WIK • Diskussionsbeitrag

Nr. 471

Consumer-IoT in Deutschland – Anwendungsbereiche und möglicher Regelungsbedarf

Autoren:
Julian Knips
Christin Gries
Christian Wernick

Bad Honnef, Dezember 2020

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Impressum

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik.org
www.wik.org

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin und Direktorin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzende des Aufsichtsrates	Dr. Daniela Brönstrup
Handelsregister	Amtsgericht Siegburg, HRB 7225
Steuer-Nr.	222/5751/0722
Umsatzsteueridentifikations-Nr.	DE 123 383 795

Stand: Dezember 2020

In den vom WIK herausgegebenen Diskussionsbeiträgen erscheinen in loser Folge Aufsätze und Vorträge von Mitarbeitern des Instituts sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten. Mit der Herausgabe dieser Reihe bezweckt das WIK, über seine Tätigkeit zu informieren, Diskussionsanstöße zu geben, aber auch Anregungen von außen zu empfangen. Kritik und Kommentare sind deshalb jederzeit willkommen. Die in den verschiedenen Beiträgen zum Ausdruck kommenden Ansichten geben ausschließlich die Meinung der jeweiligen Autoren wieder.

ISSN 1865-8997

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Der Consumer-IoT-Bereich entwickelt sich mit hoher Dynamik. Die Anzahl vernetzter Produkte für Verbraucher nimmt kontinuierlich zu und bietet gegenüber herkömmlichen Produktvarianten vielfach erweiterte Anwendungsmöglichkeiten und damit zusätzlichen Nutzen. Es besteht erhebliches Potential für innovative Lösungen u.a. aufgrund von Fortschritten bei Sensorik, KI-Technologien, Kameras, Mikrofonen und Prozessen.

So eröffnet sich für zahlreiche Akteure im erweiterten Ökosystem grundsätzlich Wachstumspotential. In den meisten Produktkategorien im Consumer-IoT hat sich aufgrund niedriger Markteintrittsbarrieren ein ausgeprägter Wettbewerb entwickelt, in dem sowohl klassische Hersteller aus der analogen Welt, als auch Start-Ups eine Rolle spielen. Dies gilt insbesondere für die Anwendungsbereiche Smart Home sowie Tracking und Monitoring. Bei Entertainmentprodukten und Wearables gibt es hingegen Teilbereiche, in denen eine hohe Anbieterkonzentration zu beobachten ist. Hier nehmen einige Anbieter Gatekeeper-Rollen ein, mit denen ein entsprechender Einfluss auf die Diensteauswahl und damit verbunden wettbewerbs- und verbraucherschutzrelevante Probleme einhergehen. Darüber hinaus drohen Lock-In-Effekte in Ökosystemen globaler Konzerne.

Vernetzte Produkte erheben in großem Umfang personenbezogene und teils sensible Daten, die schutzwürdig sind. Datenschutz und IT-Sicherheit sind jedoch oft verbesserungsbedürftig. Darüber hinaus können einige Geräte aufgrund spezifischer Ausstattungsmerkmale (insbesondere Mikrofon und Kamera) für Abhörzwecke genutzt werden, was jedoch nach § 90 TKG verboten sind.

Es muss davon ausgegangen werden, dass im dynamischen Consumer-IoT-Bereich mit zunehmender Durchdringung aller Lebensbereiche weitere und zum Teil auch neue Problemfelder entstehen. Auch wenn die bestehenden rechtlichen und regulatorischen Instrumente für die segementspezifischen Herausforderungen hinreichend erscheinen, ist vor diesem Hintergrund eine kontinuierliche und sorgfältige Beobachtung von neuen Anbietern und Produkten sowie eine Bewertung der daraus resultierenden Veränderungen der Marktverhältnisse erforderlich.

Summary

The consumer IoT sector is highly dynamic. The number of connected products for consumers is continuously increasing and offers new possible applications and thus additional benefits compared to conventional products. There is considerable potential for innovative solutions due to progress in sensor and AI technologies, cameras, microphones and processes.

This opens up fundamentally new market opportunities for numerous players in the extended ecosystem. In most of the product categories within the application fields relevant to consumer IoT, in particular smart home and tracking/monitoring, low barriers to market entry have led to the development of strong competition with established manufacturers and start-ups competing with each other.

However, a high concentration of suppliers can be observed in some areas of consumer IoT. Here, some players take on gatekeeper roles, which impact the selection of services and may cause problems relating to competition and consumer protection. In addition, there is a risk of lock-in effects in the ecosystems of global corporations, which especially affects the areas of entertainment and wearables.

Connected devices collect large amounts of personal and sometimes sensitive data that are worth to be protected. Nevertheless, Data protection and IT security are often in need for improvement. In addition, some devices can be designed for spy purposes due to specific equipment features (in particular microphone and camera), which are prohibited according to § 90 TKG.

It must be assumed that further and even new problems will arise in the dynamic consumer IoT sector as more and more areas of life are affected. Even though the established legal and regulatory instruments seem appropriate to address sector-specific consumer issues and market failure, it is necessary to continuously and carefully monitor new market players and products and to evaluate the resulting changes in the market conditions.

1 Hintergrund, Fokus und methodisches Vorgehen

Die Bedeutung vernetzter Consumer-Produkte hat in den vergangenen Jahren global stark zugenommen. **Technische Fortschritte** in relevanten Bereichen wie Sensortechnologie, Künstlicher Intelligenz, bei Prozessoren und Miniaturisierung treiben die Entwicklung von innovativen Consumer-IoT-Produkten auch zukünftig weiter an. Damit geht einher, dass hochqualitative Aufnahmegeräte (Mikrofone und Kameras) immer kleiner und günstiger werden.

Bereits heute können **Anwendungen** wie Beleuchtung, Heizung, Alarmanlagen und andere Bereiche des Haushalts fernüberwacht bzw. geregelt werden. Smarte Fernsehgeräte reagieren auf Sprachbefehle, vernetzte Medizingeräte erheben und übertragen Messwerte, GPS-Tracker orten Wertgegenstände und Smartwatches sammeln rund um die Uhr bewegungs- und gesundheitsbezogene Daten ihrer Träger.

Viele vernetzte Produkte und Dienstleistungen haben **für den Verbraucher Vorteile** gegenüber herkömmlichen Produktvarianten oder bieten gar komplett neue Lösungen. Darüber hinaus ist mit einigen Consumer-IoT-Produkten auch ein **volkswirtschaftlicher und gesellschaftlicher Nutzen** verbunden. So können z. B. vernetzte Medizinprodukte als Frühwarn- und Präventionssystem zu Effizienzsteigerungen im Gesundheitswesen führen oder Smart-Home-Lösungen den Energieverbrauch senken und damit zum Klimaschutz beitragen.

Allerdings können mit der Vernetzung von vormals komplett eigenständigen Geräten und insbesondere mit einigen Ausstattungsmerkmalen wie z. B. Kameras oder Mikrofonen auch **Risiken in Bereichen des Daten- und Verbraucherschutzes** einhergehen. Verschiedene Vorfälle haben IT-Sicherheitsrisiken an Schnittstellen aufgedeckt. Angesichts der zunehmenden Vernetzung verschiedener, bisher getrennter Bereiche stellt sich auch die Frage, ob Markteintrittsbarrieren für Wettbewerber aufgebaut und damit die Wahlmöglichkeiten für Verbraucher eingeschränkt werden.

Bereits in dieser relativ frühen Marktphase zeichnen sich kritische und komplexe Entwicklungen ab, die auch mit Blick auf nachgelagerte Märkte Wettbewerbsprobleme durch **Gatekeeper-Rollen und geschlossene Ökosysteme** umfassen. Entsprechend sollte durch geeignete Regelungen sichergestellt werden, dass Rahmenbedingungen für die Förderung von Consumer-IoT (z. B. Plattformwettbewerb, Verfügbarkeit von Frequenzen und Nummernressourcen) vorausschauend ausgestaltet sind und werden.

Die vorliegende Studie über den Markt für Consumer-IoT soll auf Basis einer Analyse der derzeit wichtigsten Anwendungsbereiche mögliche Problemfelder identifizieren und den regulatorischen Handlungsbedarf bewerten.

Der Begriff „**Consumer-IoT**“ ist nicht eindeutig definiert und wird daher in der Fachöffentlichkeit und von Marktakteuren unterschiedlich verwendet. Im Rahmen der vorliegenden Studie bezieht sich Consumer-IoT auf alle **von Verbrauchern genutzten Produkte und Dienstleistungen, die mit einem Netzwerk verbunden sind und aus der Ferne (z. B. über einen Sprachassistenten oder ein Mobilgerät) gesteuert werden können**.[1]

Unter dieses breite Begriffsverständnis fallen somit alle Consumer-IoT-Anwendungen, die über **verschiedene Konnektivitätslösungen** wie z. B. Ethernet, Short-Range-Funktechnologien und öffentliche Mobilfunknetze[2] realisiert werden.

Innerhalb des breiten Spektrums an Consumer-IoT-Anwendungen liegt der Schwerpunkt der Studie auf den Bereichen **Smart Home, Entertainment, Tracking und Monitoring sowie Wearables** (siehe Abbildung 1-1). Die Auswahl dieser Anwendungsbereiche erfolgte auf Basis vorhandener Marktstudien und umfasst nach eingehender Analyse die relevantesten Felder im gegenwärtigen Consumer-IoT.[3]

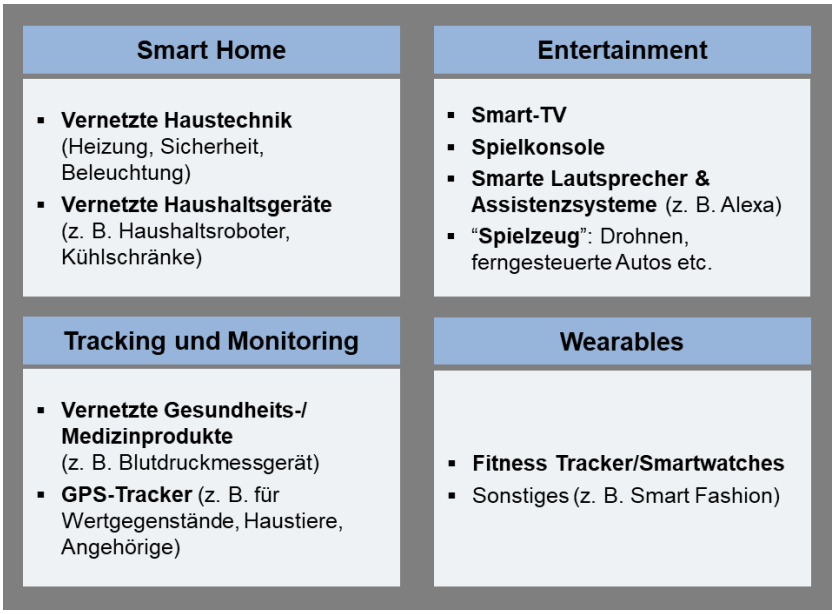
---

1 Diese Auffassung teilt auch die Europäische Kommission in einer laufenden Sektoruntersuchung im Kontext der Digitalstrategie der Kommission. Die Kommission plant im Frühjahr 2021 die Veröffentlichung eines vorläufigen Berichts zu Konsultationszwecken. Der abschließende Bericht soll im Sommer 2022 vorliegen, siehe Europäische Kommission (2020): Kartellrecht - Kommission leitet Sektoruntersuchung zum verbraucherbezogenen Internet der Dinge ein, Pressemitteilung vom 16. Juli 2020, elektronisch verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1326.

2 Vgl. zu technischen Realisierungsmöglichkeiten im IoT: Gries, C.; Knips, J.; Wernick, C. (2019): Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, WIK-Diskussionsbeitrag Nr. 455, Dezember 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_455.pdf, S. 2-9.

3 Marktstudien zum Consumer-IoT befassen sich überwiegend mit globalen Entwicklungen und konzentrieren sich vielfach auf spezifische Anwendungsbereiche, vgl. z. B. Strategy Analytics (siehe Waltzer, S. (2020): Global Smartwatch Shipments Grow 20 Percent to 14 Million in Q1 2020, May 07 2020, Strategy Analytics Blogs and Podcasts, elektronisch verfügbar unter: https://www.strategyanalytics.com/strategy-analytics/blogs/wearables/2020/05/07/global-smartwatch-shipments-grow-20-percent-to-14-million-in-q1-2020) oder IDC (2019): Earwear and Watches Expected to Drive Wearables Market at a CAGR of 7.9%, Says IDC, 19 Juni 2019, elektronisch verfügbar unter: https://www.idc.com/getdoc.jsp?containerId=prUS45271319).

Abbildung 1-1: Consumer-IoT: Relevante Anwendungsfelder



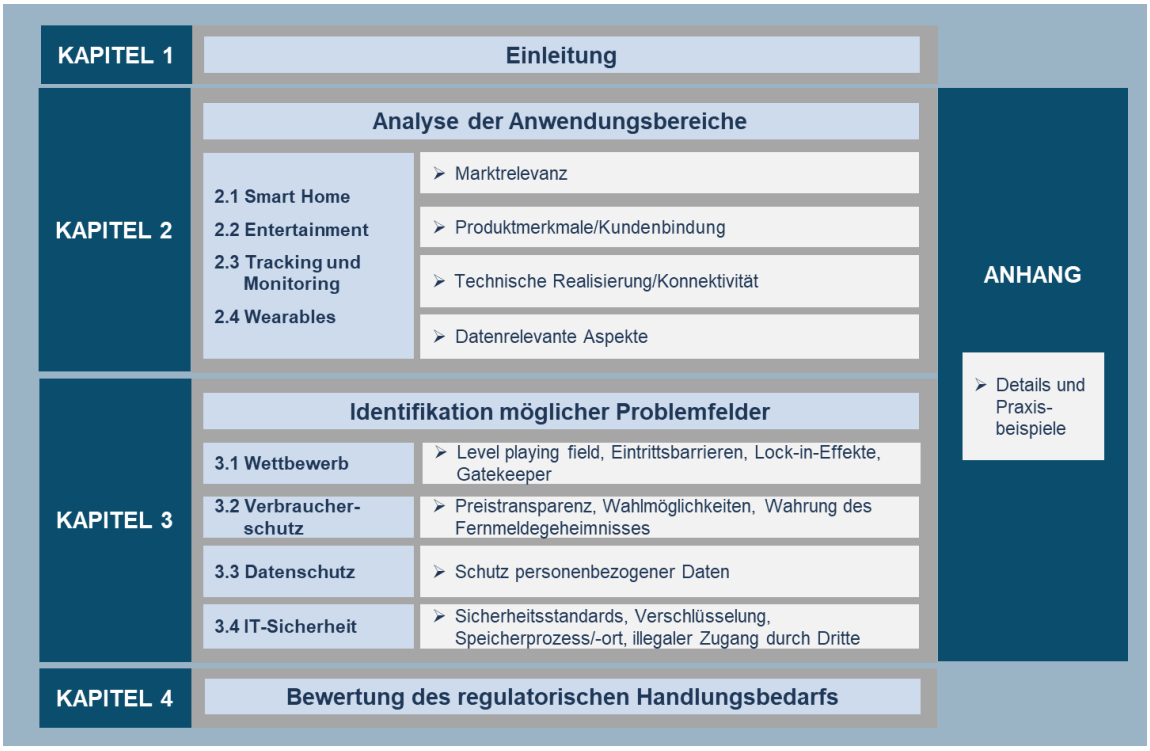
Quelle: WIK.

Die benannten Anwendungsbereiche sind jedoch **nicht immer trennscharf** voneinander abgrenzbar. Smarte Kopfhörer können als Wearables oder Entertainment-Produkte und smarte Blutdruckmessgeräte als Monitoringprodukte oder Wearables aufgefasst werden. Mit smarten Lautsprechern können andere Geräte gesteuert (Smart Home) oder Musik abgespielt werden (Entertainment). Für die vorliegende Studie erfolgt eine Zuordnung der Produkte nach dem jeweiligen Nutzungsschwerpunkt.[4]

Die Ausgangsbasis für die Studie wird mit der **Analyse des Produktspektrums in den relevanten Anwendungsschwerpunkten des Consumer-IoT** in **Kapitel 2** geschaffen. Für jeden Anwendungsbereich werden im Hauptteil der Studie die Marktrelevanz des jeweiligen Segments, typische Produktausprägungen und Ausstattungsmerkmale sowie datenrelevante Aspekte knapp zusammenfasst. Ergänzend werden im Anhang für jeden Anwendungsbereich des Consumer-IoT in einer stärkeren Untergliederung (z.B. Smart Home unterteilt in vernetzte Haustechnik und vernetzte Haushaltsgeräte mit jeweils weiteren Untergruppen) Details und einschlägige Praxisbeispiele ausführlich dargestellt (**A Smart Home**, **B Entertainment**, **C Tracking und Monitoring**, **D Wearables**).

4 Die innerhalb des IoT bedeutenden Bereiche der industriellen Anwendungen (Industrial IoT) und des vernetzten Automobils (Automotive IoT) sind hingegen nicht Gegenstand des vorliegenden Beitrags.

Abbildung 1-2: Inhalt und Gliederung der Studie



Quelle: WIK.

In **Kapitel 3** werden die **Problemfelder in den Bereichen Wettbewerb, Verbraucherschutz, Datenschutz und IT-Sicherheit** mit konkretem Bezug auf die analysierten Anwendungsbereiche erörtert. Auch hierzu enthält der **Anhang** weitergehende und umfassendere Ausführungen.

Abschließend wird in **Kapitel 4** der **regulatorische Handlungsbedarf** im Consumer-IoT-Bereich bewertet.

Die Analyse der Produkte und Anwendungsbereiche erfolgte mittels Internetrecherche in öffentlich zugänglichen Quellen. Dazu gehören neben Produktinformationen von Herstellern, Netzbetreibern und Händlern auch Daten aus der Marktforschung und Produktbewertungen/-tests unabhängiger Stellen. Zur Analyse der Problemfelder wurden insbesondere Beiträge in Fachzeitschriften sowie Informationen von Behörden und anderen öffentlichen Einrichtungen herangezogen.

2 Anwendungsbereiche im Consumer-IoT-Bereich

In den nachfolgenden **Unterkapiteln** werden die Anwendungsbereiche **Smart Home, Entertainment, Tracking/Monitoring und Wearables** hinsichtlich ihrer Relevanz und Anbieterstruktur, der überwiegend genutzten Konnektivitätslösungen sowie relevanter Ausstattungs- und Datenschutzmerkmale untersucht. Die o.g. Überbegriffe lassen sich wiederum in eine Reihe weiterer Anwendungsbereiche und eine Vielzahl von Einzelanwendungen auffächern. Diese werden in den jeweiligen Kapiteln teilweise nur kurz angerissen, weiterführende Details und ausführliche Erläuterungen anhand von Praxisbeispielen finden sich im Anhang.

2.1 Smart Home

Die relevanten Geräte im Smart Home können in die Bereiche **vernetzte Haustechnik** (zur Vernetzung zentraler Funktionen innerhalb des Hauses, wie z. B. Heizung, Haussicherheit mit Türschlössern oder Türklingeln, Beleuchtung über Sensoren) und **vernetzte Haushaltsgeräte** (z. B. Großgeräte wie Kühlschränke sowie Kleingeräte wie Küchenmaschinen, Staubsauger oder Zahnbürsten) eingeteilt werden. Abspielgeräte für Video und Audio werden, ebenso wie die teilweise im Smart Home zur Steuerung genutzten Sprachassistenzsysteme, dem Bereich Entertainment zugeordnet.[5]

Marktrelevanz und Anbieter

Anwendungen für smarte Geräte im vernetzten Zuhause („Smart Home“) reichen von intelligenten Thermostaten über smarte Rauchmelder bis hin zur automatisierten Haustierüberwachung und -fütterung.[6] Eine Umfrage des Branchenverbandes Bitkom ergab, dass 2020 37 % der Deutschen mindestens eine Smart-Home-Anwendung nutzten, Tendenz steigend (siehe Abbildung 2-1).[7]

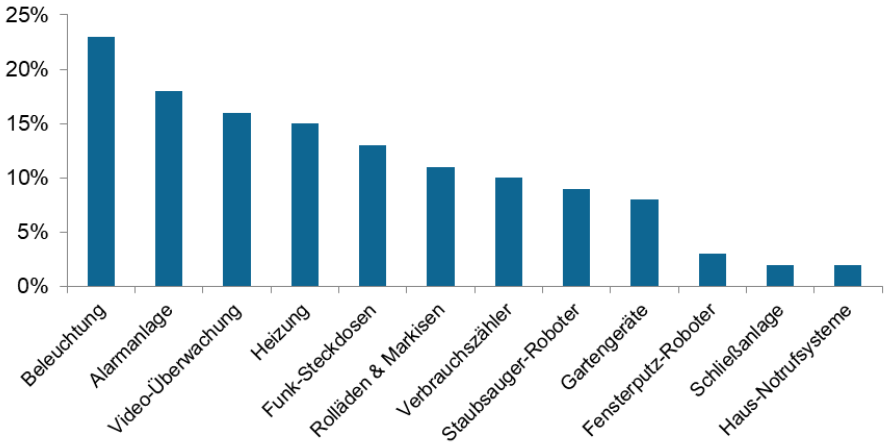
---

5 In **Anhang A** **Smart Home** werden für die genannten Unterkategorien Details und Praxisbeispiele ausführlich dargestellt.

6 Vgl. Bitkom (2020a): Familienfreundliches Smart Home, 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-03/200304_lf_smarthome_usecases.pdf.

7 Vgl. Bitkom (2020b): Das intelligente Zuhause: Smart Home 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-09/200922_studienbericht_smart-home.pdf.

Abbildung 2-1: Einsatz von Smart-Home-Geräten in Deutschland (2020)



Quelle: WIK auf Basis einer Umfrage des Bitkom.[8]

Neben **Start-Ups** mit Fokus auf das Smart Home spielen **klassische Hersteller** von Haustechnik und Haushaltsgeräten eine wichtige Rolle. So bietet der Heizungshersteller Bosch vernetzte Thermostate an, Vorwerk vernetzte Versionen von Staubsaugern und Küchenmaschinen und Philips hat sich als Marktführer bei smarten Lampen etabliert. Auch **Telekommunikationsunternehmen** positionieren sich im Smart Home-Bereich.[9] Große Internetkonzerne wie Amazon, Apple oder Google konzentrieren sich neben einem punktuellem Engagement in einzelnen Bereichen (z. B. Video-Türklingeln bzw. Heimüberwachung, vgl. Tabelle A-2) auf die Bereitstellung von Schnittstellen für Drittanbieter zu ihren Sprachassistenzsystemen.

8 Vgl. Bitkom (2020b): Das intelligente Zuhause: Smart Home 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-09/200922_studienbericht_smart-home.pdf.

9 Dies belegt z. B. der Shop der Telekom Deutschland GmbH (TDG), smarthome.de: Über dieses Portal werden eine eigene Smart-Home-Basisstation (SmartHome Home Base) und verschiedene, bei Verbindung mit der Basisstation über eine Smartphone-App (Magenta SmartHome) steuerbare Geräte aus Eigenproduktion (z. B. Magenta Smart Speaker) oder von Drittanbietern (z. B. Kameras von D-Link, Thermostate von eQ-3) vermarktet.

Konnektivität[10]

Im Smart Home kommen **hauptsächlich Funktechnologien** zum Einsatz. Aufgrund des klar abgegrenzten Einsatzgebietes (Wohnung, Haus, ggf. Garten) werden **Short-Range-Technologien** genutzt.

Grundsätzlich gilt, dass Großgeräte meist eine direkte **WLAN**-Verbindung haben, während kleinere Geräte und Haustechnik teilweise auch **Bluetooth** oder alternative Protokolle wie Zigbee nutzen. Zigbee ist eine Mesh-Netzwerk-Technologie und sorgt daher gerade beim Einsatz vieler verteilter Smart-Home Geräte für eine weitere Funkreichweite als Bluetooth oder WLAN. Je stärker sich Geräte in ihren Funktionen Smartphones oder Laptops annähern, desto eher findet eine Verbindung über WLAN[11] mit dem Internet statt. Der Stromverbrauch von WLAN Geräten ist jedoch hoch und daher für batteriebetriebene Devices ungeeignet. In der praktischen Ausgestaltung macht es für den Nutzer einen Unterschied, ob Geräte im Smart Home ein an den Router angeschlossenes Gateway benötigen oder nicht: Gateways müssen bei der Erstanschaffung eines Systems zusätzlich bzw. im Rahmen eines Starter-Sets erworben werden und erhöhen damit die Anschaffungskosten und schaffen Hürden für die Anschaffung von Smart-Home-Anwendungen. Die zusätzliche Erfordernis eines Gateways hängt von der verwendeten Technologie ab.[12]

Ausstattungsmerkmale

Charakteristisch für das vernetzte Zuhause ist das Zusammenspiel einer **Vielzahl von Sensoren**, die die Funktionen der Geräte ermöglichen. So wäre eine automatisierte Heizungssteuerung ohne Raumtemperatursensor ebenso wenig sinnvoll wie eine Waschmaschine, die ohne Gewichtssensor das Waschmittel dosiert. Anhand dieser Sensoren lassen sich Zustände durch den Nutzer fernüberwachen und einstellen - meist über eine Smartphone-App, teilweise auch über eine separate Steuerzentrale. Weniger verbreitet sind selbstlernende Systeme, die z. B. die Heizung nach einiger Zeit auf Grundlage der zuvor durch den Besitzer vorgenommenen manuellen Justierungen automatisch steuern.

Von regulatorischer Relevanz sind mit Blick auf die Regelungen in § 90 TKG insbesondere diejenigen Geräte im Smart Home, die **Audio- und/oder Videoaufnahmen** ermöglichen (siehe hierzu auch Kapitel 3.2). Diese sind im Überwachungsbereich weit

---

10 Im IoT werden fast ausschließlich Funktechnologien eingesetzt. Diese lassen sich unterscheiden in solche, die auf Kurzstreckenkommunikation (z. B. WLAN, Bluetooth, Zigbee, Z-Wave) ausgelegt sind und solche, die auf Langstreckenkommunikation ausgelegt sind. Letztere können auf lizenziertem Spektrum beruhen, was dem öffentlichen Mobilfunk zuzuordnen ist (GSM, UMTS, LTE, LTE-M, Narrowband-IoT) oder auf unlizenziertem Spektrum (z. B. LoRa, Sigfox). Für weitere Informationen siehe: Gries, C.; Knips, J.; Wernick, C. (2019): Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, WIK-Diskussionsbeitrag Nr. 455, Dezember 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_455.pdf.

11 Seltener kann eine funktionsgleiche Anbindung auch via Ethernet-Kabel zum Router stattfinden.

12 Ein Gateway ist etwa bei Zigbee oder Z-Wave notwendig, während via WLAN oder DECT an den Router angebundene Geräte ohne Gateway ferngesteuert werden können.

verbreitet, werden aber auch von Staubsaugerrobotern genutzt und sind für die bessere Orientierung von vernetzten Rasenmähern geplant. Einzelne Geräten, die sich theoretisch über Sprachbefehle steuern lassen (z. B. Küchenmaschinen) sind auch vorsorglich bereits mit Mikrofonen ausgerüstet, um eine einfache, spätere Nachrüstung mit einer Sprachsteuerung zu ermöglichen.

Datenrelevante Aspekte

Zum Teil erfolgt die Datenverarbeitung und -speicherung auf den Servern bzw. IoT-Plattformen der Hersteller, teilweise findet eine Verarbeitung auch nur lokal auf dem Smartphone des Nutzers statt (z. B. bei Haustechnik und Kleingeräten). Letzteres bietet besseren Datenschutz sowie geringere Möglichkeiten der Datenspeicherung und produktübergreifenden Profilbildung. Unabhängig vom Speicherort kann es zu einer Verknüpfung von Bewegungs- und Standortdaten der Nutzer kommen. Diese kann für den Nutzer durchaus einen Mehrwert bieten, z. B. ein automatisiertes Anschalten der Heizung bei Rückkehr des Besitzers von der Arbeit oder ein korrektes Anwählen des lokalen Supermarktes bei Lebensmittelbestellungen durch den smarten Kühlschrank. Zugleich entstehen jedoch auch Missbrauchspotentiale durch die Erstellung von Bewegungsprofilen, auf die in Kapitel 3.3 und im Anhang näher eingegangen wird.

Da es sich bei Smart-Home Anwendungen zum Teil auch um „Patchwork-Lösungen“ von unterschiedlichen Herstellern handelt, sind Verbraucher ab einem gewissen Umfang auf Meta-Plattformen zur Steuerung und Automatisierung wie z.B. Amazon Alexa, GoogleHome oder HomeKit (Apple) angewiesen. Damit lassen sich die Geräte unterschiedlicher Hersteller zentral steuern und verwalten. Diese Systeme setzen aber wieder einen Hub (z.B. Apple-TV etc.) voraus, der im Zweifel mit einem Zigbee-Hub und den WiFi und Bluetooth Geräten der einzelnen Hersteller kommuniziert. Entsprechend ist davon auszugehen, dass nicht nur die einzelnen Hersteller sondern auch die großen Plattformhersteller Zugriff auf die Daten haben.

Tabelle 2-1: Anwendungsbereich Smart Home

Marktrelevanz und Anbieter
- Stark wachsende Zahl an Anwendungen - Markt wird sowohl durch etablierte Hersteller aus der analogen Welt als auch durch Start-Ups, TK-Unternehmen und (als Händler) durch Internetkonzerne bedient.
Konnektivität
- Bei größeren Geräten häufig über WLAN, bei kleineren meist über Bluetooth - Bei Lampen, Sensoren und Thermostaten sind sowohl Zigbee oder Z-Wave als auch WiFi und Bluetooth gebräuchlich
Ausstattungsmerkmale
- Viele Geräte sind mit Kameras und/oder Mikrofonen ausgestattet - Ausnahmen insbesondere bei Kleingeräten, die nur Sensorik benutzen (Lampen, Thermostate) - Smartphone-App zur Fernsteuerung meist möglich, teilweise nötig; Fernsteuerung per Sprachassistent teilweise im Einsatz
Datenrelevante Aspekte
- Sammlung von Daten und Aggregation in der Cloud je nach Gerät möglich - Sicherheitssysteme mit Besonderheit des regelmäßigen Umgangs mit Daten Dritter (z. B. Personen, die auf ein Grundstück treten) - Einzelne Hersteller werben explizit mit Datensparsamkeit und lokaler Verarbeitung

Quelle: WIK.

2.2 Entertainment

Smarte Entertainmentgeräte nach Definition dieses Diskussionsbeitrags sind insbesondere **vernetzte Fernseher, Spielekonsolen, Sprachassistenzsysteme** bzw. die **Smart Speaker**, auf denen diese genutzt werden, sowie **vernetztes Spielzeug** (Puppen, Drohnen, ferngesteuerte Autos). Eine detaillierte Differenzierung zwischen den entsprechenden Kategorien erfolgt im Anhang.

Bei Produkten im Entertainment-Bereich müssen Hardware und Software getrennt voneinander betrachtet werden, da einige Entertainment-Geräte mit Blick auf ihren Funktionsumfang und ihre Leistungsfähigkeit zunehmend Heimcomputern ähneln.[13] Im Falle smarter Fernseher und Spielkonsolen betrifft dies das Betriebssystem und installierbare Apps, bei smarten Lautsprechern vor allem die darauf laufenden Sprachassistenzsysteme.

13 Im Smart Home muss man dafür eher zwischen Hardware-Gerät und Begleit-App auf dem Smartphone trennen.

Marktrelevanz und Anbieter

Smarte Entertainment-Produkte bedienen einen **Massenmarkt**. 88 % der von Januar bis September 2020 in Deutschland verkauften Fernseher waren Smart-TVs (insgesamt 4,1 Millionen).[14] In den letzten Jahren wurden in Deutschland jährlich im Schnitt 2,3 Millionen Spielekonsolen verkauft, die weltweiten Verkaufszahlen der aktuellen Konsolengeneration[15] liegen bei über 225 Millionen Geräten.[16] Einen smarten Lautsprecher besaßen laut einer WIK-Befragung Ende 2018 bereits 11 % der deutschen Haushalte.[17]

Die Anbieterstruktur unterscheidet sich nach Gerätegruppe deutlich. Bei Fernsehern sind weiterhin dieselben **Hersteller** relevant, die bereits bei **nicht-vernetzten Fernsehern** eine wichtige Marktstellung hatten (z. B. Samsung, Sony). Im Niedrigpreissegment drängen jedoch vermehrt neue Anbieter, insbesondere aus China (z. B. HiSense, TCL) auf den Markt. Große Internetkonzerne stellen typischerweise selbst keine Fernseher her, sondern fokussieren sich auf Set-Top-Boxen/Streaming-Media-Adapter für die Internetanbindung von Fernsehern (Apple TV, Fire TV von Amazon, Chromecast von Google) und auf Betriebssysteme (Android TV von Google, Kooperation von Amazon mit den TV-Herstellern Grundig und ok.).

