

HINTERGRUNDPAPIER DES VZBV ZUM THEMA SMART HOME

Das Zuhause der Zukunft: Wie digital werden wir wohnen?

5. September 2017

Impressum

*Verbraucherzentrale
Bundesverband e.V.*

*Team
Energie und Bauen*

*Markgrafenstraße 66
10969 Berlin*

energie@vzbv.de

INHALT

I. ZUSAMMENFASSUNG	3
II. EINFÜHRUNG	4
Sachstand und Definition.....	4
Bewertung	5
Ausblick.....	6
III. PRODUKTHAFTUNG & VERTRAGSRECHT	6
Handlungsempfehlungen.....	8
IV. INTEROPERABILITÄT & LANGLEBIGKEIT	10
Handlungsempfehlungen.....	11
V. IT-SICHERHEIT & DATENSICHERHEIT	11
Handlungsempfehlungen.....	12
VI. DATENSCHUTZ	12
Handlungsempfehlungen.....	13

I. ZUSAMMENFASSUNG

Unter „Smart Home“ werden technische Verfahren, Systeme und Dienste in der Wohnung und/oder der direkten Wohnumgebung verstanden, die auf vernetzten Geräten und Installationen sowie automatisierbaren Abläufen basieren und zur Erhöhung der Wohn- und Lebensqualität, der Sicherheit sowie zur Steuerung der Energienutzung beitragen sollen. Umfragen zeigen, dass die Hälfte bis zu einem Drittel der Verbraucher mit dem Begriff „Smart Home“ noch nichts anfangen kann.¹ Nahezu 98 Prozent zeigen jedoch Interesse, wenn sie es erklärt bekommen.² Bei den Gründen für die Nutzung von Smart Home-Angeboten überwiegt das Thema Sicherheit, gefolgt von Komfort und Lebensqualität sowie dem Wunsch, mit der Technik Energie zu sparen.³ Gefragt nach den Gründen für die Nichtnutzung wurden die hohen Kosten sowie Mangel an Kenntnissen oder Bedürfnissen angegeben.⁴

Grundsätzlich findet die Entwicklung von Smart Home in einem lückenhaft und unübersichtlich regulierten Markt statt. Jeder Verbraucher entscheidet (noch) selbstständig und entsprechend der individuellen Bewertung des Nutzens, ob er ein Produkt kaufen möchte oder nicht.⁵ Dennoch gibt es aus Verbrauchersicht dringenden Handlungsbedarf. Zum einen finden sich aktuell am Markt überzogene Versprechungen, die in der Realität nicht umsetzbar sind oder auch intransparente Bündelangebote. Teilweise sind die Preise für den versprochenen Zusatznutzen deutlich zu hoch. Zum anderen bringen die neuen Systeme auch neue Herausforderungen für Haftung, Gewährleistung, Kompatibilität, IT-Sicherheit, Datensicherheit und Datenschutz. Auch stellt sich die Frage, wie damit umzugehen ist, sollte ein „analoges“ Wohnen irgendwann nicht mehr gewährleistet werden können.

Das folgende Papier beinhaltet neben einem Überblick eine Beschreibung der vier Problemfelder und gibt Handlungsempfehlungen.

¹ TNS Infratest für Statista: „Bekanntheit digitaler Begriffe in Deutschland“, 2016, <https://de.statista.com/statistik/daten/studie/518654/umfrage/bekanntheit-digitaler-begriffe-in-deutschland/>, 31.05.2017.

² ConPolicy: Fakten und Empfehlungen aus Verbraucherpolitischer Sicht, Konferenz zum Safer-Internet-Day 2017, https://www.bmju.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/SID2017_Thesenpapier.pdf?__blob=publicationFile&v=5, 31.05.2017.

³ Bitkom Research: Umfrage unter Besitzer von Smart Home-Anwendungen, 2017, <https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/02-Februar/Bitkom-Charts-PK-Safer-Internet-Day-14-02-2017-final.pdf>, 31.05.2017.

⁴ Statista: Gründe für Nichtnutzung, 2016, <https://de.statista.com/statistik/daten/studie/164411/umfrage/bedenken-gegen-heimvernetzung/>, 31.05.2017.

⁵ Ausnahmen können im Fertighaus- oder zukünftig auch im Mietwohnungsbereich entstehen, wenn die Technik bereits verbaut ist.

II. EINFÜHRUNG

Die Diskussion in Deutschland um neue digitale Anwendungen im Wohnbereich (Smart Home) hat im vergangenen Jahr mit dem Gesetz zur Digitalisierung der Energiewende und dem daraus resultierenden Smart Meter Rollout⁶ in privaten Haushalten eine neue Dimension erreicht. Parallel dazu steigen sowohl die angebotene Vielfalt als auch die Absatzzahlen vernetzter Geräte. Mögliche Anwendungen und Mehrwertdienste werden mittel- und langfristig tiefgreifende Änderungen für Verbraucherinnen und Verbraucher mit sich bringen.

