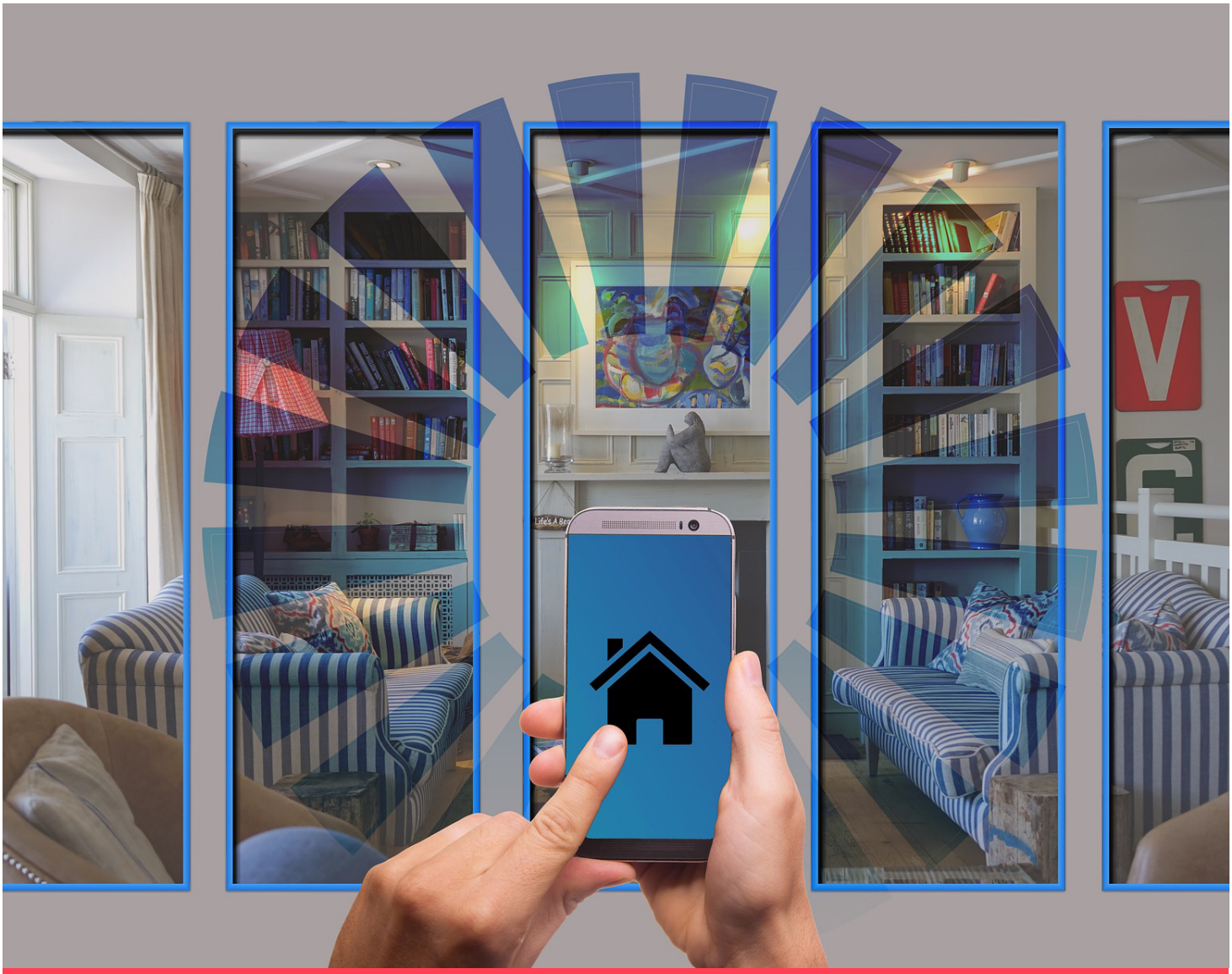
AK EUROPA

Positionspapier
Februar 2021
KonsumentInnen



Internet der Dinge – Erwartungen aus Sicht der VerbraucherInnen

Zusammenfassung

Bereits 2014 warnte eine AK-Studie (Kommerzielle digitale Überwachung von KonsumentInnen im Alltag, Wolfie Christl - Cracked Labs Institut für kritische digitale Kultur) vor den (un-)absehbaren Folgen des Internet der Dinge (Internet of Things "IoT") für die Privatsphäre der NutzerInnen. E-Book-Reader und vernetzte TV-Geräte senden Daten zum NutzerInnenverhalten 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. 2020 sollen nach Schätzungen der EU-Kommission weltweit bereits über 50 Milliarden IoT-Geräte in Betrieb sein. Ein Rechtsrahmen, der KonsumentInnen angemessen vor den Gefahren vernetzter Gegenstände schützt, ist allerdings nicht in Sicht.

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 VerbraucherInnenpolitik dürften viele der offenen Fragen zu Datenschutz und Datensicherheit, aber auch fairer Vertragsgestaltung ohne Rücksicht auf VerbraucherInnenpositionen im Sinne der Hersteller beantwortet werden.

Zum Handlungsbedarf

Insgesamt zeichnet sich ein krasses informationelles und vertragliches Ungleichgewicht in den Rechtspositionen zwischen den an IoT beteiligten AnbieterInnen und ihren KundInnen ab. Die AnbieterInnenseite

- 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, uvm) 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.

Die wichtigsten AK-Forderungen

KonsumentInnen müssen:

- In jeder Hinsicht autonom über das gekaufte Produkt verfügen können
- Eigentum an allen eingebauten Softwarekomponenten haben
- Ein uneingeschränktes Selbstbestimmungsrecht über alle Daten haben, die das gekaufte Produkt erzeugt