Bei Spielekonsolen gibt es mit **Nintendo, Microsoft und Sony** drei global tätige Anbieter mit signifikanten Marktanteilen. Diese Anbieter dominieren den Markt seit knapp 20 Jahren, vergleichbare Konkurrenten gibt es nicht.[18] Während die Microsoft **Xbox One** und die Sony **PlayStation 4** rein stationäre, am Fernseher zu betreibende Konsolen sind, kann die **Nintendo Switch** aufgrund eines eingebauten Bildschirms auch mobil genutzt werden. Im November 2020 erschienen mit der Xbox Series X[19] und der PlayStation 5 die neuen Konsolen von Microsoft und Sony, die möglicherweise zu einer Verschiebung der Marktanteile unter den drei Anbietern führen werden.

Bei smarten Lautsprechern bzw. den darauf laufenden Sprachassistenten sind **Amazon** mit dem Sprachassistenten **Alexa** und der Gerätereihe Echo, **Google** mit dem Sprach-

---

14 Vgl. Deutsche TV-Plattform (2020): Marktzahlen, elektronisch verfügbar unter: https://tv-plattform.de/infothek/marktzahlen/.

15 Unter einer Konsolengeneration versteht man Konsolen, die aufgrund der zeitlichen Nähe ihrer Veröffentlichung miteinander in Konkurrenz stehen. Streng genommen gehört die in diesem Diskussionsbeitrag nicht besprochene Konsole Wii U von Nintendo ebenfalls zur aktuellen Generation (Nintendos Veröffentlichungszyklen unterscheiden sich von denen von Microsoft und Sony). Die bis November 2020 aktuelle Generation war die achte Konsolengeneration, siehe: https://en.wikipedia.org/wiki/Eighth_generation_of_video_game_consoles.

16 Vgl. https://de.statista.com/statistik/daten/studie/190754/umfrage/absatz-von-spielkonsolen-in-deutschland/ sowie https://de.statista.com/statistik/daten/studie/160549/umfrage/anzahl-der-weltweit-verkauften-spielkonsolen-nach-konsolentypen/.

17 Vgl. Taş, S.; Hildebrandt, C.; Arnold, R. (2019): Sprachassistenten in Deutschland, WIK-Diskussionsbeitrag Nr. 441, Bad Honnef, 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_441.pdf

18 Die letzte Spielkonsole mit nennenswerten Verkäufen (etwa 10 Millionen weltweit über die Verkaufszeit), die nicht von einem der drei aktuellen Anbieter hergestellt wurde, war 1998 die Sega Dreamcast.

19 Gleichzeitig erscheint mit der Xbox Series S noch eine technisch weniger leistungsfähigere Konsole zu einem geringeren Preis, die jedoch die gleichen Spiele abspielen kann.

assistenten **Google Assistant** und den Gerätereihen Nest Mini/Audio und Google Home sowie **Apple** mit dem Sprachassistenten **Siri** und den HomePod-Geräten führend. Diese Geräte dienen den Anbietern auch als technischer Hub bzw. Steuerzentrale für ihre Smart-Home Plattformen. Einige Alexa-Geräte sind sogar gleichzeitig Zigbee-Hubs. Die Sprachassistenzsysteme finden sich außerdem in Lautsprechern von Drittanbietern aus dem Audio-Bereich (z. B. Sonos, Bose, Marshall) oder auch in Smartphones. Weitere Assistenten (z. B. von Samsung, Microsoft, Deutsche Telekom) sind als Nischenprodukte zu betrachten.[20]

Im Bereich von Spielzeug gibt es viele kleine Anbieter, vor allem im Niedrigpreisbereich. Bei smarten Puppen, die z. B. mit dem spielenden Kind sprechen, gibt es auch einzelne Modelle von traditionellen Spielwarenherstellern (z. B. Mattel).

Konnektivität

Größere Geräte aus dem Entertainment-Bereich werden mittels **WLAN** oder alternativ mittels **Ethernet-Kabel** über den Router mit dem Internet vernetzt. Nur Geräte aus dem Spielwarenbereich und einfache Lautsprecher nutzen ausschließlich **Bluetooth** zur Vernetzung mit Smartphone oder Tablet. Da Smart-TVs und Spielekonsolen in ihrem Funktionsumfang und ihrer Rechenleistung immer mehr Computern ähneln, lassen sich diese auch ohne Anbindung an einen Computer oder ein Smartphone nutzen.[21]

Telefonie mit smarten Lautsprechern über klassische Fest- und/oder Mobilfunknetze ist nur über Umwege möglich (vgl. Tabelle 2-2). So lässt sich der smarte Lautsprecher der Telekom als Mobilteil am Router anmelden und damit als mobiles Festnetztelefon nutzen; es können jedoch nur die vorher im Adressbuch hinterlegten Kontakte angewählt werden. Über andere Lautsprecher (z. B. die Echo-Geräte von Alexa) ist OTT-Telefonie mit anderen Echo-Geräten und Smartphones realisierbar, auf denen die Alexa-App installiert ist. Eine Anmeldung als Festnetz-Telefon am Router ist jedoch nur mit einem - aktuell nicht mehr in Deutschland erhältlichen - Zusatzgerät (Amazon Echo Connect) möglich.

Ausstattungsmerkmale

Kameras sind in Entertainment-Geräten die Ausnahme.[22] Fernseher mit integrierter Kamera, etwa für Videochats, haben sich in Deutschland ebenso wenig durchgesetzt

20 Samsungs Bixby ist nur auf Samsung-Geräten verfügbar, Microsofts Cortana gibt es inzwischen nur noch auf Microsoft-Computern und weder als Smartphone-App, noch in smarten Lautsprechern und Magenta von der Telekom ist nur in deren eigenen Lautsprechern zusätzlich zu Alexa verfügbar.

21 Ggf. müssen für einige Services Benutzerkonten erstellt werden, die sich nicht oder nur mit höherem Aufwand auf dem Gerät selber anlegen lassen (z. B. weil das Einloggen in ein Emailkonto notwendig ist). In einem solchen Fall ist ein Smartphone oder Computer bei der Ersteinrichtung sinnvoll bis notwendig.

22 Als Ausnahme seien hier vor allem Smarte Displays (siehe Exkurs im Anhang) hervorgehoben. Diese funktionieren vergleichbar zu smarten Lautsprechern, sind jedoch mit einem Display und einer Kamera verbunden um Videostreaming und Videotelefonie zu ermöglichen. Eine dauerhafte Aufnahme des Videobildes findet standardmäßig nicht statt.

wie fest verbaute Kameras an der Spielekonsole (vgl. Tabelle 2-2). Relativ weit verbreitet sind jedoch **integrierte Mikrofone**, die der Sprachsteuerung der Geräte und bei Spielekonsolen der Möglichkeit von Sprachchats mit anderen Nutzern dienen. Bei Fernsehern gibt es einzelne Modelle, die ein Umschalten via Sprachsteuerung ermöglichen. Eine große Rolle spielen Mikrofone bei smarten Lautsprechern, da sie die Beantwortung von Fragen oder die Steuerung weiterer Geräte im vernetzten Zuhause ermöglichen. Bei smarten Puppen gibt es auch Modelle, die nach Spracheingabe der Kinder auf deren Eingaben in kindgerechter Form reagieren.

Eine Funktionserweiterung der Fernseher und Spielekonsolen erfolgt über **Apps**, die aus entsprechenden App-Stores auf das Gerät geladen werden können und z. B. Zugang zu Videostreamingdiensten (Netflix, Amazon Prime, YouTube) bieten. Vergleichbar für Sprachassistenzsysteme sind sogenannte Skills, die von Drittherstellern programmiert werden, um Funktionen hinzuzufügen. Beliebt sind z. B. Skills, die das Fernsehprogramm ansagen oder einen bestimmten Radiosender abspielen – diese Funktionen bietet der Lautsprecher nicht unbedingt ab Werk.

Datenrelevante Aspekte

Mit der Annäherung der Funktionalitäten und Kapazitäten von Smart-TVs und Spielekonsolen an Heimcomputer werden auch Daten in entsprechendem Umfang erfasst. Um Nutzern z. B. personalisierte Werbung einzublenden, werden **Nutzungsdaten** durch Fernsehhersteller gesammelt. Über die Browser in den Geräten werden Internetnutzungsdaten gesammelt. Die Apps der Video- und Audiostreamingdienste sammeln ebenfalls Daten und geben den Nutzern auf deren Basis Empfehlungen.

Smarte Lautsprecher hören im aktiven Modus grundsätzlich immer zu, z.T. gibt es jedoch die Möglichkeit das Mikrofon manuell auszuschalten. Jedoch wird der lokale Speicher ständig überschrieben, das Gerät reagiert erst auf ein bestimmtes „Wake Word“. Die Sprachanfrage wird dann an den Server geschickt, dort verarbeitet und anschließend durch den Sprachassistenten im Lautsprecher beantwortet. Die Sprachanfragen werden gespeichert und teilweise auch stichprobenartig zur Qualitätsverbesserung von Mitarbeitern des Herstellers ausgewertet.

Tabelle 2-2: Anwendungsbereich Entertainment

Marktrelevanz und Anbieter
- Hohe Durchdringung, viele Geräte kaum mehr ohne smarte Funktionen erhältlich (z. B. Fernseher) - Sprachassistenten, entwickelt durch große Internetkonzerne, als Steuer-Schnittstelle für verschiedene Geräte unterschiedlicher Hersteller - Vernetztes Spielzeug eher Nischenprodukt
Konnektivität
- Meist WLAN (bzw. Ethernet-Kabel am Router), für technisch einfachere Anwendungen Bluetooth - Ohne Internetanbindung vielfach stark eingeschränkte Nutzungsmöglichkeiten
Ausstattungsmerkmale
- Aktuelle Konsolen und Smart-TVs funktional nahe an PCs/Tablets, viele Anwendungen werden über Apps bereitgestellt - Teilweise Mikrofone enthalten (Smart Speaker), Kameras eher selten
Datenrelevante Aspekte
- Sammlung von Daten und Aggregation in der Cloud je nach Gerät wahrscheinlich, Nutzung etwa für personalisierte Werbung, häufig wird die Erstellung von Benutzerkonten verlangt - Bei Spielekonsolen: Audio- und Textchats möglich - Bei Spielzeug: Verarbeitung von Daten besonders schutzwürdiger Personen (Kinder) in der Cloud

Quelle: WIK.

2.3 Tracking und Monitoring

Der Bereich „Tracking und Monitoring“ im Consumer-IoT kann in die Bereiche **Monitoringlösungen für gesundheitliche und/oder medizinische Zwecke** und **GPS-Tracker** unterteilt werden.

Der **Markt für vernetzte Medizinanwendungen** (teilweise auch bezeichnet als Internet of Medical Things (IoMT))[23] entwickelt sich sehr dynamisch und umfasst eine Vielzahl an Produkten und Lösungen, die teilweise auch Überschneidungen zu anderen Bereichen (z. B. Wearables oder Smart Home) aufweisen. Typische Anwendungen im Gesundheits- und Medizinbereich sind **Patientenmonitoringsysteme** im ambulanten Bereich, die z. B. nach einem Krankenhausaufenthalt, im Pflegefall oder bei chronischen

23 Siehe z. B. Deloitte (2018): Medtech and the Internet of Medical Things - How connected medical devices are transforming health care - July 2018, elektronisch verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf.

Krankheiten häufig in enger Kooperation mit Ärzten eingesetzt werden.[24] Darüber hinaus gibt es eine Vielzahl **einfacher medizinischer Messgeräte** wie z. B. Blutdruckmessgeräte oder smarte Waagen, die Patienten zur Selbstkontrolle nutzen. Ein Zukunftsfeld sind Smart Clothes (vernetzte Kleidungsstücke wie z. B. Unterhemden, die die Herzfunktion überwachen und ggf. einen Notruf auslösen können).

Mittels „**GPS-Tracking**“ können Nutzer Standorte von **Wertgegenständen (z. B. Auto, Fahrrad, Schiff, Koffer), Haustieren oder Angehörigen** (z. B. Kinder, Demenzkranke) überwachen. Dabei werden im Consumer-Bereich Geräte eingesetzt, die die Koordinaten des Trägers über das satellitengestützte Global Positioning System (GPS) erfassen und per Funk übertragen. Im gewerblichen Bereich ist diese Art von Ortung bereits deutlich stärker verbreitet (z. B. in der Logistik). Daneben stellt auch Bluetooth Tracking einen Wachstumsmarkt dar. Jeder Nutzer dieser Tracking-Lösungen installiert die entsprechende App. Alle Geräte auf denen die App installiert ist orten dabei per Bluetooth ständig die Lokation der Bluetooth-Tracker in der Umgebung. So können auch Kunden die sich nicht in direkter Bluetooth-Reichweite des eigenen Trackers befinden ihre Gegenstände finden, sobald ein anderer Kunde mit seinem Smartphone in der Nähe des Gegenstandes/Trackers ist. Die App übermittelt dann die GPS Koordinaten des Smartphones welches den Tracker per Bluetooth gefunden hat an den betreffenden Kunden. Der Vorteil entsprechender Lösungen sind die niedrigen Kosten und der geringere Strombedarf.

Marktrelevanz und Anbieter

Das IoMT ist ein Wachstumsmarkt, der durch strenge regulatorische Rahmenbedingungen bestimmt wird und einen potentiell hohen volkswirtschaftlichen Nutzen aufweist.

Im **Medizinbereich** sind sowohl **etablierte Medizintechnikhersteller** (z. B. Medtronic, Biotronik) als auch **spezialisierte Anbieter von vernetzten Gesundheitsprodukten** (z. B. Fitbit, Withings) tätig. Insbesondere bei letzteren gibt es Überschneidungen mit Herstellern von Wearables. Vernetzte Medizintechnik unterliegt ebenso wie der gesamte Medizinbereich **strengen gesetzlichen Regelungen** und ist durch spezifische komplexe Rahmenbedingungen geprägt. Als Medizinprodukte dürfen nur Produkte mit medizinischer Zweckbestimmung bezeichnet werden, die über unabhängige Prüf- und Zertifizierungsstellen zugelassen werden.[25] Dies bedeutet nicht nur für Start-Ups, sondern auch für ausländische Anbieter eine große Herausforderung und bildet gemeinsam mit den typischerweise hohen Forschungs- und Entwicklungsausgaben **relativ hohe Markteintrittsbarrieren**.

---

24 Die Abgrenzung von B2B-Bereich der vernetzten Medizinprodukte (z. B. Beatmungsgeräte oder Monitoringgeräte, die im Krankenhaus eingesetzt werden) ist dabei teilweise nicht ganz eindeutig.

25 Sie erhalten eine CE-Kennzeichnung, die durch Europäisches Recht geregelt ist, vgl. zur Zertifizierung von Medizinprodukten BfArM, elektronisch verfügbar unter: https://www.bfarm.de/DE/Medizinprodukte/RechtlicherRahmen/inverk/_node.html, Vgl. zur Zulassung im Detail auch Luther/Clarifield (2020),: Marktstudie Medizintechnik 2020, S. 2.

Die Anzahl der Anbieter variiert zwischen den einzelnen Produktkategorien deutlich. So sinkt die Herstellerzahl tendenziell mit zunehmender Komplexität der Geräte und steigendem Spezialisierungsgrad. Dies zeigt sich z. B. daran, dass von Krankenkassen zertifizierte Geräte, die bei chronischen Erkrankungen bestimmte Blutwerte überwachen, von weniger Herstellern angeboten werden als einfache Waagen, die Verbraucher zur Selbstkontrolle einsetzen.

GPS-Tracker werden häufig von spezialisierten IoT-Geräteherstellern konzipiert und in Kooperation mit einem Netzbetreiber vermarktet.[26] Die Produkte werden dann mit einem Konnektivitätspaket verkauft, das auch laufende monatliche Kosten umfasst. Darüber hinaus gibt es einfache Tracker mit SIM-Karten-Slot, die meist über global agierende Online-Portale (z. B. Alibaba, Gearbest) vertrieben werden. Bei diesen Produkten sorgt der Kunde selbst für die Konnektivität über einen entsprechenden Mobilfunkvertrag.

Im Gegensatz zu zertifizierten Medizinprodukten sind die Markteintrittsbarrieren bei GPS-Trackern niedrig; Anbieter können relativ einfach und kostengünstig neue Produkte in den Markt einführen.

Konnektivität

Bei **vernetzten Medizinprodukten** werden verschiedene Lösungen für die technische Anbindung und Auswertung genutzt. Einfache Produkte wie Waagen oder Blutdruckmessgeräte, die typischerweise eine App auf dem Smartphone zum Auswerten nutzen (anstelle oder zusätzlich zum üblichen Display), verbinden sich in der Regel über Bluetooth. Bei der Fernüberwachung des Patienten durch den Arzt, z. B. bei Herzschrittmachern, ist ein den Herzzustand auslesendes Gerät über den öffentlichen Mobilfunk mit einer anderen Anwendung verbunden, auf die der Arzt zugreifen kann. Für zukünftige Anwendungen, die vor allem auf Monitoring mobiler Patienten innerhalb des Krankenhauses zielen, wird voraussichtlich auch 5G (möglicherweise in Form von Campusnetzen) eine Rolle spielen.

Tracker bestimmen ihren Standort über GPS und sind zum Auslesen über weitere Technologien (z. B. Bluetooth, Mobilfunk, LPWAN) mit dem Nutzer verbunden. Am häufigsten werden Tracking-Lösungen für Privatkunden in öffentlichen Mobilfunknetzen realisiert (schwerpunktmäßig GSM oder Narrowband-IoT).

Ausstattungsmerkmale

Medizinprodukte nutzen **hochspezialisierte Sensorik**, um die entsprechenden Funktionalitäten (z. B. Messen von Körperfunktionen) zu ermöglichen. Kameras oder Mikrofone werden derzeit kaum in Medizinprodukte eingebaut.

26 Beispiele sind der Fahrzeugtracker Autoskope des gleichnamigen Start-Ups mit Konnektivität der Deutschen Telekom und der Haustiertracker Tractive des entsprechenden österreichischen Unternehmens mit Konnektivität von O_2/Telefónica, siehe auch Tabelle A-6.

GPS-Tracker sind teilweise eigenständige kleine Geräte, werden aber auch in Alltagsgegenstände integriert bzw. in die Gegenstände, die getrackt werden sollen.

Datenrelevante Aspekte

Die von **vernetzten Medizinprodukten** erhobenen und gespeicherten Daten sind grundsätzlich **personenbezogen und sensibel**. Datenschutzrelevante Vorfälle können zudem in höchstem Maße gesundheitsgefährdend sein. Besonders hohe IT-Sicherheitsrisiken bestehen dabei an Schnittstellen, die zur Übergabe der Daten an Dritte (z. B. Ärzte) eingerichtet werden.

Vernetzte Medizinprodukte unterliegen ebenso wie der gesamte Medizinbereich strengen gesetzlichen Vorschriften und einer kontinuierlichen Kontrolle.

Datenschutzaspekte bilden einen Teil der Risikobewertung, die kontinuierlich vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)[27] vorgenommen wird. Die Datenschutzvorschriften für Medizinprodukte[28] gehen dabei über die allgemeingültigen Regelungen hinaus. Derzeit steht die Umsetzung der europäischen Verordnung ***Medical Device Regulation (MDR)***[29] an, die auf eine Erhöhung von Sicherheit und Leistungsfähigkeit medizintechnischer Lösungen abzielt.[30] Sie enthält in Anhängen spezielle Vorschriften für Softwarenanwendungen und -entwicklung und hebt die Risikoklassen zahlreicher Produkte an, die dann einem Audit unterzogen werden müssen. Aufgrund der strengen Regelungen kann davon ausgegangen werden, dass das Datenschutz- und IT-Sicherheitsniveau im Bereich der Medizinprodukte vergleichsweise höher als in anderen Anwendungsbereichen.

GPS-Tracker erheben aufgrund ihres spezifischen Verwendungszwecks umfassende **Standortdaten**. Allerdings werden bei einigen Nutzungsszenarien nur die Gegenstände

---

27 Das BfArM ist als selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Gesundheit für die Zulassung und die Verbesserung der Sicherheit von Arzneimitteln sowie die Risikoerfassung und -bewertung von Medizinprodukten zuständig, siehe Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) (2020): Über das BfArM, https://www.bfarm.de/DE/BfArM/_node.html

28 Zum Beispiel Digitale-Versorgungs-Gesetz (DVG) vom 19.12.2019, siehe hierzu auch https://www.bfarm.de/DE/Medizinprodukte/DVG/_node.html, Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) vom 8.4.2020, siehe Bundesgesetzblatt (2020): Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale-Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020, elektronisch verfügbar unter: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'632665'%5D&skin=pdf&tlevel=-2&nohist=1.

29 Siehe Europäisches Parlament und Rat der Europäischen Union (2017): VERORDNUNG (EU) 2017/745 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.

30 Vgl. Bundesministerium für Gesundheit: Medizinprodukte – neue EU-Verordnungen, elektronisch verfügbar unter: https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/neue-eu-verordnungen.html sowie Europäische Kommission: Medical Devices -Sector, elektronisch verfügbar unter: https://ec.europa.eu/health/md_sector/overview_en.

selbst, aber nicht deren Nutzer getrackt, d.h. es handelt sich nicht zwingend um personenbezogene Daten. Einen Problembereich in datenschutzrechtlicher Hinsicht bilden insbesondere günstige GPS-Tracker aus Onlineshops, bei denen keine Datenschutzerklärung und keine Informationen zur Datenspeicherung vorliegen.

Tabelle 2-3: Anwendungsbereich Tracking und Monitoring

Marktrelevanz und Anbieter
- *Vernetzte Medizinprodukte*: Nischenmarkt mit hoher volkswirtschaftlicher Bedeutung, hohe Regulierungsintensität, ausgeprägte Markteintrittsbarrieren insbesondere bei komplexeren Lösungen - *GPS-Tracker* im privaten Bereich Nischenmarkt (höhere Bedeutung im gewerblichen Bereich: Flottenmanagement), Zunahme zu erwarten bei einzelnen Produkten (z. B. Pedelecs)
Konnektivität
- *Vernetzte Medizinprodukte:* Anbindung über WLAN oder Bluetooth, Datenverarbeitung über IoT-Plattform, für Echtzeit-Datenübertragung zukünftig 5G - *GPS-Tracker:* GPS-Sensor, Bluetooth, Anbindung meist über das öffentliche Mobilfunknetz
Ausstattungsmerkmale
- *Vernetzte Medizinprodukte:* hohe Bedeutung von hochspezialisierter Sensorik insbesondere bei komplexeren Lösungen - *GPS-Tracker:* Modul zur Standorterkennung, darüber hinaus kaum weitere Funktionen (z. B. Erschütterungsalarm über einen Bewegungssensor, ggf. Kamera, Mikrofon, Lautsprecher), teils mit (limitierter) Telefonfunktion (Alarmanruf), teils in Alltagsgegenstände integriert (z. B. Rücklicht, Hundehalsband, Schuhsohle), teils als Produktbündel konzipiert (Tracker + Vertrag für Konnektivität + ggf. App-Nutzung)
Datenrelevante Aspekte
- *Vernetzte Medizinprodukte:* umfangreiche personenbezogene und sensible Daten, strenge Datenschutzvorschriften - *GPS-Tracker:* Erhebung von Standortdaten, Monitoring/Auswertung über App

Quelle: WIK.

2.4 Wearables

Der Bereich „**Wearables**“ umfasst grundsätzlich alle IoT-Geräte, die der Verbraucher am Körper trägt. Er ist daher nicht überschneidungsfrei mit Produkten aus den Bereichen Entertainment (z. B. smarte Kopfhörer) und Tracking/Monitoring (z. B. in Armbanduhren integrierte GPS-Tracker oder tragbare Medizinprodukte).

In der vorliegenden Studie sind dem Bereich Wearables **Fitnessarmbänder** und **Smartwatches** zugeordnet. Sie werden zusammenfassend betrachtet, da eine eindeutige Abgrenzung nicht möglich ist: Fitnessarmbänder zeigen meist auch die Uhrzeit an, Smartwatches sind häufig mit Fitnessfunktionen (z. B. Pulsmessung) ausgestattet.

Marktrelevanz und Anbieter

Wearables sind ein weltweiter **Wachstumsmarkt**, der auch in Deutschland zunehmend an Bedeutung gewinnt. Einer Marktprognose von IDC zufolge wird sich der Markt für Wearables in den nächsten Jahren weltweit um 7,9 % pro Jahr vergrößern.[31] Eine WIK-Befragung stellte Ende 2018 fest, dass 9 % der Deutschen eine Smartwatch besaßen.[32] Einer Umfrage von Splendid zufolge waren im Jahr 2019 bereits knapp ein Viertel der Deutschen Smartwatch-Nutzer.[33]

Die Entstehung des Wearables-Marktes geht auf die späten 00er Jahre zurück, als spezialisierte Unternehmen wie Fitbit einfache Fitnessarmbänder entwickelten. Die erste Smartwatch wurde von Apple im Jahr 2015 in den Markt eingeführt. Inzwischen gibt es in diesem Bereich eine **Vielzahl an Anbietern** mit sehr unterschiedlichem Hintergrund und ein ebenso **vielfältiges Produktspektrum**. So werden Smartwatches u.a. von ITK-Anbietern, Uhrenherstellern und Modeunternehmen vermarktet. Ein Nischenprodukt stellen die auf die Bedürfnisse von Kindern (bzw. die Wünsche der Eltern) zugeschnittene Smartwatches spezialisierter Hersteller dar, die das Smartphone ersetzen sollen und über eine Telefoniefunktion verfügen.

Die wichtigste Anbietergruppe bilden heute globale Smartphone-Hersteller wie Samsung und **Apple**, deren **weltweiter Marktanteil an verkauften Smartwatch-Geräten[34] und Umsätzen**[35] auf **über 50 %** geschätzt wird. Die Apple Watch ist ein Premiumprodukt, das einen integralen Bestandteil von Apple's Ökosystem bildet und nur in Verbindung mit dem iPhone genutzt werden kann.

Im No name-/Niedrigpreissegment gibt es eine Vielzahl an Produkten internationaler Hersteller, die vorwiegend über Onlineportale vermarktet werden.

---

31 Vgl. IDC (2019): Earwear and Watches Expected to Drive Wearables Market at a CAGR of 7.9%, Says IDC, 19 Juni 2019, elektronisch verfügbar unter: https://www.idc.com/getdoc.jsp?containerId=prUS45271319.

32 Dies ist das Ergebnis einer jährlich vom WIK durchgeführten Panel-Befragung zu verschiedenen Nutzungsbereichen.

33 Vgl. Ergebnisse einer repräsentativen Befragung von 1.193 Personen von Splendid Research (2019): Studie: Optimized Self Monitor 2019, Repräsentative Umfrage zu Tracking-Apps, Wearables und Selbstvermessung in Deutschland, elektronisch verfügbar unter: https://www.splendid-research.com/de/studie-optimized-self.html.

34 Vgl. Waltzer, S. (2020): Global Smartwatch Shipments Grow 20 Percent to 14 Million in Q1 2020, May 07 2020, Strategy Analytics Blogs and Podcasts, elektronisch verfügbar unter: https://www.strategyanalytics.com/strategy-analytics/blogs/wearables/2020/05/07/global-smartwatch-shipments-grow-20-percent-to-14-million-in-q1-2020.

35 Vgl. Counterpoint Research (2020), zitiert nach Telecom Handel, 12. Oktober 2020, S. 15.

Konnektivität

Fitnessarmbänder und Smartwatches werden typischerweise via **Bluetooth** mit dem Smartphone des Nutzers verbunden. Sobald dieses nicht in Reichweite ist, sind einige Funktionen (wie z. B. Telefonie) nur eingeschränkt verfügbar.

Smartwatches mit eigenständiger **Telefoniefunktion**, die mit einer **SIM-Karte** (bzw. eSIM) ausgestattet sind, werden direkt über öffentliche Mobilfunknetze angebunden.[36] Gleichwohl benötigen sie ein Smartphone für die Ersteinrichtung. Als Mobilfunktechnologie wird 4G/LTE genutzt, auch neueste Modelle wie die im September 2020 erschienene Apple Watch 6 unterstützen noch kein 5G und kein internationales Roaming.[37]

Ausstattungsmerkmale

Der Funktionsumfang von Smartwatches hat in den vergangenen Jahren stark zugenommen. Neben der beschriebenen Zeitanzeigefunktion[38] müssen Uhren und Fitness-Armbänder mit der entsprechenden **Sensorik** ausgestattet sein. Die mittels Sensoren erhobenen Daten werden dann über Apps auf dem gekoppelten Smartphone ausgewertet. Zu weit verbreiteten Sensoren gehören Bewegungssensoren zur Realisierung von Funktionen wie z. B. Schrittzählen, Entfernungsmessung und Berechnung der verbrauchten Kalorien. Darüber hinaus sind auch Pulsmessung oder Schlaftracking häufig integriert. Die EKG-App der Apple Watch ist sogar als Medizinprodukt zugelassen. Zunehmend können Apps nicht nur auf dem Smartphone, sondern direkt auf der Smartwatch installiert werden, die über ein spezifisches Betriebssystem verfügt (z. B. Wear OS von Google [das Pendant zu Android auf dem Smartphone] oder watchOS von Apple [das Pendant zu iOS auf dem Smartphone]).

Über eine **SIM-Karte** zur Realisierung einer eigenständigen Telefonie-Funktion verfügen bisher nur wenige Smartwatch-Modelle. Zu diesen gehören zum einen die Premium-Modelle der führenden Smwartwatch-Hersteller (z. B. einzelne Produktvarianten der Apple Watch oder Samsung Galaxy-Watch), zum anderen einige Kinder-Smartwatches. Während die telefoniefähigen Premium-Smartwatches durchgängig eine eSIM enthalten, sind Kinder-Smartwatches entweder mit einer eSIM oder einem SIM-Schlitz zum Einschub einer eigenen SIM-Karte ausgestattet.

Datenrelevante Aspekte

Wearables erheben **in hohem Umfang personenbezogene und sensitive Daten**, die bei Geräten mit hohem Funktionsumfang vergleichbar mit denen eines Smartphones zuzüglich umfassender Gesundheitsdaten sind. Sie umfassen neben Gesundheits-,

---

36 Zumeist sind dies Modelle, die es auch in einer günstigeren Version ohne eigene Mobilfunkanbindung gibt, etwa die Samsung Galaxy Watch und die Apple Watch.

37 Vgl. Apple (2020): Apple Watch GPS + Cellular, elektronisch verfügbar unter: https://www.apple.com/de/watch/cellular/.

38 Der größte Unterschied hierbei zwischen Smartwatch und normaler Uhr ist, dass erstere über digital veränderbare Ziffernblätter/Displayanzeigen verfügt.

Fitness- und Standortdaten auch Nutzungsdaten (z. B. zu genutzten Messenger- und/oder Audiodiensten). Diese Daten haben erhebliches Potential für die Profilbildung der Kunden und können z. B. mittels personenbezogener Werbung zusätzliche Umsätze generieren. Die vielfältigen Aspekte der Datennutzung sind für den Endnutzer auch bei ausführlichen Datenschutzerklärungen nicht immer transparent, insbesondere in Bezug auf die konzerninterne Verwendung bei großen Internetkonzernen. Während jedoch die Marktführer zumindest die gesetzlich geforderten Datenschutzerklärungen bereitstellen, fehlen bei günstigen Nischenprodukten häufig jedwede Informationen über die Datenverwendung und -speicherung.

