BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65
www.arbeiterkammer.at
DVR 1048384

Parlamentsdirektion
1017 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
GZ. 13655.060/1-L1.3/2019	BAK/KS-GSt/DZ/Ho	Mag Daniela Zimmer	DW 12722	DW 12693	26.04.2019

Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes (insbesondere Smart Cars)

Die Bundesarbeitskammer (BAK) bedankt sich für die Initiative des Konsumentenausschusses, einen Aspekt des digitalen Wandels mit erheblichem verbraucherpolitischen Handlungsbedarf aufzugreifen, und die Gelegenheit zur Stellungnahme.

Die vorliegenden Entschließungsanträge enthalten das an die Konsumentenministerin gerichtete Ersuchen, sie möge dem Nationalrat einen Bericht vorlegen,

- „der die Probleme des Internet der Dinge (internet of things – IoT) für KonsumentInnen darstellt und wie die Antwort in Form eines digitalen Konsumentenschutzes sein kann."

- „der darstellt, welche Maßnahmen aus Sicht des Konsumentenschutzes notwendig sind, um KonsumentInnen das Eigentum über ihre Daten im Bereich Smart-Cars zu gewährleisten und sicherzustellen, dass Unternehmer, wie Fahrzeughersteller und Zulieferbetreibe nicht ihre eigenen Interessen gegenüber den persönlichen des Verbrauchers dahingehend durchsetzen, dass es zu einer Aushebelung der freien Werkstattwahl kommt…"

Kurze Zusammenfassung

Die Initiative wird aus BAK-Sicht überaus begrüßt. Die BAK steht bei Bedarf auch gerne bei der Erarbeitung von Lösungsvorschlägen im Rahmen des in Aussicht genommenen Berichts mit Anregungen zur Verfügung.

Schon eine AK-Studie aus 2014 (Kommerzielle digitale Überwachung von KonsumentInnen im Alltag, Wolfie Christl - Cracked Labs Institut für kritische digitale Kultur) machte auf IoT und seine (un-)absehbaren Folgen für die Privatsphäre aufmerksam: E-Book-Reader und vernetzte TV-Geräte senden Daten zum Nutzerverhalten an Unternehmen, Fitnessarmbänder messen den Puls und liefern Gesundheitsdaten an Dritte, Fernsteuerungen im Smart Home heizen das Backrohr vor und Überwachungsboxen im Auto übertragen das Fahrverhalten an Versicherungen, die die Höhe der Prämienzahlung von den gemessenen Daten abhängig machen. Im Jahr 2020 soll es nach Schätzungen der EU-Kommission weltweit über 50 Milliarden IoT-Geräte geben.

Gegenstände, die ins Internet integriert sind, erlauben Firmen noch tiefere Einblicke in unser Leben – das Erstellen von Persönlichkeitsprofilen oder Prognosen über künftiges Verhalten inbegriffen. Die Entwicklung wirft zahlreiche (und trotz Datenschutz-Grundverordnung) ungeklärte Fragen in Bezug auf die Privatsphäre auf. Zwei offene Fragen, um die ein strategisches Tauziehen auf EU-Ebene längst begonnen hat, lauten: Wann weisen die Betriebsdaten vernetzter Geräte einen Personenbezug auf und wem gehören sie eigentlich?

Derzeit laufen KonsumentInnen Gefahr, dass ihr Selbstbestimmungsrecht über ihre Daten bzw ihr Eigentumsrecht an gekauften „smarten" Produkten nicht angemessen respektiert wird. Ohne starke Intervention der Verbraucherpolitik dürften viele der offenen Fragen zu Datenschutz, Datensicherheit aber auch fairer Vertragsgestaltung ohne Rücksicht auf Verbraucherpositionen im Sinne der Hersteller beantwortet werden. Auch falsche Ergebnisse und Schlussfolgerungen aus Datenauswertungen von Geräten, die auf dem Einsatz von Algorithmen und Künstlicher Intelligenz basieren, werden negative Auswirkungen auf KonsumentInnen haben. Ein adäquater Diskriminierungsschutz ist aber bis auf Weiteres nicht in Sicht.

Insgesamt zeichnet sich ein krasses informationelles und vertragliches Ungleichgewicht in den Rechtspositionen zwischen den an IoT beteiligten Anbietern und ihren Kunden ab. Die Anbieterseite,

- nützt vertragliche und technische Gestaltungsmöglichkeiten um personenbezogene Kundendaten und Betriebsdaten der Geräte zu analysieren und kommerziell zu verwerten,

- übernimmt wenig Verantwortung (Zusicherung von Qualitäten, Haftung bei Schäden, Gewährleistung bei Defekten) für IoT-immanente Risiken (Softwarefehler, Hackingangriffe, Databreaches, Insolvenzen mitbeteiligter Anbieter, schädigender Einsatz unausgereifter Algorithmen und Künstlicher Intelligenz) und investiert auch selten ausreichend in präventive Sicherheit,

- schwächt KonsumentInnen dadurch, dass mit einem Kauf verbundene Eigentumsrechte auf einzelne Komponenten bezogen immer öfter ausgehebelt und durch bloße urheberrechtliche Nutzungsrechte ersetzt werden.

Vor diesem Hintergrund wäre bei der Berichtserstellung zu prüfen, ob dem Verbraucherschutz in Bezug auf IoT-Risiken in folgenden Bereichen Rechnung getragen wird:

- Vertragsrecht
- Produkthaftung
- Schutz von Kundendaten und der Privatsphäre
- Transparente Information
- Schutz vor Diskriminierung
- Wettbewerbsrecht (wettbewerbshinderliches Verhalten durch unfaire Praktiken marktdominanter Anbieter, Koppelungsgeschäfte, aggressive Werbeformen)
- Rechtsdurchsetzung (Beweiserbringung, Schwierigkeiten grenzüberschreitender Rechtsdurchsetzung)
- Schutz von Jugendlichen vor Ausbeutung ihrer Unerfahrenheit
- Schutz geistigen Eigentums

Warum ist eine eingehende Befassung mit den Folgen des Internet der Dinge für Verbraucher nötig?

Die Rechenleistung von Computern steigt nach dem Moorschen-Gesetz exponentiell. Sensoren in Geräten stellen in rasch wachsendem Umfang Daten zur Verfügung. Die Algorithmus-Forschung macht Fortschritte (maschinelles Lernen mit selbstadaptiven Algorithmen, tiefgehendes Lernen über künstliche neuronale Netze). Die EU-Kommission befand 2018 zusammengefasst in ihren Mitteilungen zu IoT und zu Künstlicher Intelligenz (Artificial Intelligence, AI): Europa sei Weltklasse in der Robotik-Disziplin und habe starke Industrie- und Dienstleistungssektoren, die sich bestens für IoT und AI-Anwendungen eignen (Autos, Gesundheitsversorgung, landwirtschaftliche Produkte) sowie exzellente Forschung. Vor diesem Hintergrund gibt es auch einen starken wirtschaftspolitischen Rückhalt dafür, dass smarte Uhren, internetfähige Heizungen, Online-Gegensprechanlagen und intelligente Kühlschränke mit dem Internet verbunden sind und Einzug in die Privathaushalte halten. Erste Sicherheitspannen, Verletzungen der Privatsphäre und signifikante Machtungleichgewichte bei der Vertragsgestaltung illustrieren allerdings, dass die Vernetzung aller Alltagsdinge für Verbraucher mit Vorsicht zu genießen ist:

- **Datenschutzrisken:** 2017 wurden smarte Kinderpuppen auch im heimischen Handel vertrieben, die über ihre Spracherkennungsfunktion nicht nur nette algorithmen-gesteuerte Antworten auf Fragen von Kindern gaben, sondern auch deren sonstige Gespräche mitlauschen und auf US-Server übermitteln konnten („Die Spionage Puppe Cayla“, der Standard vom 9.9.2017).

- **Datensicherheitsrisken:** Mit dem Internet verbundene Auto-Bordsysteme verursachen Verbraucherprobleme, die ohne Schutzmaßnahmen in Zukunft gängiger werden dürften. Im Infotainmentsystem einiger Autotypen (zB UConnect von Fiat Chrysler) klafften laut Sicherheitsforschern kritische Schwachstellen, durch die Hacker das Fahrzeug komplett fernsteuern konnten („Hacker steuern Jeep Cherokee fern“ Heise.de vom 22.7.2015). Auch das Bordsystem von BMW (ConnectedDrive) fand seinen Weg in die Schlagzeilen, nachdem es Sicherheitsexperten im Auftrag des deutschen Verkehrsclubs ADAC gelang, bspw die Türverriegelung der Fahrzeuge unberechtigterweise von der Ferne aufzuschließen.

- **Vertragsrisiken:** Der US-Traktorenhersteller John Deere versucht mit großem Nachdruck, seinen Kunden das Eigentum an ihren Maschinen abzusprechen. Über Geschäftsklauseln und den Gerichtsweg sollen Nutzer davon abgehalten werden, ihre hochmodernen Traktoren zu reparieren, vor allem umzuprogrammieren. Eine selbstbestimmte Reparatur (Heimwerker, durch selbst gewählte Professionisten) wird bei stark software-basierten Produkten im Vergleich zu mechanischen Teilen schwierig. Das Austauschen eines kaputten Teils durch ein Nicht-Original-Teil oder die selbst vorgenommene Reparatur kann dazu führen, dass die Elektronik dies erkennt und das Starten des Motors verhindert. John Deere begründet den Schritt mit seinen Urheberrechten. Bei ihm darf nur eine offizielle Vertragswerkstätte beauftragt werden. Unabhängigen Werkstätten und Bauern wird weder Zugriff auf Original-Teile noch auf die Software gestattet. (https://www.idgconnect.com/ 5.6.2018; „Finger weg von deinem eigenen Traktor“, Heise.de vom 22.4.2015).

Der Kampf um Eigentums- bzw umfassende Nutzungsrechte bei vernetzten Geräten erstreckt sich aber längst nicht nur auf Landmaschinen für Profis. Auch Massenprodukte wie Smartphones sind betroffen. Der Konsument erwirbt zwar das physische Produkt, erhält aber für die Software nur eine eingeschränkte Nutzungslizenz. Wer bspw die Betriebssoftware seines Handys modifiziert (Jailbreak), um sein iPhone mit anderen Programmen kompatibel zu machen, umgeht technische Schutzmechanismen und verstößt gegen die Nutzungsvereinbarung. Anbieter verweigern diesfalls häufig den Support und lehnen Gewährleistungsansprüche generell ab.