SACHSTAND UND DEFINITION

Unter Smart Home werden technische Verfahren, Systeme und Dienste in der Wohnung und/oder der direkten Wohnumgebung verstanden, die auf vernetzten Geräten und Installationen sowie automatisierbaren Abläufen basieren und zur Erhöhung der Wohn- und Lebensqualität, der Sicherheit sowie zur Steuerung der Energienutzung beitragen sollen. Hierunter fallen derzeit insbesondere die Vernetzung von Haus- und Sicherheitstechnik, von Haushaltsgeräten und von Komponenten der Unterhaltungselektronik. Kennzeichnend für Smart Home sind u.a. die Kommunikation der Geräte untereinander sowie die Kommunikation der Geräte mit Anwendern und gegebenenfalls weiteren beteiligten Stellen. Die Geräte reagieren auf Datenübertragungen hausinterner und -externer Art sowie auf lokale Sensoren. Sie besitzen Schnittstellen, die über verschiedene Technologien, zum Beispiel über Internet und spezielle Apps, angesprochen werden können.⁷

Grundsätzlich gibt es unterschiedliche Ausprägungsgrade eines intelligenten Zuhauses. Auf der einen Seite steht die Komplettlösung im Neubau, wo mögliche Entwicklungen beispielsweise durch Leerverrohrung für neue Kabel oder Anbindung an die haus-eigene Photovoltaik-Anlage von Anfang an mitgedacht werden. Auf der anderen Seite stehen die sogenannten „Plug & Play“-Angebote, die sich i.d.R. ohne wesentliche bauliche Veränderungen in bestehende Wohnungen und Häuser sofort „einstecken“ lassen.⁸ Insbesondere letztere sind aktuell durch den Vertrieb im Elektronikfachmarkt und Entwicklungen im Informations- und Kommunikationstechnologien auf dem Vormarsch.

⁶ Smart Meter Rollout bezeichnet den Einbau neuer Stromzähler und Messsysteme. Diese Modernisierung der Messtechnik soll eine bessere Kommunikation im Stromnetz ermöglichen und als sichere Schnittstelle für Anwendungen wie beispielsweise Smart Home dienen.

⁷ Siehe auch Verbraucherzentrale Rheinland-Pfalz: Vierten Verbraucherdialog „Smart Home“ – Chancen nutzen, Risiken minimieren, 2016, https://mjv.rlp.de/fileadmin/mjv/Themen/Verbraucherschutz/Ergebnispapier_mit_Empfehlungen_zum_Verbraucher_und_Datenschutz_bei_Smart_Home_Angeboten_fuer_Anbieter_sowie_Verbraucherinnen_und_Verbraucher_.pdf, 30.05.2017

⁸ Andreas Frank: Smart Home per Funk oder Kabel?, 21.07.2017, <https://homepioneers.de/smart-home-per-funk-oder-kabel/>, 31.05.2017.

Umfragen zeigen, dass die Hälfte bis zu einem Drittel der Verbraucher mit dem Begriff Smart Home noch nichts anfangen kann.⁹ Nahezu 98 Prozent¹⁰ zeigen jedoch Interesse, wenn sie es erklärt bekommen.¹¹ Bei den Gründen für die Nutzung von Smart Home-Angeboten überwiegt das Thema Sicherheit, gefolgt von Komfort und Lebensqualität sowie dem Wunsch, mit der Technik Energie zu sparen.¹² Gefragt nach den Gründen für die Nichtnutzung wurden die hohen Kosten sowie Mangel an Kenntnissen oder Bedürfnissen angegeben.¹³

Allerdings ist schon heute die vernetzte Unterhaltungselektronik weit verbreitet: So stehen in 40 Prozent der deutschen Haushalte Smart TV, wobei jedoch nur 22 Prozent die Internetverbindung aktiv für Streaming-Portale und Mediatheken nutzen.¹⁴ Nicht überraschend steht daher auf der Liste zukünftiger Anschaffungen auch der Smart TV (36 %) sowie Lautsprecher (33 %) ganz oben, gefolgt von energierelevanten Anwendungen wie Heizungssteuerung (31 %), Beleuchtung (29 %) und Smart Meter (25 %). Aber auch Sicherheitsanwendungen sind für viele Verbraucher interessant: Rollläden (18 %), Videoüberwachung (17 %) oder Alarmanlagen (17 %).¹⁵ Die Marktprognose für Smart Home-Anwendungen scheint durchaus positiv: Die Zahl der deutschen Haushalte mit zentraler Steuerung soll bis zum Jahr 2020 auf 2,4 Millionen steigen.¹⁶ Wenn funkfähige Geräte jeder Art dazu genommen werden, gehen Prognosen sogar von mehr als 800 Millionen vernetzten Geräten in Deutschland bis zum Jahr 2020 aus (durchschnittlich zehn Produkte pro Person).¹⁷

BEWERTUNG

Grundsätzlich findet die Entwicklung von Smart Home in einem lückenhaft und unübersichtlich regulierten Markt statt. Jeder Verbraucher entscheidet (noch) selbstständig und entsprechend der individuellen Bewertung des Nutzens, ob er ein Produkt kaufen möchte oder nicht.¹⁸ Dennoch gibt es aus Verbrauchersicht dringenden Handlungsbedarf. Zum einen finden sich aktuell am Markt überzogene Versprechungen, die in der Realität nicht umsetzbar sind oder auch intransparente Bündelangebote. Teilweise sind

⁹ TNS Infratest für Statista: „Bekanntheit digitaler Begriffe in Deutschland“, 2016, <https://de.statista.com/statistik/daten/studie/518654/umfrage/bekanntheit-digitaler-begriffe-in-deutschland/>, 31.05.2017.