- Ohne jeden Zwang darüber entscheiden können, ob und wem sie diese Daten zugänglich machen
- Ihre Werkstätten und Serviceanbieter in jeder Hinsicht frei wählen dürfen und nicht gezwungen sein, Koppelungsverträge zu akzeptieren
- 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
- Das Wahlrecht haben: Produkte müssen (de-) aktivierbare IoT-Funktionen haben

Die Position der AK

1. Warum ist eine eingehende Befassung mit den Folgen des Internet der Dinge für VerbraucherInnen nötig?

Erste Sicherheitspannen, Verletzungen der Privatsphäre und signifikante Machtungleichgewichte bei der Vertragsgestaltung illustrieren, dass die Vernetzung aller Alltagsdinge für VerbraucherInnen 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 VerbraucherInnenprobleme, die ohne Schutzmaßnahmen in Zukunft gängiger werden dürften. Im Infotainmentsystem einiger Autotypen (zB UConnect von Fiat Chrysler) klafften laut Sicherheitsforschern kritische Schwachstellen, durch die HackerInnen das Fahrzeug komplett fernsteuern konnten („HackerInnen steuern Jeep Cherokee fern“ Heise.de). Auch das Bordsystem von BMW (ConnectedDrive) fand seinen Weg in die Schlagzeilen, nachdem es SicherheitsexpertInnen im Auftrag des deutschen Verkehrsclubs ADAC gelang, bspw. die Türverriegelung der Fahrzeuge unberechtigterweise von der Ferne aufzuschließen.

- **Vertragsrisken**: Der US-Traktorenhersteller John Deere versucht, seinen Kunden das Eigentum an ihren Maschinen abzusprechen. Über Geschäftsklauseln und den Gerichtsweg sollen NutzerInnen davon abgehalten werden, ihre hochmodernen Traktoren zu reparieren, vor allem umzuprogrammieren. Eine selbstbestimmte Reparatur wird bei stark softwarebasierten 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 BäuerInnen wird weder Zugriff auf Original-Teile noch auf die Software gestattet.