Konsumenten stehen folglich in einer Welt mit immer mehr smarten Geräten nicht nur vor geläufigen, sondern auch vor neuartigen Problemen:

- **Überwachung “zum Quadrat“:** Verbraucher bewegen sich durch einen dicht vernetzten Alltag. Jeder Berührungspunkt mit smarten Geräten hinterlässt persönliche Datenspuren, die in umfassenden Nutzungs- und Standortprofilen münden können. Die mit dem Tracking von PC- und Handynutzern begonnene Entwicklung der Überwachung der Alltagshandlungen und Alltagsgeschäfte von Verbrauchern erlangt mit IoT eine neue Dimension. Die Schnittstellen mit dem Internet, an denen Verbraucherverhalten beobachtet, gespeichert, ausgewertet und Dritten übermittelt werden kann, verdichten sich und ergeben ein einzigartig genaues Bild über das, was wir tun, lassen, denken, mit wem wir in Kontakt stehen uvm.

- **Sicherheitsrisken ohne Ende:** Im Wettlauf um innovative Produkte, die man rascher als die Konkurrenz auf den Markt bringt, landen auch völlig unausgereifte vernetzte Geräte in Haushalten. Darüber hinaus gilt systembedingt, dass Software zwar gut getestet, aber so gut wie nie völlig fehlerfrei sein kann. Sicherheitsupdates tragen diesem Umstand Rechnung. Was den KonsumentInnen an Entwicklungsrisiken, fehlender Marktreife und mangelnden präventiven Sicherheitsmaßnahmen gegen Schadsoftware, Databreaches und Hackingangriffen zugemutet werden kann bzw was nicht, befindet sich bestenfalls im Diskussionsstadium. Auch die im März 2019 beschlossene EU-Richtlinie über den Warenhandel ändert diesbezüglich wenig.

Es besteht die Gefahr, dass KonsumentInnen als „Versuchskaninchen“ von aus technischer oder Datenschutz-Sicht unsicheren Produkten dienen. Oft wird nicht präventiv, sondern reaktiv in Produkt- und Datensicherheit investiert, wenn Pannen mit erheblichen Auswirkungen (und Medienecho) bereits passiert sind.

- **Nutzungslizenz statt Eigentum, Kaufvertrag versus Urheberrecht:** Mit der Entwicklung von IoT laufen KonsumentInnen Gefahr, auch über den Umfang ihrer Gebrauchsmöglichkeiten an einer Sache gehörig in die Irre geführt zu werden. Sie entrichten zwar einen „Kaufpreis“ und vermeinen damit Eigentümer am Produkt mit all seinen Komponenten geworden zu sein. Oft trifft das aber nur mehr auf das äußere Erscheinungsbild, also etwa das Gehäuse eines vernetzten Fernsehers oder die Karosserie eines Fahrzeuges, zu. Das Innenleben ist software-dominiert und steht unter Eigentumsvorbehalt der Anbieter. Der bestimmungsmäßige Gebrauch wird durch Lizenzen geregelt. Was Nutzer damit anfangen können oder nicht, regeln die Anbieter einseitig zu ihren Gunsten vertraglich und über technische Schranken (Digital Right Management Systeme). Daraus ergeben sich neue Abhängigkeiten:

- KonsumentInnen sind unter Umständen in der selbstbestimmten Nutzung stark eingeschränkt und können Geräte zB nicht selbst reparieren (lassen), verleihen, verkaufen, verändern.

- Die Onlineanbieter setzen zum Teil proprietäre (geschlossene) Hardware- und Softwaresysteme ein, um Nutzer alternativlos an sich zu binden.

- Die Anbieter bieten KonsumentInnen keine Garantien, dass die eingesetzte Technik auf die Lebensdauer des Produktes zur Verfügung steht. Damit fehlen Sicherheiten vor einer vorzeitigen, völligen Entwertung von Geräten.

- KonsumentInnen geraten unter Druck, auch unerwünschten Softwareänderungen zuzustimmen. Andernfalls droht ihnen, ein Gerät zu besitzen, dass offline nicht mehr gebrauchsfähig ist.

Die Rolle der EU

Die im März 2019 beschlossene EU-Warenhandels-Richtlinie bringt nicht den BAK-seits erhofften Schutz aber doch einige Verbesserungen

- Einbeziehung von IoT in den Anwendungsbereich

Waren, die der Richtlinie unterliegen, sind auch solche, die „digitale Elemente“ einschließen. Die Ware umfasst damit auch alle digitalen Inhalte/Dienste, die in diesen Waren enthalten sind (zB Betriebssysteme, andere Software) oder so mit der Ware verbunden sind, dass die Waren ohne diese digitalen Inhalte/Dienste ihre Funktion nicht erfüllen können (zB Software „as a Service“ in Cloud-Computing-Umgebung, Verkehrsdaten für Navis oder Trainingspläne für die Smart Watch). Gleichgültig ist dabei, ob die digitalen Inhalte oder Dienste vom Verkäufer oder einem Dritten bereitgestellt werden.

Kritisch anzumerken ist: Mit dieser komplizierten Definition sollen die Anwendungsbereiche der Richtlinie für den Warenhandel und der nahverwandten Richtlinie über digitale Inhalte voneinander abgegrenzt werden. Unzureichend, wie die BAK findet. Denn viele Fragen bleiben offen. Wohin ressortieren zB die Entertainment- oder Notrufsysteme eines smarten Autos? Grundsätzlich sind sie im Sinn der obigen Definition im Auto „enthalten" bzw mit dem Auto und seinen Funktionen mehr oder weniger eng „verbunden". Ein Erwägungsgrund (EG 16) deutet jedoch an, dass es auch darauf ankommt, ob die digitalen Elemente Teil des Autokaufvertrags oder eines davon getrennt abgeschlossenen Servicevertrages sind (Im letzteren Fall fallen die IoT-Anwendungen unter die Richtlinie zu digitalen Inhalten). Damit würden Anbieter allein durch die Wahl des Abschlusses von einem oder zwei Verträgen entscheiden, welches Recht für sie zur Anwendung kommt.

- **Gewährleistungsfähige Eigenschaften von IoT**

Waren mit digitalen Elementen haben nur dann einen vertragsgemäßen Zustand, wenn sie (neben den vertraglichen Zusicherungen) auch bestimmte objektive Qualitäten aufweisen. Dazu zählt, dass „Funktionalität, Kompatibilität und Sicherheit dem entsprechen muss, was bei Waren der gleichen Art üblich ist und was der Verbraucher… insbesondere aufgrund der Werbung oder des Etiketts vernünftigerweise erwarten kann". Überaus positiv zu bewerten ist, dass bei IoT-Gegenständen die gesetzliche Vermutung besteht (Umkehr der Beweislast), dass innerhalb von zwei Jahren auftretende Vertragswidrigkeiten auch schon bei der Lieferung vorgelegen sind (bei fortlaufender Bereitstellung gilt dies für die gesamte Laufzeit).

Kritisch anzumerken ist: Diese Regelung könnte eigentlich das Herzstück für den Verbraucherschutz bei IoT sein. Die vom Unionsgesetzgeber gewählten vagen Kriterien werden dem Verbraucher in der Praxis allerdings wenig weiterhelfen. Eine Branche, bei der es „üblich" ist, Geräte nur in bescheidenem Ausmaß vor Databreaches und Hackingangriffen abzusichern, bietet bspw kein dem Stand der Technik entsprechendes Best-Practice-Beispiel, an dem sich KonsumentInnen im Beschwerdefall orientieren und die Einhaltung dieser Standards verlangen können. Und was kann der Verbraucher „vernünftigerweise" noch „erwarten", wenn eine gesamte Branche dazu übergeht, KonsumentInnen bestimmte (bei traditionellen Käufen vorausgesetzte) „Funktionalitäten" und „Kompatibilitäten" bei IoT vorzuenthalten?

- **Updates**

Der Verkäufer von Waren mit digitalen Elementen soll dafür sorgen, dass der Verbraucher „über Aktualisierungen, einschließlich Sicherheits-Updates, die für den Erhalt der Vertragsmäßigkeit der Waren erforderlich sind, informiert wird und solche erhält." Die in der Praxis so entscheidende Frage: „wie lange?" beantwortet die Richtlinie wiederum äußerst vage: Während des Zeitraums, in dem der Verbraucher „vernünftigerweise" Updates erwarten kann (wenn der digitale Inhalt/Dienst einmalig bereitgestellt wird). Bei vereinbarten Dauerschuldverhältnissen wird ein Mindestzeitraum von zwei Jahren bestimmt bzw auf die Länge der vereinbarten Vertragslaufzeit abgestellt. Unterlässt es ein Konsument, Updates zu installieren, so haftet der Verkäufer grundsätzlich nicht für dadurch bedingte Vertragswidrigkeiten.

Kritisch anzumerken ist: KonsumentInnen werden erst aufgrund von produktspezifischen Gerichtsentscheidungen wissen, was sie vom Anbieter erwarten dürfen. Anbieter von Dauerschuldverhältnissen wiederum können längere Fristen als zwei Jahre dadurch umgehen, dass

sie dem Verbraucher einen Basisvertrag und Zusatzverträge vorlegen. Damit dürften die längeren Vertragslaufzeiten von der Verantwortung für Updates entkoppelt sein. Im Endeffekt dürfen KonsumentInnen nur damit rechnen, dass ihnen Updates im bescheidenen Ausmaß von 2 Jahren zugestanden werden. Dies entspricht (auch ohne gesetzlicher Festlegung) den Marktusancen bei Smartphones und widerspricht dem Postulat nach einer Entwicklung zu einer nachhaltigen Gesellschaft.