Tabelle 2-4: Anwendungsbereich Wearables

Marktrelevanz und Anbieter
- Wachstumsmarkt - Vielzahl von Anbietern verschiedener Herkunft - Hohe Bedeutung globaler Hersteller, Apple etwa 50% globaler Marktanteil - Apple Watch Teil des Apple-Ökosystems
Konnektivität
- I.d.R. Verbindung mit Begleitgerät (Smartphone) per Bluetooth - Datenspeicherung auf IoT-Plattformen - Mobilfunktelefonie bisher nur in wenigen Modellen integriert (eSIM)
Ausstattungsmerkmale
- Große Produktvielfalt, zunehmender Funktionsumfang, auch gesundheitsrelevante Apps - Teils mit Telefonie-Funktion über SIM (Apple Watch, Samsung Galaxy, Kinder-Smartwatches)
Datenrelevante Aspekte
- Hoher Umfang an personenbezogenen Daten: Erhebung und Speicherung des Bewegungs- und Nutzerverhaltens (rund um die Uhr) sowie einer Vielzahl an Gesundheitsdaten - Zustimmung des Verbrauchers zur Freigabe seiner Daten für interne Datenverwendung für Nutzung des vollen Funktionsumfangs meist unumgänglich.

Quelle: WIK.

3 Mögliche Problemfelder für Markt und Verbraucher

Einige der in Kapitel 2 skizzierten und im Anhang detailliert beschriebenen Consumer-IoT-Produkte und -Anwendungen sind unter wettbewerblichen, verbraucher- und datenschutz- und IT-sicherheitsrelevanten Aspekten problematisch. Um der unterschiedlichen Relevanz einzelner Problembereiche in den verschiedenen Consumer IoT-Bereichen gerecht zu werden, gehen wir im Folgenden auch auf anwendungsspezifische Besonderheiten ein.

3.1 Wettbewerb

Grundsätzlich bestehen **in den meisten Bereichen des Consumer-IoT eher geringe Markteintrittsbarrieren und ein relativ stark ausgeprägter Wettbewerb**. Vernetzte Produkte werden sowohl von klassischen Herstellern aus der „nicht-smarten Welt“ als auch von Start-Ups entwickelt und vermarktet. Dies gilt insbesondere für günstige und einfache Wearables, Tracking- und Monitoring sowie für viele Smart Home- und einzelne Entertainment-Produkte (z. B. ferngesteuerte Autos oder Drohnen mit Kamera).

Anders stellt sich die Situation in den Teilbereichen dar, in denen für Produktherstellung und -vermarktung **hohe Forschungs- und Entwicklungsausgaben** erforderlich sind. So gibt es bei smarten Fernsehern neben den klassischen Fernsehherstellern kaum neue Player außerhalb des Niedrigpreissegments. Auch smarte Kühlschränke werden nur von wenigen, bereits bei nicht-smarten Geräten aktiven, Herstellern angeboten. In den Bereichen Spielekonsolen und Sprachassistenzsysteme treten jeweils nur drei große Anbieter auf. Der Mehrwert dieser Produkte wird hauptsächlich mit Software[39] und weniger mit Hardware generiert. Ähnliches gilt auch für hochwertige Smartwatches.

In vielen Bereichen des Consumer-IoT nehmen Hersteller von IoT-Hard-/Software **Gatekeeper-Rollen** ein. Dies gilt insbesondere für Sprachassistenzsysteme und Geräte mit einem Betriebssystem und einem App Store (z. B. Fernseher, Spielekonsolen, Smartwatches).[40] Diese können bestimmen, welche Apps und Dienste angeboten werden und sie den Nutzern mit Präferenz empfehlen (z. B. Medien/Streaming oder Information/Nachrichten). Außerdem erhalten App-Store-Anbieter bei jedem Kauf einer App eine Vergütung. Bei Kaufmöglichkeiten über Sprachassistenten sind Auswirkungen auf den Wettbewerb zwischen Händlern und Marktplätzen und ggf. auch auf Produktebene denkbar.

Eng verbunden mit Gatekeeper-Effekten sind **Lock-In-Effekte in Ökosystemen**. Hierbei können im Extremfall Produkte nur bzw. nur im gewünschten Funktionsumfang ge-

39 Die Software wird meist von Drittherstellern erstellt, die ein gewisses Vertrauen in die Größe der Plattform haben müssen (oder vom Plattforminhaber vergütet werden müssen) um Software für eben diese Plattform, möglicherweise sogar exklusiv, zu entwickeln.

40 So lässt Apple beispielsweise alle mit HomeKit kompatiblen Smart-Home Geräte vorher durch sein MFi-Programm zertifizieren. Die Kompatibilität mit der Smart-Home Plattform wird somit zur Kontrolle genutzt.

nutzt werden, wenn gleichzeitig auch andere Geräte aus dem gleichen Ökosystem verwendet werden. Dies ist etwa bei der Apple Watch der Fall, die nur in Verbindung mit einem Apple iPhone nutzbar ist. In geringerem Maße trifft dies auch auf den Smart-Home-Bereich zu, da Kunden tendenziell die mit dem von ihnen genutzten Sprachassistenten kompatiblen Produkte bzw. der Smart-Home Plattform erwerben.[41] Bei Wearables, die für das Angebot von Telefoniefunktionen einer Mobilfunkverbindung bedürfen, gibt es Bindungen an Mobilfunkanbieter, die nutzerseitig nicht aufgehoben werden können. In der Tendenz betrifft dies eher hochwertige Geräte.

Tabelle 3-1: Mögliche Wettbewerbsbeschränkungen in den betrachteten Anwendungsfeldern

Smart Home
- Wettbewerbsprobleme z. B. durch bedingte Unterstützung von Sprachassistenten (Kunde kauft nur Produkte, die sich durch seinen Sprachassistenten steuern lassen) - Ggf. Exklusivverträge mit Händlern, z. B. für Lebensmittellieferung nach Bestellung am smarten Kühlschrank
Entertainment
- Teils hohe Marktkonzentration: Sprachassistenten und Spielekonsolen mit lediglich jeweils drei großen Anbietern - Große Herausforderungen bzgl. Gatekeeper- und Lock-In-Effekten bei Sprachassistenten, Fernsehern und teilweise auch bei Spielekonsolen
Tracking und Monitoring
- Wettbewerblich unkritisch
Wearables
- Bei Premium-Smartwatches: Geschlossene “Ökosysteme“ und damit verbundene Lock-In-Effekte (Apple Watch ist z. B. nur mit iPhone nutzbar) - Beschränkte Auswahl bei der Nutzung der Telefoniefunktion in Premium-

Quelle: WIK.

3.2 Verbraucherschutz

Im Consumer-IoT-Bereich besteht insgesamt eine **zunehmende Intransparenz** für den Verbraucher, die insbesondere auf die steigende Komplexität der Produkte und damit verbundene erschwerte Vergleichbarkeit von Funktionalität und Qualität zurückzuführen ist.

Aufgrund der **stark unterschiedlichen Funktionsumfänge** der Produkte (auch für Produkte mit vergleichbarem Ziel und Zweck) ist es für Endkunden häufig schwierig,

41 Dies ist unter anderem ein weniger schwerer Fall von Lock-In, da viele Sprachassistenten kompatibel mit den Smart-Home-Geräten diverser Hersteller sind und die Geräte teils auch über mehrere Assistenzsysteme ansteuerbar sind, eine Exklusivität ist also seltener.

informierte Entscheidungen ohne intensive Beschäftigung mit der Materie zu treffen. Es ist bspw. sehr aufwendig, einen umfassenden Überblick über die Verfügbarkeit von bestimmten Apps und Diensten auf smarten Fernsehgeräten zu gewinnen.

Auch eine **Qualitätsprüfung** der smarten Funktionen vor der Installation, z. B. bei Haustechnik, ist kaum möglich. Externe Expertise von Handwerkern, Ladenmitarbeitern oder insbesondere (Online-)Produkttests hat daher bei smarten Produkten einen hohen Stellenwert. Durch die „Vermarktung“ klassischerweise sehr simpler Geräte erhöht sich außerdem die Komplexität der Bedienung und erfordert einen höheren Einarbeitungsaufwand. Gleichzeitig wird es schwieriger, Geräte bei Defekten selbst zu reparieren.

Ein großer Teil des Mehrwertes der Geräte, insbesondere bei smarten Fernsehern, ergibt sich durch **auf dem Gerät laufende Dienste (Apps)**. Diese setzen häufig (vor allem im Bereich Musik/Videostreaming) kostenpflichtige Abonnements voraus. Bei Wearables mit SIM-Profil ist ein Mobilfunkvertrag zum Herstellen der Konnektivität erforderlich. In Bereichen wie dem Smart Home beziehen sich Abonnements, wenn überhaupt vorhanden, meist auf Zusatzfunktionen. Dabei ist die Transparenz für den Nutzer jedoch oft gering. So können Funktionen, die bei einem Anbieter ein kostenpflichtiges Abonnement erfordern, bei anderen Anbieter gratis oder aber gar nicht verfügbar sein.

Über geringe Eingriffe können versteckte Kamera oder Mikrofone in viele Produkte eingebaut werden. Verbreitet sind eingebaute **Abhörfunktionen** insbesondere in Kinder-Smartwatches und smartem Spielzeug, vereinzelt jedoch auch in Haushaltskleingeräten wie Staubsaugern und Rasenmähern. In Anbetracht der Marktdynamik und den sinkenden Preisen für qualitativ hochwertige Kameras und Mikrofone erscheint eine engmaschige und zeitnahe Überprüfung seitens der Bundesnetzagentur notwendig, um frühzeitig zu identifizieren, wenn missbräuchliche Sendeanlage nach § 90 TKG vorliegen.

Tabelle 3-2: Verbraucherschutzaspekte nach Anwendungsfeldern

Smart Home
- Wechsel des Herstellers/Produktes bei Haustechnik mit (teils großem) Montageaufwand verbunden - Missbräuchliche Sendeanlagen teilweise bei Staubsaugern und zukünftig bei Rasenmähern (Kameras) bzw. in Küchenmaschinen (Mikrofone zur Sprachsteuerung) - Käufe über Sprachassistenten möglich, jedoch ohne vergleichbar große bzw. einfach überblickbare Auswahl wie auf Webseiten
Entertainment
- Viele Dienste basieren auf Abo-Modellen, insbesondere Streamingdienste - Teils geringe Transparenz bzgl. Diensteverfügbarkeit auf einzelnen Geräten; relativ unzureichend verfügbare Informationen - Einige Videospiele wegen umfangreicher und teils intransparenter kostenpflichtiger Zusatzdienste in der Kritik, insbesondere bei Spielen, die Kinder/Jugendliche als Zielgruppe haben. - Im Bereich Spielzeug (Puppen, ferngesteuerte Autos) teils (möglicherweise) missbräuchliche Sendeanlagen mit Abhörfunktion
Tracking und Monitoring
- Teils Bündelprodukte mit einmaligen und laufenden Kosten: Gerät + Abo + Konnektivitätsvertrag (Mobilfunk); freie Mobilfunkanbieterwahl daher nicht möglich - Medizinprodukte streng geregelt und überwacht - Unerlaubte Abhörfunktionen potenziell möglich
Wearables
- Grundsätzlich Preistransparenz (nur Anschaffungskosten, Ausnahme: Wearables mit SIM) und große Produktauswahl, jedoch steigende Komplexität - Nutzungseinschränkungen bei der Apple Watch: Keine freie Wahl des Mobilfunkanbieters, Begrenzung auf die drei deutschen Netzbetreiber - Bei Kinder-Smartwatches teils unerlaubte Abhörfunktionen

Quelle: WIK.

3.3 Datenschutz

Anwendungsübergreifend erheben viele **vernetzte Geräte umfassende Daten** und lassen damit relativ weitreichende Rückschlüsse auf Präferenzen und Lebenswandel des Nutzers zu. Der **Schutz dieser Daten** durch entsprechende Vorkehrungen auf Anbieterseite ist dabei **nicht immer gewährleistet**.

Bei großen Internetkonzernen besteht zudem die Möglichkeit einer **plattformübergreifenden Profilbildung**. Ob und in welchem Umfang diese Möglichkeiten genutzt werden, ist nicht vollständig nachprüfbar.

Ein nicht geringer Teil der Daten fällt nicht durch die Messungen des Gerätes selbst an, sondern durch **Begleit-Apps** auf den Smartphone, die zur Steuerung genutzt werden an. Dies gilt gerade im Smart-Home-Bereich, wo anhand von Standortdaten in der App gewisse automatische Einstellungen am Haus vorgenommen werden können, wie das Anschalten der Heizung, wenn ein Bewohner in Reichweite des Hauses kommt.

Vor allem bei **kleineren Anbietern mit günstigeren Produkten** sind oft Speicherzeitraum und Möglichkeiten zur Löschung der gespeicherten Daten nicht transparent beschrieben. So müssen beispielsweise Käufer von einfachen Wearables, die über Online-Marktplätze global vertrieben werden, de facto das Risiko einer sehr umfangreichen Speicherung der Daten ohne Löschungsmöglichkeit hinnehmen. Bei großen Anbietern sind entsprechende Klauseln meist transparenter, enthalten dafür teilweise jedoch eine unbegrenzte Speicherung der Daten (vorausgesetzt der Nutzer löscht diese nicht von sich aus bzw. lässt sie löschen).

Tabelle 3-3: Datenschutzaspekte nach Anwendungsfeldern

Smart Home
- Sehr unterschiedlicher Umfang der Datenspeicherung und Cloud-Nutzung, bei kleineren Anbietern mit begrenztem Produktportfolio eher geringerer Grad der Datenspeicherung. - Problematisch sind oft die Begleit-Apps auf dem Smartphone (z. B. bei standortbasierten Funktionen, die auf die entsprechenden GPS-Daten des Smartphones zugreifen). - Kritisch sind Videoüberwachung und Speicherung der dabei entstehenden Bilder.
Entertainment
- Sehr intensive Datenspeicherung und Nutzung, etwa zur „Verbesserung der Angebote“. - Datenschutzbestimmungen formal rechtskonform, aber wegen allgemeiner Formulierungen oft wenig hilfreich - Geräteübergreifende Profilbildung kann/wird für Werbung und zugeschnittene Angebote genutzt - Sprachassistenten kontrollieren Aufnahmen teils händisch durch Mitarbeiter - Daten von Kindern und Jugendlichen werden genauso erfasst wie von Erwachsenen
Tracking und Monitoring
- Standortüberwachung dauerhaft möglich, problematisch insbesondere bei Personentracking - Einfache GPS-Tracker oft ganz ohne Datenschutzerklärung und Information über Speicherung/Verarbeitung - Komplexere medizinische Monitoringlösungen aufgrund sensibler Daten und mehrerer IT-Schnittstellen besonders anfällig, jedoch mittels starker Regulierung gut geschützt
Wearables
- Großer Umfang der Erhebung personenbezogener Daten - Einhaltung von Datenschutzvorschriften bei günstigen Produkten im Massenmarkt problematisch - Marktführer/Anbieter von Premium-Smartwatches halten Datenschutz gemäß DSGVO zwar ein, können jedoch erheblichen Spielraum bei konzerninterner Verwendung der Daten nutzen und so auch Wettbewerbsvorteile erlangen Bei vielen Nischenprodukten Datenschutzaspekte aufgrund fehlender Datenschutzerklärungen nicht nachvollziehbar

Quelle: WIK.

3.4 IT-Sicherheit

Die Risiken für IT-Sicherheitsvorfälle steigen mit dem **Grad der Vernetzung**. Geräte, die sich aus der Ferne steuern lassen und nicht nur lokal im Netzwerk oder über Bluetooth ansteuerbar sind, sind grundsätzlich gefährdeter.

Äußerst problematisch ist, dass bei vielen vernetzten Geräte keine oder nur unzureichende **Sicherheitsupdates** bereitgestellt werden bzw. diese nur für eine relativ kurze Zeit nach Marktstart erhältlich sind. Dies ist sowohl bei günstigen Geräten von No-Name-Herstellern als auch bei etablierten Herstellern mit geringer Expertise im Bereich vernetzter Geräte zu beobachten. Dies kann dazu führen, dass Geräte, bei denen eine Sicherheitslücke publik geworden ist, nicht mehr sicher benutzt werden können, solange sie fernsteuerbar sind. In Konsequenz verlieren sie für den Nutzer dadurch deutlich an Wert.

Verschlüsselungstechniken bei der Datenübertragung werden fast durchgängig verwendet. Ausnahmen sind Kleingeräte (z. B. Wearables) von unbekannten Anbietern, bei denen nicht nachvollziehbar ist, ob bzw. wie diese Anwendung finden.

Mit der immer größer werdenden Rechenleistung und der Annäherung vieler smarter Geräte an die Funktionsfähigkeiten von Computern oder Tablets werden auch die Möglichkeiten für den Einsatz von **Schadsoftware** immer größer. Durch die wenigen Sicherheitsupdates wird es auch in Zukunft immer wieder Fälle geben, in denen smarte Geräte etwa für Botnets genutzt werden. Ein Einfallstor hierfür sind Standard-Passwörter und Standard-Benutzernamen, die bei vielen Geräten bis heute genutzt werden. Dies ist insbesondere bei Geräten, die aus dem Internet ansteuerbar sind, wie bspw. einfache, über IP-Adressen anwählbare, Überwachungskameras ein Sicherheitsproblem.

Tabelle 3-4: IT-Sicherheitsaspekte nach Anwendungsfeldern

Smart Home
- Hohe Anforderungen, insbesondere an Sicherheitsprodukte, die nicht immer erfüllt werden - Standardpasswörter und -nutzernamen als großes Sicherheitsrisiko, insbesondere bei günstigen Geräten (etwa preiswerten IP-Kameras) - Gehackte Geräte lassen sich für Botnetze missbrauchen, ohne dass der Endkunde es merkt - Fernsteuerung, etwa über Sprachassistenten, kann Einfallstor für Angreifer bieten - Länge der Bereitstellung von Softwareupdates nicht transparent, Geräte ohne Updates teils unsicher
Entertainment
- Viele Produkte nähern sich in Rechenleistung und Funktionsumfang immer mehr Computern an und sind damit ähnlichen Gefahren ausgesetzt - Bereitstellung von Softwareupdates nicht transparent, Geräte ohne Updates teils unsicher - Browser in smarten Geräten sollten aufgrund der seltenen Updates nicht für sensitive Anwendungen genutzt werden
Tracking und Monitoring
- Je komplexer das Gerät bzw. die Gesamtlösung und die darauf laufenden Anwendungen, desto kritischer - Datenmanipulation kann bei Medizinprodukten gesundheitsgefährdend sein
Wearables
- Zahlreiche Schnittstellen und zugreifende Apps machen grundsätzlich angreifbar - Führende Anbieter wie Apple erfüllen in der Regel hohe Sicherheitsstandards; Nischenprodukte kleinerer Anbieter haben teilweise ein geringeres IT-Sicherheitsniveau

Quelle: WIK.

4 Bewertung des regulatorischen Handlungsbedarfs

Die vorangegangene Analyse der Anwendungen im Consumer-IoT-Bereich weist auf mögliche Probleme in Bezug auf Wettbewerb, Verbraucherschutz, Datenschutz und IT-Sicherheit hin. Nichtsdestotrotz ist ein großer Teil der Produkte nach geltender Rechtslage unbedenklich und bietet dem Nutzer einen Mehrwert. Einige Produkte und dazugehörige Services und Apps verletzen allerdings potenziell **Schutzgüter des TKG** und werden bei konkreten Verdachtsfällen fallbezogen geprüft. Das offensichtlichste Beispiel hierfür sind missbräuchliche Sendeanlagen als Verstoß gegen § 90 TKG. Stand heute erscheinen diese Praxis und das **bestehende rechtliche und regulatorische Instrumentarium** mit Blick auf die sektorspezifischen IoT-bedingten Herausforderungen jedoch **hinreichend.**

Aufgrund der hohen Dynamik im Consumer-IoT-Bereich gibt es eine immer breitere Palette an angebotenen Produkten und Services. Auch potenziell **problematische Ausstattungsmerkmale wie Kameras und Mikrofone** werden immer günstiger, qualitativ hochwertiger und unauffälliger, so dass diese in immer mehr Geräten verbaut werden.

Verbraucherschutzthemen betreffen darüber hinaus Produkte, die nicht den **technischen Produktstandards** (z. B. in Form gefährlicher Stromanschlüsse) genügen oder **rechtlich unzureichend** sind (z. B. dadurch, dass keine deutschsprachige Bedienungsanleitung mitgeliefert wird), jedoch über **Onlinemarktplätze** vermarktet werden.

Weitere regulatorische Herausforderungen, mit denen sich die Bundesnetzagentur bereits kontinuierlich befasst[42], können sich in Bezug auf die **Frequenznutzung** von Consumer-IoT-Produkten ergeben. Günstige Massenmarktgeräte nutzen zum Teil Funkfrequenzen, die in Deutschland nicht für den Betrieb entsprechender Geräte vorgesehen sind.[43]

Regulierungsrelevante Aspekte, die sich insbesondere auf Mobilfunkübertragung im lizenzierten Funkspektrum beziehen, haben zum aktuellen Zeitpunkt hingegen nur eine geringe Relevanz im Consumer-IoT, da die meisten Produkte über lokale Short-Range-Verbindungen (Bluetooth, WLAN, Zigbee) angebunden werden. Die wenigen Produkte, die öffentliche Mobilfunknetze nutzen, verwenden schwerpunktmäßig internationale und ausländische (exterritoriale Nutzung) Nummern (IMSI und Rufnummern), mit einem starken Anstieg der Nutzung wird in der näheren Zukunft nicht gerechnet. Auch der Anbieterwechsel im Sinne des § 46 TKG ist durch die Art der Nutzung vieler IoT-Geräte

42 Vgl. Winkelmann, S. (2019): Statistik Marktüberwachung 2018, Bericht der Bundesnetzagentur, 09.01.19, elektronisch verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Verbraucher/WeitereThemen/Marktueberwachung/StatistikMarktueberwachung2018.pdf?__blob=publicationFile&v=2.

43 Aus diesem Grund mussten z. B. einige Funkkopfhörer aus dem Verkehr gezogen werden.

weniger relevant.[44] Bei Smartwatches mit eigenem SIM-Profil und eigener Nummer sind jedoch die gleichen Regularien wie bei Nummern für SIM-Karten/Profile in Smartphones zu beachten.

Über diese Aspekte hinaus soll auf zwei weitere Bereiche von grundsätzlicher Bedeutung hingewiesen werden, die im Kontext von Consumer-IoT eine Relevanz haben:

Auffallend ist, dass **Wettbewerbsbeschränkungen**, für die im Kontext der Diskussion über Plattformregulierung nach Lösungen gesucht wird, auch im Feld der Consumer-IoT an Relevanz gewinnen.[45] Neben produktübergreifender Profilbildung durch intensive Datensammlung und Lock-In-Effekte in Ökosystemen spielen hier Gatekeeper-Funktionen eine Rolle, die nicht nur wirtschaftliche, sondern auch medienpolitische und gesellschaftliche Fragen aufwerfen können. Die wachsende Nutzung von Smart Home Lösungen (auf der Metaebene) erhöht den Ökosystem Lock-In der Kunden weiter und erlaubt es den Plattformbetreibern gegenüber den Anbietern von Smart-Home Komponenten Kontrolle auszuüben.

Andererseits stellt sich die grundsätzliche Frage, welche Erwartungen und Anforderungen Politik und Regulierung im Hinblick auf **Wissen, Bewusstsein und Sensibilität der Verbraucher** hinsichtlich Fragen des Daten- und Verbraucherschutzes stellen können und sollen. Viele mögliche Problemfelder in diesem Bereich hängen von der Eigeninitiative des Kunden ab, etwa mit Blick auf die einzuholenden Informationen vor dem Kauf, das Lesen von Datenschutzerklärungen, die Änderung von Standardpasswörtern oder eine regelmäßige Installation von Updates.

Es muss davon ausgegangen werden, dass im dynamischen Consumer-IoT-Bereich mit zunehmender Durchdringung der Lebensbereiche zusätzliche rechtliche und regulatorische Problemfelder entstehen. Daher ist eine sorgfältige und kontinuierliche Auseinandersetzung mit den Anbietern und Produkten sowie daraus resultierenden Veränderungen der Marktverhältnisse erforderlich.

---

44 Vgl. Diskussion zu Nummernnutzung und Anbieterwechsel im M2M-Umfeld: Gries, C.; Knips, J.; Wernick, C. (2019): Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, WIK-Diskussionsbeitrag Nr. 455, Dezember 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_455.pdf.

45 Mit entsprechenden Fragestellungen beschäftigt sich unter anderem die Europäische Kommission in der entsprechenden Sektoruntersuchung: Europäische Kommission (2020): Kartellrecht - Kommission leitet Sektoruntersuchung zum verbraucherbezogenen Internet der Dinge ein, Pressemitteilung vom 16. Juli 2020, elektronisch verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1326.

Literaturverzeichnis

Allianz für Cyber-Sicherheit (2019): Sicherheit von Medizinprodukten - Leitfaden zur Nutzung des MDS2 aus 2019, elektronisch verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed___MDS2.pdf;jsessionid=0908BB5DA77EDE4F6C5CF1E879BD252D.1_cid501?__blob=publicationFile&v=3

Bitkom (2020a): Familienfreundliches Smart Home, 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-03/200304_lf_smarthome_usecases.pdf

Bitkom (2020b): Das intelligente Zuhause: Smart Home 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-09/200922_studienbericht_smart-home.pdf

Bitkom (2020c): Die Zukunft der Consumer Technology – 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-08/200826_ct_studie_2020_online.pdf

Bundesgesetzblatt (2020): Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020, elektronisch verfügbar unter: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'632665'%5D&skin=pdf&tlevel=-2&nohist=1

Bundeskartellamt (2020): Sektoruntersuchung Smart-TVs, Juli 2020, elektronisch verfügbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf

Bundesministerium der Justiz und für Verbraucherschutz sowie Bundesamt für Justiz (2002): Verordnung über die Erfassung, Bewertung und Abwehr von Risiken bei Medizinprodukten (Medizinprodukte-Sicherheitsplanverordnung – MPSV), 24.06.2002, elektronisch verfügbar unter: https://www.gesetze-im-internet.de/mpsv/MPSV.pdf

Bundesministerium für Gesundheit: Verordnung über das Verfahren und die Anforderungen der Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale-Gesundheitsanwendungen-Verordnung – DiGAV), Referentenentwurf, Stand: 09.04.2020, elektronisch verfügbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/DiGAV_RefE.pdf

Deloitte (2018): Medtech and the Internet of Medical Things - How connected medical devices are transforming health care - July 2018, elektronisch verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf

Deloitte (2018): Smart Home Consumer Survey 2018 – Ausgewählte Ergebnisse für den deutschen Markt, elektronisch verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_Home_Studie_18.pdf

ECONUM (2018): Den Puls gefühlt Was beschäftigt die mittelständischen Medizintechnikunternehmen? Studie zur Medizintechnikbranche und Unternehmen in Deutschland, elektronisch verfügbar unter: https://www.johner-institut.de/blog/wp-content/uploads/2017/02/ECONUM-Medizintechnikstudie_2018.pdf

Europäisches Parlament und Rat der Europäischen Union (2017): VERORDNUNG (EU) 2017/745 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, elektronisch verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0745

Frost & Sullivan (2019): Global Smart Thermostats Market, Forecast to 2025, August 2019, elektronisch verfügbar unter: https://www.researchandmarkets.com/reports/4828672/global-smart-thermostats-market-forecast-to-2025

Frost & Sullivan (2019): Patient Monitoring Industry— Analysis of Investment and Trends, 2018, February 2019, elektronisch verfügbar unter: https://www.researchandmarkets.com/reports/4753092/patient-monitoring-industry-analysis-of

Gries, C.; Knips, J.; Wernick, C. (2019): Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, WIK-Diskussionsbeitrag Nr. 455, Bad Honnef, Dezember 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_455.pdf

Luther/Clairfield International (2020): Marktstudie Medizintechnik 2020, elektronisch verfügbar unter: https://www.bvmed.de/download/marktstudie-medizintechnik-2020-luther-clairfield.pdf

Splendid Research (2019): Studie: Optimized Self Monitor 2019, Repräsentative Umfrage zu Tracking-Apps, Wearables und Selbstvermessung in Deutschland, elektronisch verfügbar unter: https://www.splendid-research.com/de/studie-optimized-self.html

Taş, S.; Hildebrandt, C.; Arnold, R. (2019): Sprachassistenten in Deutschland, WIK-Diskussionsbeitrag Nr. 441, Bad Honnef, Juli 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_441.pdf

Winkelmann, S. (2019): Statistik Marktüberwachung 2018, Bericht der Bundesnetzagentur, 09.01.19, elektronisch verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Verbraucher/WeitereThemen/Marktueberwachung/StatistikMarktueberwachung2018.pdf?__blob=publicationFile&v=2

Anhang

A Smart Home

Nachfolgend untergliedern wir die Anwendungen im Smart Home in zwei Bereiche: Zum einen die Vernetzung des Hauses selbst (**Vernetzte Haustechnik**, d.h. Heizung, Beleuchtung oder auch etwaige Sicherheitsmaßnahmen), zum anderen Geräte mit smarten Funktionen innerhalb des Hauses (**Vernetzte Haushaltsgeräte**). Der Bereich der Haushaltsgeräte wird dabei weiter untergliedert in Groß- (z. B. Kühlschränke, Waschmaschinen) und Kleingeräte (z. B. Staubsauger, Zahnbürsten).

A.1 Vernetzte Haustechnik

Vernetzte Hausfunktionen werden immer einfacher nachrüstbar, auch für Mieter und Eigentümer von Wohnungen in Mehrfamilienhäusern. Insbesondere bei Heizungsthermostaten und Licht ist Vernetzung relativ leicht implementier- und bei Bedarf auch wieder zurückbaubar. Auch bei smarten Türschlössern gibt es von innen montierbare Aufsätze. Sicherheitssysteme wie Videokameras oder -türklingeln richten sich, aufgrund der in Mehrfamilienhäusern geteilten Hausflure und -türen, eher an Besitzer von Einfamilienhäusern.

A.1.1 Smarte Heizung

Der Bereich der vernetzten Heizungssteuerung besteht insbesondere aus **fernsteuerbaren und/oder automatisierbaren Heizungsthermostaten**, die auf bestehende Heizkörper montiert werden. Auch zentrale Steuerungen sind in automatisierbaren und fernsteuerbaren Versionen verfügbar.

Marktrelevanz und Anbieterstruktur

Neben eher **klassischen Thermostat- und Energietechnikherstellern** wie Bosch oder Danfoss gibt es solche Systeme auch von **Netzwerktechnikherstellern** wie devolo oder AVM (bekannt durch die Marke Fritz!). Von den großen Internetkonzernen bietet nur das Google-Unternehmen Nest eigene smarte Thermostate an.[46] Schnittstellen zu den Sprachassistenzsystemen von Amazon, Apple und Google zur Steuerung der Geräte sind jedoch von vielen Anbietern implementiert.

46 Die aktuelle Version des Nest-Thermostats wird in Deutschland nicht vertrieben und ist nur gegen hohe Versandkosten importierbar.

In einer repräsentativen **deutschen Smart-Home-Konsumentenbefragung (2018)** gaben 10 % der Befragten an, bereits vernetzte Heizungslösungen bzw. Thermostate zu nutzen, 12 % planten sie für das kommende Jahr und weitere 33 % äußerten ein grundsätzliches Interesse.[47] Stand 2020 nutzten bereits 15 % der deutschen Haushalte eine Art von smarter Heizungssteuerung; es ist also ein Wachstum erkennbar.[48] Analystenschätzungen über die Größe des Weltmarktes für **smarte Thermostate** divergieren stark voneinander. So schätzt Mordor Intelligence diesen auf ca. 850 Millionen USD in 2019[49], während Frost & Sullivan diesen schon für 2018 auf die fast doppelte Größe (1,6 Milliarden USD) bemisst.[50] Die prognostizierten Wachstumsraten belaufen sich auf 16-23 % pro Jahr.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Grundsätzlich sollen intelligente Thermostate bzw. entsprechende Steuerungen dafür sorgen, unnötiges Heizen zu vermeiden und Raumtemperaturen ohne manuelles Verstellen der Heizung auf dem vom Nutzer gewünschten Niveau zu halten. Für die Heizungssteuerung gibt es smarte Wandthermostate, die bestehende Wandthermostate ergänzen oder ersetzen und mit denen sich herkömmliche Heizungselemente zentral steuern lassen. Weiter verbreitet sind jedoch smarte Thermostate, die direkt am Heizkörper angebracht werden und entweder über das Gerät selbst oder über eine Smartphone-App (oder ggf. Weboberfläche) gesteuert werden können (teilweise ist dabei eine zusätzliche Basisstation nötig, etwa um als Gateway zum Router eine Vernetzung zu ermöglichen[51]).