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

- **Überwachung “zum Quadrat“**: Jeder Berührungspunkt mit smarten Geräten hinterlässt persönliche Datenspuren, die in umfassenden Nutzungs- und Standortprofilen münden können. Die mit dem Tracking von PC- und HandynutzerInnen begonnene Entwicklung der Überwachung der Alltagshandlungen und Alltagsgeschäfte von VerbraucherInnen erlangt mit IoT eine neue Dimension. Die Schnittstellen mit dem Internet, an denen VerbraucherInnenverhalten 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 u.v.m.

- **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 Entwicklungsrisken, 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 Datenschutzsicht unsicheren Produkten dienen.

- **Nutzungslizenz statt Eigentum, Kaufvertrag versus Urheberrecht:** KonsumentInnen entrichten zwar einen „Kaufpreis" und vermeinen damit, EigentümerInnen 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 softwaredominiert und steht unter Eigentumsvorbehalt der AnbieterInnen. Der bestimmungsmäßige Gebrauch wird durch Lizenzen geregelt. Was NutzerInnen damit anfangen können oder nicht, regeln die AnbieterInnen einseitig zu ihren Gunsten vertraglich und über technische Schranken (Digital Right Management Systeme). Daraus ergeben sich 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 NutzerInnen alternativlos an sich zu binden.

  - AnbieterInnen 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.

2. Die Rolle der EU

Die im März 2019 beschlossene EU-Warenhandels-Richtlinie bringt nicht den erhofften Schutz:

- **Einbeziehung von IoT in den Anwendungsbereich:** Waren, die der RL unter-liegen, 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, ob digitale Inhalte oder Dienste von VerkäuferInnen oder Dritten bereitgestellt werden.

  Kritisch anzumerken ist: Mit dieser komplizierten Definition sollen die Anwendungsbereiche der RL für den Warenhandel und der nahverwandten Richtlinie über digitale Inhalte voneinander abgegrenzt werden. Unzureichend, wie die AK 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 RL zu digitalen Inhalten). Damit würden AnbieterInnen allein durch die Wahl des Abschlusses von einem oder zwei Verträgen entscheiden, welches Recht anzuwenden ist.

- **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 VerbraucherInnenschutz bei IoT sein. Die vagen Kriterien werden 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 können VerbraucherInnen „vernünftigerweise" noch „erwarten", wenn eine Branche KonsumentInnen bestimmte (bei traditionellen Käufen vorausgesetzte) „Funktionalitäten" und „Kompatibilitäten" bei IoT vorenthält?

- **Updates**. VerkäuferInnen von Waren mit digitalen Elementen sollen dafür sorgen, dass VerbraucherInnen „über Aktualisierungen, einschließlich Sicherheits-Updates, die für den Erhalt der Vertragsmäßigkeit der Waren erforderlich sind, informiert werden und solche erhalten". Die in der Praxis so entscheidende Frage: „wie lange?" beantwortet die Richtlinie wiederum äußerst vage: Während des Zeitraums, in dem VerbraucherInnen „vernünftigerweise" Updates erwarten können (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/e KonsumentIn, Updates zu installieren, so haften VerkäuferInnen grundsätzlich nicht für dadurch bedingte Vertragswidrigkeiten.

  Kritisch anzumerken ist: KonsumentInnen werden erst aufgrund von produktspezifischen Gerichtsentscheidungen wissen, was sie von dem/der AnbieterIn erwarten dürfen. AnbieterInnen von Dauerschuldverhältnissen wiederum können längere Fristen als zwei Jahre dadurch umgehen, dass sie den VerbraucherInnen 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.

3. Beispiele für Verbraucherrisiken

3.1. Vom Assistenzsystem zum Autopiloten – Vernetzte Fahrzeuge

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 (zB 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 von den HerstellerInnen abrufbar.

Je höher der Automatisierungsgrad, desto mehr Daten mit und ohne Personenbezug benötigt das Fahrzeug. Für manche Datenarten lässt sich kaum ein legitimer Zweck finden, etwa wenn es um die Profilerstellung der NutzerInnen 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 KonsumentInnen ausgelesen werden.