EU-Strategien zu IoT

Das EU-Parlament hat am 16.2.2017 einen Bericht über zivilrechtliche Regelungen im Bereich Robotik (2015/2103 (INL)) angenommen und die EU-Kommission 2018 eine Mitteilung zu Künstlicher Intelligenz für Europa (COM (2018) 237/2 vom 25.4.2018) vorgelegt. Die darin festgelegte EU-Strategie lautet: verstärkte Investitionen in die Grundlagenforschung (Erklärbarkeit von AI, effiziente Datennutzung uvm), Unterstützung für anwendungsorientierte Forschung (ua autonome Autos, Spital der Zukunft), Errichtung einer AI-On-Demand Plattform („AI4EU“ führt 79 Forschungsinstitute mit Unternehmen aus 21 Ländern zusammen) und AI-fokussierter Innovation Hubs. 2018 veröffentlichte die EU-Kommission auch ihre Strategie für smarte Autos („Auf dem Weg zur automatisierten Mobilität“, COM (2018) 283). Das Hauptaugenmerk der EU-Kommission gilt der:

- **Datenverwertung:** Die Devise der EU-Kommission lautet „Making more data available“. Umgesetzt wird sie durch Überarbeitung der Public-Sector-Information-Richtlinie, Guidelines für das kommerzielle „Sharing“ von Daten aus der Privatwirtschaft, eine überarbeitete Empfehlung über den Datenzugang für die Wissenschaft und Forschung und einer Mitteilung über die digitale Transformation im Bereich der Gesundheits- und Pflegeeinrichtungen inklusive des „Sharings“ von Gesundheitsdaten (vor allem genomischer Daten).

- **Vorbereitung auf den sozioökonomischen Wandel:** Umbrüche auf Arbeitsmärkten sollen rechtzeitig antizipiert, sektorale Berufsausbildungen an die digitalen Erfordernisse angepasst, einschlägige Trainee-Programme für StundentInnen angeboten und ethische Prinzipien für AI in Form von Guidelines entwickelt werden.

- **Rechtsanpassungsbedarf wird erst geprüft:** Die EU-Kommission plant überdies, die Produkthaftungs-Richtlinie bis Mitte 2019 in Bezug auf ihre Zeitgemäßheit angesichts der technischen Entwicklungen zu prüfen, einen Bericht über den Anpassungsbedarf des Rechtsrahmens für Haftung und Sicherheit in Bezug auf AI auszuarbeiten und Pilotprojekte wie die „AI-Alliance“ (eine Diskussionsplattform plus eine High-Level-Arbeitsgruppe mit Vertretern aus Industrie, Universitäten und NGOs, darunter auch der EU-Verbraucherverband BEUC) und zu „Algorithmischer Bewusstseinsbildung“ zu initiieren.

Und welche Rolle spielt der Verbraucherschutz bei IoT auf EU-Ebene?
Zu wenig findet bspw der europäische Verbraucherverband BEUC, und legte schon 2017/2018 der EU-Kommission detaillierte Forderungspapiere zu IoT-spezifischen Verbraucheranliegen vor:

- Protecting European Consumers with Connected and Automated Cars (https://www.beuc.eu/publications/beuc-x-201138_dve_beuc_connected_autonomous_cars.pdf)

- Cybersecurity for connected goods (https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf)

- Securing Consumer Trust in the Internet of Things – Principles and Recommendations (https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf)

- Automated Decision Making and Artificial Intelligence – A Consumer Perspective (https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf)

- Ethics Guidelines for Trustworthy AI der von der EU-Kommission eingesetzten High Level Expert Group unter Mitwirkung der BEUC (https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai)

Auf diese Stellungnahmen sei an dieser Stelle ausdrücklich hingewiesen.

Akuelle IoT Anwendungsfelder und ihre Risiken

Einen guten Überblick über das Heranwachsen neuer Produkte und Probleme geben die seit 2014 publizierten BAK-Studien zum „Digitalen Verbraucherschutz“:

- **Kommerzielle digitale Überwachung im Alltag:**
https://www.arbeiterkammer.at/infopool/wien/Digitale_Ueberwachung_im_Alltag.pdf

Smartphones und mobile Apps gelten als Einfallstor für Datensammler, die Spuren und Interessen der NutzerInnen verfolgen. Die Datenschutzpolitik ringt noch um Antworten, wie KonsumentInnen vor übertriebener Datenverwertung im (mobilen) Internet geschützt werden können: So sind zB die Verhandlungen zur e-Privacy-EU-Verordnung aufgrund erheblicher Divergenzen beinahe zum Stillstand gekommen. Dabei zeichnen sich bereits neue kritische Trends ab. Immer mehr Firmen bieten mit Sensoren ausgestattete und dem Internet verbundene Geräte an, die noch viel tiefere Einblicke in unser Leben erlauben.

- **Vom Assistenzsystem zum Autopiloten – Vernetzte Fahrzeuge:**
https://www.arbeiterkammer.at/service/studien/konsument/Vernetzte_Automobile.html

Viele Assistenzsysteme überwachen bereits jetzt täglich die Fahrten mit dem Auto. Extrem gläsern werden AutofahrerInnen aber mit der Umstellung auf fahrerlose Autos. Die Elektronik im Auto und ihre Vernetzung mit der Umgebung werden zum Werbe- und Verkaufsfaktor. Kartendaten zur Routenberechnung und Verkehrslage werden heruntergeladen, Sensordaten über den Autozustand erzeugt, Smartphones eingebunden, Daten über das Fahrverhalten gespeichert. Bald werden auch Daten mit anderen Autos, mit Versicherungen, Pannendiensten oder Werkstätten laufend ausgetauscht. Es lassen sich präzise Bewegungsprofile erstellen, die viel über Lebensgewohnheiten verraten.

Während früher nur gravierende Ereignisse für die Reparatur in der Werkstatt im Fehlerspeicher abrufbar waren, werden inzwischen enorme Datenmengen erhoben. Gesammelt werden Statusdaten (Motordaten, Füllstände), der aktuelle Standort (bei Mercedes alle zwei Minuten), überhöhte Drehzahl oder Temperatur, Betriebsstunden der Fahrzeugbeleuchtung, wie oft, wie und wo die Antriebsbatterie geladen wurde (Das Laden der Antriebsbatterie von Elektroautos kann bei Renault per Mobilfunkverbindung unterbunden werden. Der Verkehrsclub ADAC vermutet, um bei nicht gezahlten Leasingraten eine weitere Nutzung zu verhindern). Die 100 letzten Abstellpositionen sind bei BMW auslesbar: Wenn das Mobiltelefon mit der BMW-Software gekoppelt wurde, werden Kontakt- und Anrufdaten mit dem Fahrzeug synchronisiert und sind vom Hersteller abrufbar.

Für manche Datenarten lässt sich kaum ein legitimer Zweck finden, etwa wenn es um die Profilerstellung der Nutzer oder die Überwachung der Aufenthaltsorte geht. Aber auch aus Fahrzeugdaten lässt sich bspw auf die individuelle Fahrweise schließen. Diese Daten könnten, wenn sie dem risikoarmen Gebrauch widersprechen, etwa durch Versicherungen zum Nachteil der Konsumenten ausgelesen werden.

Experimentiert wird mit Car2Car-Kommunikation. Vorausfahrende Fahrzeuge sollen die nachfolgenden bspw über Baustellen, Umleitungen usw informieren. Die Verständigung kann von Fahrzeug zu Fahrzeug oder aber auch durch zentrale Infrastruktur erfolgen. Beim automatisierten Fahren gelten die Stufen 0-3 (Fahrerkontrolle bis teilautomatisiert) bereits als Stand der Technik. An den Stufen 4-6 (hochautomatisiert bis fahrerlos) wird unter Hochdruck gearbeitet. Sie unterscheiden sich durch die Zeit, die ein menschlicher Fahrer benötigt, um wieder die volle Kontrolle zu übernehmen. Je höher der Automatisierungsgrad, desto mehr Daten mit und ohne Personenbezug benötigt das Fahrzeug.

Aktuell bieten die Hersteller (noch) getrennte Verträge an – einen für den Autokauf und einen weiteren, mit dem der Zugang und die Nutzung für Zusatzservices (Entertainment, Routenplaner uvm) gebucht wird. Noch kann jeder Besitzer frei entscheiden, ob er die Zusatzleistungen in Anspruch nehmen will, denn die Fahrfunktion ist davon unabhängig. Es besteht das Risiko, dass über kurz oder lang viele Funktionen nur mehr als Gesamtpaket erworben werden können. Denn Autohersteller sehen ihre Umsatzerwartungen in der Autoproduktion schwinden und verlegen ihre Anstrengungen auf Kundenbindung durch Services, die auf Abonnementzahlungen beruhen. Das wirtschaftlich erfolgreiche, geschlossene Ökosystem von Apple dient dabei als Vorbild. Im ungünstigsten Fall werden Kunden künftig vom Abschleppservice über Versicherungen und den Assistenten für (teil)autonomes Fahren bis hin zur Wartung fix an einen Hersteller gebunden sein.

- **Geodatennutzung bei mobilen Geräten:**
https://www.arbeiterkammer.at/service/studien/konsument/Geodatennutzung_bei_mobilen_Geraeten.html

Die heute selbstverständliche Verfügbarkeit von Geodaten sowie die genaue Zuordenbarkeit der einzelnen Geräte zu bestimmten Personen ermöglichen Werbetreibenden eine neue Dimension der Profilerstellung, die hohe Profite verspricht. Während NutzerInnen sich der Folgen dieser Profiling-Prozesse kaum bewusst sind und das Grundrecht auf Privatsphäre oft als vernachlässigbares Gut in Frage stellen, entledigen sich Hersteller und Service-Anbieter ihrer Verantwortung.

Datenschutzeinrichtungen sind oftmals nicht in der Lage, bestehendem Recht zur Durchsetzung zu verhelfen, was aber aufgrund der unübersehbaren Menge an Apps und der hohen Dynamik in diesem Feld nicht verwundert.

- **Onlinezwang und löchrige Privatsphäre bei Spielen:**
https://www.arbeiterkammer.at/service/studien/konsument/Privatsphaere_in_Online-Spielen.html

Mit dem Einzug von IoT in Kinderspielzeugen sind Überwachungspraktiken auch in Kinderzimmern angekommen. Bevor sich Kleinstkinder noch an Computerspielen versuchen, konnten sie schon mit der Puppe Cayla, die laut Produktwebsite "fast wie eine richtige Freundin" sei, erste Erfahrungen mit kommerziellen Vertraulichkeitsverletzungen sammeln. Über Bluetooth-Verbindung, Mikrofon und Spracherkennung können Unterhaltungen an den US-Hersteller **weitergeleitet werden. Probleme, die auch mit Online-Spielen für ältere Kinder verbunden** sind: verstecktes Aufzeichnen des Spielverhaltens und Intransparenz der Datenempfänger oder Datennutzungszwecke. KonsumentInnen werden überdies um ihre Wahlfreiheit gebracht: Bei vielen Spielen besteht Onlinezwang, auch dann, wenn ein Spiel alleine gespielt wird und eine Internetverbindung nicht erforderlich wäre. Dieser Druck zu einem „always-on“ dürfte sich bei vielen IoT-Produkten verstärken. Ohne ein explizit verankertes „Offline“- Recht werden Verbraucher nur die Wahl des „take it – or leave it“ (Akzeptiere oder verlasse das Angebot) haben.

