Bundesministerium
Arbeit, Soziales, Gesundheit
und Konsumentenschutz

sozialministerium.at

BMASGK – III (Konsumentenpolitik)

Mag. Christian Palmetzhofer
Sachbearbeiter III/5

Stubenring 1, 1010 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an post@sozialministerium.at zu richten.

Parlamentsdirektion
Dr.-Karl-Renner-Ring 3
1017 Wien

Geschäftszahl: BMASGK-90180/0016-III/2019

Ausschuss für Konsumentenschutz, Ersuchen um Stellungnahme zu den Anträgen 102/A(E) "Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes" und 105/A(E) "Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes - insbesondere der Smart-Cars" | Stellungnahme

Das Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz nimmt zum oben angeführten Ersuchen wie folgt Stellung:

Unter Internet of Things (Internet der Dinge, IoT) wird im engeren Sinn die zunehmende Vernetzung und Internetfähigkeit von Produkten verstanden; weiter definiert versteht man darunter alle Vernetzungstechnologien, die letztlich die Kommunikation und das Zusammenspiel von Gegenständen ermöglichen. Dies nicht nur für den eigentlichen Bereich der Telekommunikation wie etwa Smartphones oder für Produkte, bei denen Konnektivität eine wesentliche Voraussetzung ihrer Funktonalität ist, sondern auch für Produkte, deren Grundfunktionen ohne diese Konnektivität verfügbar wären (zB Kühlschrank, Waschmaschine, Fahrzeuge...). Es ist abzusehen, dass der Vertrieb von vernetzten Alltagsgeräten, die das Leben leichter machen sollen, wie zB „smarte" Kühlschränke oder internetfähige elektrische Zahnbürsten, rasch ansteigen wird.

Aus verbraucherpolitischer Sicht stehen folgende Problembereiche im Vordergrund:
- (Technische) Sicherheit im Hinblick auf Informationstechnologie

- Haftungsfragen
- Gewährleistung
- Datenschutz
- Information und Aufklärung über Rechte der Bürgerinnen und Bürger beim Datenschutz

- Bei der Sicherheit bezüglich Informationstechnologie ist vor allem daran zu denken, dass über simple IoT-Produkte der Einbruch in Netzwerke gelingen kann. Über eine Sicherheitslücke könnten theoretisch nicht nur Zugangsdaten zum jeweiligen Netzwerk ausgelesen, sondern auch die Steuerung von IoT-Geräten von außen übernommen oder zB Bankdaten ausgekundschaftet werden. Dieser Problembereich bedarf daher entsprechender Sensibilität bei den Herstellern, die auch für IoT-Produkte hohe technische Standards anwenden müssen.

Rechtlich ist in diesem Bereich vor allem auf die europäische Funkgeräterichtlinie 2014/53/EU in der Zuständigkeit des Bundesministers für Verkehr, Innovation und Technologie zu verweisen. Sie umfasst unter anderem Fernsehgeräte, Mobiltelefone, WLAN-Einrichtungen, Bluetooth und GPS. Außerdem sind die Richtlinie über elektromagnetische Verträglichkeit (2014/30/EU) sowie die Niederspannungs–Richtlinie (2014/35/EU), beide in der Kompetenz der Bundesministerin für Digitalisierung und Wirtschaftsstandort, relevant.

- Im Zusammenhang mit möglichen Schäden in Folge von Sicherheitslücken bei IoT-Produkten stellen sich freilich auch Haftungsfragen. Die europäische Kommission hat dies erfreulicherweise zum Anlass genommen, sich damit zu beschäftigen, ob der vorhandene Rechtsrahmen, insbesondere die Produkthaftungsrichtlinie 85/374/EWG, angesichts der neuen Herausforderungen des IoT noch ausreichend ist oder einer Überarbeitung bedarf. 2018 hat die Kommission dazu eine Mitteilung veröffentlicht und in Folge auch ein öffentliches Konsultationsverfahren eingeleitet. Welche weiteren Schritte folgen werden, etwa eine Änderung der Produkthaftungsrichtlinie, bleibt abzuwarten. Es spricht aber vieles dafür, dass der Anwendungsbereich der Produkthaftungsrichtlinie in ihrer derzeitigen Fassung zu eng ist. Auch die angesichts auftretender Entwicklungsrisiken zeitlich eingeschränkte Haftung ist hinterfragungswürdig.