Bei der Vernetzung der Geräte untereinander und mit dem Nutzer kommt es insbesondere auf einen geringen Energieverbrauch an, damit Batterien in Thermostaten möglichst lange halten. Die Realisierung geschieht über verschiedene Technologien. Je nach Anbieter kommen proprietäre Lösungen auf Basis des 868 MHz-Frequenzbandes, Zigbee oder auch Z-Wave zum Einsatz. Während diese Lösungen alle ein eigenes Gateway benötigen, lassen sich Lösungen auf Basis von Bluetooth oder auch DECT direkt

---

47 Vgl. Deloitte (2018): Smart Home Consumer Survey 2018 – Ausgewählte Ergebnisse für den deutschen Markt, elektronisch verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_Home_Studie_18.pdf.

48 Vgl. Bitkom (2020b): Das intelligente Zuhause: Smart Home 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-09/200922_studienbericht_smart-home.pdf.

49 Vgl. Mordor Intelligence (2020): Smart Thermostat Market – Growth, Trends, and Forecast (2020 – 2025), August 2020, elektronisch verfügbar unter: https://www.researchandmarkets.com/reports/4535767/smart-thermostat-market-growth-trends-and.

50 Vgl. Frost & Sullivan (2019): Global Smart Thermostats Market, Forecast to 2025, August 2019, elektronisch verfügbar unter: https://www.researchandmarkets.com/reports/4828672/global-smart-thermostats-market-forecast-to-2025.

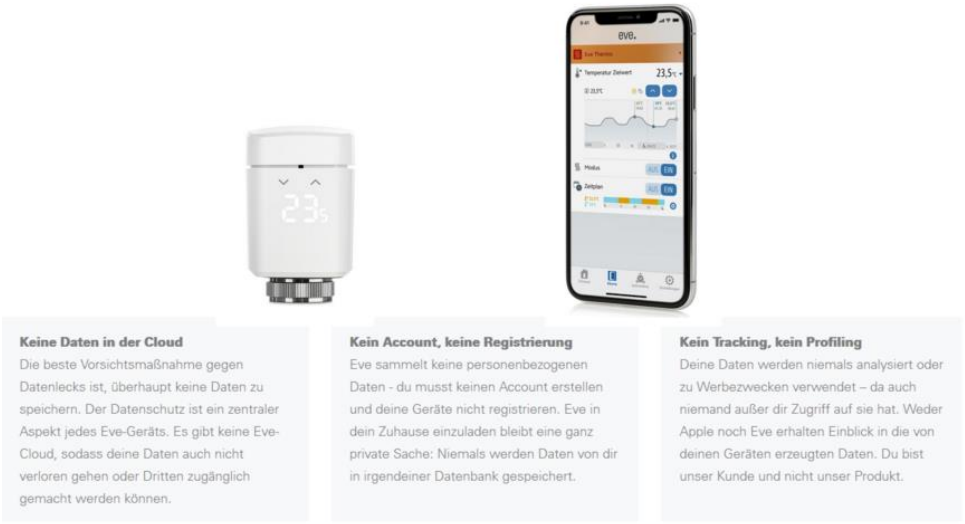
51 Ausschließlich am Gerät programmierbare Heizungssteuerungen, auf die nicht aus der Ferne zugegriffen werden kann und die nicht mit anderen Heizelementen und/oder dem Nutzer kommunizieren, werden nicht als smarte Geräte eingestuft und sind daher nicht von der IoT-Definition dieses Diskussionsbeitrages erfasst.

mit Smartphone oder Router verbinden.[52] Da keine großen Datenmengen übertragen werden müssen, unterscheiden sich die Standards, neben dem Gateway, vor allem in der Reichweite (z. B. bei Bluetooth und Z-Wave geringer als bei Zigbee).

Erhobene Daten und Datenschutz

Die Geräte selbst erfassen Daten zur Raumtemperatur und haben dafür entsprechende Sensorik. Außerdem kann ein Teil der verfügbaren Geräte erkennen, ob bspw. ein Fenster offen steht und die Heizleistung in diesem Falle herunterregeln. Bei der Datenerhebung gibt es relativ **große Unterschiede zwischen den Anbietern**. Einige Anbieter speichern alle Daten lokal und verwenden nach eigenen Angaben weder Cloudspeicherung noch Nutzertracking.

Tabelle A-1: Produktbeispiel: Eve Thermo - Smartes Heizkörperthermostat[53]

<table>
<tr><td> 
</td></tr>
<tr><td>– Anbindung auf Bluetooth-Basis (Bluetooth Low Energy)
– Nur mit Apple-Geräten kompatibel
– iPhone oder iPad für Steuerung nötig, Apple Homepod oder Apple TV für Fernsteuerung, Sprachsteuerung über Siri möglich
– Datensparsamkeit als Teil des Geschäftsmodells, jedoch Teil des erweiterten Apple-Ökosystems → Lock-In-Effekte
– Gleiches gilt für weitere Produkte des Herstellers (z. B. Lampen, Kameras)</td></tr>
</table>

Quelle: WIK.

Andere Anbieter nutzen deutlich mehr Daten und analysieren und verknüpfen diese auch. So erfasst die App des Herstellers Tado die Entfernung der Haushaltsmitglieder

52 Vgl. Sternkopf, M. (2020): Vergleichstest 2020: Die besten smarten Heizkörperthermostate, 30.03.2020, in: techstage.de, elektronisch verfügbar unter: https://www.techstage.de/ratgeber/UPDATE-Vergleichstest-Sechs-Smart-Home-Heiz-Thermostate-4324482.html.

53 Vgl. https://www.evehome.com/de/eve-thermo sowie https://www.evehome.com/de/privatsphaere.

zum Smart Home und regelt die Heizung dementsprechend (als kostenpflichtige Zusatzfunktion). Dies führt dazu, dass jedes Haushaltsmitglied durch Blick auf den Heizungsstand aus der Ferne weiß, ob jemand zu Hause ist und ggf. auch Entfernungen des nahesten Haushaltsmitgliedes zum Haus approximieren kann.[54]

Verbraucherschutz und IT-Sicherheit

Die verbraucherrechtlichen Herausforderungen bei smarter Heizungstechnik sind relativ gering. Smarte Steuerelemente, die klassische Elemente des Hauses mit Konnektivität versehen, können ggf. einen hohen Montageaufwand nach sich ziehen. Ein Produkt/Herstellerwechsel bringt daher den gleichen Montageaufwand wie die Erstinstallation mit sich. Laufende Kosten, wie Abonnements, sind nur bei wenigen Modellen vorhanden und betreffen meist Zusatzfunktionen.[55] Teilweise sind solche Funktionen auch in einer ersten Testphase nach Kauf noch kostenlos und erst nach längerer Nutzung kostenpflichtig.

Mit Blick auf die IT-Sicherheit bestehen ähnliche Probleme wie bei anderen Geräten im Bereich der vernetzten Haustechnik. Standard-Passwörter und Nutzernamen können einen Missbrauch der Geräte, bspw. für Botnetze nach sich ziehen. Ein Verstellen der Heizung durch einen Angreifer ist denkbar, jedoch weniger wahrscheinlich.

Wettbewerbliche Aspekte

Durch eine Sprachsteuerung verstärken sich die verbraucherrechtlichen und wettbewerblichen Herausforderung eines Smart Homes. Zum einen ist jedes zusätzliche Gerät (etwa ein smarter Lautsprecher zur Steuerung) eine potenzielle Quelle für IT-Sicherheitsvorfälle, zum anderen wirkt sich Marktmacht auf dem Markt für smarte Lautsprecher und Sprachassistenten nicht nur auf den Markt für smarte Heizungssteuerung, sondern auch auf den Markt für Smart-Home-Systeme aus.[56]

Abschließend muss bei smarten Heizungssteuerungselementen herausgestellt werden, dass sie zum Erreichen gesamtgesellschaftlicher Umweltziele beitragen, sofern sie zum von den Herstellern propagierten **niedrigeren Energieverbrauch** führen. Sie haben daher tendenziell stärkere **positive externe Effekte** (für Volkswirtschaft und Gesellschaft) als andere IoT-Geräte im Privatkundenumfeld.

---

54 Vgl. Sternkopf, M. (2019): Tado Thermostat V3+ im Test: Wirklich smart nur im Abo, in: techstage.de, elektronisch verfügbar unter: https://www.techstage.de/test/Tado-Thermostat-V3-im-Test-Wirklich-smart-nur-im-Abo-4308029.html.

55 So bietet etwa innogy gegen Aufpreis die Möglichkeit, sich Benachrichtigungen ihrer Smart-Home-App auch via SMS zustellen lassen zu können. Im Shop zu finden unter: https://webshop.livisi.de/INTERSHOP/web/WFS/Stores-B2CStore-Site/de_DE/-/EUR/ViewProduct-Start?SKU=70011716&CategoryName=Apps&CatalogID=SmarthomeCatalog.

56 Grundsätzlich ist dies auch andersherum denkbar, wenn Nutzer etwa ein Smart-Home-System benutzen und dann gezielt einen smarten Lautsprecher kaufen, der den Sprachassistenten benutzt, der mit ihrem System kompatibel ist.

A.1.2 Smarte Haussicherheit

Im Bereich der Haussicherheit gibt es mit **Türklingeln**, **Überwachungskameras** für Innen- und/oder Außenbereiche, **Alarmanlagen** und **Türschlössern** verschiedene Anwendungsbereiche. Gemeinsam haben sie die **hohe Kritikalität**, da ein Versagen der Systeme weitreichende Folgen haben kann.

Marktrelevanz und Anbieterstruktur

Vernetzte Überwachungskameras sind in den letzten Jahren immer preiswerter geworden und produzieren gleichzeitig **immer hochauflösendere Bilder und Videos**. Anwendungsbereiche sind im Innen- wie im Außenbereich (Garten) des Hauses denkbar sowie als Video-Türklingel im Eingangsbereich. In Deutschland nutzt immerhin ein zweistelliger Anteil der Haushalte solche Systeme (siehe Abbildung 2-1).

Insbesondere **Video-Türklingelsysteme** werden inzwischen auch von **großen Internetkonzernen** stark beworben, insbesondere Amazon (mit der Marke Ring) und Google (mit der Marke Nest) sind im Bereich der Videoüberwachung tätig. Im Nischenbereich der smarten Türschlösser sind jedoch auch verschiedene kleinere Anbieter tätig und erfolgreich.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Smarte Türklingeln mit Kamera ermöglichen - teils als kostenpflichtige Option - den Zugriff auf das Kamerabild über das Smartphone sowie in unterschiedlicher Form[57] auch die Aufzeichnung des Bildes. Häufig gibt es weiterführende Funktionen wie eine automatische Benachrichtigung bei Personenerkennung oder die Implementierung von Mikrofon und Lautsprecher (bzw. Gegensprechfunktion) an der Kamera. Angebunden sind die Kameras via WLAN, um die relativ hohen Datenmengen der Videoaufzeichnung[58] zum Nutzer zu streamen.

Smarte Alarmanlagen können entweder Kameras oder spezifische Sensorik nutzen, um das Eindringen von Einbrechern zu erkennen. Alarmanlagen sind häufig in das WLAN eingebunden, so dass der Nutzer die Abschaltung über eine Smartphone-App vornehmen kann. Es gibt auch Alarmanlagen (z. B. für Ferienhäuser), bei denen die Konnektivität über öffentliche Mobilfunknetze hergestellt wird. Die Kommunikation mit dem Nutzer findet in diesem Falle über SMS statt.

Als Weiterentwicklung von Schließsystemen über Fernbedienungen können smarte Türschlösser gesehen werden. Die Türen werden in diesem Falle über eine Smartphone-App oder über Annäherung des Nutzers bzw. des Smartphones des Nutzers an die Tür, seltener auch über Sprachsteuerung, geöffnet. Einige dieser Schlösser sind auch

57 Dauerhaft oder in bestimmten Situationen.

58 Hochauflösende Videoüberwachung, insbesondere bei Speicherung des Geschehens auch ohne konkreten Anlass (etwa Auslösen einer Klingel), ist die von der Datenmenge her intensivste Anwendung im Smart Home nach der Definition dieses Diskussionsbeitrags.

nachrüstbar, können also von innen auf ein gängiges, bestehendes Schloss montiert werden. Vernetzt werden sie meist via Bluetooth, seltener auch über Z-Wave, Zigbee oder WLAN. Unterschiedlich sind hierbei die Reichweite, die Erfordernis eines separaten Gateways und die Komplexität in der Handhabung.[59]

Erhobene Daten und Datenschutz

Bei Außen- und Türklingelkameras ergeben sich grundsätzliche rechtliche Fragen bzgl. der informationellen Selbstbestimmung, insbesondere von unbedarften Dritten. Der Überwachungsgrad auf Privatgrundstücken und ggf. über die Grundstücksgrenze hinaus wird schon lange diskutiert. So entschied der Bundesgerichtshof 2011, dass Video-Türklingelsysteme in Mehrfamilienhäusern auch bei fehlender Zustimmung aller Wohnungseigentümer installiert werden dürfen, sofern nur eine temporäre Bildübertragung erfolgt.[60] Eine **Überwachung**, die ausschließlich **auf dem eigenen Grundstück** stattfindet, ist **grundsätzlich erlaubt.** Das Filmen fremder Personen hingegen darf nur bei konkretem Anlass (z. B. vergangene Wohnungseinbrüche) und bei sichtbarer Kamera zu Abschreckungszwecken erfolgen.[61] Öffentlicher Raum darf ebenfalls nur bei berechtigtem Interesse und in sehr begrenztem Maße (z. B. Filmen eines schmalen Gehwegstreifens, weil das dahinter stehende Auto mehrmals beschädigt wurde) überwacht werden. Besucher sollten auf die Überwachung hingewiesen werden (z. B. über Schilder).[62] Im Innenbereich ist eine Überwachung, z. B. von Babysitter oder Putzkraft, nur in akuten Verdachtsfällen oder bei erteilter Zustimmung möglich. Die günstige und einfache Verfügbarkeit von Überwachungskameras kann zu einer stärkeren Nutzung durch nicht ausreichend informierte Haus- und Wohnungsbesitzer führen, so dass Rechtsbrüche ggf. zunehmen.

---

59 Vgl. Price, M.; Crist, R. (2020): How to buy the right smart lock for your front door, in: cnet.com, 08.07.20, elektronisch verfügbar unter: https://www.cnet.com/news/how-to-buy-the-right-smart-lock-guide-tips/.

60 Auch die ohne konkreten Anlass geäußerte Befürchtung, dass unbemerkt eine Aufrüstung zu einer dauerhaften Videospeicherung erfolgt, genügt nicht, siehe: Tölle, D. (2014): Bundesgerichtshof: „Klingel-Cam“ zulässig, in: rechtambild.de, 17.01.14, elektronisch verfügbar unter: https://www.rechtambild.de/2014/01/bundesgerichtshof-klingel-cam-zulaessig/.

61 Vgl. Landgericht Essen (2019): Urteil zu Aktenzeichen 12 O 62/18, 30.01.19, elektronisch verfügbar unter: https://www.justiz.nrw.de/nrwe/lgs/essen/lg_essen/j2019/12_O_62_18_Urteil_20190130.html.

62 Vgl. Stiftung Warentest (2020): FAQ Private Videoüberwachung – Das ist erlaubt – und das nicht, in: test.de, 24.07.20, elektronisch verfügbar unter: https://www.test.de/FAQ-Private-Videoueberwachung-Das-ist-erlaubt-und-das-nicht-5045901-0/.

Tabelle A-2: Produktbeispiel: Videoüberwachungssysteme der Amazon-Tochter Ring[63]

- Kameras für Innen- und Außenbereich sowie Video-Türklingeln erhältlich
- Videoprojektion auf die App auf dem Smartphone oder auf Amazon-Geräte mit Display -> Mehr Nutzungsmöglichkeiten im Amazon-Ökosystem
- Live-Video und bewegungsaktivierte Benachrichtigungen möglich
- Gegensprechfunktion inkludiert
- Abonnement (ab 3€/Monat) möglich für 30-Tage-Videoverlauf und Speicher- und Teilmöglichkeit
- Datenspeicherung von Aufnahmen von Dritten denkbar

Quelle: WIK.

In der Vergangenheit gab es Berichte über Fälle, in denen die Geschäftsführung und Entwicklungsabteilung des Anbieters Ring über die Mailadressen auf Kundenvideos zugegriffen haben; dies wurde von Ring jedoch dementiert.[64] Ähnliche Praktiken wurden auch über Amazons Cloud Cam berichtet, die in Deutschland jedoch nicht erhältlich ist.[65]

Auch smarte Türschließanlagen können problematisch sein. Sie bieten häufig eine sogenannte „Auto Unlock"-Funktion für die automatische Öffnung der Haustür, sobald der Bewohner (mit dem Smartphone in der Tasche) von außen in die Nähe der Tür kommt.[66] Dies bringt die gleichen Datenschutzherausforderungen mit sich wie auch andere Dienste, die Standortdaten der Nutzer erfassen und über eine App managen.

63 Vgl. https://de-de.ring.com/pages/protect-plans.

64 Vgl. Tremmel, M. (2019a): Mitarbeiter konnten in Kundenwohnungen blicken, in: golem.de, 11.01.19, elektronisch verfügbar unter: https://www.golem.de/news/amazon-tochter-ring-mitarbeiter-konnten-in-kundenwohnungen-blicken-1901-138682.html.

65 Vgl. Tremmel, M. (2019c): Amazon-Mitarbeiter sichten Bilder von Cloud-Kameras, in: golem.de 10.10.19, elektronisch verfügbar unter: https://www.golem.de/news/ueberwachung-amazon-mitarbeiter-sichten-bilder-von-cloud-kameras-1910-144371.html.

66 Beispielhaft beim Anbieter Nuki: https://nuki.io/de/hilfe/smart-lock-de/sl-funktionen/auto-unlock/ Hierbei wird per GPS registriert, dass der Nutzer in die Nähe des Hauses kommt (z. B. auf 100m). Wenn er dann innerhalb eines gewissen Zeitrahmens in die Nähe der Haustür kommt (z. B. auf 10m), dann wird diese per Bluetooth automatisch aufgeschlossen.

Außerdem ist es damit möglich, mit einem gefundenen oder gestohlenen Smartphone Türen zu entriegeln, auch ohne das Gerät zu entsperren.

Verbraucherschutz und IT-Sicherheit

Sicherheitssysteme müssen **hohen Ansprüchen an die IT-Sicherheit** genügen. Eine Sicherheitslücke kann nicht nur zum Ausrauben des Nutzers führen, sondern auch einen nicht behebbaren Reputationsverlust für den Anbieter bedeuten. In der Praxis werden immer wieder gravierende Sicherheitslücken identifiziert, die aus Verbraucherschutzsicht schnellstmöglich nach Bekanntwerden geschlossen werden müssen.[67]

Einige der modernen Systeme lassen sich in Smart-Home-Systeme integrieren und über Sprachassistenten steuern, so dass die Tür per Sprachsteuerung geöffnet und abgeschlossen werden kann. Um Angriffe zu erschweren (etwa durch Einbrecher, die einen Sprachassistenten durch ein geöffnetes, aber außer Reichweite befindliches, Fenster aktivieren), muss dabei zusätzlich ein Sicherheits-PIN eingesprochen werden.[68] Da jedoch z. B. auch das Abgreifen eines solchen PINs durch einen Beobachter in Hörweite denkbar ist, raten selbst Befürworter smarter Türschlösser von der Nutzung solcher Sprachsteuerungen ab.[69]

Wenn kameragestützte Alarmsysteme oder Hausschutzsysteme über WLAN angebunden sind, weisen sie auch die entsprechenden Schwachstellen dieser Konnektivitätslösung auf. So können die Systeme relativ einfach über sogenannte Deauther bzw. Deauth-Attacken ausgeschaltet werden. Hierbei lässt sich auch ohne Einwahl ins WLAN, die Verbindung der Kamera mit dem Netzwerk kappen. Die wenigsten Systeme sind gegen solche Angriffe geschützt.[70]

Bei einigen Anbietern kann es außerdem sein, dass das Ein- und Ausschalten der Alarmanlage über das Smartphone nur funktioniert, wenn die Cloud des Anbieters verfügbar ist. Während Wartungsarbeiten des Anbieters an seiner Infrastruktur ist der Nutzer also möglicherweise aus seinem eigenen Haus ausgesperrt bzw. löst bei Eintreten

---

67 Beispiel: Bei Systemen des Herstellers Abus gelang es Hackern durch das Abfangen und die Manipulation eines regelmäßig gesendeten Funkcodes Überwachungsanlagen ohne Autorisation abzuschalten. Die Sicherheitslücke der Anlage wurde drei Monate nach Entdeckung aufgrund des Ausbleibens einer Reaktion des Anbieters veröffentlicht, siehe: Tremmel, M. (2020a): Abus-Alarmanlage aus der Ferne ausgeknipst, in: golem.de, 03.08.20, elektronisch verfügbar unter: https://www.golem.de/news/sicherheitsluecke-abus-alarmanlage-aus-der-ferne-ausgeknipst-2008-150020.html.

68 Vgl. Költzsch, T. (2017): Nuki-Smart-Lock lässt sich mit Alexa öffnen, in: golem.de, 26.04.17, elektronisch verfügbar unter: https://www.golem.de/news/spracheingabe-nuki-smart-lock-laesst-sich-mit-alexa-oeffnen-1704-127513.html.

69 Vgl. Clausing, E. (2019): Zertifiziert! Nuki Smart Lock 2.0, in: iot-tests.org, 21.05.19, elektronisch verfügbar unter: https://www.iot-tests.org/de/2019/05/zertifiziert-nuki-smart-lock-2-0/.

70 Vgl. Tremmel, M. (2019b): Wer hat die Winkekatze geklaut?, in: golem.de, 02.10.19, elektronisch verfügbar unter: https://www.golem.de/news/wlan-kameras-ausgeknipst-wer-hat-die-winkekatze-geklaut-1910-144199.html.

den Alarm aus. Auch die Internetverbindung des Hauses muss funktionieren, damit der Nutzer die Anlage aus der Ferne an- und ausschalten kann.

Unter Experten gelten smarte Kameras als die unsichersten Geräte im Smart Home, da sie direkt und dauerhaft ein Videobild ins Internet streamen, das dann mit dem Smartphone von unterwegs abgerufen werden kann. Wenn etwa Mailadresse und Passwort des Nutzers kompromittiert sind[71], dann kann damit auch auf die Kamerabilder zugegriffen werden.[72]

Wettbewerbliche Aspekte

Wettbewerbliche Probleme sind bei smarten Sicherheitssystemen aktuell nicht ersichtlich.

A.1.3 Smarte Beleuchtung

Sensitive Beleuchtungssysteme auf Basis von Bewegungs- oder Geräuschmeldern gibt es schon seit Jahren, in letzter Zeit gewinnen aber auch fernsteuerbare Systeme an Bedeutung.

Marktrelevanz und Anbieterstruktur

Intelligente Beleuchtungssysteme werden aufgrund der relativ geringen Komplexität und Kosten, der einfachen Installation und Deinstallation häufig als Einstiegslösung für das smarte Zuhause gesehen.[73] Hergestellt und vertrieben werden diese Systeme von **Lampenherstellern** (z. B. Philips), **Möbelhäusern** (z. B. IKEA) und **Technologie/Vernetzungsherstellern** (z. B. AVM/Fritz!).

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

In der einfachsten Form sorgt ein smartes Beleuchtungssystem dafür, dass der Nutzer via eines Steuergerätes (i.d.R. Smartphone) das Licht ein- und ausschalten sowie Helligkeit und Farbe regulieren kann. Oft sind die Systeme auch mit einem Bewegungsmelder ausgestattet. Fortgeschrittene Funktionen beinhalten Zeitschaltungen, die das Licht mit einer Weckfunktion ausstatten oder bei Abwesenheit des Bewohners Aktivität im Haus simulieren, um potenzielle Einbrecher abzuschrecken.

Bei der genutzten Art der Konnektivität gibt es verschiedene Möglichkeiten. Während einige Modelle über WLAN oder Bluetooth angeschlossen werden, nutzen viele Zigbee-

---

71 Dies kann der Fall sein, wenn diese leicht zu erraten sind oder wenn der Nutzer die gleichen Anmeldedaten schon bei einem anderen Dienst verwendet hat und es dort ein Datenleck gab.

72 Vgl. Fuest, B. (2019b): Die smarten Kameras werden zum Sicherheitsrisiko, in: gruenderszene.de, 27.12.19, elektronisch verfügbar unter: https://www.gruenderszene.de/technologie/smarten-kameras-ring-sicherheitsrisiko.

73 Vgl. Maaß, S. (2019): Der günstigste Einstieg in ein smartes Zuhause, in: welt.de, 16.02.19, elektronisch verfügbar unter: https://www.welt.de/finanzen/immobilien/article188885697/Smart-Home-So-laesst-sich-die-Beleuchtung-steuern.html.

Technologie. Die Steuerung der Geräte kann über eine App, ein Steuergerät oder auch über Sprachsteuerung mit einem verbundenen Sprachsteuerungssystem erfolgen. Es ist auch möglich, Lampen mit Multimediageräten zu synchronisieren.

Erhobene Daten und Datenschutz

Durch das Abgreifen der Daten, die von den smarten Lampen verarbeitet werden bzw. von den Steuerungs-Apps gesendet werden, lassen sich Tagesabläufe der Besitzer auslesen. Es gibt außerdem die (bisher noch theoretische) Möglichkeit, genutzte Multimediainhalte zu identifizieren, falls sich die Lampenfarben und Leuchtintensitäten im Takt dazu bewegen.[74]

Verbraucherschutz und IT-Sicherheit

Der Nutzer kann sein Beleuchtungssystem grundsätzlich relativ leicht wechseln, insbesondere im Vergleich zu anderen vernetzten Systemen. Bei einer (teilweisen) Kompatibilität ist es auch möglich, nur einzelne Leuchtmittel das Gateway/Steuergerät zu tauschen. Laufende Kosten fallen bei Beleuchtungssystemen typischerweise nicht an.

Es gibt in diesem Bereich kaum IT-Sicherheitsbedenken.

Wettbewerbliche Aspekte

Eine Besonderheit von smarten Beleuchtungssystemen im Vergleich zu anderen Smart-Home-Lösungen ist der relativ hohe Grad der Interoperabilität. Lampen eines Herstellers, deren Konnektivität auf dem Zigbee-Protokoll beruht. können oftmals auch mit einem Gateway eines anderen Herstellers verbunden und über die entsprechende App gesteuert werden.[75]

A.2 Vernetzte Haushaltsgeräte

In der Gruppe der smarten Haushaltsgeräte (unterschieden in **Groß- und Kleingeräte)** gibt es verschiedenste Anwendungsfälle, in denen Vernetzung eine Rolle spielt. Es gibt nur wenige Haushaltsgeräte, bei denen es inzwischen keine fernsteuerbaren oder fernüberwachbaren Varianten gibt.

---

74 Vgl. Maiti, A.; Jadliwala, M. (2019): Light Ears: Information Leakage via Smart Lights, in: Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., Vol. 3, No. 3, Article 98, elektronisch verfügbar unter: https://sprite.utsa.edu/publications/articles/maitiIMWUT19.pdf.

75 Eines der gängigsten und kompatibelsten Systeme für die Lichtsteuerung ist Philips Hue, dessen Gateway etwa auch mit Lampen von Osram oder Ikea genutzt werden kann, siehe: Günder, A. (2019): Philips Hue kompatible Geräte und Systeme | Aktuelle Übersicht, 16.09.19, in: homeandsmart.de, elektronisch verfügbar unter: https://www.homeandsmart.de/philips-hue-kompatible-geraete-systeme-apps.

A.2.1 Haushaltsgroßgeräte[76]

Marktrelevanz und Anbieterstruktur

Die gängigsten vernetzten Haushaltsgroßgeräte sind **Kühlschränke** mit integrierten Displays und einer potentiellen Überwachung und Nachbestellung von Lebensmitteln. Auch mit Apps oder Sprachsteuerung steuer- und überwachbare **Spülmaschinen, Waschmaschinen und Wäschetrockner** werden in zunehmenden Umfang vermarktet. Smarte Funktionen sind bisher jedoch auf hochpreisige Geräte beschränkt.

Verkauft werden diese vorrangig von den **etablierten Herstellern** (z. B. Miele, Siemens oder Bosch bei Waschmaschinen und Samsung oder LG bei Kühlschränken). Große Internetkonzerne spielen höchstens im Bereich Sprachsteuerung über Sprachassistenzsysteme eine Rolle. Start-Ups haben in diesem Segment keine große Bedeutung.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Angebunden werden große Haushaltsgeräte über WLAN, damit sie einerseits auf Inhalte und Updates aus dem Internet zugreifen können und andererseits über Apps auch von Nutzern aus der Ferne steuer- und kontrollierbar sind.

Der Anbieter LG stellte 2020 seine neue Generation eines intelligenten Kühlschranksystems („InstaView ThinQ“) vor. Diese soll über Kameras und künstliche Intelligenz erkennen, was im Kühlschrank vorhanden ist und darauf basierend Rezeptvorschläge machen und Vorschläge für Nachbestellungen machen. Auf dem Display in der Tür lassen sich in der Küche Entertainment-Inhalte anzeigen.[77] Ein vergleichbares System will auch Samsung anbieten („Family Hub“), das außerdem als Smart-Home-Steuerungszentrale fungieren soll. Bisherige Modelle haben jedoch allenfalls eine Kamera zur Anzeige des Kühlschrankinhalts, aber keine Analysefunktion.[78] Denkbar wären bei smarten Kühlschränken auch in das Display integrierte Kameras für Videotelefonie oder die Einbindung von Apps für Videostreaming.

Andere Geräte aus dem Bereich der weißen Ware lassen sich zum jetzigen Zeitpunkt mit Apps meist nur an- und ausschalten bzw. fernüberwachen. Bei einigen Waschmaschinen gibt es zusätzlich eine automatische Waschmitteldosierung. Dabei muss der

---

76 Die Abgrenzung zwischen Haushaltsgroß- und -kleingeräten ist nicht in jedem Einzelfall klar. Gerichte mussten diese in der Vergangenheit insbesondere im Zusammenhang mit Recyclinggesetzgebung und Annahme von ausrangierten Altgeräten durch Händler treffen. Hier wird die Annahme getroffen, dass Haushaltsgroßgeräte solche sind, die sich nicht ohne fremde Hilfe durch den durchschnittlichen Nutzer bewegen lassen, alles andere sind Haushaltskleingeräte, daran orientiert sich auch dieser Diskussionsbeitrag.

77 Vgl. http://www.lgnewsroom.com/2020/01/lgs-evolving-instaview-refrigerator-technologies-offer-glimpse-into-kitchen-of-the-future-at-ces/.

78 Vgl. La Rocco, N. (2020): Smarte Kühlschränke: LG und Samsung wissen per Kamera, was auf Lager ist, in: computerbase.de, 03.01.20, elektronisch verfügbar unter: https://www.computerbase.de/2020-01/lg-samsung-smarte-kuehlschraenke-ces-2020/.

Nutzer nur einen Vorratsbehälter auffüllen und die Waschmaschine regelt über Sensorik die nötige Waschmittelmenge und das Waschprogramm für jeden Waschgang.[79]

Erhobene Daten und Datenschutz

Die Datenerhebung bei großen Haushaltsgeräten kann aufgrund der frühen Marktphase nur schwierig beurteilt werden. Aus Datenschutzperspektive sind vernetzte Haushaltsgeräte potenziell mit einer eher hohen Kritikalität ausgestattet, da sie Daten über höchstpersönliche Lebensbereiche sammeln und verarbeiten.[80]

Verbraucherschutz und IT-Sicherheit

Smarte Haushaltsgroßgeräte sind oft hochpreisig, die Produktqualität der Grundfunktionen ist in der Regel hoch. Wie bei allen IoT-Geräten besteht auch hier die grundsätzliche Gefahr eines Hackings oder der Infektion mit Schadsoftware. Insbesondere wenn in Kühlschränken vollwertige Tablets mit hoher Rechenleistung integriert sind, stellen sie für Betreiber von Botnetzen attraktive Ziele dar.

Wettbewerbliche Aspekte

Aufgrund der geringen Absatzzahlen und der noch nicht sehr ausgereiften Produkte sind wettbewerbliche Probleme bei smarten Haushaltsgroßgeräten noch selten. Potentiell könnte bei smarten Kühlschränken über Voreinstellungen zum Nachbestellen von Lebensmitteln Einfluss auf die Auswahl von Lebensmittellieferanten ausgeübt werden.[81] Es ist davon auszugehen, dass dabei kleine und/oder lokale Anbieter von Lieferdiensten nur unzureichend berücksichtigt werden. Bei Wasch- oder Spülmaschinen ist ein vergleichbares Problem weniger relevant und auf die die Möglichkeiten einer automatischen Nachbestellung von Wasch- bzw. Spülmittel beschränkt.

In Abhängigkeit von der konkreten Ausgestaltung einer solchen Nachbestellung kann sie auch verbraucherschutzrelevant sein. Dies gilt z. B. wenn keine Preisansage erfolgt oder der voreingestellte Lieferdienst die Lebensmittel nur zu überhöhten Preisen anbietet. Darüber hinaus sind Abonnement-Lösungen mit verbraucherrechtlich relevante Herausforderungen denkbar (z. B. Kündigungsfristen, Informationen über Preiserhöhungen).

---

79 Vgl. Wendel, M. (2020): WLAN-Waschmaschinen Test-Überblick 2020: Die besten im Vergleich, 12.08.20, in: homeandsmart.de, elektronisch verfügbar unter: https://www.homeandsmart.de/smarte-intelligente-waschmaschinen.

80 So können durch die genutzten Lebensmittel Rückschlüsse auf Lebensstil, Anwesenheitszeiten oder auch Lebensverhältnisse geschlossen werden. Die Daten könnten Versicherungen Einblicke in die Ernährungsweise der Versicherten gewähren oder potenziellen Einbrechern Informationen über die Anwesenheit der Bewohner geben. Auch die Profilbildung für Werbetreibende kann damit intensiviert werden, da herausgefunden werden kann, ob sich für die Mitglieder in einem Haushalt etwa Werbung für Fast Food lohnt.

81 Ein vergleichbares Beispiel wurde auch von EU-Kommissarin Margrethe Vestager genannt, als diese eine, zum aktuellen Zeitpunkt noch laufende, Sektoruntersuchung der Kommission im Bereich Consumer-IoT ankündigte (siehe https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1326).

A.2.2 Haushaltskleingeräte

Als Haushaltskleingeräte gelten alle Geräte im Haushalt, die der Nutzer ggf. ohne Hilfsmittel oder fremde Hilfe transportieren kann. Im Bereich vernetzter Geräte sind dies z. B. **Küchenmaschinen, Staubsauger oder Zahnbürsten,** aber auch außerhalb des Hauses genutzte Geräte wie z. B. **Rasenmäher.**

Marktrelevanz und Anbieterstruktur

Die Produkte werden überwiegend von **etablierten Haushaltsgeräteherstellern** angeboten. So gibt es vernetzte Zahnbürsten von Oral-B, Küchenmaschinen von Vorwerk oder Staubsauger von Dyson.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Größere Kleingeräte nutzen häufig WLAN für die Vernetzung, während kleinere Geräte oft über Bluetooth direkt mit dem Smartphone gekoppelt und damit nicht ohne Weiteres von unterwegs steuerbar sind.

Rasenmähroboter gehören aufgrund der räumlichen Distanz zu den Geräten, die nicht zwingend nur WLAN zur Verbindung nutzen. Entsprechende Elemente sind vielmehr oftmals nur gegen Aufpreis erhältlich und damit nicht in jedem Gerät verbaut. So gibt es z. B. für den „Landroid“ des Unternehmens Worx die Zusatzmodule „Radiolink“ und „Find my Landroid“. Während Radiolink über das 868 MHz-Frequenzspektrum kommuniziert, ist im Modul „ Find my Landroid“ eine SIM-Karte verbaut.

Weitere Ausstattungsmerkmale spielen eine Rolle, unterscheiden sich jedoch je nach Gerät. Insbesondere Staubsauger nutzen Sensorik um „Ecken und Kanten“ eines Haushaltes zu erkunden und sich ggf. auch zu merken. Smarte Zahnbürsten haben Sensoren, die den Anpressdruck messen.

Auch Kameras und insbesondere Mikrofone in Haushaltsgeräten werden immer prävalenter. Im Extremfall können diese sogar ohne Wissen des Nutzers versteckt sein. So haben Experten beim Auseinandernehmen der von Lidl verkauften Küchenmaschine „Monsieur Cuisine connect“ ein Mikrofon entdeckt, das weder beworben noch in der Bedienungsanleitung erwähnt wurde. Dieses ist inaktiv, kann jedoch für die mögliche Nachrüstung einer Sprachsteuerung genutzt werden ohne, dass dies für den Nutzer beim Kauf transparent ist.[82]

---

82 Des Weiteren läuft die Küchenmaschine mit einem relativ alten Betriebssystem, für dass es schon zum Verkaufszeitpunkt Mitte 2019 keine Sicherheitsupdates mehr gab, siehe: Rohm, B. (2019): Geheimes Mikrofon: Thermomix-Klon von Lidl hat schwere Sicherheitslücken, in: oekotest.de, 21.06.19, elektronisch verfügbar unter: https://www.oekotest.de/freizeit-technik/Geheimes-Mikrofon-Thermomix-Klon-von-Lidl-hat-schwere-Sicherheitsluecken-_10717_1.html.

Erhobene Daten und Datenschutz

Insbesondere vernetzte Staubsauger vermessen die Wohnung und geben Rückschlüsse auf die Lebensverhältnisse in einem Haushalt. Je nach Ausstattung filmen diese auch die Umgebung. Dies bedeutet eine missbräuchliche Sendeanlage nach § 90 TKG, wenn diese Personen filmen bzw. wenn ein Filmen für den Gefilmten nicht erkennbar ist.[83] Ein ähnlich gelagerte Problematik besteht bei einem vernetzten Rasenmäher. Hier ist die Wahrscheinlichkeit eines unerlaubten Filmens Dritter aufgrund des Einsatzes im Außenbereich sogar noch größer.

Im April 2021 soll in Deutschland der Rasenmähroboter Toadi auf den Markt kommen.[84] Dieser wird der erste in Deutschland erhältliche Roboter mit einer Kamera sein, der auf Basis der Kamerabilder seine Laufwege unter Nutzung künstlicher Intelligenz plant und ggf. anpasst. Aus rechtlicher Sicht bietet das Gerät damit verschiedene Herausforderungen. Während die Kamerabilder im Fahrbetrieb direkt verarbeitet und für das Mähen genutzt werden, kann der Toadi auch automatisiert Menschen in seiner Umgebung fotografieren, die ins Bild treten und das Bild aufs Smartphone des Besitzers senden.[85]

Verbraucherschutz, IT-Sicherheit und Wettbewerbliche Aspekte

Bei smarten Küchenmaschinen bestehen ähnliche Risiken wie beim smarten Kühlschrank.[86] Ähnliches gilt für Kaffeemaschinen, die selbstständig Kaffee nachbestellen. Sprachsteuerungen können die im entsprechenden Kapitel noch weiter ausgeführten Lock-In-Effekte bzw. Kaufanreize aufgrund von Kompatibilität auslösen.

Im Bereich (IT-)Sicherheit sind manche Haushaltsgeräte aufgrund fehlender Updates teils sehr anfällig. So werden z. B. Küchengeräte oftmals über 10 Jahre lang genutzt[87], erhalten jedoch selten über die gesamte Zeit Updates. Auch bei vergleichsweise jungen Geräten bestehen Sicherheitslücken, die oft nicht vom Hersteller durch Updates behoben werden. So wurde eine smarte Kaffeemaschine von einem Forscher mit einem mit Schadcode infizierten Firmware-Update dazu gebracht, eine Lösegeldforderung einzublenden und alle Funktionen (Kaffeebohnen mahlen, Wasserauslauf etc.) gleichzeitig

---

83 Vgl. Bundesnetzagentur (2018): Bundesnetzagentur warnt vor vernetztem Spielzeug, Pressemitteilung, 07.12.18, elektronisch verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2018/20181207_SmartToys.html.

84 Angabe auf Website des Herstellers, elektronisch verfügbar unter: https://www.toadi.com/de_DE/buy.

85 Dies funktioniert durch eine Infrarotkamera auch nachts auf bis zu 15 Metern Entfernung, siehe https://www.toadi.com/de_DE/keeps-the-one-you-love-safe.

86 So könnte man sich die Lebensmittel, die für ein bestimmtes Rezept benötigt werden, direkt an der Küchenmaschine bestellen.

87 Die durchschnittliche Erstnutzungsdauer im Bereich Haushaltsgroß- und -kleingeräte lag in Deutschland in den Jahren 2004 bis 2012/13 bei 13,0 bzw. 10,6 Jahren, Tendenz jedoch bei Großgeräten fallend. Siehe: Prakash, S. et al. (2016): Einfluss der Nutzungsdauer von Produkten auf ihre Umweltwirkung: Schaffung einer Informationsgrundlage und Entwicklung von Strategien gegen „Obsoleszenz“, Studie des Öko-Instituts für das Umweltbundesamt, Februar 2016, elektronisch verfügbar unter: https://www.umweltbundesamt.de/sites/default/files/medien/378/publikationen/texte_11_2016_einfluss_der_nutzungsdauer_von_produkten_obsoleszenz.pdf.

einzuschalten; Abhilfe brachte nur das Ziehen des Netzsteckers.[88] Bei Küchenmaschinen, die von Aldi verkauft wurden, wurde nach Medienberichten mithilfe einer Sicherheitslücke eine Fernaktivierung durchgeführt, die zu Schäden am Gerät führte.[89]

88 Vgl. Goodin, D. (2020): When coffee makers are demanding a ransom, you know IoT is screwed, in: arstechnica.com, 26.09.20, elektronisch verfügbar unter: https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/.

89 Vgl. Tremmel, M. (2020b): Küchenmaschine von Hofer und Aldi mit Sicherheitslücke, in: golem.de, 07.08.20, elektronisch verfügbar unter: https://www.golem.de/news/thermomix-klon-kuechenmaschine-von-hofer-und-aldi-mit-sicherheitsluecke-2008-150134.html.

B Entertainment

Die Vorstellung von IoT-Anwendungen im Bereich Entertainment unterteilt sich in die Kapitel **smarte Fernseher (B1), Spielekonsolen (B2), smarte Lautsprecher inkl. der darauf installierten Sprachassistenzsysteme (B3),** sowie **smartes Spielzeug (B4)**.

B.1 Smart-TV

Als smarter Fernseher wird jeder Fernseher deklariert, der mit dem Internet verbunden ist und damit Funktionen hat, die über die Übertragung von linearem Fernsehen hinausgehen.

Marktrelevanz und Anbieterstruktur

Die zunehmende Vernetzung und Verbreitung von Smart-TVs hat zu keinen spürbaren Veränderungen bei den Marktteilnehmern geführt. Einige Anbieter von Smart-TVs bieten jedoch weitere vernetzte Geräte wie Tablets und Smartphones an, wie bspw. Samsung, LG oder Sony.

Die Verbreitung von Smart-TVs in Deutschland wird immer größer. So gaben 2019 56,4 % der Haushalte an, ein solches Gerät zu besitzen.[90] Eine Studie des Bitkom in 2020 beziffert den Anteil der Smart-TV-Nutzer in Deutschland sogar auf 63 %.[91] Dies hat auch damit zu tun, dass kaum noch Fernsehgeräte komplett ohne die Möglichkeit einer Internetanbindung verkauft werden. Bei den aktuell verkauften Fernsehern beträgt der Marktanteil der Smart-TVs 88 %.[92] Laut Bitkom nutzen 82 % der Videostreaming-Nutzer Smart-TVs.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

In aller Regel werden internetfähige Fernseher über WLAN oder Ethernet-Kabel an den Router angebunden. Bei vielen Modellen ist außerdem ein Bluetooth-Modul verbaut, das der Anbindung von Audio-Geräten dient. Über Adapter ist eine solche Funktionalität auch nachrüstbar. Es ist außerdem oft möglich, einen Fernseher mit dem Smartphone zu verbinden und als Video- und Audioausgabegerät zu nutzen.

De facto übernehmen smarte Fernseher meist die Funktion eines Entertainment-Hubs im vernetzten Zuhause. Das Abspielen der Entertainment-Inhalte wird über auf dem Fernseher installierte Apps realisiert, z. B. zum Nutzen von Video- oder Musikstreamingdiensten, die ggf. ein separates Abonnement benötigen. Auch Smart-TVs lassen das Anschließen externer Geräte wie Receiver, Bluray-Player oder Spielekonso-

---

90 Vgl. Statista (2019): Anteil der TV-Haushalte in Deutschland mit internetfähigem Fernsehgerät (Smart-TV) im Haushalt in den Jahren 2013 bis 2019, Oktober 2019, elektronisch verfügbar unter: https://de.statista.com/statistik/daten/studie/325527/umfrage/anteil-der-tv-haushalte-in-deutschland-mit-smart-tv/.

91 Vgl. Bitkom (2020c): Die Zukunft der Consumer Technology – 2020, elektronisch verfügbar unter: https://www.bitkom.org/sites/default/files/2020-08/200826_ct_studie_2020_online.pdf.

92 Vgl. https://tv-plattform.de/infothek/marktzahlen/.

len zu. Ein TV-Tuner zum Empfang von Fernsehsignalen über Kabel, Antenne oder Satellit ist inzwischen meist direkt eingebaut. Über den roten Knopf auf der Fernbedienung lässt sich während des Schauens eines TV-Senders die HbbTV-Funktion (Hybrid Broadcast Broadband TV) ansteuern, mit der sich ohne Notwendigkeit des Installierens von Apps etwa Mediatheken des entsprechenden Senders ansteuern lassen.[93]

Kameras und Mikrofone sind meist nicht verbaut. Bei Geräten mit entsprechender Ausrüstung wurde in der Vergangenheit über „Lauschangriffe" des US-Geheimdienstes CIA berichtet.[94] So war es nach Aufspielen einer Schadsoftware über einen USB-Stick möglich, auf die Kameras und Mikrofone einiger Samsung-Modelle auch bei abgeschaltetem Gerät zuzugreifen.

Eine Besonderheit stellen die von Grundig und ok in Zusammenarbeit mit Amazon produzierten Fernseher dar, bei denen der Sprachassistent Alexa je nach Modell entweder in die Fernbedienung oder über Mikrofon in den Fernseher integriert ist.[95]

Erhobene Daten, Datenschutz, Verbraucherschutz und IT-Sicherheit

Auch ohne Kameras und Mikrofone ist eine Datensammlung durch Fernsehgeräte möglich. So musste der Anbieter VIZIO Anfang 2017 in den USA ein Bußgeld in Höhe von 2,2 Millionen Dollar zahlen, da die Nutzungsverläufe der Kunden ohne Einwilligung gesammelt und mit demographischen Daten verknüpft wurden. Dies wurde etwa dazu genutzt, Werbung auf den Nutzer anzupassen.[96] Vergleichbare Datensammlungen wurden auch von deutschen Gerichten untersagt.[97]

Die Erstellung eines Benutzerkontos ist zumeist nötig, um nicht vorinstallierte Apps auf dem Fernsehgerät zu nutzen. Das Benutzerkonto erfordert wiederum Angaben zu persönlichen Daten, die die Profilbildung erleichtern.

---

93 Diese Funktion wird oft auch als Fortentwicklung des Videotextes bezeichnet, siehe: https://www.hbbtv-infos.de/hbbtv-fragen.php.

94 Siehe: de Leuw, C. (2017): Schnüffelnde Samsung-Fernseher: So finden Sie heraus, ob Sie betroffen sind!, in: computerbild.de, 08.03.17, elektronisch verfügbar unter: https://www.computerbild.de/artikel/avf-News-Fernseher-Samsung-Fernseher-Spionage-Modelle-17641477.html.

95 Die Datenschutzherausforderungen bei Sprachassistenten werden im Kapitel B.3 im Rahmen der Diskussion solcher Systeme erörtert.

96 Vgl. FTC (2017): VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent, 06.02.17, elektronisch verfügbar unter: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

97 Vgl. Geiger, C. S. (2016): Vorsicht vor diesem Fernseher: Samsung-TV spioniert Sie aus, in: chip.de, 13.06.16, elektronisch verfügbar unter: https://www.chip.de/news/Vorsicht-vor-diesem-Fernseher-Samsung-TV-spioniert-Sie-aus_95298905.html.

In einer Sektoruntersuchung zu Smart-TVs hat das Bundeskartellamt 2020 diverse Probleme hinsichtlich des Daten- und Verbraucherschutzes bei smarten Fernsehern bemängelt, etwa:[98]

- Zu komplizierte Datenschutzbestimmungen,[99]
- Fehlen von Informationen wie Datenschutzbestimmungen oder Allgemeinen Geschäftsbedingungen (AGB) vor dem Kauf.[100]
- „Digital Nudging“, d.h. ein „Anstupsen“ des Nutzers um ihn zu einer Erlaubnis der Nutzung personenbezogener Daten zu bewegen.
- Mangelhafte Information über die Bereitstellung von Sicherheitsupdates.

In Anlehnung daran empfiehlt das Bundeskartellamt unter anderem:

- Eine Prüfung vor dem Kauf, wie lange Software-Updates bereitgestellt werden.
- Eine sorgfältige Ersteinrichtung insbesondere mit Blick auf die Datennutzung.
- Die Trennung des Smart-TVs vom Internet, wenn die Gerätesoftware nicht mehr aktualisiert wird.[101]

Mit steigender Leistungsfähigkeit nähern sich auch die IT-Sicherheitsrisiken von Fernsehgeräten denen für Laptops und PCs an. Da viele Geräte auch einen Internetbrowser besitzen, mit dem man beliebige Internetseiten ansteuern kann, kann auch Schadcode auf diese Weise auf dem Fernseher ausgeführt werden. Virenscanner existieren zwar vereinzelt, Betriebssysteme und Browser erhalten jedoch meist nur unregelmäßige Sicherheitsupdates.[102] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt daher, kritische Dienste wie Online-Banking nicht auf dem Fernseher zu nut-

98 Vgl. Bundeskartellamt (2020): Sektoruntersuchung Smart-TVs, Juli 2020, elektronisch verfügbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf.

99 Diese werden mit dem Ziel der förmlichen DSGVO-Konformität konzipiert und sind oft deutlich zu allgemein formuliert, so dass sie für alle mit dem Smart-TV nutzbaren Angebote gelten, was dem Nutzer jedoch in der Praxis keine echten Informationen bietet.

100 Einen Verstoß gegen das Lauterkeitsrecht stellt dies jedoch nur dar, wenn der Nutzer nicht ohne Eingabe von persönlichen Daten alle wesentlichen Funktionen nutzen kann und auf diese Notwendigkeit der Eingabe persönlicher Daten nicht vor dem Kauf hingewiesen wurde.

101 Smarte Funktionen können dann über ein externes Gerät (Streaming-Adapter) zugespielt werden.

102 Samsung bietet beispielsweise einen Virenscanner an, dieser muss jedoch manuell durch den Nutzer aktiviert werden und bietet keine automatische Hintergrunderkennung, siehe: Der Standard (2019): Samsungs [sic] blamiert sich mit Smart-TV-Tipp: „Bitte regelmäßig Virenscanner starten“, in: derstandard.de 18.06.19, elektronisch verfügbar unter: https://www.derstandard.de/story/2000105041950/samsung-blamiert-sich-mit-smart-tv-tipp-bitte-regelmaessig-virenscanner.

zen.[103] Smart-TVs wurden auch schon ohne Wissen der Besitzer in Botnets missbraucht, um Attacken auf Webseiten durchzuführen und diese damit lahmzulegen.[104]

Wettbewerbliche Aspekte

Als Gatekeeper für die Nutzung vielfältiger Dienste auf dem internetfähigen Fernseher fungiert das jeweilige Betriebssystem und der damit verbundene App Store, über den (ähnlich wie bei Smartphones) Apps heruntergeladen werden können. Die auf der Verpackung des Fernsehers bzw. in der Produktbeschreibung beworbenen Apps sind zumeist schon vorinstalliert, weitere können über die Benutzeroberfläche des Fernsehers heruntergeladen werden. Die gängigsten Betriebssysteme sind das von Google entwickelte Android TV, das mehrere Hersteller, wie etwa Sony, nutzen, sowie Tizen von Samsung.

Die Betriebssysteme nutzen einen Standard-App-Store, aus dem der Nutzer sich die Apps auf den Fernseher laden kann. Eine Nutzung alternativer App Stores ist bei Android TV grundsätzlich möglich, bei Tizen nicht. Betriebssystemhersteller und App-Store-Betreiber haben damit Einfluss darauf, welche Apps in den Stores gelistet und damit vom Nutzer installiert werden können und welche nicht. Dies bietet den Vorteil einer Kuratierung, d.h. dass Nutzer sich darauf verlassen können, dass die gelisteten Apps funktional und nicht indiziert sind. Andererseits kann dies aber auch zur Nicht-Zulassung bestimmter Apps, etwa von Konkurrenzprodukten des App-Store-Betreibers oder nahestehender Anbieter führen und negative Gatekeeper-Effekte erzeugen.[105]

Eine Beeinflussung der Dienste, die der Nutzer auf dem Smart-TV kostenpflichtig nutzt, findet außerdem durch die Fernbedienung statt. So haben die Fernbedienungen moderner Fernseher oft mit dem Logo eines Streaming-Anbieters beschriftete Funktionstasten für den direkten Zugriff auf dessen Dienste (z. B. Netflix, Amazon Prime). Die Hersteller von Fernsehern erhalten mutmaßlich hohe Zahlungen von den Streamingplattformen für entsprechende Tasten auf der Fernbedienung, was für kleinere Content-Anbieter einen Wettbewerbsnachteil darstellt.[106]

---

103 Vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartTV/SmartTV_node.html.

104 Vgl. Briel, R. (2018): First botnet attack on smart TV sets identified, in: broadbandtvnews.com, 19.11.18, elektronisch verfügbar unter: https://www.broadbandtvnews.com/2018/11/19/first-botnet-attack-on-smart-tv-sets-identified/.

105 Für eine detailliertere Diskussion der potenziell negativen Folgen von Gatekeeping, siehe Kapitel B.3.

106 So wird angenommen, dass der große US-amerikanische Anbieter von Streamingboxen und Smart-TVs Roku $1 pro Kunde pro gebrandeter Fernbedienungstaste verdient, siehe Shaw, L.; Smith, G. (2019): Roku built the Dominant Streaming Box. Now It's Under Siege, in: Bloomberg.com, 11.12.19, elektronisch verfügbar unter: https://www.bloomberg.com/news/articles/2019-12-11/streaming-box-king-roku-is-under-seige-from-amazon-and-apple.

B.2 Spielekonsolen

Marktrelevanz und Anbieterstruktur

Marktrelevant im Bereich der Spielekonsolen sind aktuell die Konsolen **Xbox One von Microsoft**, **PlayStation 4 von Sony** sowie **Nintendo Switch von Nintendo**. Im November 2020 erschienen von Microsoft mit der Xbox Series X (sowie der weniger leistungsstarken Series S) und Sony mit der PlayStation 5 neue, leistungsfähigere Spielkonsolen.

Weltweit wurden bis einschließlich September 2020 über 225 Millionen Geräte aus der aktuellen Konsolengeneration der drei großen Hersteller verkauft.[107] In Deutschland wurden in Abhängigkeit von Neuerscheinungen und Kampagnen zuletzt zwischen 1,8 und 3 Millionen Konsolen pro Jahr verkauft.[108]

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Spielekonsolen können wie Smart-TVs auch als Entertainment-Hubs genutzt werden, über die nicht nur Spiele gespielt, sondern auch Video- und/oder Audiostreaming-Apps genutzt werden. Für das Nutzen einer Spielekonsole ist i.d.R. ein Ausgabegerät, also ein Fernsehgerät oder ein Monitor erforderlich.[109]

Vernetzt wird die Spielkonsole mit dem Internet entweder über Ethernet-Kabel oder WLAN. Zusätzlich verfügen die Geräte teilweise über Bluetooth, um externe Geräte (z. B. Kopfhörer) anzuschließen.[110]

Erhobene Daten und Datenschutz

Die Erstellung eines online registrierten Benutzerkontos bei Nutzung der Konsole ist erforderlich, um zusätzliche Apps herunterzuladen, Onlinefunktionen in Spielen zu nutzen oder Downloadspiele zu kaufen. Falls Zahlungen durchgeführt werden, müssen auch Zahlungs- und Adressdaten eingegeben und verarbeitet werden.

---

107 Vgl. Statista (2020c): Verkaufszahlen der weltweit meistverkauften Spielkonsolen bis September 2020, elektronisch verfügbar unter: https://de.statista.com/statistik/daten/studie/160549/umfrage/anzahl-der-weltweit-verkauften-spielkonsolen-nach-konsolentypen/.

108 Vgl. Statista (2020a): Absatz von Spielkonsolen auf dem Konsumentenmarkt in Deutschland von 2005 bis 2019, elektronisch verfügbar unter: https://de.statista.com/statistik/daten/studie/190754/umfrage/absatz-von-spielkonsolen-in-deutschland/.

109 Von den aktuellen Konsolen lässt sich nur die Nintendo Switch mit dem ins Gerät integriertem Bildschirm und Akku auch mobil ohne externe Stromversorgung und externen Bildschirm nutzen.

110 Die Nintendo Switch kann nur via WLAN angeschlossen werden und lässt sich, ebenso wie die Xbox One nur über zuzukaufende Adapter mit Bluetooth-Kopfhörern verbinden. Bei Xbox One und PlayStation 4 gibt es außerdem die Möglichkeit ein Headset direkt in den Controller einzustecken (3,5mm Klinkenanschluss).

Verbraucherschutz und IT-Sicherheit

Aufnahmegeräte, insbesondere Kameras, sind typischerweise als optionale Ausstattungselemente für Spielekonsolen erhältlich, jedoch kein Teil der Standardausstattung.

In die Controller der im November 2020 erschienenen PlayStation 5 von Sony ist ein Mikrofon für Sprachchats mit anderen Spielern integriert.[111] Einen Monat vor Marktstart wurde bekannt, dass die letzten fünf Minuten eines Sprachchats laufend im lokalen Speicher der Konsole ohne Möglichkeit eines Abschaltens der Funktion hinterlegt werden. Dies soll der Nachverfolgung von Beleidigungen und Belästigungen dienen, da der Nutzer eine Beschwerde beim Kundendienst so direkt mit einem Audio-Mitschnitt belegen kann.[112]

Mit Nutzung der Online-Features der Konsolen ist die Notwendigkeit der Kontoerstellung verbunden. Danach kann dann etwa auch mit anderen Nutzern aus der Kontaktliste (Identifizierung erfolgt über Benutzernamen) über die Benutzeroberfläche gechattet und (entsprechende Hardware vorausgesetzt) über Audio-Chat gesprochen werden. Außerdem ist es möglich, per Verknüpfung des Kontos mit Streamingdiensten wie Twitch direkt das Bild der Konsole per Knopfdruck auf dem Controller auf die entsprechenden Plattformen live hochzuladen.[113] Innerhalb vieler populärer Spiele gibt es die Möglichkeit, Gegenstände mit echtem Geld zu kaufen, die im Spiel einen Vorteil bieten, z.T. auch in Form von sogenannten Lootboxen.[114]

Die Mehrzahl dieser Funktionalitäten ist grundsätzlich unproblematisch, da sie nur auf Nutzerwunsch passieren – gleichwohl muss im Auge behalten werden, dass Spielekonsolen in ihrer Vermarktung insbesondere auch Kinder und Jugendliche und damit eine besonders schützenswerte Bevölkerungsgruppe adressieren.

In einer Reihe von Fällen sahen sich Konsolenhersteller auch Beschwerden von Verbraucherschützern ausgesetzt. Besonders umstritten ist, ob die Regelungen zur Rückgabe von digital gekauften Spielen verbraucherschutzrechtlich zu beanstanden sind. Nintendo hat Anfang 2020 ein Gerichtsurteil erwirkt, dass den Verzicht von Kunden auf

---

111 Vgl. Holt, K. (2020): Sony's PS5 DualSense controllers has a built-in mic and adaptive triggers, in: engadget.com, 22.10.20, elektronisch verfügbar unter: https://www.engadget.com/playstation-5-controller-dualsense-photos-202718532.html.

112 Vgl. Steinlechner, P. (2020): Playstation 5 zeichnet Sprachchat auf, in: golem.de, 19.10.20, elektronisch verfügbar unter: https://www.golem.de/news/sony-playstation-5-zeichnet-sprachchat-auf-2010-151588.html.

113 Siehe Johnson, D. (2019): How to stream live gameplay on your PS4 to Twitch, YouTube, or other streaming sites, in: businessinsider.com, 02.10.19, elektronisch verfügbar unter: https://www.businessinsider.com/how-to-stream-on-ps4?r=DE&IR=T bzw. Montelli, C. (2019): How to stream on your Xbox One using the Twitch app, in: businessinsider.de, 01.11.19, elektronisch verfügbar unter: https://www.businessinsider.de/international/how-to-stream-on-xbox-one/?r=US&IR=T.

114 Auch Beuteboxen genannt. Dabei handelt es sich um Behälter in Spielen, die zufällige Gegenstände enthalten, siehe: Weber, M. (2017): Lootboxen: Warum ist das kein Glücksspiel? – Das sagt der Anwalt, in: gamestar.de, 08.11.17, elektronisch verfügbar unter: https://www.gamestar.de/artikel/lootboxen-als-gluecksspiel-das-sagt-der-anwalt,3321951.html.

Ihr Rückgaberecht zulässt.[115] Bei Sony ist die Rückgabe eines gekauften, aber noch nicht heruntergeladenen Spiels innerhalb von 14 Tagen möglich, bei Microsoft darf der Kauf höchstens 14 Tage zurückliegen und die bisherige Spieldauer 2 Stunden nicht überschreiten.[116]

Zudem sind regelmäßige und äußerst datenintensive[117] Updates für Spielen insbesondere im Online-Modus erforderlich. Problematisch für Nutzer sind diese jedoch bei unzureichender Bandbreite: Bei langsamer oder gar getakteter bzw. im Downloadvolumen begrenzter Internetleitung können Spiele durch Updatenotwendigkeit de facto unspielbar werden. Dies gilt auch dann, wenn diese als physische Version im Laden erworben wurden.[118]

Wettbewerbliche Aspekte

Die wettbewerbliche Stellung der Konsolenhersteller, die auch die Spieleplattform auf den Konsolen betreiben, ist vergleichbar mit der eines App-Store-Betreibers auf dem Fernseher oder dem Smartphone. Eine Besonderheit ist jedoch, dass sich dies bei Spielekonsolen auch auf den physischen Markt erstreckt. So müssen alle Spiele vom Konsolenhersteller zertifiziert sein, unabhängig davon, ob es sich um physische Datenträger oder Downloads handelt.

B.3 Smarte Audiogeräte und Sprachassistenzsysteme

Bei vernetzten Audiogeräten muss zwischen Hardwaregeräten (zumeist Lautsprechern) und der darauf laufenden Software (insbesondere Sprachassistenten) differenziert werden.

Marktrelevanz und Anbieterstruktur

Sprachassistenzsysteme wie **Alexa (Amazon), Google Assistant oder Siri (Apple)** finden bei Konsumenten in Deutschland immer mehr Einzug. Ende 2018 nutzten laut einer Konsumentenbefragung des WIK 26 % der Teilnehmer einen Sprachassistenten. Eine repräsentative Umfrage des Branchenverbandes Bitkom weist für Mai 2020 bereits eine Nutzungsrate von 39 % aus.[119]

---

115 Vgl. Deutschbein, R. (2020): Nintendo-Nutzer können digitale Käufe im eShop nicht zurückgeben, in: techbook.de, 23.01.20, elektronisch verfügbar unter: https://www.techbook.de/gaming/nintendo-eshop-kein-widerrufsrecht.

116 Siehe Rückerstattungsrichtlinie von Sony: https://www.playstation.com/de-de/get-help/help-library/store---transactions/payments---refunds/playstation-store-cancellation-policy/ und Deutschbein, R. (2020): Nintendo-Nutzer können digitale Käufe im eShop nicht zurückgeben.

117 Bei modernen Spielen sind Updates mit Größen über 10 Gigabyte keine Seltenheit, in Einzelfällen sind sogar über 50 Gigabyte möglich.