Weitere Anwendungsfelder sind:

Smart Home

Smart Home gilt als eines der großen Hoffnungsgebiete von IoT. Die Anbieter versprechen damit Arbeitserleichterungen und mehr Sicherheit. Momentane Entwicklungsziele sind die einfache, intuitive Bedienung von Geräten und Diensten für KonsumentInnen ohne besondere technische Anwenderkenntnisse gepaart mit Komfort- oder Sicherheitsfunktionen fürs Haus und für Wohnungen. „Early adopter“ können Zugangs-, Überwachungs- und Schließsysteme (wie programmierbare Fenster-Rolläden, Beleuchtung oder Heizungen, ferngesteuerter Einbruchsschutz, Unterhaltungselektronik und Hausgeräte mit Internetanschluss) erwerben. Einen praktisch nachvollziehbaren Bedarf dürften aber vor allem Assistenzsysteme zur Unterstützung der selbständigen Lebensführung im Alter bzw im Falle von Beeinträchtigungen decken. Vorhut dieser Entwicklung sind smarte Armbänder mit Notfallsalarmfunktion, wenn eine pflegebedürftige Person stürzt oder automatisch gemessene Pulswerte außer der Norm liegen. Erhofftes Ziel ist es, Nischen zu Massenmärkten zu machen, ua gekennzeichnet durch:

- komplett vernetzte Neubauten schon beim Bezug durch Mieter, Smart Home-Funktionen als Basisausstattung von neu vermieteten Wohnungen und nicht bloß im Luxus-Segment,
- Integration von Services zum Energiemanagement (Ressourcenschonung, Energieeffizienz),

- Fernsteuerung von vielen Alltagsgeräten, virtuelle Butler als Weiterentwicklung von digitalen Sprachassistenten, intuitivere Befehle über Mensch-Maschine-Kommunikation wie Sprache oder Gestik,
- starke Personalisierung der Zugriffe (Kindersicherung, Authentifizierung an der Haustür, algorithmenbasierte Individualisierung nach Vorlieben usw),
- Plattformen-Angebote, die wie der Google Play Store ständig um neue App-Angebote von Drittentwicklern erweitert wird; Heranwachsen dominanter Player (Google Nest, Samsung Smart Home uÄ)

Smart Meter

Smarte Messgeräte ersetzen sukzessive elektromechanische Stromzähler: 2020 sollen mindestens 80 Prozent der privaten Haushalte in Österreich damit ausgestattet sein. Die Umrüstung wurde national und auf EU-Ebene politisch nicht zuletzt mit dem Argument forciert, notwendiger Teil der Energiewende zu sein. Der Stromverbrauch wird für automatisierte Abrechnungen erfasst, kann aber aufgrund der Abrufbarkeit von Verbrauchsständen in kurzen Intervallen auch für genaue Verbrauchsanalysen und damit Prognosen über Lastspitzen und einen effizienteren Betrieb der Stromnetze herangezogen werden. Anbieter sollen durch Fern-Ein- und Abschaltung rascher gewechselt, flexible, etwa tageszeitabhängige Tarife eingeführt und der Energieverbrauch dadurch optimiert werden, dass vernetzte Geräte automatisch erst dann in Betrieb gehen, wenn die Stromkosten gerade niedrig sind.

Die Wirkung einer IoT-Einflussnahme auf Kühlschränke und Waschmaschinen nimmt sich allerdings sehr bescheiden aus, bedenkt man, dass Heizung und Warmwasser die entscheidenden Energieverbraucher in privaten Haushalten sind. Wesentlich größer ist hingegen die Sorge der Verbraucher vor einer Überwachung ihres Alltagslebens durch intelligente Zähler, die im 15 Minuten-Takt Messungen durchführen und die Messdaten einmal im Monat vom Netzbetreiber an den Stromlieferanten übermitteln. Dadurch sind Rückschlüsse auf die Anwesenheit von Personen im Haushalt und ihre Tätigkeiten möglich (Wird gerade gegessen, geschlafen? Sogar die Auswahl des Fernsehprogrammes ließe sich nachvollziehen – siehe etwa die Studie der FH Münster (http://1lab.de/pub/smart-meter-debatte.pdf , 26.04.16), die folgende Dateninteressenten ausmacht: Werbewirtschaft für gezielte Werbung, Versicherungen, um zu prüfen, ob Geräte beim Verlassen des Heims ausgeschaltet waren, Überwachung im Rahmen eines Partnerstreits und von Zivilrechts- oder Strafverfolgung (Vermieter: Wohnung bewohnt? Leben mehr Personen als angegeben in der Wohnung?; Sorgerechtsstreit: werden Kinder alleine gelassen?; Strafrechtsbehörden: Alibi-Überprüfung uvm). Nach langem Ringen um angemessene Datenschutzstandards wurde Verbrauchern in Österreich eine gesetzliche Opt-Out-Möglichkeit zugebilligt. Macht der Verbraucher davon Gebrauch, so wird das smarte Gerät zwar dennoch installiert, die 15-minütige Verbrauchskontrolle aber deaktiviert und es bleibt bei der Basisfunktion einer jährlichen Verbrauchskontrolle.

Auch die Fernabschaltfunktion der Messgeräte gibt Anlass zur Sorge. Nicht nur bei Vertragsabschluss bzw -kündigung oder Zahlungssäumnis kann die Energiezufuhr ein- und ausgeschaltet werden. Auch unbefugte Dritte könnten sie unterbinden. Die möglichen Folgen eines Hackingangriffs wurden im Roman „Blackout“ (Marc Elsberg) 2012 geschildert. Das Buch verarbeitet Ergebnisse des Berliner Projekts TankNotStrom, in dem Szenarien eines flächendeckenden Stromausfalls dargestellt wurden.

Die Absicherung vor unbefugten Fremdzugriffen wird oft unterschätzt (https://www.berliner-feuerwehr.de/fileadmin/bfw/dokumente/Forschung/tanknotstrom/Forschungsprojekt_TankNotStrom.pdf). Ende 2018 wurde in Österreich das Netz- und Informationssystemsicherheitsgesetz (NISG) beschlossen, womit es immerhin erstmals Regelungen für Störfälle durch mangelnde Cybersicherheit bei versorgungskritischen Netz- und Informationssystemen im Bereich Energie, Verkehr, Banken, Gesundheit, Wasser und Internet gibt.

- Weitere Details zu Smart Meter:
https://www.arbeiterkammer.at/service/studien/konsument/Smart_Meter.html

Fitnesstracker

Sieht man von den offenbar unentbehrlichen Smartphones einmal ab, so haben KonsumentInnen mit „Wearables“ (vor allem Smart Watches und Fitness-Tracker) IoT erstmals massenhaft und lifestyletauglich in ihren Alltag übernommen. Die Tracker messen Puls und Schritte des Trägers. Die Apple Watch integriert mit Apple Pay auch gleich ein berührungsloses Zahlungsmittel mit biometrischen Sicherheitsmerkmalen (Fingerabdruck, Gesichtsscan). 2019 soll das Marktvolumen allein von smarten Armbanduhren bei 17,5 Milliarden Dollar liegen (International Data Corporation). Sensoren sammeln fitness- und gesundheitsrelevante Daten und werten sie aus (Uhrzeit, GPS-Distanzmessung, Schrittzähler, Schlafanalyse, Kalorienzähler, Herzfrequenz- und Pulsmessung). Gespeichert werden diese sensiblen Daten (zusammen mit den Registrierungsdaten des Nutzers wie Alter, Geschlecht, Größe, Gewicht) in der – nicht unbedingt in jeder Hinsicht sicheren – Cloud.

Die medizinische Fernüberwachung kranker, beeinträchtigter oder älterer Personen über smarte Armbänder ist ein vielversprechendes Anwendungsfeld für Spitäler, die Pflege daheim und das Leben in ländlichen Räumen mit geringer ärztlicher Versorgung. In einem nächsten Schritt dürften die Daten von Fitnessbändern in ein umfassendes e-Health-System eingebunden werden. So interessieren sich Krankenkassen und Versicherungen für ein Tracking ihrer Kunden, um sie bspw zu gesundem Verhalten zu animieren oder die Durchführung von Rehab-Übungen daheim zu begleiten und zu kontrollieren. Versicherungen denken bereits laut über „Gamification“-Methoden nach (spielerische Anreize für ernsthafte Zwecke), wie einen Versicherungsbonus bei Bewegungsaktivitäten, die KonsumentInnen durch die Aufzeichnungen ihrer Fitness-Tracker nachweisen.

Forderungen in Bezug auf IoT

Der EU-Rechtsrahmen ist zu verbessern

- Die **EU-Warenhandelsrichtlinie** beschäftigt sich nur mit Gewährleistungsansprüchen bei bestimmten Mängeln am IoT-Produkt. Andere wichtige Rechtsmaterien – vom allgemeinen Schadenersatzrecht bis zum Produktsicherheits – und Produkthaftungsrecht – werden nicht IoT-tauglich angepasst.

- Die **e-Privacy Richtlinie** entspricht nicht mehr dem aktuellen Schutzbedarf der KonsumentInnen gegen Überwachung ihres Verhaltens im Internet. Die Verhandlungen zu einer Nachfolger-Verordnung sind aber zum Stillstand gekommen. Würden sie wiederaufgenommen, droht KonsumentInnen eine Absenkung des Datenschutzniveaus. Internet- bzw Medienkonzerne und die Onlinewerbewirtschaft setzen sich gegen bessere Schutzstandards, die das Ausspähen des Internetnutzerverhaltens mit Cookies und anderen Techniken erschweren, mit aller Macht zur Wehr.