¹⁰ Telekom, Qivicon: Marktanalyse- Wachstumschancen für Unternehmen im Smart Home Markt. 2015, <https://www.qivicon.com/assets/PDF/Deutsche-Telekom-QIVICON-Marktanalyse-Smart-Home.pdf>, 21.07.2017.

¹¹ Siehe auch ConPolicy: Fakten und Empfehlungen aus Verbraucherpolitischer Sicht, Konferenz zum Safer-Internet-Day 2017, https://www.bmju.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/SID2017_Thesenpapier.pdf?__blob=publicationFile&v=5, 31.05.2017.

¹² Bitkom Research: Umfrage unter Besitzer von Smart Home-Anwendungen, 2017, <https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/02-Februar/Bitkom-Charts-PK-Safer-Internet-Day-14-02-2017-final.pdf>, 31.05.2017.

¹³ Statista: Gründe für Nichtnutzung, 2016, <https://de.statista.com/statistik/daten/studie/164411/umfrage/bedenken-gegen-heimvernetzung/>, 31.05.2017.

¹⁴ GfK: Wie smart sind deutsche TV-Nutzer?, 2016, <http://www.gfk.com/de/insights/press-release/wie-smart-sind-deutsche-tv-nutzer/>, 21.07.2017.

¹⁵ Bitkom Research: Umfrage unter Kennern von Smart Home-Anwendungen, 2017, <https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/02-Februar/Bitkom-Charts-PK-Safer-Internet-Day-14-02-2017-final.pdf>, 31.05.2017.

¹⁶ Statista: Digital Market Outlook, Stand 2015, <https://de.statista.com/infografik/3910/smart-home-prognose-fuer-ausgewahlte-maerkte/>, 31.05.2017.

¹⁷ A&D: 10 vernetzte Geräte pro Kopf bis 2020 in Deutschland, 2016, <http://www.industr.com/de/A-und-D-Magazin/news/vernetzte-geraete-pro-kopf-bis-in-deutschland-1674298>, 31.05.2017.

¹⁸ Ausnahmen können im Fertighaus- oder zukünftig auch im Mietwohnungsbereich entstehen, wenn die Technik bereits verbaut ist.

die Preise für den versprochenen Zusatznutzen deutlich zu hoch. Zum anderen bringen die neuen Systeme auch neue Herausforderungen für Haftung, Gewährleistung, Kompatibilität, IT-Sicherheit, Datensicherheit und Datenschutz. Auch stellt sich die Frage, wie damit umzugehen ist, sollte ein „analoges“ Wohnen irgendwann nicht mehr gewährleistet werden können.

AUSBLICK

Ob und wann Smart Home-Anwendungen trotz der hohen Preise zum Massenmarkt werden oder auf eine Minderheit technikbegeisterter Verbraucher beschränkt bleiben, ist noch nicht absehbar.

Grundsätzlich lässt aber der übergreifende Digitalisierungstrend aller Lebensbereiche eher auf eine anwendungsübergreifende Zunahme schließen. Wenn beispielsweise die Automobilität der Zukunft autonom und elektrisch wird, bekommt die Kommunikation zwischen Auto und eigener Photovoltaik-Anlage auf dem Hausdach einen Wert. Wenn Strompreise variabel und Blockchain-gesteuert¹⁹ sind anstatt jährlich zentral vom Energieversorger festgelegt werden, werden selbst handelnde Haushaltsgeräte unter Umständen für Verbraucher interessant.

Nicht überraschend greift der Europäische Gesetzgeber das Thema im energiespezifischen EU-Winterpaket an diversen Stellen²⁰ auf und erwartet insbesondere für den Strommarkt zahlreiche Impulse. Die Absicherung und Aktualisierung der Verbraucherrechte in den entsprechenden Rechtsstellen lässt allerdings bislang auf sich warten.

Aus Sicht des Verbraucherzentrale Bundesverbandes gilt es, dafür zu sorgen, dass die Investition in die Vernetzung einen klaren und akzeptierten Mehrwert für Verbraucher generiert und dass der Verbraucher im Zuhause der Zukunft genauso abgesichert ist, wie im analogen Zuhause.

III. PRODUKTHAFTUNG & VERTRAGSRECHT

Intelligente vernetzte Produkte können Anweisungen nicht nur vom Besitzer als Nutzer sondern auch von Dritten empfangen. Auch können diese Produkte ihre Funktionen im Verbund eigenständig weiterentwickeln oder mit anderen Produkten interagieren. Problematisch ist daher beim Einsatz intelligenter Produkte, dass ab einem bestimmten Grad der Autonomisierung nicht mehr mit Sicherheit gesagt werden kann, ob die vom digitalen Produkt erzeugte Informationen vom Nutzer des Systems oder von Dritten stammen oder vom Produkt selbst kreiert wurden. Insbesondere wenn hierbei Vertragsbeziehungen betroffen sind (beispielsweise wenn der intelligente Kühlschrank eigenständig im Supermarkt bestellt), stellt sich die Frage, wer der jeweilige Vertragspartner

¹⁹ Blockchain ist eine gemeinsam genutzte Datenbanktechnologie, bei der Verbraucher und Lieferant einer Transaktion direkt miteinander verknüpft werden.

