Bereich Bildung, Wien, Konsumenten – Aschauer-Nagl
Konsumentenpolitik – Daniela Zimmer

TOP 3.4.8 Mehr Konsumentenschutz fürs „Internet der Dinge"

Hintergrund

Das Internet der Dinge gilt als nächster Entwicklungsschritt des Internets: Alltagsgegenstände der realen Welt sind virtuell miteinander verbunden. „Smarte", „intelligente" Produkte, wie Autos, Kühlschränke, Heizungen, Puppen, Uhren, Zahnbürsten u.v.m. sind mit Sensoren ausgestattet, rund um die Uhr online und tauschen auch untereinander Informationen aus. Die Geräte sammeln permanent Betriebsinformationen und damit Verhaltensdaten über NutzerInnen. Die dabei erzeugten Daten werden mithilfe von Software-Algorithmen ausgewertet. Dadurch kann auch eine vordefinierte Aktion ausgelöst werden (Funktionen im Haushalt ein- und ausschalten, automatische Nachbestellung knapper Haushaltsgüter, Erinnerungsmeldungen u.v.m.). Unternehmen, Wissenschaft, aber auch Kommunen erhoffen sich zudem, aus den in den Haushalten anfallenden Daten strategisch nützliche Prognosen, Erkenntnisse und Optimierungen ableiten zu können. Überwachung und Kommerzialisierung durchdringen so letzte, geschützte Bereiche der Privatsphäre.

Das Schutzbedürfnis privater Haushalte illustriert „Cayla", „die Spionin im Kinderzimmer". Sie sei "fast wie eine richtige Freundin", steht auf der Produktwebsite jener Puppe, die via Bluetooth-Verbindung und Spracherkennung auf Fragen antwortet und Unterhaltungen zwischen Kind und Puppe an den US-Hersteller weiterleitet. Sie steht beispielshaft für jene Probleme, die mit vernetzten Haushaltsgeräten verbunden sein können: versteckte Abhöreigenschaft und Intransparenz der Empfänger bzw Nutzungszwecke der Daten. Ein leichtes Hacking-Opfer ist die Puppe aufgrund ungesicherter Verbindungen auch. Amazons Echo Box ist ein „intelligenter" Lautsprecher und Sprachassistent. KonsumentInnen können über ihn per Sprachbefehl Musiktitel abspielen und Antworten auf Wissensfragen (wie hoch ist der Mount Everest...) finden. Das Gerät eignet sich aber auch für Lauschangriffe, da grundsätzlich alles aufgezeichnet werden kann, was im Wohnraum besprochen wird.

Wie dem Verbraucherschutz in einer völlig vernetzten Alltagswelt am besten Rechnung getragen werden kann, muss bald geklärt werden, fordert die AK. Wer haftet etwa, wenn bei einem intelligenten Gerät Defekte auftreten und Schäden verursacht werden? Das ist bei einem Produkt, in das Sensoren und Software unterschiedlichster Hersteller eingebettet sind, keine triviale Frage.

Was macht die AK:

- Schon 2014 erschien die medial viel beachtete AK-Studie „Kommerzielle digitale Überwachung im Alltag - Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data" (Autor Wolfie Christl; https://media.arbeiterkammer.at/PDF/Digitale_Ueberwachung_im_Alltag.pdf)

- Die AK bringt sich in die EU-Diskussion ein. Die EU-Kommission befragte 2017 im Rahmen der Konsultation „Aufbau einer europäischen Datenwirtschaft" Anbieter wie Verbraucherorganisationen nach ihren Wünschen zu einem Rechtsrahmen für Produkte mit integrierter Software und Sensoren. Im Mittelpunkt stand die Frage: Wie soll künftig mit den Betriebsdaten smarter Geräte vor allem in Hinblick auf das Eigentum, den Zugriff, ihre Weiterverwendung für andere Zwecke, der Übertragbarkeit und Haftung umgegangen werden.

- Für die AK-Publikationsreihe „digital - policy papers" wurde das Thema mit dem Ziel aufbereitet, Problembewusstsein zu schaffen und Handlungsempfehlungen zu geben.

- Mit Andrus Ansip, dem **Vizepräsidenten** der Europäischen Kommission und Kommissar für den digitalen Binnenmarkt, wurden bei seinem Besuch im Juni in Wien (Sozialpartnergespräch im Haus der EU) die offenen Fragen erörtert und ihm ein AK-Forderungspapier übergeben. Ansip unterstrich dabei die Bedeutung des Themas, wies aber darauf hin, dass die Kommission für einen Richtlinienvorschlag noch Zeit brauche. Vor allem die Frage der Zurechnung der Verantwortlichkeit sei nicht abschließend geklärt.

AK-Forderungen:

- **Gerätedaten „gehören" den NutzerInnen:** Von Geräten erzeugte Metadaten (Verbindungs- und Standortdaten, IP-Adresse usw) wirken nicht wie personenbezogene Daten. Der Eindruck täuscht aber. Oft sind Zuordnungen zu einer Person möglich. Weisen Gerätedaten einen Personenbezug auf, dann darf nur die/der KonsumentIn über ihre Verwendung entscheiden. Ob und wie das Internet der Dinge mit dem Grundrechtsprinzip der Datensparsamkeit zu vereinbaren ist, ist zu klären. Big Data-Analysten dürfen sich nicht auf Geschäftsgeheimnisse berufen: Die hinter Datenanalysen mit Algorithmen stehenden Regeln und Datenarten sind KonsumentInnen verständlich zu erklären. Die Methoden müssen durch unabhängige Aufsichtsstellen („Algorithmen-TÜV") auf Rechtskonformität geprüft werden.

- **Produkthaftung für digitale Güter:** Die Produkthaftungsregeln müssen auf digitale (unkörperliche) Waren und Dienste ausgedehnt werden. Dem Verbraucher kann bei Produkten mit Komponenten verschiedenster Hersteller im Schadensfall nicht zugemutet werden, den Hauptverantwortlichen herauszufinden. Jeder potentiell verantwortliche Gerätehersteller bzw Softwarelieferant sollte deshalb gesamtschuldnerisch gegenüber dem Verbraucher haften. Regressansprüche der beteiligten Unternehmen untereinander bleiben unberührt.

- **„Updates":** KonsumentInnen haben bei Software-Aktualisierungen wenig Rechtssicherheit bezüglich ihrer Rechte und Pflichten. So fehlen: ein Mindestzeitraum für die Lieferverpflichtung funktionell wichtiger Updates nach dem Gerätekauf, transparente Infos über den Inhalt von Updates (sicherheitstechnisch nötig, optional, funktionsändernd oder -erweiternd), Klärung der Mitverantwortung, wenn wichtige Updates von KonsumentInnen nicht durchgeführt werden usw.

- **Wettbewerbs- und Verbrauchervertragsrecht**: KonsumentInnen müssen in jeder Hinsicht autonom über das gekaufte Produkt verfügen können. Sie dürfen bspw nicht gezwungen werden, nur vom „smarten" Produktanbieter Services zu beziehen. Sie müssen Eigentum an allen eingebauten Softwarekomponenten erwerben. Sie sollen ihre Werkstätten in jeder Hinsicht frei wählen dürfen und nicht gezwungen sein, Koppelungsverträge zu akzeptieren (Warenkauf plus Wartungs- und Serviceverträge, Versicherungen, Drittanbieterdienste). Smarte Geräte selbst zu reparieren, muss zulässig sein. Anbieter dürfen sich auch nicht auf Haftungs- und Gewährleistungsausschlüsse berufen, wenn der Verbraucher sich seine Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht.