ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
ITA – INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

An den
Nationalrat/Ausschuss für Konsumentenschutz
Per E-mail

2.5.2019
Dr. WalterPeissl | wpeissl@oeaw.ac.at | 6584

Betreff: Ausschuss für Konsumentenschutz;
Ersuchen um Stellungnahme zu den Anträgen 102/A(E) und 105/A(E)

Das Institut für Technikfolgen-Abschätzung (ITA) der Österreichischen Akademie der Wissenschaften wurde zur Stellungnahme zu den Anträgen 102/A(E) und 105/A(E) eingeladen und führt dazu aus:

Zweifellos ist die Verwirklichung der Vision des Internet of Things (IoT) eines der Ziele der zunehmenden Vernetzung und Digitalisierung vieler Lebensbereiche. Durch die Kopplung autonomer Systeme, die auf Basis algorithmischer Entscheidungen untereinander kommunizieren, entstehen Netzwerke hoher Komplexität und damit einhergehender Verwundbarkeit. Gleichzeitig werden dabei digitale Endgeräte in Bereichen eingesetzt und vernetzt, in denen es bislang kaum solche gab und entsprechend wenig Bewusstsein über mögliche Folgen und auch geringes professionelles Wissen der NutzerInnen/KonsumentInnen zum Umgang mit digitaler Technik gibt. Daraus entstehen neue Herausforderungen für den Konsumentenschutz. Bestehende Datenschutzregelungen sind wichtige Bestandteile für den Schutz von KonsumentInnen. Es ist daher davon auszugehen, dass Datenschutzaspekte vernetzter Geräte im Bereich des IoT künftig einen noch höheren Stellenwert im Rahmen des Konsumentenschutzes einnehmen werden. Hinzu kommt, dass die mit dem IoT einhergehende Zunahme an digital vernetzten Geräten und Systemen auch massive Sicherheitsprobleme mit sich bringt.[1] Das gilt nicht nur für mögliches Ausnützen von Sicherheitslücken durch Kriminelle sondern auch durch systembedingte Schwachstellen, die zu Kaskadeneffekten und damit zu gravierenden Sicherheitsproblemen führen können. IT-Sicherheit wird also zu einem zentralen Thema. Erste Ansätze dazu gibt es im Rahmen der ETSI TS103645 mit Guidelines für Cyber Security for Consumer Internet of Things.[2] Diese sollten als Startpunkt gesehen und weitere regulatorische Aktivitäten gestärkt werden.

Für die einzelnen KonsumentInnen ist es kaum möglich, in vernetzten Systemen Übersicht und Kontrolle zu behalten und alle möglichen Konsequenzen abzuschätzen. Die zentrale Institution des „informed consent" – die bewusste Zustimmung – ist unabdingbar für den Datenschutz, allerdings als einziger Schutzmechanismus allei-

[1] Das ITA hat im Jahre 2017 einen Bericht zum Digitalen Stillstand erarbeitet, der die Verletzlichkeit der digital vernetzten Gesellschaft am Beispiel kritischer Infrastrukturen beleuchtet: Strauß, Stefan; Krieger-Lamina, Jaro (2017) Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Projekt-Endbericht. Bericht-Nr. ITA 2017-01; Institut für Technikfolgen-Abschätzung: Wien; im Auftrag von: Präsidium der Österreichischen Akademie der Wissenschaften, http://epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf.
[2] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

WWW.OEAW.AC.AT/ITA
APOSTELGASSE 23 | 1030 WIEN, ÖSTERREICH
T: +43 1 51581-6582 | F: +43 1 51581-6570 | TAMAIL@OEAW.AC.AT
IBAN: AT541100000262650519 | BIC: BKAUATWW | UID: ATU37116303

ne unzureichend. Aus dieser Perspektive ergibt sich eine erhöhte Regelungsnotwendigkeit auf gesellschaftlicher Basis. Es erscheint angezeigt, bestehende Konsumentenschutz-Regelungen zu evaluieren und zu überprüfen, inwieweit die Durchsetzbarkeit bestehender Bestimmungen gegeben ist, sowie diese bei Bedarf den neuen Gegebenheiten der digitalen Konsumwelt anzupassen und entsprechende Kontrollmechanismen einzuführen. Insbesondere scheint es geboten, Produkthersteller stärker in die Pflicht zu nehmen sowie Datenschutz und Sicherheit in der Produktentwicklung stärker als bislang zu gewährleisten.