²⁰ Beispielsweise in der Richtlinie über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt (COM(2016) 864 final) oder in der Richtlinie über die Gesamteffizienz von Gebäuden (COM (2016) 765 final)

ist, wie Verbraucherinformationspflichten erfüllt werden können und ob diese gegebenenfalls an die neuen Bedingungen angepasst werden müssen.²¹

Bei intelligenten Produkten kann es zu Haftungslücken kommen, wenn zum Beispiel ein erlerntes Verhalten der Software nicht vorhersehbar war. Vertragsrechtliche Gewährleistungsansprüche sind davon abhängig, dass das Erlernen im konkreten Fall als Mangel anerkannt wird. Auch müssen Verbraucher nachweisen, dass der Mangel bereits zum Zeitpunkt des Kaufes bestand und dass er nicht erst nachträglich etwa durch das Zusammenspiel mit weiteren IT-Komponenten entstanden ist. Auch kann die Durchsetzung vertraglicher Ansprüche an kurzen Verjährungsfristen scheitern, wenn Fehler erst später auftreten.

Eine darüber hinausgehende, außervertragliche Haftung des Herstellers oder Importeurs ist nach jetziger Rechtslage kaum prognostizierbar, da weitgehend ungeklärt ist, inwieweit autonomes Handeln von intelligenten Systemen einem Hersteller als Produktfehler zugerechnet werden kann. Das Problem wächst mit der Zahl der Produkte und Plattformen, die gleichzeitig in Interaktion treten und „eigenständig“ handeln. Verbraucher sind dann unter Umständen nicht mehr in der Lage zu beurteilen, welches Produkt fehlerhaft und welcher Verkäufer (Gewährleistung) oder Hersteller (Produkthaftung) in Anspruch genommen werden muss. Erschwerend kommt hinzu, dass bei Gewährleistungsansprüchen die Beweislast für einen Mangel bei Übergabe des Produkts nach sechs Monaten auf Seiten des Klägers liegt, der selbst bei Einsicht in die technischen Daten und Algorithmen oftmals kaum in der Lage sein wird, einen Gerätemangel darzulegen und zu beweisen.

Genauso fraglich ist, wer bei groben Sicherheitslücken haftet. Bisher fehlen rechtliche Grundlagen, um Hersteller oder Anbieter zur Rechenschaft zu ziehen. Hintergrund ist, dass das europäische Produkthaftungsrecht nur für körperliche Gegenstände gilt, so dass es im Internet der Dinge nur Anwendung findet, wenn der Hardwarehersteller auch für den Softwarefehler verantwortlich gemacht werden kann.²²

Der Richtlinienentwurf über digitale Inhalte der EU-Kommission sollte ursprünglich moderne Regelungsansätze für die vertragliche Haftung bei digitalen Anwendungen etablieren.²³ Ziel der Richtlinie war es, für alle Verträge über digitale Inhalte und digitale Dienste ein Gewährleistungsrecht zu etablieren. Mittlerweile ist fraglich, ob die Richtlinie für vernetzte Produkte tatsächlich Verbesserungen bringen wird, da der Ministerrat in der gemeinsamen Ausrichtung vom 8.06.2017 beschlossen hat, dass „Smart Devices“ von der Richtlinie nicht erfasst sein sollen.²⁴ Für eine verbesserte vertragsrechtliche Haftung für Smart Home-Anwendungen ist entscheidend, wie die Verhandlungen zwischen Rat und Parlament an diesem Punkt ausgehen. Sollten vernetzte Produkte am Ende nicht von der Richtlinie über digitale Inhalte erfasst werden, müssen sie in der parallel diskutierten Richtlinie über den Online-Warenhandel²⁵ geregelt werden.

²¹ Artz, Markus: Braucht die digitale Welt ein neues Recht?, Vortrag auf der Vortrags- und Diskussionsveranstaltung des Bayerisches Staatsministerium für Umwelt und Verbraucherschutz am 5. Oktober 2016.

²² Schmon, Christoph: Fitness-Test der Europäischen Produkthaftung, 10.01.2017, Blog Consumer Law, <https://vkiakademie.wordpress.com/2017/01/10/fitness-test-der-europaeischen-produkthaftung/>, 01.06.2017.

²³ COM(2015) 634 final, 09.12.2015.

²⁴ Vgl. dazu die Onlinemeldung des vzbv vom 8.06.2017, <http://www.vzbv.de/meldung/nachbesserungsbedarf-bei-vertragsrecht-40>, 18.07.2017.

²⁵ COM (2015) 636 final, 09.12.2015.

Abgesehen davon müssen die inhaltlichen Vorgaben der Richtlinie zum Gewährleistungsrecht bei digitalen Inhalten verbessert werden. Der Richtlinienentwurf der Kommission berücksichtigt, dass Verträge über digitale Inhalte oft den Charakter von Dauerschuldverhältnissen haben und dass in diesem Fall der digitale Inhalt für die Dauer des Vertragsverhältnisses mangelfrei sein muss. Allerdings ist dies im Richtlinienentwurf bislang abhängig von der Gestaltung des jeweiligen Vertragsverhältnisses, beispielsweise ob ein Vertrag über einen digitalen Inhalt ein Kaufvertrag ist oder ein Dauerschuldverhältnis ähnlich der Miete gleich kommt. Auch inwieweit und für welchen Zeitraum Anbieter zur Lieferung von Updates verpflichtet sind, lässt der Entwurf der EU-Kommission offen.

Generell klärungsbedürftig ist schließlich die Frage der Haftung für den Service Dritter, von denen die Leistungserbringung abhängig ist, ohne dass diese selbst Vertragspartner sind. Wird ein solcher Dienst eingestellt, kann dies zur dauerhaften Funktionsunfähigkeit des Produkts führen.

Der vzbv setzt sich für Klarstellungen zu diesen Punkten ein.²⁶ Auch hier wird es vom Verhandlungsergebnis zwischen Rat und Parlament abhängen, ob die Richtlinie mehr an Rechtssicherheit und Verbraucherschutz im Bereich von Smart Home-Anwendungen bringen wird.

HANDLUNGSEMPFEHLUNGEN

- ❖ Der vzbv fordert eine umfassende Prüfung des gesetzlichen Rahmens für Smart Home-Produkte und Anwendungen. Der Fokus sollte dabei auf der Identifizierung von Haftungslücken im Vertragsrecht (Gewährleistung) und außervertraglichen Bereich (Delikts- und Produkthaftungsrecht) liegen. Ziel ist, dass Verbraucher im Zuhause der Zukunft auch genauso abgesichert sind wie heute.
- ❖ Die EU-Richtlinie über digitale Inhalte muss auch für vernetzte Produkte einschließlich Smart Home-Produkten gelten. Tritt bei solchen Produkten ein Fehler auf, sollten die tendenziell günstigeren Regelungen über digitale Inhalte parallel zum sonstigen Gewährleistungsrecht gelten. Um eine Haftung für digitale Inhalte abzuwenden, müsste der Händler dann nachweisen, dass kein Problem mit der Software, sondern ein Problem mit der Hardware vorliegt. Sollten Smart Devices von der Richtlinie über digitale Inhalte nicht erfasst werden, so müssen sie von der parallel diskutierten Richtlinie über den Onlinekauf erfasst sein.
- ❖ Im Zuge der Diskussion um die EU-Richtlinie über digitale Inhalte sollte sichergestellt werden, dass Updates auch über die verpflichtende Gewährleistungsdauer hinaus verfügbar sein müssen. Ziel muss es sein, dass Produkte durch Updates während der gesamten Nutzungsdauer vor Sicherheitslücken geschützt sind und dass die Gebrauchstauglichkeit durch fehlender Aktualisierungen während der gesamten Nutzungsdauer sichergestellt wird.
- ❖ Die Einbeziehung Dritter in die Leistungserbringung darf nicht zu Nachteilen für Verbraucher führen. Aus dieser Überlegung heraus müssen sowohl die Ansprüche des Verbrauchers gegenüber dem Verkäufer (also der Person, mit der der Verbraucher

²⁶ vzbv, Digitale Inhalte: Für eine zielgenaue und kohärente Gesetzgebung. Stellungnahme zum Vorschlag der EU-Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte – COM(2015) 634 endg., 9. Januar 2017, http://www.vzbv.de/sites/default/files/17-01-10_vzbv_stellungnahme_digitale_inhalte.pdf

den Kaufvertrag über das physische Gut geschlossen hat) also auch gegenüber dem Hersteller (also demjenigen Unternehmen, das das Smart Home-Produkt auf den Markt gebracht hat) der besonderen Situation eines digitalisierten Produkts angepasst werden.

