der anwesenden Geräte somit nicht mehr möglich, da jederzeit mit einer Übertragung des Gesagten zu Servern der Betreiber gerechnet werden muss. Dies unabhängig davon, ob man selbst derartige Dienste nutzt oder nicht.

Dieses Beispiel zeigt bereits sehr gut, dass die Datenverarbeitung des Internet der Dinge sich immer weiter aus dem Wahrnehmungsbereich der Betroffenen zurückzieht. Dem sollte einerseits mit einer aktiven Durchsetzung der zeitgerechten Erfüllung der Informationspflichten gem. Art. 13f DSGVO begegnet werden. Dabei ist insbesondere auf die leichte Verständlichkeit der zur Verfügung gestellten Informationen zu achten.

Andererseits kommt den Grundsätzen des Datenschutzes durch Technikgestaltung (Privacy by Design) sowie der datenschutzfreundlichen Voreinstellungen (Privacy by Default) im Internet der Dinge eine entscheidende Rolle zu. Auch diese in Art. 25 DSGVO verankerten Konzepte bedürfen einer konsequenten Rechtsdurchsetzung.

Im Beispiel der Staubsaug-Roboter könnte Datenschutz durch Technikgestaltung bedeuten, dass die Datenverarbeitung direkt durch den Roboter in den jeweiligen Wohnungen der KonsumentInnen erfolgt und diese den Roboter über ihr Smartphone steuern können, das beispielsweise mittels Bluetooth direkt mit dem Roboter verbunden wird. Lediglich für eine Steuerung des Roboters von Unterwegs wäre dann eine Kommunikation über das Internet erforderlich, die unter Beachtung des Grundsatzes der Datenminimierung weiterhin über ein System des Herstellers erfolgen könnte, das nach Durchführung der jeweiligen Interaktion mit dem Roboter die erhobenen personenbezogenen Daten unverzüglich löscht.

Datenschutzfreundliche Voreinstellungen könnten im Falle digitaler Assistenzsysteme bedeuten, dass derartige Systeme so an die KonsumentInnen ausgeliefert werden, dass von Haus aus keine Analyse des im Umfeld des Geräts Gesagten erfolgt, sondern diese Funktionalität durch die KonsumentInnen ausdrücklich auf Wunsch aktiviert werden muss. Datenschutz durch Technikgestaltung könnte darüber hinaus dafür sorgen, dass aktivierte Assistenzsysteme durch optische oder akustische Signale alle Anwesenden darauf aufmerksam machen, dass eine vertrauliche Unterhaltung aktuell nicht möglich ist. Bei Mikrofonen an Rednerpulten beispielsweise ist ein derartiger optischer Hinweis durch ein meist rotes Licht bereits seit langem Standard, obwohl diese Mikrofone in der Regel an weit weniger privaten Orten zum Einsatz kommen als digitale Assistenzsysteme, die auch für den Einsatz in Kinder- und Schlafzimmern beworben werden.

Nochmals schwieriger wird die Situation für KonsumentInnen bei Anwendungen des Internet der Dinge, die sich bereits vollständig ihrer Wahrnehmung entziehen. Dies ist etwa der Fall, wenn Daten über das Verhalten oder Interessen der KonsumentInnen ohne unmittelbares Zutun der betroffenen Personen mittels Sensoren und anderen Systemen erfasst und ausgewertet werden.

Ein in der Praxis durchaus häufig auftretendes Beispiel dafür ist die Auswertung des Mobilitätsverhaltens oder die Interessensanalyse in Einkaufszentren und Supermärkten mittels Bluetooth- bzw. WLAN-Tracking. Im Rahmen derartiger Anwendungen wird die eindeutige Kennung des Mobiltelefons (Bluetooth-ID oder MAC-Adresse) von eigens dafür in Verkehrsmitteln oder an geeigneten Orten in Einkaufszentren und Supermärkten angebrachten Empfängern erfasst und in weiterer Folge analysiert, an welcher Station des Verkehrsmittels die jeweilige Person eingestiegen und an welcher Station sie wieder ausgestiegen ist.

In Einkaufszentren und Supermärkten lässt sich auf diese Art der Weg von KonsumentInnen durch das Einkaufszentrum bzw. durch einzelne Geschäfte verfolgen. Da die Position der Geschäfte bzw. der jeweiligen Waren oder Warengruppen dem Betreiber ebenfalls bekannt ist, kann aufgrund der

Verweildauern der KonsumentInnen an bestimmten Orten auf ihr Interesse an bestimmten Waren geschlossen werden. Mit dieserart erfassten Daten soll einerseits die verkaufsfördernde Platzierung von Waren und Webebotschaften optimiert werden. Andererseits ist aber auch eine Kopplung der gewonnenen Interessensprofile mit den an der Kassa erhobenen personenbezogenen Daten der KonsumentInnen grundsätzlich vorstellbar, die über Kunden-, Bankomat- oder Kreditkarten gegebenenfalls sogar eindeutig identifiziert werden könnten.

Manche derartige Verhaltensanalysen bemühen sich aber durchaus darum, lediglich anonymisierte Daten zu erfassen. Dies ist angesichts der grundsätzlichen Problematik, dass die Anzahl der Messungen, Analysen und Auswertungen des Verhaltens nicht nur im Internet weit verbreitet ist, sondern nunmehr auch zunehmend in das physische Lebensumfeld der KonsumentInnen vordringt, nur ein geringer Trost.

Derartige Datenverarbeitungen sind für KonsumentInnen in der Praxis nicht feststellbar. Es besteht daher auch keinerlei Möglichkeit für KonsumentInnen ihre Rechte gegenüber den Verantwortlichen der Datenverarbeitung wahrzunehmen. Der wirksamste Schutz vor unerwünschter Verhaltensanalyse besteht für KonsumentInnen derzeit darin, an öffentlichen Orten am Smartphone und anderen persönlichen Geräten Bluetooth und WLAN gänzlich zu deaktivieren. Lediglich der vollständige Rückzug aus der vernetzten Welt bietet also noch die Möglichkeit, öffentlich zugängliche Orte ohne Auswertung des eigenen Verhaltens zu nutzen.

Neben der Stärkung des Konsumentenschutzes in Bezug auf Produkte, die den zugesagten Funktionsumfang nur bereitstellen, wenn eine zusätzliche und meist versteckte Datenverarbeitung ermöglicht wird, wäre eine konsequente Durchsetzung der einschlägigen Datenschutzbestimmungen für einen besseren Schutz der KonsumentInnen dringend erforderlich.

Insbesondere der Erfüllung der Informationspflichten sowie die Umsetzung der Anforderungen des Datenschutzes durch Technikgestaltung sowie der datenschutzfreundlichen Voreinstellungen kommt in diesem Zusammenhang eine wesentliche Rolle zu. Darüber hinaus sollten bei Internet-der-Dinge-Anwendungen und –Geräten unabhängige technische Produkttests durchgeführt werden, die neben Sicherheits- und Funktionstests unbedingt auch Überprüfungen auf Datenschutzkonformität beinhalten sollten.

Fragen des technischen Datenschutzes können im Bereich des Internets der Dinge nicht den einzelnen KonsumentInnen überlassen werden. Diese verfügen meist nicht über die Möglichkeiten, Mittel und Kenntnisse um die zugrundeliegenden Sachverhalte zu überblicken und korrekt einzuschätzen.

Die Sicherstellung einer vertrauenswürdigen IT-Infrastruktur wird mit zunehmender Digitalisierung zu einer immer bedeutenderen staatlichen Aufgabe, die aufgrund der Komplexität der Fragestellungen durch einzelnen KonsumentInnen nicht mehr in ausreichendem Maße wahrgenommen werden kann. Eine entsprechende Stärkung der zuständigen Behörden durch Bereitstellung ausreichender personeller und finanzieller Mittel ist daher dringend geboten. Soweit entsprechende behördliche Zuständigkeiten derzeit noch nicht bestehen, sollten diese umgehend geschaffen werden.