- **Abkehr von der „Zahlen mit Daten"-Fiktion:** Noch ist völlig offen, ob und unter welchen Umständen die Betriebsdaten von IoT-Geräten unter den Schutz der Datenschutzverordnung fallen. Die entscheidende Frage, wann ein Personenbezug herstellbar ist, muss von den Datenschutzbehörden bzw dem Unionsrechtsgeber erst geklärt werden. Inzwischen bringen sich einige IoT-Hersteller und Softwarelieferanten bereits mit ihrer verbraucherunfreundlichen Haltung in Stellung: Betriebsdaten gehören ihrer Ansicht zufolge der produzierenden Wirtschaft und können wie sonstige urheberrechtliche Werke auch veräußert und lizensiert werden. Liegt ein Personenbezug vor, so können KonsumentInnen ihre Daten wie eine Ware irreversibel „verkaufen" – Persönlichkeitsrechten (zB jederzeitigen Widerrufsrechten) sollen einmal verkaufte Daten nicht mehr zugänglich sein. Dieses Rechtsverständnis ist mit den unveräußerlichen, verfassungsrechtlich geschützten Grundrechten auf Datenschutz und die Privatsphäre nicht in Einklang zu bringen. Vorschub leistet dieser Ansicht allerdings die EU-Richtlinie für digitale Inhalte, die das „Bezahlen mit Daten" in den Anwendungsbereich ausdrücklich aufgenommen und damit erst salonfähig gemacht hat.

- **Cybersicherheits-Verordnung:** Die Verordnung setzt auf freiwillige Zertifizierung. Das ist eindeutig zu wenig. Ohne verbindliche Anforderungen können Hersteller weiter vernetzte Produkte verkaufen, denen grundlegende Sicherheitsstandards fehlen. Das Engagement beschränkt sich auf eine Art europäisches Gütesiegel für vernetzte Produkte. Um ein IoT-Gütesiegel zu erhalten, müssen die Hersteller Mindeststandards rund um die Cybersicherheit der Produkte und Angebote einhalten. Die Zertifikate sollen Verbrauchern anzeigen, dass zB vernetzte Fernseher zur Zeit des Prüfprozesses keine bekannten Schwachstellen haben und die Geräte internationale technische Normen einhalten. Hersteller müssen beim Zertifizierungsprozess die Vertraulichkeit, Integrität, Verfügbarkeit und den Datenschutz der integrierten Online-Services nachweisen. Sie sollen auch sichtbar machen, wenn eine Wartung nur durch autorisiertes Personal möglich ist. Die Anbieter müssen Risiken rund um "Cybervorfälle" minimieren und eine Zeitspanne angeben, in denen sie Sicherheitsupdates und Support liefern. Das augenfällige Defizit: Der Einwand von Verbraucherschützern, nur verpflichtende Mindeststandards schützen KonsumentInnen verlässlich, wurde überhört. Die Teilnahme am Zertifizierungsverfahren ist freiwillig.

- **Produkthaftungs-Richtlinie:** Das Produkthaftungsrecht geht auf eine über 30 Jahre alte EU-Richtlinie (85/374 EG) zurück und stellt hohe Anforderungen an geschädigte KonsumentInnen: Sie müssen einem bestimmten Hersteller gegenüber belegen können, dass dieser einen Fehler gemacht hat. Das Produkthaftungsrecht gilt für „bewegliche" Sachen, nicht für Dienstleistungen. Ein Gerätesoftwarefehler, der einen Schaden verursacht, würde eventuell noch als Produktfehler gelten. Rein webbasierte Dienste (zB Cloudanwendungen) sind jedenfalls nicht erfasst.

Der EUGH hat 2015 die Produkthaftung für einen nur „möglicherweise“ defekten Herzschrittmacher in Bezug auf „vorbeugende“ Maßnahmen zur „Vermeidung möglicher Schäden“ verschärft (https://www.lto.de/recht/hintergruende/h/eugh-urteil-c-503-13-produkthaftung-medizin-herzschrittmacher/). Unklar ist aber, ob die Entscheidung auch für andere digitale medizinische Geräte oder gesundheitsbezogene Produkte wie Gesundheits-Apps gilt. Bei Gesundheits-Apps ist bspw noch völlig offen, ob sie selbst oder in Kombination mit Geräten wie Sensoren der Produkthaftung unterliegen.

Entsprechend ungeeignet ist der Rahmen, adäquate Antworten auf komplexe Haftungsfragen zu IoT zu geben. Auf den Anpassungsbedarf angesichts IoT weist auch ein im Auftrag des deutschen Verbraucherverbands VZBV erstelltes Gutachten zur Evaluierung der europäischen Produkthaftungsrichtlinie (85/374/EWG) hin (https://www.vzbv.de/meldung/produkthaftung-digitale-herausforderungen-anpassen). Die zunehmende technische Komplexität und eine durch die Vernetzung von Geräten bedingte Vielzahl möglicher Schadensverursacher erfordert neue Regeln. Die EU-Kommission kommt in ihrem Evaluierungsbericht zum Ergebnis, dass die Diskussion über die Zukunftsfähigkeit der Richtlinie fortgesetzt werden muss. Ein Überarbeitungsvorschlag wurde aber noch immer nicht vorgelegt.

Forderungen im Detail

IoT Sicherheit allgemein

- Sicherheit muss im Produkt verankert sein und in Bezug auf die Vernetzung über Schnittstellensicherheit technisch abgesichert werden (Safety by Design).

- Sicherheit darf keine optionale Zusatzleistung sein, die KonsumentInnen zusätzlich erwerben müssen.

- Gefahren, die sich aus für KonsumentInnen weitgehend unsichtbaren Softwareprozessen bei Automatisierung und vernetzten Systemen ergeben, müssen vom Hersteller und seinen Softwarelieferanten beherrscht werden.

Produkthaftung

- KonsumentInnen müssen vor Schäden durch Softwareschwachstellen besser geschützt sein. Der Anwendungsbereich der Produkthaftung ist so zu erweitern, dass nicht nur das Gerät, sondern auch verbundene Software und digitale Dienste, die nicht unmittelbar im körperlichen Produkt eingebettet sind, erfasst sind. Es ist klarzustellen, dass sowohl auf einem Datenträger vorinstallierte Software als auch Software, die erst nach Onlineübertragung in einem Gerät oder auf einem Datenträger installiert wird, in den Anwendungsbereich des Produkthaftungsrechts fällt.

- Die Produkthaftungsrichtlinie muss zur Anwendung kommen, wenn IoT-Geräte zwar bei der Lieferung fehlerfrei waren, aber nach Softwareupdates oder durch Fernsteuerung Schäden verursachen.

- KonsumentInnen sind mit dem Nachweis von Sicherheitslücken und der Kausalität für die Verursachung eines Schadens überfordert. Damit die Anspruchsdurchsetzung auch bei IoT gelingt, muss es Beweiserleichterungen für KonsumentInnen geben. Bei bestimmungsgemäßen Gebrauch sollte die Beweislast auf der Anbieterseite liegen. Dieser sollte widerlegen müssen, dass ein Produktfehler (und ein Kausalzusammenhang zwischen Fehler und Schaden) den Schaden herbeigeführt hat.

- Der Selbstbehalt der KonsumentInnen bei bis zu 500 Euro Sachschäden ist angesichts der IoT- immanenten Risiken nicht mehr zeitgemäß. Ebenso überholt ist der bloße Schutz von (körperlichen) Schäden an Menschen oder Sachen. Auch immaterielle Schäden durch die Verletzung von Persönlichkeitsrechten und Schäden an unkörperlichen Sachen (zB Datenverlust) sollten vom Anbieter ersetzt werden. Überlegenswert ist auch, reine Vermögensschäden im Rahmen der Produkthaftung abzugelten.

- Mit Blick auf das Insolvenzrisiko von Anbietern haben diese den KonsumentInnen den Abschluss einer verpflichtenden Produkthaftpflichtversicherung nachzuweisen.

- Mehrere Anbieter in vernetzten Systemen sollten gesamtschuldnerisch haften, solange keine klare Fehlerzuordnung zu einem Anbieter möglich ist. Der vertragliche Schadenersatzanspruch könnte auch verschuldensunabhängig ausgestaltet sein. Der Umfang des Schadenersatzes sollte vertraglich nicht reduziert werden können.

Produktsicherheitsnormen

- Solange es keine verbindlichen Normen zur IT-Sicherheit gibt, dürfen unklare Haftungssituationen nicht zulasten geschädigter KonsumentInnen gehen. So weist der EU-Verbraucherverband BEUC darauf hin, dass es vielen IoT-Geräten an elementaren Sicherheitsmerkmalen, wie einer zeitgemäßen End-zu-End-Verschlüsselung, Zwei-Faktor-Authentifizierung oder zumindest Passwortschutz, mangelt. Die internationale Normung ist voranzutreiben und ihre Beachtung in der EU-Cybersicherheits-Verordnung obligatorisch (statt nur freiwillig) vorzusehen.

- Zumindest bei hochriskanten Anwendungen (autonomes Fahren, Produkte für Kinder, Smart-Home-Sicherheitsprodukte, Smart City-Anwendungen, medizinische Anwendungen) sind verbindliche Normen alternativlos.

- Es müssen nationale Aufsichtsbehörden bestimmt werden, die gegebenenfalls gefährliche Produkte vom Markt rasch entfernen können.

Schutz vor Beeinträchtigungen durch Algorithmen und KI

- Automatisierte Entscheidungen und Prognosen, die auf dem Einsatz von Algorithmen bzw KI basieren, können ebenfalls materielle und immaterielle Schäden auf Konsumentenseite verursachen.

Nach der Datenschutzgrund-Verordnung gebührt allerdings nur Schadenersatz, wenn bei der Erhebung und Speicherung des Datensatzes gegen datenschutzrechtliche Bestimmungen verstoßen wird. Fehlprogrammierungen und fehlerhafte selbstlernende Prozesse, die zu unrichtigen, verzerrenden, diskriminierenden Annahmen, Analyseergebnissen, Entscheidungen und Prognosen führen, sollten in den Anwendungsbereich der Produkthaftung fallen oder Gegenstand einer eigenen EU-Richtlinie werden.

- Es ist klarzustellen, dass Fehlentscheidungen eines automatisierten oder autonomen Systems als Produktfehler anzusehen und dem Hersteller zuzurechnen sind.