- ❖ Bezogen auf die Ansprüche des Verbrauchers gegenüber dem Verkäufer heißt das folgendes: Sofern ein bestimmter Dienst für die Funktionstauglichkeit der Ware erforderlich ist, sollte der Verkäufer des physischen Gutes als dauerhafter, einheitlicher Ansprechpartner für den Verbraucher festgelegt werden. Der Verkäufer würde dann für die Funktionstauglichkeit der Ware umfassend haften, auch sofern Funktionsstörungen auf einen in das Smart Home-System eingebundenen Dritten zurückzuführen sind, etwa den Anbieter eines Cloud-Dienstes. Eine entsprechende Regelung sollte in der Richtlinie über digitale Inhalte verankert werden.
- ❖ Bezogen auf den Hersteller heißt das folgendes: Insbesondere aus präventiven Überlegungen sollte eine gewährleistungsähnliche Herstellerhaftung für vernetzte Produkte eingeführt werden.²⁷ Der Verkäufer kann die für Smart Home-Anwendungen typische Einbindung von Dritten bislang nicht wirklich kontrollieren und würde aber gegebenenfalls dafür haften. Der Hersteller des Produkts legt bei seiner Produktkonzeption fest, ob die Smart Home-Anwendung mit einem herstellereigenen Dienst betrieben wird oder die Dienste eines Dritten erforderlich sein werden und legt dafür die Modalitäten des Zusammenspiels fest. Um den Verbraucher vor Haftungslücken zu schützen, sollte dem Verbraucher ergänzend zu den Ansprüchen gegen den Verkäufer ein gewährleistungsähnlicher Anspruch gegen den Hersteller zustehen. So könnten Hersteller für bestimmte Situationen (z.B. Serverabstimmung, sonstige massive Einschränkungen von Diensten, Unterlassen sicherheitskritischer Updates, Verhinderung der Weiterveräußerung) haften, bei Ausfalls eines Dritten die Funktionsfähigkeit der Sache wiederherstellen oder auch den entstehenden Schaden ersetzen.
- ❖ Das Produkthaftungsrecht muss eingehend auf seine „digitale Leistungsfähigkeit“ untersucht werden. Problematisch ist vor allem, dass Hersteller nur für körperliche Produkte haften und nur körperliche Produkte geschützt werden. Darüber hinaus ist unklar, in welchem Umfang Fehler in weitgehend automatisierten und vernetzten Systemen einem Hersteller zugerechnet werden können. Zur Vermeidung von Haftungslücken müssen die Anforderungen an das Vorliegen eines Fehlers so reduziert werden, dass Verbraucher die ihnen obliegende Beweislast angesichts der technischen Komplexität tatsächlich erfüllen können. Mehrere Hersteller vernetzter Produkte sollten gesamtschuldnerisch haften, solange sich ihre individuelle Haftung aus der Perspektive des Verbrauchers nicht darlegen lässt.
- ❖ Produktsicherheit erfordert möglichst verlässliche technische Vorgaben, an denen sich Hersteller orientieren können und sollen. Solche Vorgaben müssen verstärkt im Rahmen der globalen Normung entwickelt werden. Solange und soweit es an einer Normung von IT-Sicherheit mangelt, darf dies nicht zu einem Haftungsvakuum zu Lasten von Verbrauchern führen. Der vzbv regt an, dass IT-Sicherheit in der Normung und Standardisierung eine größere Rolle spielt.

²⁷ Vgl. dazu Christiane Wendehorst, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Studie im Auftrag des Sachverständigenrats für Verbraucherfragen, 2016, <http://www.svr-verbraucherfragen.de/wp-content/uploads/Wendehorst-Gutachten.pdf>, S. 120 ff.

IV. INTEROPERABILITÄT & LANGLEBIGKEIT

Für Verbraucher ist es von Vorteil Produkte unterschiedlicher Hersteller miteinander verbinden zu können. Mit Interoperabilität kann die Angebotsvielfalt unterschiedlicher Funktionalitäten sichergestellt, marktbeherrschende Stellungen vermieden und auch das sogenannte „Bricking“²⁸ unterbunden werden.

Interoperabilität ist aktuell nicht immer gewährleistet, da gemeinsame Standards, Schnittstellen und Prozesse fehlen. Es gibt einzelne Hersteller- und systemübergreifende Standardisierungsbemühungen wie die EEBus-Initiative, die auf bestehende Kommunikationswege wie KNX, ZigBee und TCP/IP setzt.²⁹ Mitglieder der EEBus-Initiative sollten so miteinander kompatibel sein. Diese Initiativen decken jedoch nicht den kompletten Markt ab. Aktuell müssen sich Verbraucher vor dem Kauf selbst aufwändig über kompatible Produkte informieren und Zukunftsvertrauen mitbringen, dass sich „ihr“ System am Markt durchsetzt oder mit neuen Systemen kompatibel ist.

Grundsätzlich ist aktuell auch offen, wie die von Verbrauchern gewohnte Nutzungsdauer auch bei intelligenten Produkten sichergestellt werden kann. Smart Home-Anwendungen benötigen wie IT-Produkte in regelmäßigen Abständen Updates, um Sicherheitslücken zu schließen oder auf Neuerungen zu reagieren. Ob eine Verpflichtung zur Lieferung von Updates besteht, hängt nach der geltenden Rechtslage davon ab, ob das Produkt im Wege eines Kaufvertrags erworben wurde – und dann muss es nur zum Zeitpunkt der Übergabe mangelfrei sein –, oder ob es sich um ein Dauerschuldverhältnis – ähnlich einer Miete – handelt. Anders als Computertechnik sind insbesondere größere Elektrohaushaltsgeräte wie Waschmaschinen oder Kühlschränke in einem Haushalt oft mehr als zehn Jahre in Benutzung und haben häufig auch noch im Anschluss ein Leben als Zweitgerät oder Second-Hand-Produkt.³⁰ Die Vernetzung der Produkte darf nicht dazu führen, dass die Lebensdauer begrenzt wird.

Die notwendige Konsequenz ist es, dass Anbieter von Smart Devices verpflichtet sein müssen, für die gesamte Lebensdauer des Produktes zumindest sicherheitsrelevante Updates ohne weitere Zusatzkosten zur Verfügung zu stellen. Die entsprechende Rechtspflicht muss in der Richtlinie über digitale Inhalte verankert werden. Andernfalls würden Smart Devices vor Ablauf der physischen Haltbarkeit unbrauchbar – zum Nachteil für Verbraucher und für die Umwelt. Wenn die Geräte trotzdem weiterbenutzt würden, würden sie zur Gefahr für die Allgemeinheit. Ausbleibende Updates können auch Dritte betreffen und potentiell schädigen, wenn beispielsweise ungesicherte Produkte dazu verwendet werden, Angriff auf kritische Infrastrukturen zu starten.