118 Dies ist unbedarften Nutzern, etwa Eltern, die Spiele für ihre Kinder kaufen, nicht immer bewusst, auf die grundsätzliche Notwendigkeit einer Internetverbindung wird bei solchen Spielen jedoch auf der Packungsrückseite hingewiesen.

119 Vgl. Bitkom Research (2020): Beliebte Helfer: Sprachassistenten haben sich durchgesetzt, 24.07.20, elektronisch verfügbar unter:

Eine Ursache hierfür ist, dass die entsprechenden Dienste oftmals bereits auf Endgeräten vorinstalliert sind (ohne dass dies für die Kaufentscheidung von Relevanz ist). Aber auch Endgeräte, die einen Großteil ihres Mehrwerts aus der Sprachassistenzfunktion ziehen, erreichen immer höhere Penetrationsraten. So besaßen Ende 2018 11 % der Befragten einen smarten Lautsprecher (Smart Speaker).[120] Die Einführung des **Telekom Smart Speakers** in 2019 bzw. des günstigeren Telekom Smart Speaker mini in 2020 könnte die Marktdurchdringung in Deutschland noch einmal verstärken. Diese Produkte verfügen sowohl über den Telekom-eigenen Sprachassistenten Magenta als auch über Alexa, so dass der Nutzer zwischen zwei voneinander unabhängigen Assistenzsystemen entsprechend seiner Präferenzen wählen kann.[121] Dies ist nicht der einzige Smart Speaker, der mehrere Sprachassistenten in einem bietet.

Die höchste Marktdurchdringung erreichen aktuell Alexa von Amazon, Siri von Apple und der Google Assistant. Die größere Produktvielfalt und schnelleren Innovationszyklen deuten darauf hin, dass Amazon im Markt am stärksten positioniert ist.[122]

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Die smarten Lautsprecher sind typischerweise über WLAN ins lokale Netzwerk eingebunden. Teilweise kann über Bluetooth eine Verbindung zum Smartphone/Tablet oder weiteren Bluetooth-Boxen hergestellt werden.[123]

Genutzt werden die Lautsprecher etwa, um eingesprochene Fragen über die Audioausgabe zu beantworten.[124] Relevant ist aber auch die Steuerung anderer smarter Geräte durch die Sprachsteuerung. So kann man bei kompatiblen IoT-Geräten etwa Lampen anschalten, Raumtemperaturen verändern oder das Fernsehprogramm umschalten. Grundsätzlich können mit smarten Lautsprechern auch Telefonate geführt werden, allerdings bestehen gegenüber einem Telefon Funktionseinschränkungen sowie deutliche Unterschiede zwischen den Herstellern. Die weitreichendsten Funktionalitäten bieten Amazon Echo und der Telekom Smart Speaker.

---

https://www.bitkom.org/Presse/Presseinformation/Beliebte-Helfer-Sprachassistenten-haben-sich-durchgesetzt.

120 Vgl. Taş, S.; Hildebrandt, C.; Arnold, R.: Sprachassistenten in Deutschland, WIK-Diskussionsbeitrag Nr. 441, Bad Honnef, 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_441.pdf.

121 Produktbeschreibung der Telekom: https://www.telekom.de/smarte-produkte/smart-speaker/telekom-smart-speaker.

122 Vgl. Pakalski, I. (2020): Amazon setzt Impulse, Google ist abgeschlagen, in: golem.de, 01.10.20, elektronisch verfügbar unter: https://www.golem.de/news/smarte-lautsprecher-amazon-setzt-impulse-google-ist-abgeschlagen-2010-151210.html.

123 Vgl. Allison, C. (2020): How to use Bluetooth to connect Amazon Echo to phones or speakers, in: the-ambient.com, 21.08.20, elektronisch verfügbar unter: https://www.the-ambient.com/how-to/connect-alexa-echo-bluetooth-phone-speaker-531.

124 Etwa „Wie wird das Wetter morgen?“ oder „Wie hoch ist der Mount Everest?“.

Tabelle A-3: Telefonie mit smarten Lautsprechern[125]

Amazon Echo (bzw. Alexa)	Telekom Smart Speaker
	
- **Telefonie bei Verbindung mit Alexa-Smartphone-App möglich** - **App greift auf Kontakte auf dem Smartphone zu** - **Angerufener Kontakt muss ebenfalls Alexa-App nutzen** - **Anruf per Sprachbefehl möglich** - **Anruf über App auch ohne Speaker möglich (OTT-Dienst vergleichbar zu Sprachanruf über WhatsApp oder Telegram)** - **Über Adapter (Echo Connect) Anschluss an Router möglich für Telefonie über Festnetzanschluss -> In Deutschland nicht mehr verfügbar, Produktqualität wurde vielfach kritisiert**	- Beworben mit „Festnetz-Telefonieren per Freisprechfunktion - kein zusätzliches Gerät notwendig“ - Speaker wird als DECT-Telefon am Router angemeldet - Telefonie über den Festnetz-Anschluss - Vorher im t-online-Adressbuch hinterlegte Kontakte können via Sprachsteuerung angerufen werden - Mit entsprechendem Router (Fritzbox) Rufnummernwahl in Router-Benutzeroberfläche möglich - Freie Rufnummernwahl am Speaker derzeit nicht vorgesehen

Quelle: WIK basierend auf Amazon und Telekom.

Bei anderen Anbietern ist die Telefonie über den smarten Lautsprecher in Deutschland noch nicht vollumfänglich verfügbar. Diese wird bis dato nur über den entsprechenden OTT-Dienst (Google Duo für Telefonie via Google Assistant) bzw. über eine Kopplung mit dem Smartphone realisiert (für die Telefonie mit Siri über Apple-Geräte).[126]

---

125 Vgl. https://www.telekom.de/zuhause/geraete-und-zubehoer/smart-speaker/telekom-smart-speaker-schwarz-weiss; https://telekomhilft.telekom.de/t5/Smart-Home/Telefonie-mit-Telekom-Magenta-Smart-Speaker-und-Smart-Speaker/ta-p/4620064; https://www.amazon.de/Amazon-Echo-Connect-Alexa-Telefonanschluss/dp/B071D5NW6R und Pakalski, I. (2019): Telefonieren mit Alexa-Lautsprecher macht so keinen Spaß, in: golem.de, 22.01.19, elektronisch verfügbar unter: https://www.golem.de/news/echo-connect-im-test-telefonieren-mit-alexa-lautsprecher-macht-so-keinen-spass-1901-138848.html.

126 Vgl. Bourennani, K. (2019): Google Duo Telefonate nun über den Google Home möglich, in: smarthomeassistent.de, 04.10.19, elektronisch verfügbar unter: https://www.smarthomeassistent.de/google-duo-telefonate-nun-ueber-den-google-home-moeglich/ sowie Gillhuber, F. (2019): Apple HomePod zum Telefonieren nutzen – so geht’s, in: chip.de,

Google bietet in den USA bereits die Möglichkeit, jegliche Festnetz- und Mobilfunknummern über den mit dem heimischen WLAN verbundenen Smart Speaker anzuwählen. Anrufe mit unterdrückter Nummer, bei denen kein Rückruf möglich ist, sind kostenlos. Alternativ kann die Mobilfunkrufnummer mit dem Lautsprecher verknüpft werden, wodurch eine Zuordnung möglich wird. Bei aktiver Verknüpfung können auch Anrufe mit der Mobilfunkrufnummer vom Lautsprecher aus getätigt werden, wenn das dazugehörige Smartphone ausgeschaltet oder außer Reichweite ist.[127] Ab dem Zeitpunkt der Verknüpfung wird der Mobilfunkvertrag des Nutzers zu dessen Konditionen genutzt.[128]

Erhobene Daten und Datenschutz

Laut Herstellerangaben wird erst durch die Aktivierung eines Wake-Words durch den Nutzer (z. B. „Alexa“ oder „Hey Siri“) eine Verbindung zur Cloud des Anbieters hergestellt.[129] Die Aufnahme wird durch ein Licht und/oder Tonsignal angezeigt, was die mögliche Einstufung als missbräuchliche Sendeanlage nach § 90 TKG unwahrscheinlicher macht. Allerdings besteht die Möglichkeit, dass ein smarter Lautsprecher unbeabsichtigt und möglicherweise unbemerkt aktiviert wird, weil er fälschlicherweise ein Wake Word versteht.[130]

Bei der Verarbeitung der Nutzereingaben in der Cloud gab es in der Vergangenheit schon Sicherheitsvorfälle. So waren sich viele Kunden nicht bewusst, dass Amazon Sprachaufzeichnungen nicht nur automatisiert verarbeitet, sondern diese unter bestimmten Voraussetzungen auch manuell von Mitarbeitern zur Qualitätsverbesserung analysiert.[131] Auf diesen Umstand wird inzwischen zwar in den FAQ verwiesen, die Funktionalität ist jedoch weiterhin standardmäßig eingestellt.[132]

Auch in Kopfhörern und Headsets, die ebenfalls über Bluetooth an Endgeräte wie Smartphones angeschlossen werden und als Lautsprecher und ggf. Mikrofon fungieren, gibt es inzwischen verbaute Sprachassistenten.[133] Funktional unterscheiden sich diese nicht von den in Smart Speakern genutzten Assistenten. Aus Datenschutzsicht sind

---

19.03.19, elektronisch verfügbar unter: https://praxistipps.chip.de/apple-homepod-zum-telefonieren-nutzen-so-gehts_109050.

127 Vgl. Hilfeseiten von Google zu dem Thema: https://support.google.com/googlenest/answer/7363847?co=GENIE.Platform%3DAndroid&hl=en.

128 Da bei einigen Anbieter keine Notruffunktionalitäten vorgesehen sind, wäre bei einer Anwendung in Deutschland zu prüfen, ob ein Verstoß gegen § 108 TKG vorliegt.

129 Exemplarisch für Alexa von Amazon hier beschrieben: https://www.amazon.de/b/?node=17084415031.

130 Vgl. Eckert, S. et al. (2020): Die lauschenden Lautsprecher, in: tagesschau.de, 30.06.20, elektronisch verfügbar unter: https://www.tagesschau.de/investigativ/ndr/smart-speaker-101.html.

131 Vgl. Fuest, B. (2019b): Amazon Echo: Wie Mitarbeiter Alexa-Aufnahmen mithören, in: gruenderszene.de, 12.04.19, elektronisch verfügbar unter: https://www.gruenderszene.de/technologie/amazon-echo-wie-mitarbeiter-alexa-aufnahmen-mithoeren?interstitial.

132 Siehe Häufige Fragen zu Alexa/Echo-Geräten bei Amazon: https://www.amazon.de/b/?node=17084417031.

133 Ein prominentes Beispiel sind die in Deutschland noch nicht erhältlichen Amazon Echo Buds, in die der Sprachassistenzdienst Alexa integriert sind, siehe: Klein, U. (2020): Echo Buds im Test-Überblick – ANC In-Ear Bluetooth-Kopfhörer, in: homeandsmart.de, 15.01.20, elektronisch verfügbar unter: https://www.homeandsmart.de/amazon-echo-buds-kopfhoerer.

Sprachassistenzsysteme in Kopfhörern noch problematischer, da diese regelmäßig auch unterwegs genutzt werden und damit noch häufiger Gespräche und Geräusche von unbedarften Dritten in Hörweite des Kopfhörers aufnehmen können.[134] Auch diese Geräte müssen jedoch über Wake-Words aktiviert werden und verarbeiten nicht durchgehend Audioaufnahmen ihrer Umwelt.

Verbraucherschutz und IT-Sicherheit

Ein verbraucherschutzrelevantes Thema im Zusammenhang mit Sprachassistenten ist die Möglichkeit des Einkaufens über diese Programme bzw. Geräte. So kann bei Amazons Alexa ein Kauf bei Amazon via Sprachbefehl ausgelöst werden.

Dabei kann es zu Pannen kommen, z. B. ein möglicherweise unbeabsichtigtes Bestellen von Dingen durch Dritte.[135] Darüber hinaus ist eine mögliche Beeinflussung des Nutzers beim Kauf kritisch zu sehen: Falls der Kunde nicht genau Marke und/oder Modell des gewünschten Kaufgegenstandes spezifiziert, bekommt er von Amazon einen Vorschlag (die sogenannte „Amazon's Choice"). Warum das entsprechende Produkt vorgeschlagen wird, kann der Nutzer nicht nachvollziehen. Theoretisch gibt es, zumindest auf der US-Seite von Amazon aufgelistete, Kriterien für die algorithmengesteuerte Auswahl eines solchen Artikels als „Amazon's Choice" (z. B. möglichst gute und zahlreiche Bewertungen, möglichst viele Käufe von Kunden mit gleichem Suchbegriff, geringe Retourenquote)[136], in der Praxis bemängeln Verbraucherzentralen jedoch die ausgewählten Artikel auf der deutschen Amazon-Webseite. So wurden dem Nutzer in Stichproben etwa Gegenstände mit wenigen Bewertungen oder mit deutlich teureren Preisen als bei Konkurrenz-Shops empfohlen.[137]

Auch bei smarten Lautsprechern können fehlende Software-Updates die volle Funktionsfähigkeit des Gerätes einschränken. So hat **Microsoft** kürzlich die **Abschaffung des Sprachassistenten Cortana als separate Smartphone-App** angekündigt. Auch der einzige Smart Speaker, der Cortana nutzt, wird damit seine smarten Funktionen verlieren und zu einer reinen Bluetooth-Box „downgegradet".[138]

---

134 Vgl. Lindsey, N. (2019): Amazon's New Smart Products Raise All Kinds of Alexa Privacy Concerns, in: CPO Magazine, 09.10.19, elektronisch verfügbar unter: https://www.cpomagazine.com/data-privacy/amazons-new-smart-products-raise-all-kinds-of-alexa-privacy-concerns/.

135 So hat 2017 ein Nachrichtensprecher in San Diego versehentlich durch das Fernsehen mit der Alexa der Zuschauer Puppenhäuser bestellt, siehe: Kaltschmidt, T. (2017): Amazon Echo: Nachrichtensprecher löst Massenbestellung aus, in: heise.de, 08.01.17, elektronisch verfügbar unter: https://www.heise.de/newsticker/meldung/Amazon-Echo-Nachrichtensprecher-loest-Massenbestellung-aus-3591039.html.

136 Vgl. Schanze, R. (2020): Amazon's Choice: Was ist das? Welche Kriterien gibt es?, in: giga.de, 07.02.20, elektronisch verfügbar unter: https://www.giga.de/artikel/amazons-choice-was-ist-das-welche-kriterien/.

137 Vgl. Verbraucherzentrale NRW (2020): Stichprobe zum Gütesiegel „Amazon's Choice" – Amazons fragwürdige Empfehlungen, in: Verbraucher Aktuell, 05.02.20, elektronisch verfügbar unter: https://www.verbraucherzentrale.nrw/sites/default/files/2020-02/02_Amazons_Choice.pdf.

138 Vgl. Nickel, O. (2020): Microsoft schaltet Cortana für Smartphones ab, in: golem.de, 04.08.20, elektronisch verfügbar unter:

Wettbewerbliche Aspekte

Grundsätzlich besteht die Problematik, dass Alexa ausschließlich bei Amazon und nicht in einem anderen Onlineshop bestellt. Darüber hinaus können mittelbar auch unerwünschte Effekte auf den Wettbewerb auf Produktmärkten entstehen.

Sprachassistenzsysteme können die **Gatekeeper-Funktion** von Amazon verstärken. Die Verkaufsplattform nimmt dort einen größeren Einfluss auf die Kaufentscheidung als bei Anordnung von Suchergebnissen, Listing und Delisting auf der Website. Eine Bevorzugung von Eigenmarken oder Partnerunternehmen sowie eine Priorisierung gegen Bezahlung ist nicht auszuschließen und hätte negative Effekte auf Wettbewerb und Innovationstätigkeit. Zudem kann sich die Produktvielfalt verringern, wenn ein Anbieter Produktvarianten bewusst vom Marktplatz nimmt, um sicherzugehen, dass durch den Sprachassistenten als das profitabelste Produkt erkannt und bestellt wird.[139]

Dieselbe Problematik gilt auch für andere Sprachassistenten, z. B. Google Assistant, der Preisvergleiche und Käufe über die Produktsuchmaschine Google Shopping durchführt[140] oder auch für Siri von Apple. Beide Anbieter arbeiten z. B. in den USA mit dem Einzelhändler und Amazon-Konkurrenten Walmart zusammen.[141]

Ein solches Gatekeeping kann nicht nur Produktmärkte wettbewerblich beeinflussen, sondern **auch gesellschaftlich unerwünschte Folgen** haben. So könnte der Betreiber des Sprachassistenzsystemes entscheidet, welche Dienste für Nachrichten Informationensabfrage genutzt werden. Die Entscheidung des zu konsumierenden Nachrichtenmediums wird dem Nutzer durch das Assistenzsystem abgenommen, nach Parametern, die nicht nach außen transparent sind. Gleiches gilt für die Auswahl von weiteren Medien, die vom Nutzer angefragt werden, wie Buch- oder DVD-Empfehlungen.[142]

Auch die Kompatibilität mit anderen Geräte im Smart Home kann große Effekte auf die jeweiligen Märkte haben. So kaufen Kunden, die aktiv einen Sprachassistenten nutzen wahrscheinlich nur ein smartes Thermostat, das auch über diesen Assistenten steuer-

---

https://www.golem.de/news/sprachassistentin-microsoft-schaltet-cortana-fuer-smartphones-ab-2008-150049.html.

139 Vgl. Meyersohn, N. (2018): Amazon's Alexa is the biggest challenge for brands since the internet, in: CNN Business, 10.05.18, elektronisch verfügbar unter: https://money.cnn.com/2018/05/10/news/companies/alexa-amazon-smart-speakers-voice-shopping/index.html.

140 Siehe Support-Seite von Google unter: https://support.google.com/assistant/answer/9130767.

141 Vgl. Gärtner, M. (2019): Voice Commerce: Walmart bietet jetzt Shopping mit Siri, in: onlinehaendler-news.de, 13.11.19, elektronisch verfügbar unter: https://www.onlinehaendler-news.de/online-handel/haendler/131987-walmart-bietet-shopping-mit-siri.

142 So steht Amazon generell unter der Kritik, dass dort etwa verschwörungsmythische Literatur prominent platziert ist, siehe: Meineck, S.; Laufer, D. (2020): So penetrant empfiehlt Amazon den Kauf von Verschwörungsliteratur, in: netzpolitik.org, 02.09.20, elektronisch verfügbar unter: https://netzpolitik.org/2020/desinformation-so-penetrant-empfiehlt-amazon-den-kauf-von-verschwoerungsliteratur/.

bar ist.[143] Hier zeigt sich in der Praxis schon jetzt ein großer Vorteil der großen Technologiekonzerne.

Innerhalb des Marktes für Sprachassistenten kann es zur einer Verfestigung von Marktmacht kommen, wenn diese aufgrund ihrer großer Nutzer- und damit auch analysierbaren Datenbasis immer bessere Assistenzfunktionen bieten können. Dies führt dann zu einem qualitativ hochwertigen Produkt, aus dem sich eine Feedbackschleife ergibt.[144]

B.4 Smartes Spielzeug

Der Bereich „smartes Spielzeug“ umfasst neben **smarten Puppen**, die auf Spracheingaben antworten, auch **ferngesteuerte Autos und Drohnen mit vernetzten Kameras**. Smartes Spielzeug kommuniziert mit einem Sendegerät, anderem Spielzeug oder mit einem Internetserver.

Marktrelevanz und Anbieterstruktur

Der Markt für vernetztes Spielzeug wird immer größer. Dabei richtet sich das Spielzeug an eine besonders schützenswerte Gruppe, nämlich Kinder und ggf. Jugendliche. In diesem Segment spielen sowohl große Hersteller als auch Nischenanbieter wichtige Rollen.

Bei Drohnen und ferngesteuerten Autos mit Kamera gibt es viele Nischenanbieter, die sehr kostengünstige No-Name-Geräte mit einer günstigen Kamera und einem Vernetzungs-Chip ausstatten und so ein smartes Gerät „schaffen“.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Die Anbindung von smarten Puppen erfolgt entweder über Bluetooth mit einem Smartphone, um eine App-Steuerung zu ermöglichen oder über WLAN, um direkt an die Cloud angebunden zu werden. Ferngesteuerte Autos und Drohnen mit Videokameras bauen oft eine eigene WLAN-Verbindung mit dem Smartphone auf.

---

143 52 % der Nutzer von Smart-Home-Anwendungen in Deutschland steuern diese via Sprachbefehl, 85 % davon nutzen einen stationären Sprachassistenten (Smart Speaker), siehe: Vgl. Bitkom (2020b): Das intelligente Zuhause: Smart Home 2020.

144 Taş, S.; Hildebrandt, C.; Arnold, R.: Sprachassistenten in Deutschland, WIK-Diskussionsbeitrag Nr. 441, Bad Honnef, 2019, elektronisch verfügbar unter: https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_441.pdf.

Erhobene Daten, Datenschutz, Verbraucherschutz und IT-Sicherheit

Zu den bekanntesten kritischen Produkten gehört die Puppe „My Friend Cayla“[145], die Anfang 2017 aus dem Verkehr gezogen wurde.[146] Diese konnte Kindern unter anderem über Sprachsteuerung gestellte Fragen beantworten. Hierfür wird die Sprache aufgezeichnet, in die Cloud übertragen und dort verarbeitet und analysiert.[147]

Nach Ansicht von Verbraucherschutzorganisationen ist dies jedoch nicht die einzige problematische Funktionalität. Die Puppe lässt sich ohne physischen Kontakt über Bluetooth aktivieren, wenn die Aktivierung über die Begleit-App erfolgt, wird die Aktivierung auch nicht an der Puppe angezeigt. Die Werbeeinwilligungen zur Nutzung seien zu unspezifisch und weitreichend, die Sprachaufzeichnungen werden an eine US-Firma zur Analyse weitergegeben und von dort aus womöglich auch noch an Dritte. Dazu gibt es auf Kinder zugeschnittene Werbebotschaften durch die Puppe, die nicht explizit als solche gekennzeichnet sind.[148]

Neben Puppen sind auch weitere Arten von Spiel- und Freizeitgeräten mit Sendeanlagen ausgestattet. So gibt es ferngesteuerte Autos oder Drohnen mit Kamera, die die Umgebung aufnehmen. Hierbei wird die komplette Umgebung gefilmt und/oder fotografiert, bei Fahrten im öffentlichen Raum ist eine Aufnahme von unbeteiligten Dritten damit nicht nur nicht ausgeschlossen, sondern sogar wahrscheinlich.

Bei smarten ferngesteuerten Autos, oftmals simple Modelle mit angebrachter Kamera, läuft die Videoübertragung live auf einer App auf dem Smartphone des Steuernden, wo diese dann auf Wunsch gespeichert werden kann. Für eine Einstufung als missbräuchliche Sendeanlage nach § 90 TKG kommt es laut Bundesnetzagentur insbesondere auf die Eigenschaften der Kamera an, die die Möglichkeiten zum Identifizieren der aufgenommenen Personen bedingen (z. B. den Aufnahmewinkel). Bei Drohnen ist die aktuelle regulatorische Auffassung, dass hier die Ausstattung mit Kameras so gängig und allgemein bekannt sei, dass diese nicht als missbräuchliche Sendeanlage einzustufen sind.[149]

---

145 Es ist zu erwarten, dass die Puppe vorher einen gewissen Absatz gefunden hat. Sie war ca. drei Jahre am Markt und für diverse Preise nominiert bzw. in Bestenlisten vertreten, siehe: Stiftung Warentest (2017): Puppe Cayla – Verbotene Spionin im Kinderzimmer, in: test.de, 20.02.17, elektronisch verfügbar unter: https://www.test.de/Puppe-Cayla-Verbotene-Spionin-im-Kinderzimmer-5144210-0/.

146 Vgl. Bundesnetzagentur (2017): Bundesnetzagentur zieht Kinderpuppe “Cayla” aus dem Verkehr, Pressemitteilung, 17.02.17, elektronisch verfügbar unter: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=690686.

147 Technisch musste die Puppe via Bluetooth mit einem Smartphone oder Tablet verbunden sein, das dann wiederum über die Begleit-App mit dem Internet kommuniziert.

148 Vgl. Myrstad, F. (2016): Connected toys violate European consumer law, in: forbrukerradet.no, 06.12.16, elektronisch verfügbar unter: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws.

149 Vgl. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/MissbrauchSendeanlagen/HinweiseProduktkategorien/hinweiseproduktkategorien-node.html#doc733922bodyText6.

Wettbewerbliche Aspekte

Wettbewerbsprobleme bei smartem Spielzeug sind aktuell nicht bekannt, der Markt ist relativ breit aufgestellt und noch vergleichsweise klein ist.

C Tracking und Monitoring

Der Bereich Tracking und Monitoring lässt sich aufteilen in **Gesundheits- und Medizintracker**, die das Tracking mit einem gesundheitlichen Hintergrund ermöglichen sowie einfache **Tracker von Wert- und Vermögensgegenständen** auf GPS-Basis.

C.1 Gesundheits- und Medizinprodukte

Vernetzte Gesundheits- und Medizinprodukte sind dem Bereich der Medizintechnik zuzuordnen und bilden einen **Wachstumsmarkt** innerhalb der Gesundheitswirtschaft. Die dynamische Entwicklung wird u.a. durch die steigende Lebenserwartung, die Zunahme chronischer Krankheiten und eine Verlagerung in der medizinischen Versorgung von der Behandlung zur Prävention befördert. Vernetzte medizinische Geräte zur Fernüberwachung von Patienten sollen dazu beitragen, die Wiederaufnahmequoten im Krankenhaus zu senken und Patienten in entlegenen Gebieten besser zu versorgen. Vernetzte Medizinprodukte haben vor diesem Hintergrund eine hohe volkswirtschaftliche Bedeutung.

Das Marktforschungsunternehmen IDTechEx erfasst Medizinprodukte im Wearables-Bereich und schätzt, dass im Zeitraum 2010 bis 2019 etwa ein Drittel der gesamten Wearables-Umsätze mit Medizinprodukten erwirtschaftet wurde. Dabei wurden 20 unterschiedliche Typen von tragbaren Medizinprodukten betrachtet (darunter z. B. Hörgeräte, Herzgeräte, Insulinpumpen, Glukosemonitore, elektronische Hautpflaster).[150]

Das Interesse der Verbraucher an vernetzten Medizinprodukten ist bereits hoch und steigt kontinuierlich. So zeigte eine Studie von YouGov bereits im Jahr 2016, dass die Hälfte der Befragten vernetzten Health-Trackern zur Kontrolle der Vitalfunktionen positiv gegenübersteht. Dabei wurden besondere Vorteile in der Prävention und in Lösungen für Pflegefälle gesehen. Bedenken hatten die Befragten am stärksten in Bezug auf die Sicherheit der Datenübertragung und den vertrauensvollen Umgang mit ihren Gesundheitsdaten (ca. 70 % der Befragten).[151]

Marktrelevanz und Anbieterstruktur

Der gesamte Medizinbereich unterliegt **strengen gesetzlichen Regelungen** und ist durch spezifische komplexe Rahmenbedingungen geprägt, die einen starken nationalen Bezug haben. Daher müssen Medizinprodukte aufwendige Zertifizierungsprozesse[152]

---

150 Vgl. Heyward, James (2019): The future of wearables is medical, 10 September 2019, elektronisch verfügbar unter: https://www.idtechex.com/fr/research-article/the-future-of-wearables-is-medical-part-1/18057.

151 Vgl. YouGov (2016): Smart Health: Überwachung der Vitalfunktionen für Viele attraktiv, Pressemitteilung vom 15.06.2020, elektronisch verfügbar unter: https://yougov.de/news/2016/06/15/smart-health-uberwachung-der-vitalfunktionen-fur-v/.

152 Vgl. zu Marktzugangsvoraussetzungen für Medizinprodukte, zur Zertifizierung und entsprechenden Regelungen auch Bundesministerium für Gesundheit: Marktzugangsvoraussetzungen, elektronisch verfügbar unter: https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/marktzugangsvoraussetzungen.html.

durchlaufen und ihr Markterfolg hängt auch von Faktoren wie z. B. der Erstattungsfähigkeit durch gesetzliche Krankenkassen[153] ab.[154] Dieser Kontext ist nicht nur für Start-Ups, sondern auch für ausländische Anbieter eine große Herausforderung und bildet gemeinsam mit den typischerweise hohen Forschungs- und Entwicklungsausgaben **relativ hohe Markteintrittsbarrieren**.

Das **Anbieterspektrum** im traditionellen Medizintechnik-Bereich ist durch **internationale Großunternehmen** geprägt, wobei auch **deutsche Mittelständler** mit hohem Spezialisierungsgrad eine Rolle spielen.[155] Im Bereich vernetzter Medizinprodukte eröffnen sich jedoch auch Chancen für **branchenfremde Unternehmen**, die z. B. über Erfahrungen mit Software und Sensoren verfügen.

So haben sich zum einen etablierte Anbieter aus dem Medizintechnik-Bereich (z. B. Medtronic (USA), Biotronik (Deutschland)) und zum anderen auf den Bereich vernetzter Gesundheitsprodukte spezialisierte Unternehmen etabliert (z. B. Fitbit, Withings). Tendenziell ist die Zahl der Anbieter von sehr komplexen und spezifischen Produkten begrenzt und bei Massenprodukten (z. B. vernetzten Waagen) hoch.

Ebenso wie in anderen Anwendungsbereichen des Consumer-IoT hat sich auch im medizinischen Bereich ein **spezifisches Ökosystem** entwickelt, bestehend aus Geräteherstellern, Softwareentwicklern, Netzbetreibern, Systemintegratoren und Akteuren aus dem medizinischen Bereich (insbesondere Medizingerätehersteller).[156]

Produktspektrum: Merkmale, technische Realisierung und Konnektivität

Als Medizinprodukte werden Produkte mit medizinischer Zweckbestimmung bezeichnet, die über unabhängige Prüf- und Zertifizierungsstellen zugelassen werden.[157] Es zeigt sich dabei ein Trend zu immer stärkerer Regulierung im Bereich der Medizintechnik.[158]

Die **Anzahl vernetzter Medizingeräte nimmt kontinuierlich zu**. Ein wesentlicher Treiber für vernetzte Medizingeräte sind dabei Fortschritte im Bereich der Sensorik und

---

153 Vgl. zur Erstattung von Medizinprodukten ausführlich auch BVMed: Branchenbericht Medizintechnologien 2020, 12. Mai 2020, S. 27 ff.

154 Vgl. Luther/Clairfield (2020): Marktstudie Medizintechnik 2020, S. 25.

155 Vgl. Luther/Clairfield (2020): Marktstudie Medizintechnik 2020, S. 27. Innerhalb Deutschlands befindet sich in Tuttlingen ein Medizintechnikcluster mit insgesamt 450 Unternehmen, die vielfach internationale Bedeutung haben, siehe https://www.weltzentrum-der-medizintechnik.de/start.

156 Vgl. z. B. Deloitte (2018): Medtech and the Internet of Medical Things - How connected medical devices are transforming health care - July 2018, elektronisch verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf, S. 9.

157 Sie erhalten eine CE-Kennzeichnung, Vgl. zur Zertifizierung von Medizinprodukten BfArM, elektronisch verfügbar unter: https://www.bfarm.de/DE/Medizinprodukte/RechtlicherRahmen/inverk/_node.html, Vgl. zur Zulassung im Detail auch Luther/Clarifield (2020),: Marktstudie Medizintechnik 2020, S. 21.

158 Vgl. z. B. ECONUM (2018): Den Puls gefühlt Was beschäftigt die mittelständischen Medizintechnikunternehmen? Studie zur Medizintechnikbranche und Unternehmen in Deutschland, elektronisch verfügbar unter: https://www.johner-institut.de/blog/wp-content/uploads/2017/02/ECONUM-Medizintechnikstudie_2018.pdf.

der Miniaturisierung.[159] Mit zunehmendem Fortschritt im Bereich der Künstlichen Intelligenz sind darüber hinaus Weiterentwicklungen zur Analyse der Datenmengen zu erwarten. Zu gebräuchlichen Sensoren in vernetzten Medizinprodukten gehören Bewegungssensoren (z. B. zur Sturzerkennung oder Aktivitätscharakterisierung) und Sensoren zur Herzfrequenzüberwachung (für unterschiedliche Herzmetriken). Weniger verbreitet sind Sensoren zur Bestimmung der Körpertemperatur, zur Erkennung bestimmter chemischer Analyten oder zur Beurteilung physiologischer Reaktionen auf bestimmte Reize.