- Derzeit wird überwiegend verschuldensabhängig gehaftet. Das Verschulden wird bei Beteiligung mehrerer Akteure auf Anbieterseite nicht einem einzigen Anbieter unzweifelhaft zuordenbar sein. Das Problem wächst mit der Zahl der Produkte und Plattformen, die gleichzeitig in Interaktion treten und ohne menschliches Zutun selbständig handeln. Bei selbstlernenden algorithmischen Prozessen verneint die Anbieterseite schon jetzt, über das Wesen dieser Lernvorgänge selbst Bescheid zu wissen, geschweige denn KonsumentInnen darüber aufklären zu können. Entsprechend schwierig gestaltet sich auch die Frage nach der Verantwortung und dem Verantwortlichen an schädigenden oder benachteiligenden Outputs der Berechnungsvorgänge.

- Mit dem Angebot von IoT-Produkten samt erforderlichen Schnittstellen sollten die beteiligten Hersteller und Lieferanten als Haftungsgemeinschaft angesehen werden. Bei besonders hohen oder unabsehbaren Entwicklungsrisiken darf nicht auf das Vorliegen von Verschulden abgestellt werden. Um KonsumentInnen angemessen zu schützen, sollte daher je nach Risiko eine gesamtschuldnerische bzw verschuldensunabhängige Haftung in Betracht gezogen werden.

- Mit Blick auf das Insolvenzrisiko von Anbietern haben diese den KonsumentInnen den Abschluss einer verpflichtenden Produkthaftpflichtversicherung nachzuweisen.

Information und Transparenz

Verbraucher benötigen zeitgemäß ausgebaute Informationsrechte. Nur so können sie verstehen, worauf vernetzte digitale Produkte und Dienste aufbauen, wie sie funktionieren, wer die beteiligten Hard- und Softwareanbieter sind, wofür sie jeweils verantwortlich sind, welche Prozesse im Hintergrund ablaufen und welche Verbraucherrechte im Beschwerdefall bestehen. Nur in Kenntnis der Tragweite der Nutzung eines vernetzten Produktes oder Dienstes sind KonsumentInnen in der Lage, informierte Entscheidungen zu treffen.

- Informationen müssen etwa um Risikohinweise erweitert und leicht zugänglich, verständlich, klar und präzise sein. Wichtige, vor allem anwendungskritische Informationen, etwa über Datensicherheitslücken, denkbare nachteilige Konsequenzen aus Profiling und automatisierten Entscheidungsprozessen uvm, müssen KonsumentInnen vor der Nutzung erhalten und ihre Kenntnisnahme bestätigen.

- Auch die komplexe Zusammensetzung von IoT-Produkten in Form verschiedenster Komponenten und mitbeteiligter Akteure ist NutzerInnen verständlich zu erklären.

- Die Souveränität der KonsumentInnen bei ihrer Willensbildung ergibt sich aufgrund mangelnden technischen Anwenderwissens und von außen nicht nachvollziehbarer Softwareprozesse nicht allein durch die Bereitstellung von Informationen. Sie muss intensiv unterstützt werden. Dafür braucht es enorme unternehmerische / wissenschaftliche Anstrengung, damit Informationen so gestaltet sind, dass sie auch von KonsumentInnen ohne einschlägige Fachkenntnisse und mit geringen Zeitbudgets angenommen werden.

  Anmerkung: Eine vom deutschen Sachverständigenrat für Verbraucherfragen 2016 erstellte Marktstudie über verbraucherrelevante Probleme zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge untersuchte die Ausgestaltung der Verträge bei bereits gängigen Anwendungsfeldern des Internets der Dinge mit folgendem Fazit: die rechtliche Bewertung der Verbraucherposition wird dadurch erschwert, dass bei smarten Gegenständen typischerweise sechs Komponenten zu unterscheiden sind: Die Sachsubstanz (zB das Auto und die dort eingebaute Hardware, etwa das Navigationssystem), die eingebettete Software (zB Betriebssoftware des Multimediasystems oder lokal gespeicherte Navigationskarten), die Zubehör-Software (zB Smartphone-App, mit der die Standheizung eingeschaltet werden kann), Aktualisierungen (zB Updates des eingebetteten Betriebssystems, Aktualisierungen der lokal gespeicherten Navigationskarten), digitale Dienstleistungen (zB Routenplanung unter Berücksichtigung der aktuellen Verkehrslage, automatischer Unfall-Notruf), nutzergenerierte Daten (zB Bewegungsdaten, Betriebsdaten des Motors).

- In der Regel kommen die einzelnen Elemente nicht von einem einzigen Hersteller sondern mehreren Anbietern. Vor allem das Verhältnis aller beteiligter Unternehmen untereinander ist äußerst unklar und müsste verständlich offengelegt werden. In der Regel übernimmt keiner der mitwirkenden Anbieter nach gängiger Vertragsgestaltung die Gesamtverantwortung für das reibungslose Zusammenspiel aller Komponenten. Das hat eminente Auswirkungen auf die Transparenz. Dem Verbraucher erschließt sich überwiegend nicht, mit wem was genau vereinbart wird. Hier besteht ein Handlungsbedarf des Gesetzgebers. Bei Einführung einer gesetzlichen verschuldensunabhängigen Solidarhaftung könnten die Transparenzanforderungen entsprechend herabgesetzt werden.

- Für jedes IoT-Produkt muss eine garantierte Mindestlaufzeit, die sich einheitlich auf alle einzelnen Komponenten bezieht, festgelegt und – weil es ein entscheidendes Merkmal ist – beim Kauf unübersehbar am Produkt angegeben werden.

Eigentum

Mit der Verbreitung von vernetzten Gegenständen etablieren sich neue Geschäftsmodelle. Statt einem klassischen Kauf mit vollständigem Eigentumsübergang werden immer öfter bloße Nutzungsrechte eingeräumt. Der Bezug kann einmalig sein, ein Dauerschuldverhältnis mit Abonnement, mit Geld oder Daten bezahlt werden. Die Geschäftsmodelle nehmen Anleihen bei den Werk-Nutzungsrechten von urheberrechtlich geschützten Werken.

Vernetzte Produkte weisen eine starke Servicekomponente auf. Herkömmliche Eigentumserwartungen der KonsumentInnen in Bezug auf erworbene (körperliche oder auch digital abrufbare, unkörperliche) Sachen werden dabei häufig enttäuscht. An die Stelle des Kaufs mit Eigentumsübergang tritt ein Nutzungsrecht, das der Anbieter nach Gutdünken ausgestalten kann. Nur hinsichtlich einiger weniger Rechte, etwa auf Gewährleistung für einige (objektive) Anforderungen an das vernetzte Gerät setzt bspw die Warenhandels-Richtlinie Grenzen.

- Nutzungsmöglichkeiten der KonsumentInnen sind vertraglich beschränkbar (Veräußerung, Vermietung, Privatkopien, Verleihen, Verändern usw). Umgekehrt können Anbieter ihre Zugriffsrechte auf vernetzte Geräte unangemessen erweitern (etwa durch Onlinezwang, Absaugen von Daten für andere als betriebsnotwendige Zwecke – zum Teil Marketing, Missbrauchsprävention, Schutz geistigen Eigentums, Abschaltungen bei Zahlungsverzug, Zugriffe für Behörden, Wissenschaft und Forschung uvm). Gegen das sich abzeichnende Ungleichgewicht von Rechten und Pflichten der Vertragspartner besteht ein Handlungsbedarf des Gesetzgebers.

- Eigentümer können andere vom Zugriff auf ihr Eigentum in der Regel ausschließen. Urheberrechtsinhaber können hingegen Lizenzerwerbern durch internetspezifische Überwachungsmethoden ungleich leichter „auf die Finger schauen“ und freie Werknutzungen unterbinden. KonsumentInnen entscheiden dann nicht mehr autonom, wie, wie lange und wie anonym sie etwas nutzen, wem sie etwas leihen oder weiterverkaufen wollen. Sie unterliegen stärkeren Kontrollen und Verboten, wenn sie die Sache verändern, selbst reparieren oder reparieren lassen wollen. Außerdem sind Nutzer viel mehr der Willkür der Softwarelieferanten ausgeliefert: wenn diese das Produkt nicht mehr (etwa durch Updates) unterstützen oder beschließen wichtige technische Features oder Interoperabilitäten zu ändern, werden KonsumentInnen gegen ihren Willen an der Weiternutzung gehindert. Die Eigentümerrolle der KonsumentInnen ist deshalb unbedingt zu stärken.

- KonsumentInnen sollten dabei folgende Wahlrechte zukommen:

  - Kauf von Offline-Produkten, die nicht smart sind, bei denen kein Onlinezwang besteht.
  - Kauf von Offline-Produkten mit (de-)aktivierbaren IoT-Funktionen, die bei Bedarf durch Abschluss von Zusatzverträgen unterstützt werden.
  - Kauf von IoT-Produkten, bei denen die Komponenten im Zweifel ins Nutzereigentum übergehen. Ein Eigentumsvorbehalt der Anbieter und die Vergabe bloßer Nutzungslizenzen ist auf sachlich gerechtfertigte Situationen beschränkt, dem Nutzer gegenüber zu begründen und gut sichtbar zu machen. KonsumentInnen sind dabei durch nicht abbedingbare Mindestvertragsinhalte geschützt. Für die Kernfunktionen des Geräts nicht erforderliche Dienste dürfen nicht Gegenstand von Koppelungsverträgen sein (sondern können separat abgeschlossen werden).

- Um ein gebrauchtes vernetztes Produkt auf Ebay gefahrlos weiterverkaufen zu können, bedürfte es Klarstellungen zur Erschöpfung des Verbreitungsrechts in der Software-Richtlinie, die der EUGH (etwa C-128/11, 3.7.2012,– Used Software) noch nicht vorgenommen hat.