Auch muss die europäische Produktpolitik den Vernetzungstrend stärker berücksichtigen. So muss im Rahmen der Ökodesign- und Energielabel-Gesetzgebung der durch

²⁸ Bricking bezeichnet den Vorgang, bei dem teure Endnutzengeräte nutzlos werden, weil die Anbieterfirma entweder vom Markt verschwindet (bankrott oder aufgekauft durch Wettbewerber) oder bestimmte Dienstleistungen und Updates nicht länger angeboten werden, die aber für die Reparatur oder Nutzung des Systems notwendig wären. Auch kann Bricking bedeuten, dass der Endnutzer sein Gerät durch eigene Eingriffe unbrauchbar macht.

²⁹ EEBus Initiative: Sofortige Offenlegung des EEBus-Standards auch für Nicht-Mitglieder, vom 18.05.2016, Sofortige Offenlegung des EEBus-Standards auch für Nicht-Mitglieder, 25.07.2017.

³⁰ Prakash, Siddharth et. al: Einfluss der Nutzungsdauer von Produkten auf ihre Umweltwirkung: Schaffung einer Informationsgrundlage und Entwicklung von Strategien gegen „Obsoleszenz“, S. 104, Dessau: Umweltbundesamt.

Vernetzung auftretende Mehrverbrauch sinnvoll begrenzt und bei den Informationspflichten aufgegriffen werden. Auch sollten sich insbesondere Alltagsprodukte wie Waschmaschinen oder Kühlschränke immer auch offline benutzen lassen, um die Möglichkeit zur analogen Nutzung zu gewährleisten. Bei der Vernetzung sollte zusätzlich sichergestellt werden, dass die Produkte auf variable Tarife reagieren können, um alle potentiellen Entwicklungen am Strommarkt auch langfristig mitdenken zu können.

HANDLUNGSEMPFEHLUNGEN

- ❖ Der vzbv fordert die Hersteller auf, verstärkt auf gemeinsame Standards oder Meta-Plattformen zu setzen und fordert den Gesetzgeber dazu auf, durch Forschung und Förderung ggf. unterstützend tätig zu werden. Die Entwicklung einer übergreifenden Meta-Plattform würde den Informationsaufwand auf Seiten der Verbraucher verringern und eine zentrale Steuerung über eine App die Bedienungsfreundlichkeit erhöhen.
- ❖ Die Gewährleistungsfristen müssen angepasst werden. Zu den berechtigten Erwartungen der Verbraucher gehört, dass bestimmte Produkte länger als zwei Jahre problemfrei nutzbar sind. Smart Home-Anwendungen sind aber teure Produkte, von denen Langlebigkeit deutlich über diese zwei Jahre hinaus erwartet werden darf. Das Gewährleistungsrecht sollte den Gesichtspunkten der Nachhaltigkeit folgen und die Gewährleistungsfrist der zu erwartenden Lebensdauer anpassen.
- ❖ In der Richtlinie über digitale Inhalte muss sichergestellt werden, dass Anbieter verpflichtet sind, zumindest sicherheitsrelevante Updates während der gesamten Nutzungsdauer des Smart Device ohne weitere Zusatzkosten zur Verfügung zu stellen.
- ❖ Auch sollten Verbraucher stärker für die Notwendigkeit von Updates und den Konsequenzen ausbleibender Updates sensibilisiert werden. Grundsätzlich gilt zu prüfen, ob neben der Pflicht der Hersteller Sicherheitsupdates anzubieten, Verbraucher auch dazu verpflichtet sind, Updates anzuwenden, wenn sonst Schäden für eigene und fremde Produkte entstehen könnten.
- ❖ Der vzbv fordert den europäischen Gesetzgeber auf, den Vernetzungstrend in Zukunft bei der europäischen Produktpolitik stärker zu berücksichtigen. Das betrifft insbesondere die Begrenzung des Netzwerk-Stand-by sowie Informationspflichten.

V. IT-SICHERHEIT & DATENSICHERHEIT

Die Sicherheit der Systeme ist aus Verbrauchersicht eine notwendige Voraussetzung. Dennoch kommt die Sicherheit der Systeme bislang häufig zu kurz. Ein Bericht der EU-Kommission hatte kürzlich z. B. gezeigt, dass in der Smart Home-Forschung IT-Sicherheit und Datenschutz nahezu keine Rolle spielen. In der Softwareentwicklung fürs intelligente Heim rangiert Cybersicherheit mit vier Prozent auf dem letzten Platz.³¹

Die Gefahr von Missbrauch und Manipulation der Systeme durch unerwünschten Zugriff muss verhindert oder zumindest minimiert werden. Neben verpflichtenden Mindeststandards fehlt es hier aktuell auch an verlässlichen Differenzierungsmöglichkeiten in

³¹ European Commission: Smart Grid Laboratories Inventory 2016, 2016, S. 59, Joint Research Centre: Brüssel.