Aktuell bieten die HerstellerInnen (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 jede/r BesitzerIn frei entscheiden, ob sie/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 AutoherstellerInnen sehen ihre Umsatzerwartungen in der Autoproduktion schwinden und verlegen ihre Anstrengungen auf KundInnenbindung durch Services, die auf Abonnementzahlungen beruhen. Das wirtschaftlich erfolgreiche geschlossene Ökosystem von Apple dient dabei als Vorbild. Im ungünstigsten Fall werden KundInnen künftig vom Abschleppservice über Versicherungen und den Assistenten für (teil) autonomes Fahren bis hin zur Wartung fix an die Hersteller gebunden sein.

Für weiterführende Informationen, siehe die AK-Studie „Vernetzte Automobile".

3.2. Onlinezwang und löchrige Privatsphäre bei Spielen

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 VerbraucherInnen nur die Wahl des „take it – or leave it" (Akzeptiere oder verlasse das Angebot) haben.

Für weiterführende Informationen, siehe die AK-Studie „Privatsphäre in Online-Spielen".

3.3. Smart Home

Smart Home gilt als eines der großen Hoffnungsgebiete von IoT. Die AnbieterInnen 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.

3.4. 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. AnbieterInnen sollen durch Fernein- 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 bescheiden aus, bedenkt man, dass Heizung und Warmwasser die entscheidenden Energieverbraucher sind. Wesentlich größer ist hingegen die Sorge der VerbraucherInnen 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 Studie der FH Münster), die folgende Dateninteressenten ausmacht: Werbewirtschaft für gezielte Werbung, Versicherungen, um zu prüfen, ob Geräte beim Verlassen des Heims ausgeschaltet waren, Überwachung im Rahmen eines PartnerInnenstreits und von Zivilrechts-oder Strafverfolgung (VermieterIn: Wohnung bewohnt? Leben mehr Personen als angegeben in der Wohnung? Sorgerechtsstreit: werden Kinder alleine gelassen? Strafrechtsbehörden: Alibi-Überprüfung uvm). 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.

3.5. 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. 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 der NutzerInnen wie Alter, Geschlecht, Größe, Gewicht) in der – nicht unbedingt in jeder Hinsicht sicheren – Cloud.

4. Forderungen in Bezug auf IoT

- Die **e-Privacy Richtlinie** entspricht nicht mehr dem aktuellen Schutzbedarf der KonsumentInnen gegen Überwachung ihres Verhaltens im Internet. Mit der Nachfolgeverordnung 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 erst geklärt werden. Inzwischen bringen sich einige IoT-HerstellerInnen und SoftwarelieferantInnen bereits mit ihrer verbraucherInnenunfreundlichen Haltung in Stellung: Betriebsdaten gehören ihrer Ansicht zufolge der produzierenden Wirtschaft und können wie sonstige urheberrechtliche Werke auch veräußert und lizensiert werden.

- **Produkthaftungsrichtlinie**: 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. Entsprechend ungeeignet ist der Rahmen, adäquate Antworten auf komplexe Haftungsfragen zu IoT zu geben. Auf den Anpassungsbedarf weist auch ein im Auftrag des deutschen Verbraucherverbands VZBV erstelltes Gutachten hin

  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 geben. Bei bestimmungsgemäßen Gebrauch sollte die Beweislast auf der AnbieterInnenseite 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 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 von AnbieterInnen ersetzt werden.
  Mit Blick auf das Insolvenzrisiko von AnbieterInnen 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.

4.1. IoT Sicherheit

- 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 von HerstellerInnen und den Softwarelieferanten beherrscht werden.
- Solange es keine verbindlichen Normen zur IT-Sicherheit gibt, dürfen unklare Haftungssituationen nicht zulasten geschädigter KonsumentInnen gehen. So weist der EU-VerbraucherInnenverband 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.
- Es müssen nationale Aufsichtsbehörden bestimmt werden, die gegebenenfalls gefährliche Produkte vom Markt rasch entfernen können.