- Auch die Klauselverbote für Geschäftsbedingungen sollten erweitert werden, etwa um ein Verbot, bei IoT funktionsnotwendige Leistungen vor Beendigung der gewöhnlichen

Lebensdauer einzustellen, die Unwirksamkeit von Veräußerungsverboten, das Verbot von privaten Softwarekopien für mehrere Endgeräte oder der gewerblichen Nutzung uvm:

Denn KonsumentInnen müssen unter Umständen den vollen „Kaufpreis“ als Vorleistung und im Vertrauen darauf entrichten, dass auch die damit verbundenen Dienstleistungskomponenten auf Dauer erbracht werden. Dabei besteht keine Sicherheit, dass die an die eingebettete Software geknüpften Services auch ein Produktleben lang erbracht werden. Werden Apps, Software-Updates, die Cloud-Speicherung uÄ nicht oder schlecht erbracht, ist auch der erworbene Gegenstand weniger oder nichts wert. Diese einseitige Risikoverlagerung in die Sphäre des Verbrauchers ist unangemessen. Es braucht entsprechende Schutzmaßnahmen.
Auch die urheberrechtlichen Ausnahmen, Werknutzungen wie Privatkopien zu dulden bzw dem Verbraucher auch aktiv zu ermöglichen, ist unzureichend abgesichert. In der Praxis können legitime Werknutzungsrechte der Verbraucher durch technische Sperren unterbunden werden. Eine Nutzung vernetzter Gegenstände durch andere Familienmitglieder und Freunde wäre bei einer Beschränkung der Zahl parallel nutzbarer Accounts und heruntergeladener Versionen nicht möglich.

- Die Rechtsposition des Konsumenten wird auch dadurch verschlechtert, dass Anspruchsgegner häufig außerhalb der EU niedergelassen sind. Selbst wenn Nutzungsbedingungen gegen geltendes Recht verstoßen, kann der Verbraucher bei der Rechtsdurchsetzung rasch an Grenzen stoßen. Anbieter aus Drittländern können sich faktisch durchsetzen, indem sie Services einfach einstellen oder nicht mehr an der Diensterbringung mitwirken (etwa Konten sperren, nicht auf andere Nutzer übertragen, usw).

Schutz der Privatsphäre

- Fehlende Eigentumsrechte sind der Privatsphäre der NutzerInnen abträglich. Mit der Verschiebung der Vertragsform in Richtung bloßer Nutzungslizenzen verschaffen sich Anbieter aus wenig triftigen Gründen Zugang zu den Geräten: Neben der Diensterbringung und systemwichtigen Updates zählen oft auch die Betrugsprävention, die Verbesserung der Dienste, Datenzugriffe zur Werbefinanzierung, Verkauf anonymisierter Daten für Marktforschungszwecke an Dritte uvm zu den Überwachungsmotiven. Wird die Eigentümer- gegenüber der Urheberrechtsposition gestärkt, ließen sich Zugriffe auf vernetzte Dinge etwas leichter abwehren.

- Gut sichtbar wird das Kräfteungleichgewicht bei der Frage nach der „Datenhoheit“ über von IoT-Geräten produzierten Daten. „Wem gehören die Betriebsdaten eines vernetzten Gerätes?“, fragte etwa die EU-Kommission im Zuge ihrer Konsultation über den „freien Datenfluss im Binnenmarkt“ (https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-building-european-data-economy). Offeriert wurde nur ein limitiertes Set an Antworten (der Hersteller, der Softwarelieferant…). Der Konsument stand bezeichnenderweise nicht zur Wahl. Es ist folglich dringend nötig, KonsumentInnen in dieser Diskussion als gleichberechtigte Stakeholder Anerkennung zu verschaffen.

- Der Rohstoff vieler künftiger Geschäftsmodelle sind Gerätedaten, die je nach Experteneinschätzung nicht (oder doch) personenbezogen sind. Der Gesetzgeber ist gefordert, eine konsumentenfreundliche Klarstellung vorzunehmen, die das Selbstbestimmungsrecht der KonsumentInnen stärken hinsichtlich Personendaten mit direktem oder indirekten Personenbezug, aber auch Gerätedaten, die keinen Personenbezug aufweisen oder anonymisiert sind. Denn letztere stehen auch zunehmend im Interesse kommerzieller Verwertung (Verkauf für Marketingzwecke nach Zuordnung des anonymen Individuums zu Clustern, Marktforschung, Wissenschaft, kommunalen Interessen uvm). KonsumentInnen sollte ein Widerspruchsrecht (Opt-Out) zukommen. Außerdem sollten sie ein rechtlich abgesichertes Wahlrecht haben, ob Daten, die für den ursprünglichen Zweck nicht mehr benötigt werden, anonymisiert weiterverwendet werden dürfen oder physisch gelöscht werden müssen. Siehe die detaillierten Forderungen in der BAK-Studie über die Weiternutzung von Handy-Verkehrsdaten für andere Zwecke: https://wien.arbeiterkammer.at/service/studien/Konsument/Nutzung_von_Verkehrsdaten_durch_Mobilfunkbetreiber.pdf. Siehe außerdem die Verneinung eines physischen Löschanspruchs durch die österreichische Datenschutzbehörde: https://www.dataprotect.at/2019/02/03/löschen-ist-löschen-oder-doch-nicht-reicht-anonymisierung/

- Künftig geht es um ganz andere Dimensionen des Eingriffs ins Private und der Verhaltenssteuerung. KonsumentInnen können technisch jederzeit überwacht, zu Käufen stimuliert und manipuliert werden. Computer beginnen Gefühle zu verstehen („Affektive Technologien“ https://www.uni-siegen.de/fokos/start/fokos_materialien/2017-01_wissen_computer_die_gefuehle_verstehen_-_digital.pdf).

- **Kein „Pay or Track“ bei IoT:** Im ungünstigsten Fall werden IoT-Anbieter die Geschäftsmodelle von google und Facebook kopieren: Dienstangebote kosten weniger oder vordergründig nichts, wenn Konsumentinnen mit ihrer Zustimmung zum Weiterverkauf ihrer Daten bezahlen. Die Rechtmäßigkeit der Koppelung des „kostenlosen“ Dienstbezugs an die Zustimmung zur kommerziellen Verwertung des Nutzungsprofils ist noch nicht abschließend geklärt. Die Datenschutzgrund-Verordnung schränkt die Zulässigkeit dieses Geschäftsmodells zumindest ein. Artikel 7 sieht vor, dass eine Einwilligung zur Datennutzung nur zulässig ist, wenn sie freiwillig erfolgt. Dabei muss kritisch geprüft werden, ob die Erbringung von Diensten von der Einwilligung zur Datennutzung abhängig ist, die für die Vertragserfüllung gar nicht erforderlich ist. Die österreichische Datenschutzbehörde hat im Falle der Online-Zeitung „Der Standard“ bereits entschieden, dass die Freiwilligkeit gewahrt bleibt, wenn KonsumentInnen die Wahl haben, mit Geld oder ihren Daten zu bezahlen: https://www.dataprotect.at/2018/12/07/payortrack-die-entscheidung-der-dsb-nicht-rechtskräftig/. Da Grundrechte unveräußerlich sind, sollte diesem Abtausch zumindest enge Grenzen gezogen werden.

Abkehr vom verfehlten Leitbild des informierten Verbrauchers

Viele KonsumentInnen wären weit über ihre Grenzen gefordert, wenn sie informierte Entscheidungen in Bezug auf IoT treffen sollen. Systemimmanente Fallstricke in Bezug auf Datenschutz, Urheberrechte, Internetkriminalität, Produktsicherheit werden viele nicht oder nicht rechtzeitig erkennen. Auch die schon gegenwärtig beklagte Desinformation durch ausufernde Produktinformationen und Vertragsbedingungen könnte auf neue Rekorde zusteuern.

Ein illustratives Beispiel: Auf der Webseite von Google-Nest (Smart Home Anwendungen) sind unter "Legal Items“ folgende Infos aufgelistet: Privacy Policy for Nest Web Sites, Privacy Statement for Nest Products and Services, Terms of Service, End User License Agreement, Limited Warranty, Open Source Compliance, Sales Terms (US-Fassung und spezielle Fassung für Europäische Länder), Intellectual Property and Other Notices, Community Forum Agreement, FCC Compliance Notice, Customer Agreements for Rush Hour Rewards, Customer Agreements for Rebates, Customer Agreements for Safety Rewards, Transparency Report.

- Es darf bezweifelt werden, dass Verbraucher sich gegenüber IoT-Kleingedruckten anders verhalten als bei herkömmlichen Gütern: durch Nichtbeachtung des Inhalts und bestätigenden Klick, alles zur Kenntnis genommen zu haben. Die verbraucherpolitische Maxime der vergangenen Jahrzehnte, dass Verbraucher zu selbstbestimmten, informierten Personen werden, wenn ihnen detaillierte Informationen zugänglich sind, darf überholt gelten. Der Gesetzgeber muss seiner Fürsorgefunktion in Bezug auf Übervorteilungen, Manipulationen, Irreführungen usw am Markt zumindest durch ergänzende andere Maßnahmen nachkommen.

- Dazu könnten ua zählen: sektorspezifisches IoT-Verbraucherrecht, gestärkte Datenschutz-Aufsichtsbehörden, wettbewerbsrechtliche Verfolgung des Ausnutzens von Marktdominanz für missbräuchliche Datennutzung usw.

Verbesserte Regeln für Updates

Aktualisierungen sind unzweifelhaft ein entscheidendes Merkmal vernetzter digitaler Produkte. Updates unterstützen – mit ihren Programmkorrekturen, Fehlerbehebungen, Anpassungen zwecks Kompatibilität mit anderen Programmen, der Abwehr von Schadsoftware usw – erst die verlässliche Diensterbringung. Viele Updates verfolgen aber auch oder ausschließlich andere Zwecke: es werden Funktionserweiterungen oder -einschränkungen vorgenommen, das Oberflächendesign verändert usw. Für Verbraucher ist oft nicht erkennbar, inwieweit mit ihrer Zustimmung zu einem Update die Systemsicherheit erhöht werden soll oder der Systemzugriff auch andere – darunter unter Umständen auch unerwünschte oder nachteilige – Änderungen mit sich bringt.

- Verständliche Information über Umfang und Zwecke von Updates ist die unbedingte Voraussetzung für eine selbstbestimmte Entscheidung der Verbraucher, ob sie die Durchführung eines Updates zulassen. Die Verankerung detaillierter Infopflichten zu Updates wäre ein wichtiger Beitrag dazu, dass Verbraucher sicherheitsrelevante Aktualisierungen weder vernachlässigen noch unerwünschte Änderungen aus bloßer Uninformiertheit und Unsicherheit über die Folgen autorisieren.

- Ein Anliegen vieler Verbraucher ist es außerdem, nach einem (nicht sicherheitsrelevanten) Update – wenn dem Verbraucher der neue Zustand nicht zusagt – den Zustand vor dem letzten Update wiederherstellen zu können.