Form von Zertifikaten oder einfachen Informationsmöglichkeiten für sicherheitssensible Verbraucher.

Schwierig ist, dass durch die vielen neuen Akteure der erforderliche Wissensstand auf Seiten der Hersteller über Datensicherheitskonzepte nicht immer gegeben ist. Dazu gehört die Auslieferung von Geräten mit individuellen Passwörtern, die Gewährleistung schneller Sicherheits-Updates bei Hacker-Angriffen oder die Verschlüsselung personenbezogener Daten. Da Hersteller bislang – auch nicht bei grober Fahrlässigkeit – zur Verantwortung gezogen werden können, fehlt auch dieser Hebel für eine Selbstbereinigung des Marktes.

HANDLUNGSEMPFEHLUNGEN

- ❖ Der vzbv fordert, dass IT-Sicherheit einen höheren Stellenwert bekommen muss. Gesetzliche Mindeststandards sowie verpflichtende Gütesiegel sind kurzfristig zu erarbeiten. Langfristig sollte IT-Sicherheit bei Produktsicherheit eine herausragende Rolle spielen
- ❖ Der vzbv fordert, dass IT-Sicherheit in der Forschung eine größere Rolle spielen muss. Der Gesetzgeber sollte dafür sorgen, dass die relevanten Forschungsrahmenprogramme ihre Aktivitäten im Bereich der IT-Sicherheit intensivieren.
- ❖ IT-Sicherheit muss auch im Rahmen des Produkthaftungsrechts stärker berücksichtigt werden. Die europäische Produkthaftungsrichtlinie schützt bislang nur körperliche Gegenstände sowie Leib und Leben der Verbraucher. Für Vermögensschäden und Datenverlust besteht dabei allenfalls ein verschuldensabhängiger Gewährleistungsanspruch für Mangelfolgeschäden gegen den Verkäufer, der aber grundsätzlich durch AGB ausgeschlossen werden kann.

VI. DATENSCHUTZ

Um einen adäquaten Schutz personenbezogener Daten sicherzustellen, müssen datenverarbeitende Stellen Datenschutzkonzepte bereits in die Technik integrieren („privacy by design“). Die Befolgung der Vorgaben der Datenschutzgrundverordnung muss selbstverständlich sein. Dazu gehören die Prinzipien der Datenvermeidung und Datensparsamkeit, die Beschränkung der Datenverarbeitung auf einen zuvor definierten Zweck und dass Verbraucher im Vorfeld umfassend und verständlich über die Datenverarbeitung informiert werden. Ein Kaufvertrag reicht hierfür alleine nicht aus.

Die Datenschutzgrundverordnung der EU gilt auch für Hersteller von Smart Home-Produkten.³² Die sind aber bislang nur „indirekt“ angesprochen und werden „ermutigt“, das Recht auf Datenschutz bei Entwicklung und Gestaltung zu berücksichtigen („Datenschutz durch Technik“).

Verbraucher müssen grundsätzlich das Recht und die Möglichkeit haben, die Datenübermittlung vor dem Kauf zu erkennen, zu kontrollieren und gegebenenfalls zu stoppen, und das ohne gravierende wirtschaftliche oder gesellschaftliche Nachteile. Dazu

³² VO 2016/697 vom 27.04.2016, Erwägungsgründe Ziffer 78.

gehört, dass die Produkte nach Möglichkeit hinsichtlich der Grundfunktionen auch offline funktionstüchtig sind. Beispielsweise sollte es möglich sein, intelligente Thermostate auch manuell zu regeln. Jeder Verbraucher sollte frei wählen können, welches Unternehmen Zugriff auf seine Daten hat und sollte diese Daten auch mitnehmen können bzw. anderen Unternehmen zur Verfügung stellen können.

HANDLUNGSEMPFEHLUNGEN

- ❖ Der vzbv fordert mehr Transparenz über die Datenverarbeitung von Smart Home-Anwendungen. Zu prüfen ist unter anderem der Vorschlag der VSMK, ein Label einzuführen, mit dem Verbraucher auf einen Blick erkennen können, wie datenintensiv oder -sparsam ein Produkt ist.³³
- ❖ Der vzbv betont die Bedeutung der Einhaltung der relevanten Datenschutzgesetze im Bereich Smart Home und fordert dafür eine entsprechende Überprüfung.
- ❖ Soweit Verbraucher Anwendungen oder Dienste faktisch mit Daten anstelle von Geld als Gegenleistung bezahlen, müssen sie die gleichen Rechte beim Zahlen mit Geld haben. Gleichzeitig muss es für Verbraucher jederzeit möglich sein, der Nutzung ihrer Daten zu widersprechen. Dies muss auch dann gelten, wenn der Anbieter die Daten des Verbrauchers in einem automatisierten Verfahren erhebt. Ansonsten würde das Datenschutzrecht mit seinem persönlichkeitsrechtlichen Kern durch das Vertragsrecht ausgehebelt. Dies darf nicht sein.

³³ Beschlüsse der VSMK Sonderkonferenz vom 24.11.2016, Berlin, https://www.verbraucherschutzministerkonferenz.de/documents/Protokoll_Sonder-VSMK_Endstand.pdf, 25.07.2017.