Ein zukünftiger Treiber ist in der 5G-Technologie zu sehen. Sie kann zahlreiche Anwendungen im Gesundheitsbereich ermöglichen, die hohe Ansprüche an die Übertragungsqualität und Datenraten stellen und ggf. Echtzeitmonitoring erfordern.

Das **Ausgestaltungsspektrum** im Bereich vernetzter Medizinprodukte, die dem Consumer-IoT zuzuordnen sind, ist **sehr vielfältig**. Klassische Medizingeräte werden zunehmend mit Software ausgestattet, die Funktionen automatisiert und menschliches Eingreifen reduziert. Der Trend zu patientenorientierten Komplettlösungen, die medizintechnische Geräte ergänzen, prägt den gesamten Bereich der Medizintechnik.[160] Diese stellen besonders hohe Anforderungen an Konnektivität, IT-Sicherheit und Datenschutz.

Im Bereich der Fernüberwachung können z. B. ***Patienten mit Herzschrittmachern*** kontinuierlich ärztlich überwacht werden. So bietet ***Biotronik Home Monitoring Services*** Lösungen zur Fernüberwachung von Implantatpatienten (Herzschrittmachern), bei denen das Implantat Informationen über den Herzzustand an ein Patientengerät sendet (CardioMessenger). Der CardioMessenger ist dabei mit einer SIM-Karte ausgestattet und überträgt die Daten über das Mobilfunknetzwerk an das Home Monitoring Service Center (HMSC) zur Auswertung. Ärzte haben Zugriff auf die Daten und können den Gesundheitszustand des Patienten kontinuierlich überwachen.[161]

Innovative ***Blutzuckermessysteme*** können bereits ergänzt werden um einen Sensor im Unterhautfettgewebe, der automatisch eine kontinuierliche Glukosemessung durchführt und in Kombination mit einer vernetzten Insulinpumpe die Versorgung von Diabetespatienten verbessert.[162] Dies zeigt das Produktbeispiel von Medtronik, einem führenden Medizintechnikhersteller aus den USA (siehe Tabelle A-4).

---

159 Vgl. z. B. Informationen beim Sensorhersteller TE Connectivity, elektronisch verfügbar unter: https://www.te.com und Frost & Sullivan (2019): Patient Monitoring Industry— Analysis of Investment and Trends, 2018, February 2019.

160 Vgl. z. B. ECONUM (2018): Den Puls gefühlt Was beschäftigt die mittelständischen Medizintechnikunternehmen? Studie zur Medizintechnikbranche und Unternehmen in Deutschland, elektronisch verfügbar unter: https://www.johner-institut.de/blog/wp-content/uploads/2017/02/ECONUM-Medizintechnikstudie_2018.pdf.

161 Vgl. https://www.biotronik.com/de-de/products/home-monitoring.

162 Siehe z. B. Diabetes News: Bauch oder Arm – wo messen Sensoren am besten?, elektronisch verfügbar unter: https://www.diabetes-news.de/nachrichten/bauch-oder-arm-wo-messen-sensoren-am-besten.

Tabelle A-4: Produktbeispiel: vernetzte Insulinpumpe (Medtronic)

- Das MiniMedTM 670G System dient der Adaption der kontinuierlich abzugebenden basalen Insulindosis (zur Sicherstellung des nahrungsunabhängigen Insulinbedarfs) anhand der durch einen Glukosesensor gemessenen Werte.
- Für die Abgabe der Insulin-Boli zu den Mahlzeiten teilt der Patient dem System die Kohlenhydratmenge mit.
- Das System errechnet den Insulinbolus und schlägt diesen vor. Dieser muss jedoch vor Auslösung vom Patienten bestätigt werden.

Quelle: Medtronic.[163]

Deutlich einfachere vernetzte Produkte mit gesundheitlichem Schwerpunkt sind ***Blutdruck- und Fiebermessgeräte sowie smarte Waagen***, die sich typischerweise über Bluetooth zur Übertragung der Messwerte mit dem Smartphone verbinden und über eine zugehörige App diverse Monitoring- und Kontrollfunktionen anbieten.

Ein zukünftiger Trend ist im Bereich ***Smart Clothes*** zu sehen. Hier werden Kleidungsstücke mit Sensoren ausgestattet, die Vitalparameter wie z. B. Herzfrequenz oder Atemfrequenz erfassen. In diesem Produktbereich finden bereits seit vielen Jahren[164] umfassende Forschungsprojekte statt.[165] Bisher hat sich hier allerdings noch kein Massenmarkt im Consumer-Bereich entwickelt. Im gewerblichen Bereich werden jedoch bereits Produkte zur Steigerung von Gesundheitsschutz und Arbeitssicherheit einge-

163 Vgl. https://www.medtronic.com/de-de/diabetes/home/produkte/insulinpumpe/minimed-640g-insulinpumpe.html.

164 Siehe z. B. eine Präsentation des Bekleidungsphysiologischen Instituts Hohenstein aus dem Jahr 2003: „Smart Clothes – Funktionstextilien für die Bekleidungsindustrie, elektronisch verfügbar unter: https://vibinet.de/images/Smart_Clothes.pdf.

165 Siehe z. B. die Forschungsprojekte im Forschungsfeld „Smart Textiles“ des Fraunhofer-Instituts für Zuverlässigkeit und Mikrointegration IZM, elektronisch verfügbar unter: https://www.izm.fraunhofer.de/en/abteilungen/system_integrationinterconnectiontechnologies/arbeitsgebiete/smart_textiles.html.

setzt (z. B. Shirt „Health Guard“, das als Unterhemd direkt auf der Haut getragen wird und mit Sensoren zur Erfassung von Puls, Herzrhythmus und Bewegungsdaten ausgestattet ist. So werden Bewegungsunfähigkeiten infolge eines Unfalls oder Sturzes erkannt und ein Notruf ausgelöst, siehe Tabelle A-5).[166]

Tabelle A-5: Produktbeispiel: Smart Clothes „Health Guard“

- Entwickelt von Innogy in Kooperation mit den StartUps Ambiotex (Wearables) und WearHealth (künstliche Intelligenz).
- Innerhalb der innogy Westenergie seit 2017 im Einsatz (für Monteure in Windparks, Umspannwerken, an Leitungen und Schaltschränken).
- Sensoren zur Erfassung von Puls, Herzrhythmus und Bewegungsdaten.
- Shirt plus App, die die das Stresslevel des Nutzers berechnet und bei kritischen Werten Warnhinweise und Handlungsempfehlungen gibt. Bei Bewegungsunfähigkeit (Unfall, Sturz) wird ein Notruf ausgelöst.
- Kosten: Starterset mit drei Monaten Vertragslaufzeit. Pro Mitarbeiter 99,95 Euro pro Monat (bei längerer Laufzeit 39,95 Euro pro Monat).

Quelle: WIK basierend auf Innogy Westenergie.[167]

Für die Vernetzung von Medizinprodukten sind unterschiedliche Lösungen im Einsatz. Grundsätzlich können die Daten eines einfachen vernetzten Messgeräts (z. B. Blutdruck- oder Blutzuckermessgerät) per Bluetooth an das Smartphone übertragen werden. Die über die App auf dem Smartphone angebotenen Auswertungen werden über die Datenverarbeitung auf einer IoT-Plattform realisiert. Der Nutzer kann auf der App seine Messwerte ablesen und in bestimmten Auswertungen, z. B. im Zeitverlauf, verfolgen.

166 Vgl. Innogy Westenergie, elektronisch verfügbar unter: https://www.westenergie.de/unternehmen/netzservice/produkte/arbeitssicherheit-health-guard.

167 Vgl. https://www.westenergie.de/unternehmen/netzservice/produkte/arbeitssicherheit-health-guard, https://news.innogy.com/smart-clothing-digitales-shirt-von-innogy-tragt-zu-mehr-gesundheitsschutz-bei/.

Sofern die Daten Dritten (z. B. einem Arzt) zur Verfügung gestellt werden, werden diese über eine gesicherte Verbindung an eine IoT-Plattform (bzw. in eine Cloud) weitergeleitet. Auf diese können wiederum autorisierte Dritte zugreifen, um die Daten zu überwachen und auszuwerten. Die Verschlüsselung der Datenübertragung ist dabei von zentraler Bedeutung. Insbesondere der Echtzeit-Zugriff auf die Daten gewinnt im Bereich der medizinischen Geräte perspektivisch immer größere Relevanz. Hier schafft die 5G-Technologie entsprechenden Gestaltungsspielraum für neue Produkte. Für die Realisierung komplexerer vernetzter Medizingeräte und -anwendungen (z. B. Remote Patient Monitoring-Systeme) bildet eine leistungsfähige und unterbrechungsfreie Netzwerkverbindung eine grundlegende Voraussetzung.[168]

Erhobene Daten, Aspekte des Datenschutzes und der IT-Sicherheit

Vernetzte Medizinprodukte erheben, speichern und verarbeiten in hohem Umfang personenbezogene Daten. Ein relevanter Teil dieser Daten sind sog**. „sensible Daten“**, die sich auf die Gesundheit beziehen (z. B. Seriennummer eines medizinischen Gerätes, das Datum einer Implantierung, genetische oder biometrische Daten).[169] Damit sind die erhobenen Daten im Bereich vernetzter Geräte in besonderer Weise schützenswert. Mögliche Verletzungen des Datenschutzes haben gravierendere Folgen als in anderen Anwendungsbereichen des Consumer-IoT, denn im schlimmsten Fall können Datenmanipulationen lebensbedrohlich sein.[170]

Auch die Anforderungen an die IT-Sicherheit sind für Medizinprodukte von herausragender Relevanz. Vernetzte Medizinprodukte haben **typischerweise mehr als eine Schnittstelle**, um die Verbindung mit anderen Produkten oder Dokumentationssystemen (z. B. einer App) herzustellen. Zudem werden Daten vielfach mit Dritten (z. B. Ärzten) geteilt, um ausgewertet zu werden. Jede Schnittstelle gefährdet jedoch potentiell die Datensicherheit. In Bezug auf IT-Schnittstellen stellt sich basierend auf dem Datensparsamkeitsprinzip stets die Frage, ob eine Schnittstelle tatsächlich für den Behandlungsprozess notwendig ist oder nicht.

Datenschutz und IT-Sicherheit von vernetzten Medizinprodukten unterliegen **strengen Vorschriften und einer kontinuierlichen Kontrolle**. Risiken von Medizinprodukten werden kontinuierlich bewertet (geregelt wird dies in der Medizinprodukte-Sicherheitsplanverordnung MPSV)[171]. Die Risikobewertung wird vom Bundesinstitut für

---

168 Siehe auch Frost & Sullivan (2019): Patient Monitoring Industry— Analysis of Investment and Trends 2018, S. 59.

169 Siehe z. B. Datenschutzerklärung von Medtronic, elektronisch verfügbar unter: https://www.medtronic.com/de-de/datenschutzbestimmungen.html.

170 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): Medizintechnik, elektronisch verfügbar unter: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eHealth/Medizintechnik/Medizintechnik_node.html.

171 Vgl. Bundesministerium der Justiz und für Verbraucherschutz sowie Bundesamt für Justiz (2002): Verordnung über die Erfassung, Bewertung und Abwehr von Risiken bei Medizinprodukten (Medizinprodukte-Sicherheitsplanverordnung – MPSV), 24.06.2002, elektronisch verfügbar unter: https://www.gesetze-im-internet.de/mpsv/MPSV.pdf.

Arzneimittel und Medizinprodukte (BfArM) vorgenommen, das als selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Gesundheit für die Zulassung, die Verbesserung der Sicherheit von Arzneimitteln, die Risikoerfassung und -bewertung von Medizinprodukten zuständig ist.[172] Datenschutz- und IT-Sicherheitsrisiken von Medizinprodukten unterliegen den Vorschriften, die für alle Medizinprodukte gelten und sind daher auch Bestandteil der Risikobewertung durch das BfArM.

Für Aspekte des Datenschutzes und der IT-Sicherheit gelten im Bereich vernetzter Medizinprodukte zunächst grundsätzlich die gleichen gesetzlichen Grundlagen wie für andere Anwendungsbereiche. Allerdings sind im Medizinbereich weitreichendere Regelungen getroffen worden, die den spezifischen Anforderungen an die strenge Gewährleistung von Kriterien wie Vertraulichkeit, Verfügbarkeit und Integrität gerecht werden. Die Datenschutzregelungen im Gesundheitsbereich werden kontinuierlich auf spezifische neue Entwicklungen hin angepasst.

Im ***Digitale-Versorgungs-Gesetz (DVG)***, das seit dem 19. Dezember 2019 in Kraft ist, wurden zentrale Grundlagen für den erleichterten Marktzugang softwaregestützter Gesundheitslösungen gelegt.[173] Wichtige Details der Durchführung regelt die seit dem 8. April 2020 vorliegende ***Digitale Gesundheitsanwendungen Verordnung (DiGAV)***[174], die sich auf erstattungsfähige digitale Gesundheitsanwendungen bezieht und in § 4 Anforderungen an Datenschutz und Datensicherheit aufführt.[175] In einem ausführlichen Fragebogen muss der Hersteller einer erstattungsfähigen digitalen Gesundheitsanwendungen Auskunft zu detailliert aufgeführten Anforderungen an den Datenschutz geben.[176]

---

172 Vgl. Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) (2020): Über das BfArM, elektronisch verfügbar unter: https://www.bfarm.de/DE/BfArM/_node.html.

173 Siehe hierzu auch https://www.bfarm.de/DE/Medizinprodukte/DVG/_node.html.

174 Siehe Bundesgesetzblatt (2020): Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020, elektronisch verfügbar unter: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'632665'%5D&skin=pdf&tlevel=-2&nohist=1.

175 Siehe Bundesministerium für Gesundheit: Verordnung über das Verfahren und die Anforderungen der Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale-Gesundheitsanwendungen-Verordnung – DiGAV), Referentenentwurf, Stand: 9.4.2020, elektronisch verfügbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/DiGAV_RefE.pdf.

176 Siehe Bundesgesetzblatt (2020): Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020, elektronisch verfügbar unter: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'632665'%5D&skin=pdf&tlevel=-2&nohist=1, S. 779 ff.

Die europäische Verordnung ***Medical Device Regulation (MDR)*** vom 5 April 2017[177] zielt auf eine Erhöhung von Sicherheit und Leistungsfähigkeit medizintechnischer Lösungen ab und muss bis Mai 2021 in nationales Recht umgesetzt werden.[178] Sie enthält in Anhängen spezielle Vorschriften für Softwareanwendungen und -entwicklung und hebt die Risikoklassen zahlreicher Produkte an, die dann einem Audit unterzogen werden müssen. Dieses Verfahren dient auch dem Aufdecken möglicher Sicherheitslücken.

Darüber hinaus gibt es für Hersteller von Medizinprodukten einen Leitfaden zur IT-Sicherheit, der auf der Basis einer in den USA bereits entwickelten Informationsgrundlage zu IT-sicherheitsrelevanten Eigenschaften von IT-gestützten medizinischen Systemen[179] erarbeitet wurde. Dabei handelt es sich allerdings um eine freiwillig zu nutzende Dokumentation, die nicht gesetzlich verpflichtend ist.[180]

Aufgrund der zahlreichen Detailvorgaben, Zertifizierungs- und Überwachungsstrukturen ist anzunehmen, dass das Datenschutzniveau bei zugelassenen Medizinprodukten im Bereich der Consumer-IoT deutlich höher ist als in anderen Anwendungsbereichen wie z. B. Smart Home oder Wearables. Dennoch sind in der Vergangenheit bereits zahlreiche IT-Sicherheitsvorfälle im Medizinbereich aufgetreten, darunter Malware-Angriffe auf die IT-Systeme von Krankenhäusern oder Funkangriffe auf Insulinpumpen.[181]

Wettbewerbliche Aspekte

Der Markt für Medizinprodukte ist ein Wachstumsmarkt, in dem aufgrund des technischen Fortschritts und steigenden Bedarfs ein erhebliches Marktpotential im Bereich Consumer-IoT mit **vielfältigen neuen Geschäftsmodellen** erwartet werden kann. Im Zuge von 5G erweitern sich die Möglichkeiten zudem beträchtlich. Die Markteintrittsbarrieren sind aufgrund stärkerer Regulierung als in anderen Anwendungsbereichen jedoch höher. Dennoch wächst die Zahl der Anbieter in zahlreichen Produktbereichen, insbesondere bei einfacheren Produkten wie Blutdruckmessgeräten oder Waagen. Glo-

177 Siehe Europäisches Parlament und Rat der Europäischen Union (2017): VERORDNUNG (EU) 2017/745 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.

178 Vgl. Bundesministerium für Gesundheit: Medizinprodukte – neue EU-Verordnungen, elektronisch verfügbar unter: https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/neue-eu-verordnungen.html sowie Europäische Kommission: Medical Devices -Sector, elektronisch verfügbar unter: https://ec.europa.eu/health/md_sector/overview_en.

179 MDS2 (Manufacturer Disclosure Statement for Medical Device Security), elektronisch verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed_MDS2.pdf;jsessionid=0908BB5DA77EDE4F6C5CF1E879BD252D.1_cid501?__blob=publicationFile&v=3, S. 4.

180 Vgl. Allianz für Cyber-Sicherheit (2019): Sicherheit von Medizinprodukten - Leitfaden zur Nutzung des MDS2 aus 2019, elektronisch verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed_MDS2.pdf;jsessionid=0908BB5DA77EDE4F6C5CF1E879BD252D.1_cid501?__blob=publicationFile&v=3.

181 Vgl. https://meso.vde.com/de/cybersecurity-und-medizinprodukte/.

bale Anbieter (z. B. Medtronic) spielen in einige Produktgruppen eine wichtige Rolle. Internetkonzerne wie Google oder Amazon haben im Bereich der vernetzten Medizinprodukte hingegen bisher kaum Relevanz, drängen jedoch zunehmend in den Markt.

C.2 Tracking von Wertgegenständen und Haustieren

Das Tracking von Wertgegenständen und Haustieren wird insbesondere über **kleine Geräte auf GPS-Basis** realisiert. Während Trackinglösungen für private Anwendungen eher als Nischenprodukte einzuordnen sind, haben sie für spezifische Einsatzfelder im gewerblichen Bereich eine hohe Relevanz (z. B. Fuhrparkmanagement).

Produktspektrum und Produktbeispiele

Das Ausgestaltungsspektrum von GPS-Trackern ist facettenreich. Allen Produkten gemeinsam ist, dass sie mit einem GPS-Tracker und einer Funkanbindung (z. B. Bluetooth, GSM-Modul, LPWAN-Technologie) ausgestattet sind. Darüber hinaus spielen bei der Produktgestaltung Sensoren eine Rolle (z. B. Bewegungssensor, Beschleunigungsmesser, Sturzsensor).

Unterschiede bestehen insbesondere mit Blick auf die spezifischen Ausstattungsmerkmale und Funktionen des Geräts, die eingesetzte Funktechnologie, die Monitoringmöglichkeiten über die begleitende App sowie die Preis- und Vertragsgestaltung.

Die simpelsten Trackingvarianten bestehen in einfachen Ortungsgeräten, die selbst kein eigenes GPS-Modul enthalten, sondern für die Übermittlung ihrer Standortdaten das GPS-Modul eines Smartphones in Bluetooth-Reichweite nutzen. So lassen sich jedoch nur Geräte in einer Reichweite von etwa 50 m identifizieren (z. B. über das Produkt „Musegear Finder“[182]).

Am weitesten verbreitet sind GPS-Tracker, die zur **Funkanbindung das öffentliche Mobilfunknetz** nutzen und eine hohe Abdeckung gewährleisten.[183] Dabei spielen LPWAN-Technologien (im öffentlichen Mobilfunk[184] oder im lizenzfreien Spektrum[185]) eine zentrale Rolle. Für die auf hohe Reichweite und geringe Datenübertragung ausgerichteten Technologien gilt Tracking neben gewerblichen Lösungen wie Flottenmanagement als eines der wichtigsten Einsatzfelder.

Die Möglichkeiten zur Überwachung und Steuerung, die i.d.R. über **begleitende App- und/oder Webportal-Lösungen** realisiert werden, unterscheiden sich ebenfalls. Je nach Einsatzbereich und spezifischen Anforderungen z. B. an Wasserfestigkeit oder autarke Energieversorgung variieren das Gehäuse, die Halterung/Befestigung, die Art

182 Vgl. https://musegear-finder.net/.
183 Vgl. https://iot.telekom.com/en/blog/the-lte-m-prototyping-program.
184 Zum Beipiel Velocate über LTE-M der Deutschen Telekom, elektronisch verfügbar unter: https://iot.telekom.com/de/blog/das-lte-m-prototyping-program.
185 Zum Beispiel der Lobaro GPS-Tracker (ca. 150 Euro), elektronisch verfügbar unter: https://www.lobaro.com/portfolio/lorawan-gps-tracker/.

der Stromversorgung und Auflademöglichkeiten. Einige GPS-Tracker sind in Alltagsgegenstände integriert (z. B. SmartSole[186] in eine Schuhsohle, Velocate[187] in ein Fahrrad-Rücklicht).

Ein weiteres Differenzierungsmerkmal besteht in der Preis- und Vertragsgestaltung. Grundsätzlich fallen immer Kosten für die Anschaffung des Geräts an. Darüber hinaus gibt es verschiedene Ausgestaltungsvarianten, die teilweise unübersichtlich und für den Verbraucher kaum vergleichbar sind.

Nur in wenigen Fällen entstehen keine weiteren laufenden Kosten (z. B. Fahrradtracker im Rücklicht Velocate, https://velocate.com/vcone/, 200 bis 250 Euro). Meist fallen jedoch auch monatliche Kosten für die Datenübertragung und teilweise auch für die App-Nutzung (sowie ggf. weiterer Services wie z. B. Kundenbetreuung) an.

GPS-Tracker, die der Hersteller in Kooperation mit einem Mobilfunknetzbetreiber entwickelt, sehen typischerweise die Zahlung monatlicher Gebühren an den IoT-Gerätehersteller vor. IoT-Hersteller begründen die Bindung an einen Mobilfunknetzbetreiber gegenüber dem Verbraucher häufig mit Sicherheitsaspekten.[188] Exemplarisch für diese häufige Ausgestaltungsform sind z. B. die GPS-Tracker „***Autoskope***“ und „***Tractive***“ (siehe Tabelle A-6).

186 Vgl. https://gpssmartsole.com/gpssmartsole/.
187 Vgl. https://velocate.com/?bid=143382-29355-&adcref=www.google.de%2F.
188 Siehe z. B. Autoskope: *„Eigene SIM-Karten können in unseren Ortungsgeräten nicht verwendet werden, da wir dann die Verschlüsselung und Sicherheit deiner Daten nicht gewährleisten könnten.“*, elektronisch verfügbar unter: https://shop.autoskope.de/geraete/1/autoskope-v2-starterset.

Tabelle A-6: Produktbeispiele: Fahrzeugortung „Autoskope“ und Haustiertracker Tractive

“Autoskope”	“Tractive”
	
- Einsatzgebiet: Ortung von Fahrzeugen sowie Booten oder Motorrädern - Mobilfunknetz: T-Mobile - Kostenstruktur: - *Anschaffungskosten* Autoskope Starterset: 290 Euro; Motoskope Starterset: 349 Euro; Bootskope Starterset 369 Euro - *Kosten für Datenübertragung und App-Nutzung*: im ersten Jahr keine Zusatzkosten, danach 3,99 Euro pro Monat - Roaming: enthalten - Sonstiges: Autoskope gibt an, dass die Infrastruktur in Berlin betrieben wird, wo die Server an zwei redundant angebundene Rechenzentren angeschlossen sind und vom Unternehmen selbst betrieben werden.	- Einsatzgebiet: Ortung von Haustieren (Hunde oder Katzen) - Mobilfunknetz: O2 - Kostenstruktur: - Anschaffungskosten ca. 50 Euro - *Kosten für Datenübertragung und App-Nutzung*: Basistarif oder Premiumtarif[189], monatliche Kosten variieren nach Vertragslaufzeit (z. B. Basistarif: 7,99 Euro pro Monat, 49,90 Euro für 1 Jahr, 89,90 Euro für 2 Jahre, Premiumtarif: 59,90 Euro für 1 Jahr, 99,90 Euro für 2 Jahre, 199,90 Euro für 5 Jahre) - Roaming: im Premiumtarif enthalten

Quelle: WIK basierend auf Autoskope[190], Tractive[191], O2[192].

Es gibt auch eine Vielzahl von GPS-Trackern ohne Mobilfunkanbindung, für die der Verbraucher einen separaten Vertrag mit einem Mobilfunkanbieter für die Datenübertragung abschließen muss. Sie sind insbesondere auf Online-Portalen im Internet verfügbar und umfassen in der Regel nur die Anschaffungskosten.[193] Ein Teil dieser Produkte ist mit Blick auf Daten- und Verbraucherschutz durchaus kritisch zu beurteilen.

189 Basistarif (GPS Tracking, Live Tracking, Aktivitätstracking) oder Premiumtarif (zusätzlich: Roaming für 150 Länder, Exportfunktionen, “Premium Kundenservice”).
190 Vgl. https://autoskope.de.
191 Vgl. https://tractive.com/de/?gclid=EAIaIQobChMI-pPm946f6gIVwR0YCh2iiggPEAAYASAAEgLAn_D_BwE.
192 Vgl. https://www.o2startrader.co.uk/insights/1079/the-best-gps-tracker-devices.
193 Siehe z. B. bei Pearl, https://www.pearl.de/a-NX4440-1511.shtml, Amazon, https://www.amazon.de/dp/B074W3ZLD6/?tag=sternvgl03-21 oder Alibaba,

Wettbewerbliche Aspekte

Die Angebotsstruktur im Bereich der GPS-Tracker ist vielfältig und es bestehen **niedrige Markteintrittsbarrieren**. Es gibt diverse Spezialisierungsmöglichkeiten auf einzelne Einsatzbereiche, die auch kleinen Anbietern Marktchancen bieten.

In Bezug auf die **Mobilfunkanbieter** für die Konnektivität des GPS-Trackers verfügt der Verbraucher aufgrund der Produktgestaltung jedoch vielfach über **keine eigenen Wahlmöglichkeiten**.

Dies liegt daran, dass ein relevanter Teil der in Deutschland vermarkteten GPS-Tracker in Kooperation mit einem Mobilfunknetzbetreiber als typisches IoT-Produkt mit LPWAN-Technologien realisiert wird (z. B. Velocate über LTE-M-Technologie der Deutschen Telekom). Bei diesen Produkten wird der Mobilfunknetzbetreiber vom IoT-Hersteller ausgesucht und der Endnutzer des IoT-Geräts hat keinen Einfluss auf die Betreiberauswahl.

Es gibt jedoch auch eine Vielzahl an meist günstigen GPS-Trackern, die nur das Gerät ohne bzw. mit begrenzten zusätzliche Leistungen (App etc.) umfassen. Hier ist oft auch das Einlegen einer SIM-Karte und die freie Auswahl des Mobilfunknetzbetreibers möglich (z. B. Teltonika TMT 250 Min Tracker easy[194], TKSTAR TK 906 SMS/GPS Tracker[195]). Für diese Produkte kann der Verbraucher entweder einen komplett neuen Vertrag abschließen oder eine Multi-SIM zu seinem bestehenden Vertrag hinzufügen.

Verbraucherschutz

Die Leistungscharakteristika und die verbundenen Kosten sind bei zahlreichen GPS-Trackern wenig transparent, was die Vergleichbarkeit der Angebote erschwert.

Ein weiterer verbraucherschutzrelevanter Aspekt besteht in den Funktionen und Ausstattungsmerkmalen einiger GPS-Tracker. Die Ortungsfunktion als zentrale Funktion der GPS-Tracker ist grundsätzlich unproblematisch, sofern sie nicht missbräuchlich genutzt wird. Einige Produkte sind jedoch mit einer **unerlaubten Abhörfunktion** ausgestattet, die durch Anruf des Geräts ausgelöst wird. Diese Geräte sind zwar nach § 90 TKG verbotenen, können jedoch von Verbrauchern in Deutschland erworben werden. Dabei gibt es zum einen Online-Portale, die gezielt auf Abhörmöglichkeiten ausgerichtete Produkte vermarkten[196] und zum anderen internationale Plattformen[197], auf denen Verbraucher GPS-Tracker mit Abhörfunktion erwerben können. Während bei den erst-

https://www.alibaba.com/trade/search?fsb=y&IndexArea=product_en&CatId=&SearchText=GPS+tracker.

194 Vgl. https://teltonika-sas.com/product/mini-tracker-easy/#downloads.

195 Vgl. http://www.tkstargps.com/ProductShow.asp?ID=189.

196 Siehe z. B. https://tonspy.com/en/; https://www.abhoergeraeteshop.com/store/p344/Gps_Peilsender_-_Zigarettenanzünder_mit__Abhörfunktion.html; https://www.abhoergeraeteshop.com/store/c7/GPS-Peilsender-Diskrete-Standortueberwachung.

197 Zum Beispiel www.alibaba.com.

genannten der Verbraucher diese Geräte typischerweise bereits mit dem Ziel eines missbräuchlichen Einsatzes erwirbt, kann es bei letztgenannten aufgrund häufig lückenhafter Produktinformationen auch zum unbewussten Erwerb verbotene Geräte kommen. Der Besitz von verbotenen Sendeanlagen ist jedoch grundsätzlich strafbar.

Datenschutz und IT-Sicherheit

GPS-Tracker sammeln kontinuierlich **Bewegungsdaten**. Im Consumer-Bereich sind sie meist auf die Ortung von Wertgegenständen und Tieren ausgerichtet, seltener auf die Ortung von Personen. Nichtsdestotrotz werden neben Bewegungsdaten teils auch andere Informationen (z. B. GPS-Position des mobilen Geräts des Benutzers, Adresse und Kontodaten) erhoben, die den allgemeinen Datenschutzregelungen unterliegen.[198] Insgesamt haben Datenschutzaspekte jedoch eine etwas geringere Relevanz als in anderen Anwendungsbereichen des Consumer-IoT wie z. B. Medizingeräte.

Einen Problembereich bildet die **Vielzahl von günstigen Nischenprodukten**, die vielfach im außereuropäischen Ausland hergestellt werden. Hier ist i.d.R. nicht transparent, wo und wie die erhobenen Daten gespeichert werden, wie eine Löschung der Benutzerkonten erfolgen kann oder ob die Verschlüsselung bei der Datenübertragung erfolgt. Diese Geräte werden vielfach von chinesischen Anbietern hergestellt, die auch eine zugehörige App mit den entsprechenden Funktionen zur Standortauswertung bieten. Über die Verwendung der Daten, die Art und den Ort der Speicherung sind bei diesen Produkten oft keinerlei Informationen vorhanden. In der Vergangenheit haben Experten bereits **Sicherheitslücken** bei GPS-Trackern identifiziert, die den unerlaubten Zugriff auf Daten ermöglichen.[199]

198 Siehe z. B. die Datenschutzerklärung des Haustiertrackers Tractive, elektronisch verfügbar unter: https://assets.tractive.com/static/legal/de/privacy-policy.pdf.

199 Vgl. Breithut, J. (2019): Forscher warnen vor unsicheren GPS-Trackern. 6. Juni 2019, elektronisch verfügbar unter: https://www.spiegel.de/netzwelt/gadgets/gps-tracker-forscher-warnen-vor-sicherheitsluecken-bei-peilsendern-a-1285601.html.

D Wearables

Wearables sind vernetzte Geräte, die der Nutzer am Körper trägt. Im Rahmen dieses Diskussionsbeitrages werden Fitnessarmbänder und Smartwatches zusammengefasst betrachtet.