- Zu den Gewährleistungsproblemen mit Updates und der fehlenden Nachhaltigkeit von IoT-Produkten, die nur über einen Mindestzeitraum von 2 Jahren mit Updates versorgt werden müssen – siehe weiter oben beim Punkt EU-Richtlinie zum Warenhandel.

Regulierung flankierender Vertragspartner wie Internetprovider

Mit dem Aufkommen von IoT dürften die Wahlfreiheiten von Internetnutzern noch in ganz anderem Ausmaß eingeschränkt werden – sei es mit Koppelungsgeschäften, Zerorating, branchenübergreifenden unternehmerischen Partnerschaften oder hermetisch geschlossenen „Ökosysteme“ marktbeherrschender Anbieter von Hard- und Software wie Google, Apple oder Amazon.

Abhängigkeiten entstehen etwa, wenn Betriebs- und Nutzerdaten nicht lokal endgeräteseitig gespeichert werden, sondern in fix vorgegebenen Cloud-Diensten.

Der Bezug eines Dienstes könnte auch an einen Vertragsabschluss bei einem ganz bestimmten Internetprovider gebunden sein. Die Telekommunikationsbranche bemüht sich intensiv, die bislang strengen EU-Regeln zur Netzneutralität wieder zu lockern. Nur wenn den Betreibern erlaubt sei, neue Geschäftsmodelle zu entwickeln, sei ein Ausbau des 5-G- Mobilfunkstandards sinnvoll und finanzierbar, so das Credo der Branche. Auch derzeit sind schon Eingriffe in die Netzneutralität möglich, um den Betreibern etwa Geschäftsmodelle wie das „Zerorating“ (Nichtanrechnung bestimmter vom Betreiber bevorzugter Dienste auf den Datenverbrauch) zumindest im Einzelfall zu ermöglichen.

- Das Prinzip der Netzneutralität muss auch bei IoT respektiert werden: Netzaktivisten und Konsumentenschützer sind besorgt, dass die Einführung des Mobilfunkstandards 5G das Aus für Europas Netzneutralität einläuten könnte. Die Verpflichtung zur Netzneutralität wurde erst 2016 im EU-Recht verankert. Alle Datenpakete sollen, unabhängig davon von wem sie kommen, an wen sie gehen und was sie beinhalten, vom Internetbetreiber gleichbehandelt werden (zB gleich schnell unterwegs sein). So dürfen bspw Inhalte oder Dienste nicht blockiert oder verlangsamt werden bzw jene potenten Anbieter nicht bevorzugt werden, die für eine bevorzugte Durchleitung viel zahlen. Damit wird ein „Zwei-Klasseninternet“ für Vielzahler und den Rest verhindert. Ein streng ausgelegtes Gleichbehandlungsgebot dient dem Verbraucherschutz und dem fairen Wettbewerb. Es schützt kleinere Anbieter und KonsumentInnen vor Diskriminierung und unterstützt Innovationen durch Start-Ups.

- 5G erlaubt technisch sogenanntes "Network Slicing", eine Teilung des Internets in Netzabschnitte mit ganz unterschiedlichen Qualitäten, darunter einzelne „Slices“, die Daten mit sehr hoher Geschwindigkeit und geringster Latenz (kaum Zeitverzögerung, beinahe Echtzeit) weiterleiten können. Aus Konsumentensicht besteht das Risiko, dass gewinnträchtige Industrieanwendungen, autonom fahrende Fahrzeuge und andere IoT-Anwendungen den unbedingten Vorrang erhalten.

Für KonsumentInnen, die den Zugang ins Internet nur über PC oder Handy suchen, könnten weniger Kapazitäten zur Verfügung stehen als für den digitalen Sprachassistenten, den smarten Fernseher usw. Damit könnte der Kaufdruck auf KonsumentInnen erhöht werden, über bandbreitenmäßig privilegierte IoT-Geräte ins Internet einzusteigen. Es ist deshalb weiterhin sicherzustellen, dass die Gefahren eines „Zwei-Klassen-Internets" nicht im Zuge der Bereitstellung von 5G – nun vorrangig für zahlungskräftige IoT-Anbieter – eintreten.

- Mit der Verbreitung von IoT wird eine strikte Wettbewerbsaufsicht noch bedeutsamer für die Wahlfreiheit der Verbraucher sein. Beispielshaft dafür ist das jüngste Engagement des deutschen Kartellamts, Facebook ein marktmissbräuchliches Verhalten aufgrund von Verstößen gegen die Betroffenenrechte der Datenschutz-Grundverordnung nachzuweisen.

Zusätzliche Anliegen in Bezug auf vernetzte Fahrzeuge

Eine Studie der AK in Zusammenarbeit mit dem Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften beleuchtet die voraussichtlichen Folgen der zunehmenden Digitalisierung von Fahrzeugen. Auf Österreichs Straßen läuft laut „Aktionsplan autonomes Fahren" seit Herbst 2016 ein Testbetrieb mit (teil)autonomen Fahrzeugen. Der elektronische Unfall-Notruf „eCall" ist bei Neuwagenverkäufen seit 2018 fixer Ausstattungsbestandteil von PKWs. Eine Vielzahl an elektronischen Assistenzsystemen überwacht bereits jetzt täglich die Fahrt: Einige Mercedes-Typen protokollieren den Standort alle 2 Minuten; BMW erfasst die letzten 100 Abstellpositionen und Renault kann das Laden der Antriebsbatterie aus der Ferne unterbinden (der deutsche Verkehrsclub ADAC vermutet, dass Leasinggeber künftig über Fernabschaltungen Zahlungssäumnis sanktionieren könnten).

Hersteller verbauen jedenfalls immer mehr Sensoren in den Fahrzeugen, mit deren Hilfe die Umwelt besser erfasst werden soll. Computer übernehmen die Auswertung der Sensordaten und steuern damit elektronische „Gehilfen", die während der Fahrt Entscheidungen selbst treffen, um die FahrerInnen zu entlasten und längerfristig gänzlich überflüssig zu machen. Daten werden gesammelt, um auf etwas aufmerksam zu machen (zB beim Totwinkel-Assistenten), Servicewerkstätten Anhaltspunkte für den Reparaturfall zu liefern (zB Motordaten, Füllstände, Batterieladung) oder in den Betrieb einzugreifen (zB der „Aufmerksamkeitsassistent", der Lenkfehler korrigiert). Sie gelten als erste Automatisierungsstufe auf dem Weg zu vollständig autonomen Fahrzeugen.

Die Studie beschreibt den Status quo sowie künftige Entwicklungen und fasst Fragen zum Konsumenten- und Datenschutz zusammen, die sich aus der zunehmenden Digitalisierung von Autos ergeben:

- **Transparenz:** Fraglich ist, ob KäuferInnen noch beurteilen können, was sie kaufen. Wie nachvollziehbar sind die Abläufe in einem „Computer auf vier Rädern", dessen Funktionsweise sich KonsumentInnen nicht mehr erschließt.

- **Wie viel Ware oder Dienstleistung steckt im Auto:** Welche Bestandteile eines Autos sollten unveränderlich sein, und wo greifen Hersteller nach dem Kauf vielleicht noch ein? Was bleibt vom Warenkauf übrig und was wird laufende Dienstleistung sein? Brauchen Autos künftig wöchentliche Updates über eine Internetverbindung? Wie lange müssen Hersteller die Software in ihren Fahrzeugen warten, bevor deren „Lebensende" erreicht ist und man sich ein neues Auto kaufen muss, weil es für das alte keine Sicherheitsupdates mehr gibt.

- **Datenschutz:** Aufenthaltsort, Fahrweise, Autozustand, Nutzungsprofil des Fahrers, Fehlleistungen. Wie zuvor Handy und PC dürfte als nächstes das Auto im großen Stil Konsumentendaten liefern. Daten können mit Versicherungen, Pannendiensten oder Werkstätten und bald auch mit anderen Autos (zB Hinweis auf Fahrbahnzustand oder verfügbare Parkplätze) ausgetauscht werden. Es lassen sich präzise Bewegungsprofile erstellen, die viel über Lebensgewohnheiten verraten. Hersteller, Versicherungen, Werbefirmen, Arbeitgeber, Aufsichts- und Sicherheitsbehörden, Verkehrsplaner oder auch nur kriminelle Hacker – alle werden nach und nach von den wachsenden Datenbergen in Autos profitieren wollen.

- **Freie Werkstättenwahl:** Autos werden möglicherweise vergleichsweise billig sein, das vorgeschriebene Service dafür aber sehr teuer. Es ist vorstellbar, dass Reparaturen und Wartungsarbeiten nur in bestimmten Markenwerkstätten unter Verwendung teurer Markenersatzteile erfolgen dürfen.

- **Haftung:** Die Regelung, wonach Fahrzeughalter verschuldensunabhängig für Schäden Dritter haften, greift zu kurz, wenn sich Autos nicht mehr leicht kontrollieren lassen. Diese Frage wird schon für hochautomatisiert fahrende Autos zu klären sein. Bei einer Umstellung von menschlicher auf algorithmische Entscheidungsfindung entstehen auch moralische Dilemmata etwa in Bezug auf das Unfallverhalten. Für autonome Fahrzeuge muss es deshalb auch Anweisungen für kritische Situationen mit möglichen Personenschäden geben.

Aus Verbrauchersicht lassen sich ua folgende Anliegen zusammenfassen:

- KonsumentInnen müssen noch in jeder Hinsicht autonom über das gekaufte Produkte verfügen können;

- Eigentum haben an allen eingebauten Softwarekomponenten;

- ein uneingeschränktes Selbstbestimmungsrecht haben über alle Daten, die das gekaufte Produkt erzeugt;

- ohne jeden Zwang darüber entscheiden können, ob und wem sie diese Daten zugänglich machen;

- ihre Werkstätten in jeder Hinsicht frei wählen dürfen; nicht gezwungen sein, Koppelungsverträge zu akzeptieren (Warenkauf plus Wartungs- und Serviceverträge bzw Versicherungsangebote, die ein Tracking der Produktbenutzung beinhalten)

- und darauf vertrauen dürfen, dass der Hersteller oder Verkäufer sich nicht auf Haftungs- und Gewährleistungsausschlüsse berufen kann, wenn der Verbraucher sich seine Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht.

Renate Anderl
Präsidentin
FdRdA

Melitta Aschauer-Nagl
iV des Direktors
FdRdA