Smart Cars

Unter dem Begriff „Smart Car“ oder „Intelligentes Fahrzeug“ werden Kraftfahrzeuge verstanden, die im Rahmen der Digitalisierung mit zahlreichen zusätzlichen Funktionalitäten zum besseren Betrieb, besseren Steuerung und komfortableren Nutzung ausgestattet wurden. Der Funktionsumfang reicht dabei von einzelnen Assistenzsystemen bis hin zu vollständig autonomen Fahrzeugen.

Entsprechend vielfältig gestaltet sich der Umfang der möglichen Funktionalitäten von Smart Cars von einzelnen Assistenzsystemen, die lediglich auf Basis einer im Fahrzeug selbst stattfindenden Datenverarbeitung bestimmte Funktionalitäten bereitstellen, bis hin zu vollständig autonomen Fahrzeugen, die in großem Umfang mit anderen Fahrzeugen, der Verkehrsinfrastruktur, Systemen des Herstellers und von Drittanbietern (z.B. Hersteller von Navigationsgeräten) Daten austauschen und gegebenenfalls auch aus der Entfernung gesteuert werden können.

Vernetzte Fahrzeuge können als Geräte des Internet der Dinge verstanden werden. Für sie gilt das oben bereits Ausgeführte sinngemäß.

Der genaue Umfang der Datensammlung moderner Fahrzeuge ist aktuell nicht bekannt. Im Rahmen eigener Untersuchungen hat der ADAC die Datensammlung moderner Autos im Februar 2019 anhand mehrerer Beispielfahrzeuge erhoben und Ergebnissen einer ähnlichen Untersuchung aus dem Jahr 2015 gegenübergestellt.

Die Ergebnisse der Untersuchung fasst der ADAC unter anderem folgendermaßen zusammen:

„*Bei der **Mercedes B-Klasse** wurden folgende auffällige Daten gefunden:*

- *etwa alle zwei Minuten werden die GPS-Position des Fahrzeugs sowie Statusdaten an das Mercedes-Backend übertragen (z.B. Kilometerstand, Verbrauch, Tankfüllung, Reifendruck und Füllstände von Kühlmittel, Wischwasser oder Bremsflüssigkeit)*

- *Zahl der elektromotorischen Gurtstraffungen wird gespeichert, etwa aufgrund starken Bremsens (erlaubt Rückschlüsse auf den Fahrstil)*
- *Fehlerspeicher-Einträge werden teilweise mit Informationen über zu hohe Motodrehzahl oder -temperatur abgelegt (erlaubt Rückschlüsse auf den Fahrstil)*
- *gefahrene Kilometer auf Autobahnen, Landstraßen und in der Stadt ("highway-conditions", "road-conditions" und "urban-conditions") werden getrennt gespeichert (erlaubt Rückschlüsse auf das Nutzungsprofil)*
- *Betriebsstunden der Fahrzeugbeleuchtung werden gespeichert*
- *die letzten 100 Lade- und Entladezyklen der Starterbatterie werden mit Uhrzeit und Datum sowie Kilometerstand gespeichert, woraus sich Fahr- und Standzeiten ergeben*

*Beim **Renault Zoe** wurden folgende auffällige Daten gefunden:*

- *das Aufladen der Antriebsbatterie kann von Renault via Mobilfunkverbindung jederzeit unterbunden werden (etwa aufgrund nicht bezahlter Leasing-Rechnung für die Antriebs-Batterie)*
- *Renault kann via RemDiag beliebige Informationen vom CAN-Datenbus des Fahrzeugs via Mobilfunkverbindung mitlesen. Diese Ferndiagnose ist standardmäßig ausgeschaltet, kann aber vom Hersteller jederzeit aktiviert werden*
- *bei jeder Fahrt, spätestens jedoch alle 30 Minuten, wird ein Datenpaket an Renault gesendet, das mindestens enthält: VIN, div. Seriennummern, Datum, Uhrzeit, GPS-Position, Temperatur, Ladung und Zellspannung der Hochvolt-Antriebsbatterie; diese Informationen können von Renault auch jederzeit angefordert werden*
- *neben den fest einprogrammierten Funktionen der Kommunikation zwischen dem Renault-Server und dem Renault Zoe können diese Funktionen via Mobilfunkverbindung beliebig erweitert werden*“ (ADAC 2019)

Diese Beispiele vermitteln bereits eine deutliche Vorstellung über den Umfang der Datenverarbeitung durch moderne Fahrzeuge und geben einen ersten Einblick in die Aussagekraft der Informationen, die offenbar laufend erfasst und an die Hersteller der Fahrzeuge übermittelt werden.