Die Durchdringung mit Produkten des IoT in privaten Anwendungen wird sehr stark von Technologieanbietern und Plattformen geprägt sein. Die Durchsetzung nationaler Regelungen wird, wie auch in anderen Bereichen, an Grenzen stoßen. Deshalb erscheint eine Politik im europäischen Gleichklang mit nationalen Adaptionen vielversprechend. Eine Option, um frühzeitig im Entwicklungsprozess schon Wirkung zu entfalten, wäre die Etablierung einer „digitalen Produkthaftung" für Endgeräte und vernetzte Systeme. Diese „digitale Produkthaftung" – als spezifische Produkthaftung für vernetzte digitale Geräte, könnte Fragen des Schutzes der Privatsphäre, der IT-Sicherheit, aber auch möglicher ungewollter Folgewirkungen bestimmter Anwendungen abdecken und den Herstellern und Service-Providern ein höheres Maß an Verantwortung übertragen. Vorstellbar ist, IoT-Produkte dahingehend stärker zu regulieren, dass die Funktion eines Produkts nicht zwangsläufig zu einer Datenvernetzung führen darf. D.h. IoT-Produkte wären von den Herstellern so zu gestalten, dass Datenschutz-Prinzipien wie Datensparsamkeit, Zweckbindung usw. maximal und sorgfältig gewahrt bleiben. Die Funktionsfähigkeit eines Produkts sollte nicht an die Sammlung personenbezogener Daten gekoppelt sein, d.h. das Produkt müsste auch anonym nutzbar und die Möglichkeiten dazu müssten für KonsumentInnen klar, verständlich und einfach anwendbar sein. Zum Beispiel wäre zu begründen, wofür eine digitale Zahnbürste einen WLAN-Anschluss braucht. Jedenfalls sollte gefordert sein, dass sie nicht dazu genutzt wird, die Gewohnheiten der sie benutzenden Person(en) auszuspionieren. IoT darf also nicht zu Überwachung von Individuen, Gruppen oder Haushalten missbraucht werden.

Um das Wissen und das Bewusstsein um die möglichen Folgen überbordender Vernetzung und Datafizierung zu erhöhen, sind ein breiter gesellschaftlicher Dialog und Aufklärung über den Wert des Privaten notwendig.

Speziell zu Smart Cars (betrifft 105/A(E)) hat das ITA im Jahre 2016 eine Studie[3] erstellt und unter anderem folgende Empfehlungen abgegeben:

- Breiter öffentlicher Diskurs über offene Fragen.
- Aktive und antizipierende Regulierung auf europäischer Ebene, um den Bedürfnissen nach Konsumenten- und Datenschutz nachzukommen sowie um Haftungsfragen zu klären und so nicht nur die Rechtsdurchsetzung zu vereinfachen, sondern auch die Akzeptanz in der Bevölkerung zu erhöhen.
- Besondere Bedeutung der Sicherheit der IT-Systeme – Security by Design.
- Datenschutzprinzipien wie Transparenz, Zweckbindung, Datensparsamkeit und informationelle Selbstbestimmung sollten mehr beachtet werden.
- Mehr Ressourcen für die Datenschutzbehörde, damit diese ihren Aufgaben nachkommen kann.
- Entscheidungen durch Algorithmen: Diskussion ethischer Fragen, Verhindern eines möglichen Bias in den Systemen zuungunsten der KonsumentInnen

Für das ITA: Dr. Walter Peissl, stv. Direktor

[3] Krieger-Lamina, Jaro, 2016, Vernetzte Automobile. Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. Endbericht. Bericht-Nr. 2016-02; Institut für Technikfolgen-Abschätzung (ITA): Wien; im Auftrag von: Bundesarbeitskammer, http://epub.oeaw.ac.at/ita/ita-projektberichte/2016-02.pdf.