4.2. 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 Werknutzungsrechten 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. Gegen das sich abzeichnende Ungleichgewicht von Rechten und Pflichten der VertragspartnerInnen besteht ein Handlungsbedarf der GesetzgeberInnen.
EigentümerInnen können andere vom Zugriff auf ihr Eigentum in der Regel ausschließen. UrheberrechtsinhaberInnen können hingegen LizenzerwerberInnen 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. Die EigentümerInnenrolle der KonsumentInnen ist deshalb unbedingt zu stärken.

4.3. 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". Offeriert wurde nur ein limitiertes Set an Antworten (Herstellende, SoftwarelieferantInnen, usw). KonsumentInnen standen 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 ExpertInneneinschätzung nicht (oder doch) personenbezogen sind. Wann Daten als verlässlich anonymisiert gelten, ist rechtlich abzusichern. Außerdem sollten KonsumentInnen 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.

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“).

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. Da Grundrechte unveräußerlich sind, sollte diesem Abtausch zumindest enge Grenzen gezogen werden.

4.4. 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, usw 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 VerbraucherInnen sich gegenüber IoT-Kleingedruckten anders verhalten als bei herkömmlichen Gütern: durch Nichtbeachtung des Inhalts und bestätigenden Klick, alles zur Kenntnis genommen zu haben.

Die verbraucherInnenpolitische Maxime der vergangenen Jahrzehnte, dass VerbraucherInnen zu selbstbestimmten, informierten Personen werden, wenn ihnen detallierte Informationen zugänglich sind, ist überholt. Die Gesetzgebung muss ihrer Fürsorgefunktion in Bezug auf Übervorteilungen, Manipulationen und Irreführungen besser nachkommen. Dazu könnten u.a. zählen: gestärkte Datenschutzbehörden, wettbewerbsrechtliche Verfolgung des Aus-nutzens von Marktdominanz für missbräuchliche Datennutzung usw.

4.5. 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 VerbraucherInnen 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 VerbraucherInnen, ob sie die Durchführung eines Updates zulassen. Die Verankerung detaillierter Informationspflichten zu Updates wäre ein wichtiger Beitrag dazu, dass VerbraucherInnen sicherheitsrelevante Aktualisierungen weder vernachlässigen noch unerwünschte Änderungen aus bloßer Uninformiertheit und Unsicherheit über die Folgen authorisieren.

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

Kontaktieren Sie uns!

In Wien:

Daniela Zimmer
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brüssel:

Alice Wagner
T +32 (0) 2 230 62 54
alice.wagner@akeuropa.eu

AK EUROPA
Ständige Vertretung Österreichs bei der EU
Avenue de Cortenbergh 30
1040 Brüssel, Belgien
T +32 (0) 2 230 62 54

www.akeuropa.eu

Über uns

Die Bundesarbeitskammer (AK) ist die gesetzliche Interessenvertretung von rund 3,8 Millionen ArbeitnehmerInnen und KonsumentInnen in Österreich. Sie vertritt ihre Mitglieder in allen sozial-, bildungs-, wirtschafts- und verbraucherpolitischen Angelegenheiten auf nationaler sowie auch auf der Brüsseler EU-Ebene. Darüber hinaus ist die Bundesarbeitskammer Teil der österreichischen Sozialpartnerschaft. Die AK ist im EU-Transparenzregister unter der Nummer 23869471911-54 registriert.

Die Aufgaben des 1991 eröffneten AK EUROPA Büros in Brüssel sind einerseits die Repräsentation der AK gegenüber europäischen Institutionen und Interessensorganisationen, das Monitoring von EU-Aktivitäten und die Wissensweitergabe von Brüssel nach Österreich, sowie gemeinsam mit den Länderkammern erarbeitete Expertise und Standpunkte der Arbeiterkammer in Brüssel zu lobbyieren.