KonsumentInnen stehen diesem Phänomen weitestgehend hilflos gegenüber. Selbst wenn im Rahmen des Neuwagenkaufs Informationen zur Datenverarbeitung des Fahrzeugs und zu den Datenübermittlungen an die Hersteller gegeben werden, so ist die Fahrzeugnutzung in der Praxis wesentlich davon geprägt, dass Fahrzeuge nicht nur von ihren Haltern sondern auch von

Familienmitgliedern und anderen Personen genutzt werden, die über die Umstände der Datenverarbeitung nicht informiert sind.

Ebenso kann eine entsprechende Information bestenfalls für den Neuwagenkauf von autorisierten Händlern gewährleistet werden. Beim Verkauf von Gebrauchtfahrzeugen zwischen Privaten werden Informationen über die Datenverarbeitung des Fahrzeugs mit großer Wahrscheinlichkeit nicht Gegenstand der Aufklärung des Käufers sein.

Ist ein Käufer mit der Datenverarbeitung nicht einverstanden stellt sich die Frage nach den Alternativen. Mit fortschreitender Digitalisierung und dem Wettlauf der Hersteller zum autonomen Fahren werden Fahrzeuge ohne umfangreicher Datenverarbeitung zur Mangelware und KonsumentInnen finden sich vor der Entscheidung wieder, ob sie ihrem Mobilitätsbedürfnis oder ihrem Bedürfnis nach Privatsphäre und Datenschutz einen höheren Stellenwert beimessen.

Krieger-Lamina fasst die Entwicklung folgendermaßen zusammen: „*Immer mehr wird auch das Automobil zu einer Daten sammelnden, verarbeitenden, speichernden und weitergebenden Maschine, deren Funktionsweise sich LaiInnen nicht mehr erschließt. Zur Verarbeitung dieser Datenströme kommen Algorithmen zum Einsatz, die durch die Aufbereitung der Daten schon Entscheidungen treffen, in Zukunft aber noch viel mehr Entscheidungen übernehmen werden, wenn Software autonome Fahrzeuge steuern soll.*“ (Krieger-Lamina 2016, S. 11)

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation klassifiziert die vielfältigen geplanten Anwendungen für vernetzte Fahrzeuge in folgende Bereiche (IAGDST 2018, S. 1f):

- Mobilitätsmanagement: Funktionen, die es den Fahrern ermöglichen, einen Zielort schnell und kosteneffizient zu erreichen.
- Fahrzeugmanagement: Funktionen, die den Fahrern helfen, die Betriebskosten zu senken und die Nutzung zu erleichtern.
- Straßenverkehrssicherheit: Funktionen, welche die Fahrer vor externen Gefahren warnen und interne Reaktionen des Fahrzeugs auf diese Gefahren ankündigen.
- Unterhaltung: Funktionen für die Information und die Unterhaltung von Fahrer und Mitreisenden.
- 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.
- 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.

Dabei umfasst die mögliche Datenverarbeitung nicht nur Daten des jeweiligen Fahrers, allfälliger Mitreisender sowie Daten von deren allfälligen Geräten (z.B. Smartphones), die sie mit dem Fahrzeug verbinden, sondern auch Daten der Umgebung des Fahrzeuges inklusive anderer Fahrzeuge samt KFZ-Kennzeichen und Passanten, die von den Sensoren und Kameras (z.B. bei Rückfahrassistenten) der Fahrzeuge gegebenenfalls erfasst werden können.

Krieger-Lamina bringt die Situation der KonsumentInnen prägnant auf den Punkt: „*KonsumentInnen sind chancenlos bei dem Versuch Herr/Frau ihrer Daten zu bleiben. Viel zu unklar ist, wann welche Daten erhoben werden, wie sie verarbeitet werden, ob sie gespeichert werden, an wen und zu welchem Zweck sie übertragen werden, und was dann mit ihnen passiert. Manche Hersteller lassen sich die Datennutzung durch Zusätze zum Kaufvertrag genehmigen. Das führt unweigerlich zu der Frage, inwieweit KonsumentInnen in der Lage sind, eine informierte Zustimmung zu der Datenverarbeitung zu erteilen. Bei der Vielzahl an gesammelten Daten ist es nicht wahrscheinlich, dass für sie bis zur letzten Konsequenz erkennbar ist, was das bedeutet.*“ (Krieger-Lamina 2016, S. 47)

Mit fortschreitender Automatisierung des Fahrzeugverkehrs steigt jedoch auch das Risiko für die Sicherheit der Verkehrsteilnehmer. Die Situationen, mit denen automatisierte oder autonome Fahrzeuge zurechtkommen müssen können nicht vollständig und abschließend erfasst, analysiert und durchdacht werden. Es wird vielmehr zwangsläufig eine hohe Anzahl an Verkehrssituationen geben, in denen derartige Fahrzeuge selbständig entscheiden müssen, welche Reaktion der Situation angemessen ist.

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation hält in ihrem Arbeitspapier zu vernetzten Fahrzeugen entsprechend fest, dass im Gegensatz zu den meisten Geräten des Internets der Dinge vernetzte Fahrzeuge „*kritische Systeme [sind], bei denen ein Sicherheitsvorfall das Leben der Nutzer und anderer Personen gefährden kann.*“ (IAGDST 2018, S. 10)

Krieger-Lamina wiederum verweist darauf, „*dass Zulassungsverfahren wohl nur in Form von Stichproben überprüfen werden können, ob die Programmierung ausreichend gut ist, um keine Gefahr im Betrieb darzustellen. Möglicherweise werden sich auch neue Aufsichtsbehörden etablieren, ähnlich wie es bei anderen Technologien zum Zeitpunkt der Einführung geschehen ist (bspw. Flugaufsicht), die die Funktionsweise der installierten Software laufend und nicht nur punktuell überprüfen.*“ (Krieger-Lamina 2016, S. 53)

In seinen Empfehlungen zum Themenbereich Sicherheit ergänzt Krieger-Lamina weiters, dass es *„[b]ei der Zulassungsüberprüfung […] unumgänglich notwendig [sei], auch die Sicherheit der an Bord befindlichen IT-Systeme zu kontrollieren – sowohl im Hinblick auf Informationssicherheit, als auch*

betreffend ihrer Fähigkeit in unterschiedlichen Verkehrssituationen Sicherheit für alle VerkehrsteilnehmerInnen zu gewährleisten.“ (Krieger-Lamina 2016, S. 75)

Dem ist aus dem Blickwinkel des Datenschutzes hinzuzufügen, dass eine derartige Zulassungsüberprüfung wesentlich auch eine Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben umfassen sollte. Dies einerseits da die Datenverarbeitungen moderner Fahrzeuge für KonsumentInnen nicht mehr ausreichend nachvollziehbar sind um eine informierte Entscheidung zu treffen. Andererseits, weil Zulassungsverfahren für Fahrzeuge bereits flächendeckend etabliert sind und somit – im Vergleich zu anderen Anwendungen des Internet der Dinge – einfach um Fragestellungen des Datenschutzes erweitert werden können. Drittens wird es für KonsumentInnen wohl nur schwer zu verstehen sein, weshalb im Rahmen behördlicher Zulassungsverfahren für vernetzte Fahrzeuge wesentliche Fragen des verfassungsmäßig garantierten Grundrechtsschutzes (Datenschutz und Schutz der Privatsphäre) unbeachtet bleiben und Fahrzeuge, die wesentliche Anforderungen des Datenschutzrechts nicht erfüllen eine behördliche Betriebsbewilligung erhalten.

Die Notwendigkeit und Bedeutung einer umfangreichen Prüfung von Software im Rahmen von Zulassungsverfahren ist im Hinblick auf die Sicherheit aktuell eindrucksvoll am Beispiel der Flugsicherheitsvorfälle im Zusammenhang mit Flugzeugen des Herstellers Boeing nachvollziehbar, bei denen die Abstürze zweier Maschinen offenbar auf Softwarefehler einer Steuerungssoftware zurückzuführen waren.

Zu den Datenschutzaspekten vernetzter Fahrzeuge wurden bereits – nicht zuletzt durch die europäischen Datenschutzbehörden – zahlreiche Arbeitspapiere und Studien publiziert, auf deren Ergebnisse im Rahmen dieser Stellungnahme nicht im Detail eingegangen werden kann. Auf einige dieser Publikationen sei hier daher – zusätzlich zu den bereits zitierten Quellen – verwiesen:

- Gerhart R. Baum, Julius F. Reiter, Olaf Methner, Rechtsgutachten zur Kontrolle der Daten bei vernetzten und automatisierten Pkw (Baum et al 2016)
- 39th International Conference of Data Protection and Privacy Commissioners: Hong Kong, 25-29 September 2017, Resolution on Data Protection in Automated and Connected Vehicles (ICDPPC 2017)
- Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren (BfDI 2017)
- Commission Nationale Informatique & Libertés (franz. Datenschutzbehörde): Compliance Package: Connected Vehicles And Personal Data (CNIL 2017)

- European Agency for Network and Information Security: Cyber Security and Resilience of smart cars (ENISA 2017)
- Article 29 Data Protection Working Party: Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (A29DPWP 2017)

Aus Sicht des Datenschutzes ist im Hinblick auf die im Zusammenhang mit vernetzen Fahrzeugen diskutierte „Eigentümerschaft" an Daten darüber hinaus klar festzuhalten, dass die von einer Datenverarbeitung betroffenen Personen das Recht auf Datenschutz bei der Verarbeitung der sie betreffenden Daten innerhalb der im geltenden Recht vorgesehenen Grenzen haben. Dieses Recht ist unveräußerlich und nicht übertragbar.

Entsprechend ist im Rahmen des geltenden Datenschutzrechts eine Verarbeitung personenbezogener Daten jeweils nur vorübergehend für die unbedingt erforderliche Dauer auf Basis einer spezifisch auf den festgelegten Zweck der Verarbeitung zutreffenden Rechtsgrundlage zulässig. Als personenbezogenes Datum ist dabei – wie bereits weiter oben ausgeführt – jede Information zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht. Auch wenn dieser Personenbezug lediglich in Form einer Identifikationsnummer oder eines anderen Kennzeichens vorliegt.

Die Verarbeitung personenbezogener Daten hat sich daher im Rahmen der verfassungsrechtlich garantierten Grundrechte auf Datenschutz und Schutz der Privatsphäre sowohl zeitlich als auch inhaltlich auf das unbedingt erforderliche Minimum zu beschränken und ist nach Erreichen des Verarbeitungszweckes unverzüglich einzustellen.

Hingewiesen sei im Zusammenhang der vernetzten Fahrzeuge auch auf die Stellungnahme des Datenschutzrates vom 06.03.2017 zu einer Änderung des Bundesstraßen-Mautgesetzes. In dieser Stellungnahme führt der Datenschutzrat folgendes aus: *„Aus Rechtsprechung und Literatur zu Art. 8 EMRK ist erschließbar, dass es einen Anspruch des Menschen auf Bewegung im öffentlichen Raum ohne systematische Beobachtung gibt (vgl. etwa EGMR 4.5.2000, 28341/95, Rotaru, Rn. 43 f). Konkreter kann insofern von einem „Recht auf anonyme Nutzung von Verkehrsinfrastruktur" oder von einem Recht auf eine „spurenfreie Mobilität" gesprochen [werden] (vgl. idS etwa die deutsche Datenschutzkonferenz, Entschließung vom 9./10.3.1995 [„Straßenbenutzungsgebühren"]). Auch einschlägige EU Rechtsgrundlagen zum „Intelligenten Straßenverkehr" betonen das Prinzip der anonymen Nutzung (vgl. idS etwa ErwGr. 13 und Art. 10 Abs. 3 der Richtlinie 2010/40/EU).*" (DSR 2017, S. 3, Hervorhebungen durch den Autor entfernt)