- Im Hinblick auf die Rechte der Konsumentinnen und Konsumenten bezüglich mangelhafter „intelligenter" Produkte ist auf zwei neue EU-Richtlinien zu verweisen: die Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs und die Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und

digitaler Dienstleistungen. Die Verhandlungen zu den beiden Richtlinien wurden bereits erfolgreich abgeschlossen, die Veröffentlichung im Amtsblatt der Europäischen Union wird demnächst erfolgen.

Digitale Inhalte sind beispielsweise Applikationen, also so genannte „Apps", außerdem auch Audio- und Videodateien sowie Computerprogramme und -spiele. Der Anwendungsbereich der Richtlinie über digitale Inhalte und digitale Dienstleistungen erstreckt sich neben entgeltlichen Verträgen auch auf Verträge, im Zuge derer Verbraucher/innen personenbezogene Daten bereitstellen. Somit gelten die Gewährleistungsregelungen auch für diese Verträge.

Bei mangelhaften digitalen Inhalten oder Diensten räumt die Richtlinie den Verbraucherinnen und Verbrauchern einen Anspruch auf Preisreduzierung oder die vollständige Rückerstattung des Kaufpreises innerhalb von 14 Tagen ein, wenn es nicht möglich ist, die Mängel innerhalb einer angemessenen Frist zu beheben.

Wenn sich ein Mangel innerhalb eines Jahres nach dem Zeitpunkt der Lieferung bemerkbar macht, wird davon ausgegangen, dass er zum Zeitpunkt der Lieferung bereits bestanden hat, ohne dass der Verbraucher/die Verbraucherin einen Beweis dafür erbringen muss. Das bedeutet eine Umkehr der Beweislast für die Dauer von einem Jahr. Bei fortlaufenden Lieferungen verbleibt die Beweislast überhaupt während des gesamten Vertrags beim Unternehmen. Die Gewährleistungsfrist für einmalige Lieferungen darf nicht kürzer sein als zwei Jahre; für fortlaufende Lieferungen gilt sie während der gesamten Vertragsdauer.

Die Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs zielt darauf ab, ein hohes Verbraucherschutzniveau in der gesamten EU sicherzustellen und Rechtssicherheit für Unternehmen zu schaffen, die ihre Produkte in anderen Mitgliedstaaten verkaufen möchten. Sie vereinheitlicht insbesondere die den Verbraucherinnen und Verbrauchern zur Verfügung stehenden Rechtsbehelfe, wenn ein Produkt nicht ordnungsgemäß funktioniert oder sonst einen Mangel aufweist und darüber hinaus auch die Art und Weise der Ausübung dieser Rechtsbehelfe. Durch die Richtlinie wird die derzeitige Dauer der Beweislastumkehr von sechs Monaten für alle Waren – also auch „nicht intelligente" Produkte – auf ein Jahr ausgedehnt.

Waren mit digitalen Elementen – etwa „intelligente" Kühlschränke, Smartphones, Fitnessuhren und sonstige vernetzte Geräte – fallen ebenfalls unter diese Richtlinie. Konsumentinnen und Konsumenten, die solche Produkte erwerben, haben auf Grund

dieser Richtlinie einen Anspruch auf die erforderlichen Aktualisierungen, also auf Updates der digitalen Inhalte, und zwar während jenes Zeitraums, den man je nach Art und Zweck der Waren und digitalen Elemente angemessen erwarten kann. Für digitale Inhalte außerhalb von Waren sieht die Richtlinie über digitale Inhalte einen vergleichbaren Update-Anspruch vor.

Hinsichtlich der Datenproblematik deckt die EU-Datenschutzgrundverordnung (DSGVO, VO 2016/679) viele der aufgeworfenen Probleme ab. Zu beachten ist, dass die Datenschutzgrundverordnung eine maximale Harmonisierung vorsieht, sodass nationale Regelungen nur sehr eingeschränkt möglich sind. Die Rechtsdurchsetzung und Rechtsfortbildung durch Rechtsprechung auf nationaler und europäischer Ebene ist entscheidend.

Daten, die von IoT-Produkten übermittelt werden, unterliegen der DSGVO. Diese sieht weitreichende individuelle Informations- und Schutzrechte wie Auskunft, Berichtigung oder gegebenenfalls Löschung vor. Daneben bestehen Grundprinzipien, die vorweg ein ausuferndes Datensammeln verhindern sollen. So gilt etwa das Gebot der Zweckbindung, womit Daten nur für festgelegte und eindeutige Zwecke gesammelt werden dürfen. Zu betonen ist insbesondere auch das Gebot der Datenminimierung: Daten dürfen nur soweit erhoben werden, als dies dem Zweck angemessen ist und sie müssen auch auf das notwendige Maß beschränkt werden. Auch die sichere Speicherung ist eine Verpflichtung nach der DSGVO.