Auch vor diesem Hintergrund wird deutlich, dass eine datenschutzkonforme Gestaltung künftiger Verkehrssysteme und „intelligenter“ Fahrzeuge von wesentlicher Bedeutung für eine verfassungs- und grundrechtskonforme Ausgestaltung der künftigen Verkehrsinfrastruktur ist, deren wesentliches Kennzeichen die umfassende Vernetzung von und der permanente Datenaustausch zwischen Straßeninfrastruktur, Fahrzeugen und Verkehrssteuerung sein wird.

Mit freundlichen Grüßen,

Mag. Andreas Krisch

Literatur

ADAC 2019: Diese Daten sammelt ein modernes Auto, 15.02.2019 https://www.adac.de/rund-ums-fahrzeug/assistenzsysteme-daten/daten-modernes-auto/, zuletzt abgerufen am 27.04.2019

A29DPWP 2017: Article 29 Data Protection Working Party: Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), 04.10.2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888, zuletzt abgerufen am 27.04.2019

Baum et al 2016: Gerhart R. Baum, Julius F. Reiter, Olaf Methner, Rechtsgutachten zur Kontrolle der Daten bei vernetzten und automatisierten Pkw, 02.12.2016 https://www.vzbv.de/sites/default/files/rechtsgutachten_automatisiertes_fahren_langfassung.pdf, zuletzt abgerufen am 27.04.2019

BfDI 2017: Die Bundesbeauftragte für Datenschutz und Informationsfreiheit, Bundesrepublik Deutschland: Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren, 1. Juni 2017 https://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/DatenschutzrechtlicheEmpfehlungenV

ernetztesAuto.pdf;jsessionid=A2312ED28590877521121AA7C88C6F50.1_cid344?__blob=publicationFile&v=1, zuletzt abgerufen am 27.04.2019

CNIL 2017: Commission Nationale Informatique & Libertés (franz. Datenschutzbehörde): Compliance Package: Connected Vehicles And Personal Data, Oktober 2017 https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

DSR 2017: Datenschutzrat, Bundesgesetz, mit dem das Bundesstraßen-Mautgesetz 2002 geändert wird - Stellungnahme des Datenschutzrates; in seiner 233. Sitzung am 6. März 2017 einstimmig beschlossen https://www.justiz.gv.at/web2013/file/2c94848b60c168850160e9428e565dfa.de.0/65601.pdf, zuletzt abgerufen am 27.04.2019

ENISA 2017: European Agency for Network and Information Security: Cyber Security and Resilience of smart cars, 13. Jänner 2017 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars, zuletzt abgerufen am 27.04.2019

IAGDST 2018: Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation, Vernetzte Fahrzeuge, 63. Sitzung, 9.-10. April 2018, Budapest, Ungarn https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Connected_Vehicles-de.pdf, zuletzt abgerufen am 27.04.2019

ICDPPC 2017: 39th International Conference of Data Protection and Privacy Commissioners: Hong Kong, 25-29 September 2017, Resolution on Data Protection in Automated and Connected Vehicles https://www.bfdi.bund.de/SharedDocs/Publikationen/EN/InternationalDS/2017_39thIDSK_HongKong_ResolutionOnDataProtectionAutomatedAndConnectedVehicles.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 27.04.2019

Krieger-Lamina 2016: Jaro Krieger-Lamina, Vernetzte Automobile: Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen http://epub.oeaw.ac.at/ita/ita-projektberichte/2016-02.pdf, zuletzt abgerufen am 27.04.2019

Weiser 1991: Mark Weiser, The Computer for the 21st Century. Scientific American, Februar 1991