Mit dem Grundsatz „privacy by default" soll sichergestellt werden, dass Anwendungen bei der Übergabe an Kunden und Kundinnen datenschutzfreundlich eingestellt sind. Aber auch die technische Ausgestaltung von Produkten, das „privacy by design", ist maßgeblich, wenn es um die Entscheidungsmöglichkeiten von Konsumentinnen und Konsumenten geht. Beide Grundsätze sind in der DSGVO verankert.

Die DSGVO zeigt deutlich, dass die Gefahren hinsichtlich Datenschutz bekannt sind und auch adressiert werden. Das rechtliche Datenschutz-Instrumentarium steht zur Verfügung, muss aber konsequent eingesetzt werden. Weiterere Berichte über die potentiellen Auswirkungen von IoT bezüglich Konsumentenschutz scheinen auch nicht erforderlich, zumal es Forschungstätigkeit dazu auf mehreren Ebenen gibt (Universitäten, sonstige Forschungseinrichtungen wie zB Artificial Intelligence Lab an der JKU Linz, Complexity Science Hub Vienna, Akademie der Wissenschaften). Auch der Nationalrat hat das Institut für Technikfolgenabschätzung (Akademie der Wissenschaften) gemeinsam mit dem Austrian Institute of Technology (AIT) beauftragt, aktuelle

Entwicklungen – und dazu gehört ganz wesentlich auch das Internet der Dinge – hinsichtlich ihrer Technikfolgen zu untersuchen und den Nationalrat zu beraten.

- Essenziell sind auch die Information und Aufklärung der Konsumentinnen und Konsumenten über Gefahren und Probleme der zunehmenden Vernetzung, der Datenpreisgabe und ihre Rechte. Dabei können neben öffentlichen Stellen insbesondere auch Vereine wie zB noyb oder der Internetombudsmann wichtige Unterstützung leisten.

Festzuhalten bleibt, dass die zunehmende Vernetzung und das Internet of Things eine unumkehrbare Entwicklung sind, der man sich nicht verweigern kann. Trotz aller Bedenken ist zu unterstreichen, dass diese Entwicklung Möglichkeiten eröffnet, die unser Leben in vielen Bereichen positiv verändern werden. Eine seriöse Diskussion über das Internet of Things hat auch die Chancen zu beleuchten, die sich aus diesen Entwicklungen ergeben. So sind zwar zB bei „connected cars" Probleme wie die Möglichkeit der Erstellung von Bewegungsprofilen und der Analyse des Fahrverhaltens gegeben. Andererseits können Motorschäden frühzeitig erkannt, Unfälle durch Kommunikation mit anderen Fahrzeugen verhindert und Notrufe automatisch abgesetzt werden. Allerdings müssen freilich auch hier die Konsumentinnen und Konsumenten wissen, welche Daten übermittelt werden und die Einwilligung zur Speicherung dieser Daten geben können. Letztlich muss für das Internet of Things sowie generell für die Digitalisierung gelten, dass die sich daraus ergebenden Möglichkeiten kein Selbstzweck sind, sondern so eingesetzt werden müssen, dass sie den Menschen und damit auch den Konsumentinnen und Konsumenten nützen.

Insbesondere dort, wo Produkte oder Dienstleistungen mit künstlicher Intelligenz ausgestattet sind, ist die Verfolgung eines humanzentrierten Ansatzes wesentlich, der die menschliche Entscheidungsfindung, Transparenz und Nachvollziehbarkeit beim Einsatz von künstlicher Intelligenz als maßgebliche Parameter berücksichtigt. Dies kommt auch in mehreren Dokumenten auf europäischer und internationaler Ebene (siehe ethische Guidelines der High Level Expert Group über künstliche Intelligenz und Empfehlung des OECD Ministerrates über künstliche Intelligenz) zum Ausdruck.3. Mai 2019

Für die Bundesministerin:
Mag. Arno Ebner

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, SOZIALES, GESUNDHEIT UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz
	Datum/Zeit	2019-05-06T07:30:52+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	738854333
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	