Marktrelevanz und Anbieterstruktur

Der globale Markt für Wearables entwickelt sich seit etwa 10 Jahren mit wachsender Dynamik. Dabei sind Wearables in asiatischen Märkten bereits stärker verbreitet als in anderen Teilen der Welt.[200]

IDC zufolge ist im Wearables-Markt zwischen 2019 und 2023 weltweit mit gewichteten jährlichen Wachstumsraten in Höhe von 7,9 % zu rechnen. Auf den Bereich Smartwatches entfielen im Jahr 2019 bereits 41 % aller verkauften Wearables-Produkte (siehe Tabelle A-7).[201]

Tabelle A-7: Wearables: Prognose nach Produktkategorie, weltweit (2019-2023)

Produkt-kategorie	Verkaufte Stückzahlen in Mio. (2019)	Marktanteil (2019)	Verkaufte Stückzahlen in Mio. (2023)	Marktanteil (2023)	CAGR 2019-2023
Watch	91,8	41,2%	131,6	43,5%	9,4%
Earwear	72,0	32,3%	105,3	34,8%	10,0%
Wristband	54,2	24,3%	55,0	18,2%	0,3%
Sonstige	5,0	2,2%	10,4	3,4%	20,3%
Insgesamt	**222,9**	**100,0%**	**302,3**	**100,0%**	**7,9%**

Quelle: Schätzungen im Rahmen des IDC Quarterly Wearable Device Tracker June 19, 2019.[202]

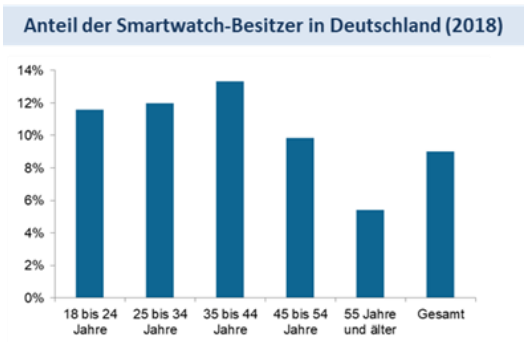
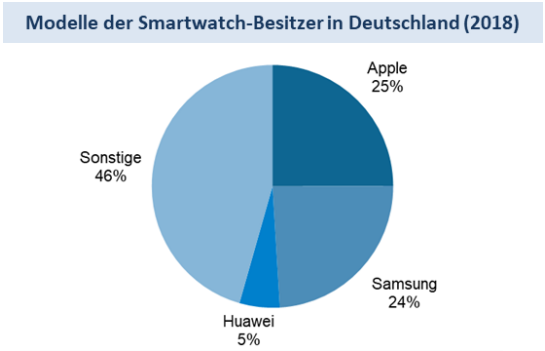
Eine empirische Untersuchung des WIK (2018) stellte fest, dass Ende 2018 in Deutschland 9 % der Befragten eine Smartwatch besaßen. Von den Smartwatch-Nutzern hatten 25 % eine Apple Watch, 24 % eine Smartwatch von Samsung (siehe Tabelle A-8).

200 Vgl. z. B. Canalys (2019): Canalys: Worldwide wearable band market grew 65% in Q3 2019 while Asia Pacific doubled in volume, Press Release, 13 December 2019, elektronisch verfügbar unter: https://www.canalys.com/newsroom/canalys-worldwide-wearable--market-q3-2019.

201 Vgl. IDC (2019): Earwear and Watches Expected to Drive Wearables Market at a CAGR of 7.9%, Says IDC, 19 Juni 2019, elektronisch verfügbar unter: https://www.idc.com/getdoc.jsp?containerId=prUS45271319.

202 Vgl. IDC (2019): Earwear and Watches Expected to Drive Wearables Market at a CAGR of 7.9%, Says IDC, 19 Juni 2019, elektronisch verfügbar unter: https://www.idc.com/getdoc.jsp?containerId=prUS45271319.

Tabelle A-8: Wearables: Nutzung in Deutschland (WIK, 2018)

Befragung des WIK (2018)	
▪ Deutschland ▪ Repräsentative Stichprobe: 3.184 Personen	
	

Quelle: WIK.

Einer Studie von Splendid Research (2019) zufolge können derzeit etwa 50 % der Bevölkerung als potentielle Nutzer von Wearables betrachtet werden.

Tabelle A-9: Wearables: Nutzung in Deutschland (Studie von Splendid, 2019)

Studie von Splendid (2019)
▪ Repräsentative Befragung zu Wearables, Tracking-Apps und „Selbstvermessung“ ▪ Deutschland ▪ Repräsentative Stichprobe: 1.193 Personen ▪ Fokus auf 18 Wearables und 36 Apps
▪ Ergebnisse: – 24 % der Befragten nutzen Fitnesstracker oder Smartwatches – Weitere 26 % haben Interesse an einer Nutzung – Hauptmotivation der Nutzer: Nutzung des Wearables für Gesundheit und Sport – Gründe für die Nicht-Nutzung von Wearables: fehlende Notwendigkeit zur Verhaltensmessung (44 % der Ablehner), Preis (33 %). – Die Bereitschaft zum Teilen der gesundheitsbezogenen Daten ist groß, wenn es dafür Vergünstigungen gibt. So würden über die Hälfte der Deutschen diese Daten mit Ärzten und Krankenkassen teilen. Knapp 20 % würden die gesundheitsbezogenen Daten ihrem Arbeitgeber oder Onlineshops zur Verfügung stellen.

Quelle: WIK basierend auf Splendid (2019).[203]

203 Vgl. Ergebnisse einer repräsentativen Befragung von 1.193 Personen von Splendid Research (2019): Studie: Optimized Self Monitor 2019, Repräsentative Umfrage zu Tracking-Apps, Wearables und

Als ein **Pionier** kann das 2007 in den USA gegründete Unternehmen **Fitbit** betrachtet werden, das sich schnell eine führende Marktposition sichern konnte und nun von Google übernommen werden soll (EU-Verfahren läuft, siehe Tabelle A-12). Andere Pioniere wie Jawbone sind inzwischen insolvent. Mitte der 2010er Jahre traten die internationalen Smartphone-Hersteller in den Wearables-Markt ein (zunächst Xiaomi mit dem Mi-Band 2014, dann Apple mit der Apple Watch 2015).[204]

Inzwischen werden Wearables von einer Vielzahl von nationalen und internationalen Anbietern aus verschiedenen Branchen vermarktet, die mit Wearables ihr bestehendes Produktportfolio ergänzen[205]:

- Smartphone-Hersteller/ITK-Hersteller: Apple, Samsung, Huawei, Xiaomi[206], LG, Lenovo, Garmin u.a.
- Uhrenhersteller: Citizen, TAG Heuer, Swatch, Fossil u.a.
- Modeunternehmen: Boss, Armani, Guess, Hilfiger, Diesel, Michael Kors u.a.
- Spezialisten mit Fokus auf den Consumer-IoT-Bereich: Zeblaze, Fitbit (USA), Belio (NL, Kinder-Smartwatches).

Über Marktanteile einzelner Unternehmen in Deutschland sind keine Daten verfügbar. Studien zum globalen Markt legen nahe, dass die Mehrzahl der verkauften Produkte auf internationale Anbieter aus dem Bereich der ITK-Hersteller entfallen.

Die Ambitionen der ITK-Hersteller im Wearables-Markt müssen im Kontext ihrer gesamten IoT-Strategie gesehen werden. Dabei besteht die Tendenz, das bestehende Produktportfolio immer stärker in Richtung eines „Ökosystems“ zu entwickeln, in dem eine steigende Anzahl von vernetzten Geräten pro Nutzer über eine einzige Plattform verwaltet wird. Führend ist in dieser Hinsicht Apple.

Produktspektrum: Merkmale, technische Realisierung/Konnektivität

Das Angebot an Wearables ist heute sehr vielfältig. Eine Unterscheidung in „Fitnesstracker“ und „Smartwatches“ kann kaum noch getroffen werden, da Fitnesstracker auch als Uhren fungieren und Smartwatches typischerweise mindestens einfache Fitnesstracker-Funktionen enthalten.

Selbstvermessung in Deutschland, elektronisch verfügbar unter: https://www.splendid-research.com/de/studie-optimized-self.html.

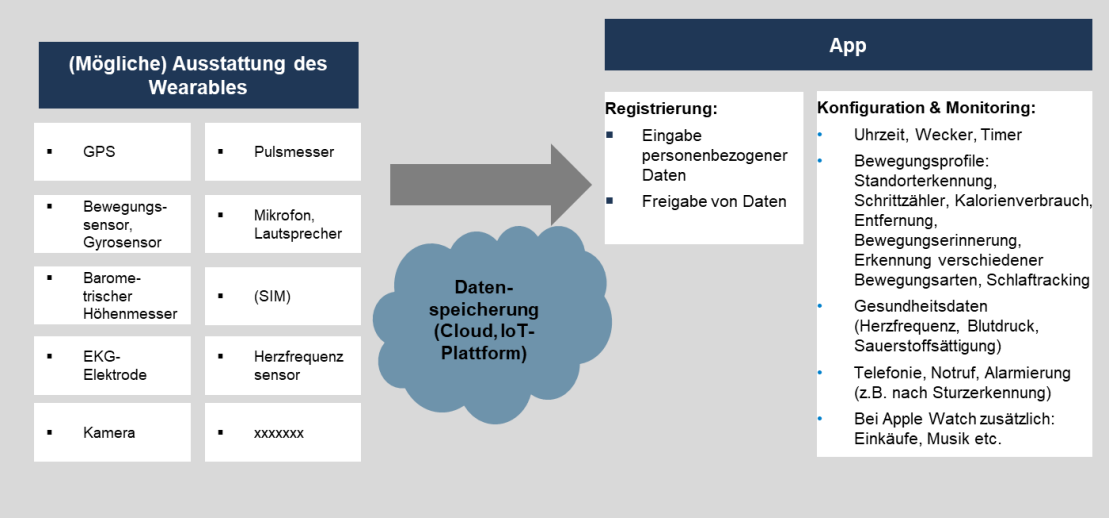
204 Siehe zu Geschichte und Entwicklung der Fitness-Armbänder auch https://fitnessarmband.eu/geschichte-und-entwicklung-der-fitness-armbaender/#2011-jawbone-erobert-den-markt.

205 Siehe z. B. https://www.smartwatch.de/smartwatch/.

206 Vgl. hierzu auch Boden, B. (2020): Xiaomi will mit smarten Produkten rund ums Smartphone weiter wachsen, in: Telecom Handel, 28.08.2020, elektronisch verfügbar unter: https://www.telecom-handel.de/consumer-communications/xiaomi/xiaomi-smarten-produkten-smartphone-wachsen-2570157.html.

Die Nutzung eines Wearables ist i.d.R. nicht ohne ein Begleitgerät (Smartphone) möglich, auf dem eine App installiert werden muss. Dieses wird i.d.R. sowohl zur Registrierung und Einrichtung des Geräts als auch für die vollumfängliche Nutzung des Wearables benötigt. Das Wearable ist mit Sensoren ausgestattet, über die Daten generiert und mittels spezifischer Apps ausgewertet werden. Die Verbindung zwischen dem Wearable und dem Begleitgerät erfolgt per Bluetooth. Die vom Wearable generierten Daten werden ebenso wie weitere benutzerbezogene Informationen zur Weiterverarbeitung auf IoT-Plattformen übertragen (siehe Abbildung A-1).

Abbildung A-1: Wearables: Produktmerkmale und Auswertungsmöglichkeiten



Quelle: WIK.

Die Produktdifferenzierung betrifft zum einen das Design der Smartwatches, das insbesondere bei Armband und Display/Ziffernblatt vielfältige Ausgestaltungsmöglichkeiten bietet. So werden auch zielgruppenspezifische Produkte wie Kinder-Smartwatches entwickelt. Am Beispiel der Apple Watch zeigt sich bei gleichem Funktionsumfang ein breites Spektrum an Wahlmöglichkeiten in Bezug auf Farbe, Material etc., das auch eine hohe Individualisierung der Produkte ermöglicht.

Zum anderen unterscheiden sich Smartwatches wesentlich in Bezug auf ihre technischen Ausstattung. Tendenziell hat der Funktionsumfang der Smartwatches in den letzten Jahren stark zugenommen. Fitness-Armbänder umfassten in der Einführungsphase zunächst die Funktionen Schrittzähler, Entfernungsmessung und verbrauchte Kalorien.

Nach und nach wurde der Funktionsumfang durch die Ausstattung mit mehr Sensoren erweitert. GPS-Sensoren, Pulsmesser sowie ein detailliertes Aktivitäts- und Schlaftracking sind heute selbst bei einfachen Modellen Standard.

Am Beispiel der Apple Watch wird dies besonders deutlich: Neuere Modelle verfügen auch über Herzüberwachungsfunktionen, die vor allem auf die Indikation Vorhofflimmern ausgerichtet sind und entsprechende Warnungen für den Nutzer generieren. Die EKG-App (nutzbar für ein 1-Kanal-EKG) und Herzrhythmus-App sind als Medizinprodukt zugelassen worden, zunächst von der US-amerikanischen Behörde FDA (September 2018) und ein halbes Jahr später (Februar 2019) in Europa (CE). Zuvor hatte Apple in der „Apple Heart Studie“ (AHS)“ die Funktion und Messgenauigkeit seiner Herzrhythmus-App selber umfassend geprüft.[207] Die im September 2020 eingeführte Apple Watch Series 6 wurde um die Messung des Blutsauerstoffs mittels eines zusätzlichen Sensors[208] erweitert.

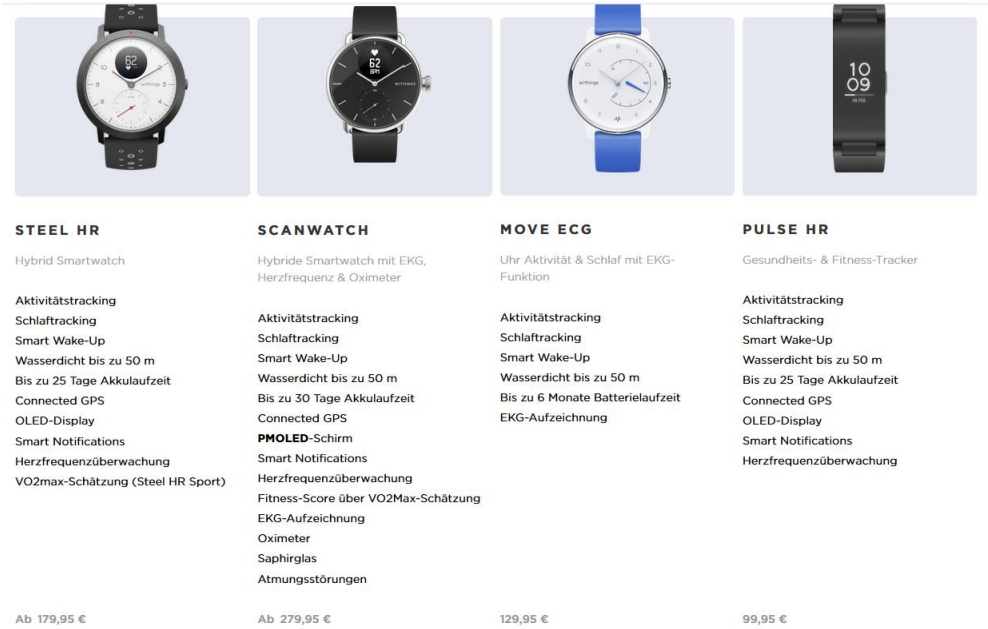
Es bestehen jedoch auch mit Blick auf den Funktionsumfang Wahlmöglichkeiten – sowohl im Markt als auch bei einzelnen Herstellern. Dies verdeutlicht beispielhaft das aktuelle Produktangebot von Withings (siehe Abbildung A-2), dessen Smartwatches mit Preisen zwischen knapp 100 Euro und ca. 280 Euro von einfachen Aktivitätstrackern mit Puls- und GPS-Funktion bis zur Smartwatch mit umfassenden Medizinfunktionen reichen. Die „Scanwatch“ verfügt über klinisch validierte Anwendungen, die das Risiko von Vorhofflimmern sowie nächtliche Atemprobleme (Schlafapnoe) identifizieren sollen.[209]

207 Vgl. z. B. Ärztezeitung (2019): Kardiologie via Smartwatch, 27.03.2019, elektronisch verfügbar unter: https://www.aerztezeitung.de/Wirtschaft/Kardiologie-via-Smartwatch-253412.html, Grätzel, P. (2019): Auch in Europa: Apple Watch kann EKG und Vorhofflimmern, 27.03.2019, elektronisch verfügbar unter: https://e-health-com.de/details-news/auch-in-europa-apple-watch-kann-ekg-und-vorhofflimmern/.

208 Vier Cluster aus grünen, roten und infraroten LEDs sowie vier Fotodioden im Glas des Gehäusebodens, der das vom Blut zurückreflektierte Licht aufnimmt.

209 Vgl. Költsch, T. (2020): Withings EKG-Smartwatch ist ab 280 Euro erhältlich, 7.9.2020, elektronisch verfügbar unter: https://www.golem.de/news/scanwatch-withings-ekg-smartwatch-ist-ab-280-euro-erhaeltlich-2009-150705.html.

Abbildung A-2: Produktbeispiele: Smartwatches von Withings (September 2020)



Quelle: Withings, https://www.withings.com/de/de/watches.

Nur wenige Smartwatch-Modelle bieten heute **eigenständige Telefonie-Funktionen**, die durch die direkte Verbindung in das öffentliche Mobilfunknetz realisiert werden. Sobald eine Smartwatch Telefonie anbietet, entstehen neben den Anschaffungskosten für das Produkt selbst zusätzlich laufende Verbindungskosten durch die Mobilfunknutzung.

Zu den vorhandenen Angeboten mit Telefonie-Funktion gehören auf der einen Seite die Premium-Produkte führender Hersteller mit ausgewählten Modellen der Apple Watch und der Samsung Galaxy Watch. Auf der anderen Seite ist die Telefonie-Funktion in Kinder-Smartwatches verfügbar, die als Ersatz für ein Smartphone dienen sollen.

Telefonie wird bei diesen beiden Produktgruppen unterschiedlich umgesetzt. Bei der Apple Watch und Samsung Galaxy werden Profile unterschiedlicher Anbieter auf eine eSIM geladen. Kinder-Smartwatches werden entweder in Kooperation mit einem Netzbetreiber über dessen Mobilfunknetz und IoT-Plattform realisiert (per eSIM oder festverbautem SIM-Chip) oder verfügen über einen SIM-Karten-Schlitz, in den der Nutzer eine SIM-Karte seiner Wahl einlegt. Mit beiden Realisierungsformen sind aus Verbraucher- und aus Wettbewerbssicht verschiedene Vor- und Nachteile verbunden.

Welche Relevanz Telefonie in Bezug auf alle im Markt verbreiteten Smartwatches hat, ist schwierig abzuschätzen. So ist nicht nur Anzahl der verkauften Smartphone-Modelle mit Telefonie-Funktion, sondern auch die Zahl der tatsächlich aktivierten eSIM nicht bekannt. Marktexperten gehen jedoch davon aus, dass Telefonie im Smartwatch-

Bereich eine zunehmend wichtige Rolle spielen wird. So erwartet beispielsweise IDC, dass bis 2023 fast die Hälfte aller Smartwatches Mobilfunkanbindung haben wird.[210]

Des Weiteren werden zusätzliche Apps für Wearables immer wichtiger. Die Entwicklung verläuft hier analog zum Smartphone, wobei für Smartwatches eigene Betriebssysteme entwickelt wurden, die der Bildschirmgröße und anderen spezifischen Anforderungen gerecht werden (z. B. watch OS von Apple).

Erhobene Daten, Datenschutz und IT-Sicherheit

Bei der Nutzung von Wearables werden in erheblichem Umfang Daten erhoben und gespeichert, die vom Funktionsumfang des jeweiligen Produkts abhängen. Mittels dieser Daten soll dem Nutzer eine umfassende Verhaltensanalyse rund um die Uhr möglich sein, die vorwiegend auf gesundheitlichen Nutzen ausgerichtet ist.

Die erhobenen Daten umfassen neben **personenbezogenen Daten** vor allem **Aktivitätsdaten** sowie weitere Informationen mit direktem Bezug zur Produktnutzung (siehe Tabelle A-10).[211]

210 Vgl. IDC (2019): Earwear and Watches Expected to Drive Wearables Market at a CAGR of 7.9%, Says IDC, 19 June 2019, elektronisch verfügbar unter: https://www.idc.com/getdoc.jsp?containerId=prUS45271319.

211 Siehe z. B. Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., & Scheibel, L. (2017): Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e. V. (Hrsg.), elektronisch verfügbar unter: https://www.verbraucherzentrale.de/sites/default/files/2019-09/mw-untersuchung_wearables_0.pdf, S. 19 sowie Anbieterinformationen, z. B. Withings, https://www.withings.com/de/de/legal/privacy-policy.

Tabelle A-10: Wearables: Überblick über erhobene Daten

Personenbezogene Daten	▪ Bei der Registrierung für die Nutzung eines Wearables müssen i.d.R. zumindest eine E-Mail-Adresse und ein Benutzername angegeben werden („Benutzerkonto“). ▪ Weitere personenbezogene Daten wie Geburtsdatum, Vor- und Nachname, Postadresse und Telefonnummer werden i.d.R. nicht abgefragt und sind für die Nutzung der Wearables auch nicht erforderlich. Geschieht dies trotzdem, so werden mehr Informationen als notwendig erhoben.
Aktivitätsdaten	▪ Während der Nutzung werden mittels Sensoren Messwerte von körperlichen Aktivitäten (z. B. Anzahl der Schritte, zurückgelegte Entfernungen, Tempo, Menge der verbrannten Kalorien, zeitlicher Verlauf) ermittelt und in einer App ausgewertet.
Physiologische Daten oder Gesundheitsdaten	▪ Zur Auswertung und Überwachung der erhobenen Messwerte werden häufig ergänzende Daten genutzt, die sich auf die Körpermerkmale u.a. beziehen (z. B. Körpergröße, Gewicht, Muskel-, Körperfett- und Wasseranteil, Kalorienzufuhr).
Umgebungsdaten	▪ Ergänzend können auch Daten über das Umfeld erhoben werden wie z. B. Standortdaten, Geräuschpegel, Lichtstärke, Temperaturwert, CO2-Konzentration.
Technische Daten	▪ Informationen über das WLAN-Netzwerk, technische Protokolle, Datum der Produktaktivierung, Batteriestand, Hersteller-ID, Behebung von Fehlern in technischen Informationen und Website-Cookies werden gesammelt.
Sonstiges	▪ Im Zuge des Kaufs und der Nutzung kann auch die Angabe von Bankkontodaten erforderlich sein.

Quelle: WIK.

Über die App nimmt der Nutzer zahlreiche Einstellungen und Anpassungen vor, durch die es zu einer weiteren Personalisierung des Dienstes kommt (z. B. Einstellung einer Weckzeit, Teilen von Informationen, Eingabe von Schrittzielen, Eingabe zusätzlicher Gesundheitsdaten etc.).

Hersteller verwenden die Nutzerdaten in anonymisierter Form, um ihr Diensteangebot zielgruppengerecht zu verbessern, Software weiterzuentwickeln (Fehlerbehebung) oder Studien durchzuführen. Die erhobenen Daten werden zudem korreliert und aufbereitet, d.h. es werden nicht nur Rohdaten wie z. B. Schritte angezeigt, sondern auch Ergebnisse von Auswertungen. Bei Anbietern, die verschiedene vernetzte Produkte vermarkten (z. B. Apple, Xiaomi, Withings) können Daten der Nutzung zudem kombiniert werden. Mit der Tendenz zur Entwicklung von Ökosystemen, in denen zahlreiche vernetzte

Produkte über eine Plattform realisiert werden, steigt das Potential für die Erstellung umfassender Kundenprofile.

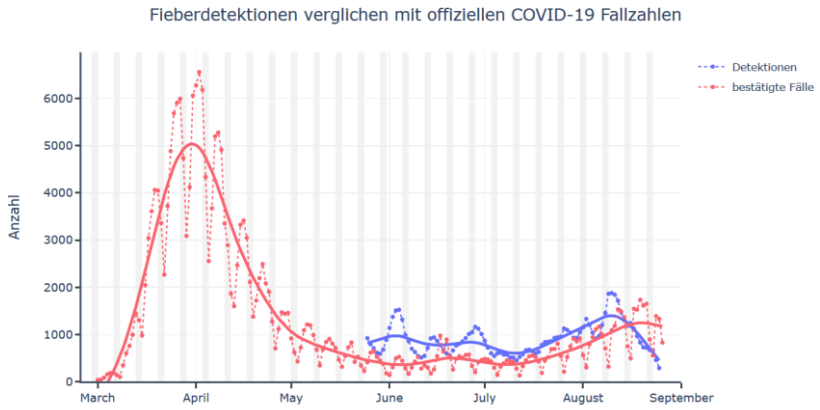
Häufig kann der Nutzer die Daten teilen – sei es mit Freunden, Ärzten oder mit Dritten zur Nutzung von weiteren Apps. Grundsätzlich muss der Nutzer dabei immer einwilligen, mit wem er seinen Daten teilen will. Wenn jedoch über Apps Dritter Zugriff auf die Daten ermöglicht wird, sind die dahinterliegenden Prozesse (wo speichert der Drittanbieter seine Daten, was wertet er aus etc.) häufig nicht erkennbar.

Auch das Robert Koch-Institut (RKI) hat eine sog. Datenspende-App entwickelt, für die Nutzer Zugriff auf die mit Wearables generierten Daten gewähren müssen (siehe Tabelle A-11).

Tabelle A-11: Corona-Datenspende-App für Wearables (2020)

- Die „Corona-Datenspende App“ ermöglicht dem RKI direkten Zugriff auf die Daten von Wearables. Sie wurde vom RKI in Zusammenarbeit mit Thryve (mHealth Pioneers GmbH) entwickelt, einem auf Digital Health spezialisierten Unternehmen.
- Mehr als 527.254 Personen in Deutschland haben die App heruntergeladen (Stand: 4.9.2020)
- Das Ziel besteht im frühzeitigen Erkennen von Symptomen einer Infektion wie dem Coronavirus und in der Erfassung seiner geographischen Ausbreitung.

- In Zeitreihen des Ruhepulses und der täglichen Schrittanzahl sollen Anomalien identifiziert und daraus Rückschlüsse auf Fiebersymptomatiken gezogen werden.[212]
- Diese Daten werden mit anderen Datenquellen wie z. B. den offiziellen Meldedaten der Gesundheitsämter korreliert, um ein besseres Bild über die Verbreitung des Coronavirus zu erhalten.
- Basierend auf den Daten werden Karten erzeugt, die die Verbreitung von möglicherweise infizierten Personen bis auf die Ebene der Postleitzahl visualisieren.
- Der Chaos Computer Club kritisiert, dass das RKI keine wirksame Einwilligung des Nutzers zur Datenverarbeitung einholen würde.[213]



Quelle: WIK basierend auf RKI.[214]

212 Das RKI weist darauf hin, dass Fieber noch nicht zwingend auf COVID-19 schließen lässt.
213 Vgl. Chaos Computer Club (2020): CCC analysiert Corona-Datenspende des RKI, 20.04.2020, elektronisch verfügbar unter: https://www.ccc.de/de/updates/2020/abofalle-datenspende.
214 Vgl. RKI (2020): Grafiken zur App „Corona-Datenspende“, elektronisch verfügbar unter: https://www.rki.de/DE/Content/Service/Presse/Pressefotos/Corona-Datenspende.html und https://corona-datenspende.de/.

Da bei der Nutzung von Wearables in erheblichem Umfang personenbezogene Daten und weitere Daten erhoben und gespeichert werden, haben Aspekte des Datenschutzes in diesem Anwendungsbereich eine sehr hohe Bedeutung. Potentiell können mit der Vielfalt an verfügbaren Daten detaillierte Kundenprofile zur Monetarisierung (z. B. in nachgelagerten Märkten wie Online-Marketing) erstellt werden.

Entsprechend der geltenden Datenschutzvorschriften[215] muss der Nutzer für alle Verwendungszwecke (interne Weiterverarbeitung, Verwendung für Verbesserung des Dienstes, Verwendung für Marketingzwecke u.a.) jeweils eine ausdrückliche Erlaubnis erteilen. Der Umgang mit den Daten muss in einer entsprechenden Datenschutzerklärung aufgeführt werden. Dabei ist die Zustimmung des Verbrauchers zur Freigabe seiner Daten (zumindest zur internen Weiterverarbeitung) jedoch meist unumgänglich für die Nutzung des vollen Funktionsumfangs.

Ein weiterer Aspekt ist im Einhalten der gebotenen Datenminimierung zu sehen. Kritisch zu sehen ist dabei die Erfassung persönlicher Daten, die für das Funktionieren der Wearables gar nicht erforderlich sind (z. B. Name, Telefon-Nr.).[216]

Führende Wearables-Hersteller scheinen bestehende Datenschutzvorschriften weitgehend einzuhalten. Einige Unternehmen veröffentlichen eine eigene Datenschutzerklärung, in der sie ausführen, wie sie die personenbezogenen Daten verarbeiten.[217] Apple bietet dem Verbraucher z. B. mittels „opt out“ auch die Möglichkeit, einzelne Datenfreigaben auszuschalten. Eine detaillierte Auseinandersetzung mit der Einhaltung der Datenschutzvorschriften würde jedoch den Rahmen der vorliegenden Studie sprengen.

Dennoch gibt es in Bezug auf führende Anbieter auch kritische Aspekte in Bezug auf die Verwendung personenbezogener Daten:

Wenn Anbieter angeben, Daten „intern“ und mit „strategischen Partnern“ zu verwenden, ist für den Nutzer der Umgang mit seinen personenbezogenen Daten nicht nachvollziehbar. Insbesondere bei großen Internetkonzernen ist selbst bei einer rein internen Verwendung ein extrem breiter Spielraum bei der Datenverarbeitung denkbar. Dabei kann auch kritisch hinterfragt werden, inwieweit die mit Wearables erhobenen Daten mit anderen im Konzern verfügbaren Daten korreliert und daraus umfassende Profile abgeleitet werden.

Ein weiterer kritisch zu sehender Aspekt, der immer mehr an Relevanz gewinnt, besteht im Datenzugriff durch Drittanbieter, die eigene Apps für Smartwatches anbieten. Das Problem ist dabei ähnlich gelagert wie bei Smartphones. Apple will der strittigen The-

---

215 Insbesondere der für den Schutz von personenbezogenen Daten am 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung (DSGVO).

216 Siehe z. B. Stiftung Warentest, Vgl. Steinlechner, P. (2019): Stiftung Warentest findet Datenschutzmängel und Schadstoff, 20.11.2019, elektronisch verfügbar unter: https://www.golem.de/news/smartwatches-stiftung-warentest-findet-datenschutzmaengel-und-schadstoff-1911-145112.html.

217 Siehe z. B. https://www.withings.com/de/de/legal/privacy-policy.

matik aktuell durch Auflagen für App-Anbieter begegnen, die ausführliche Informationen zur Datensammlung und -verwendung sowie die Einholung der Erlaubnis für die Nutzung der Identifikationsnummern umfassen. Allerdings sollen diese Maßnahmen erst im Jahr 2021 umgesetzt werden.[218]

Im Gegensatz zu den führenden Wearables-Anbietern gestaltet sich die Datenschutzproblematik bei Nischenprodukten zumeist außereuropäischer Anbieter anders. Hier ist für den Nutzer häufig nicht transparent, wie die Hersteller insgesamt mit den erhobenen Daten umgehen. So muss der Nutzer der Datenfreigabe oft nicht explizit zustimmen. Zudem wird die Freigabe nicht vollständig abgefragt, sondern nur in sehr allgemeiner Art und Weise. Darüber hinaus ist es nicht oder nur mit erheblichem Aufwand möglich, einzelne Funktionen der Datenverarbeitung zu erkennen und abzuschalten. Bei einigen Anbietern fehlen Datenschutzerklärungen völlig bzw. sind nur schwierig auffindbar. Dies gilt insbesondere für die Vielfalt an Produkten aus China, die auch deutsche Nutzer über das Internet erwerben können.

Es gibt aus dem Verbraucherschutzbereich vielfach kritische Einschätzungen, dass die explizite Einwilligung zur Nutzung und Weitergabe von personenbezogenen Daten bei zahlreichen Wearables nicht eingeholt wird und auch die Informationen über den Umgang mit den Daten oder den Möglichkeiten zu ihrer Löschung unzureichend sind.[219] In der Vergangenheit gab es mehrfach Probleme im Zusammenhang mit dem Datenschutz bei Wearables. Es kam zu Klagen und auch zu Nachbesserungen durch die Hersteller.[220] Da die Vielzahl der Produkte diesbezüglich nicht im Detail untersucht werden kann, ist hier jedoch keine abschließende Beurteilung möglich.

Für die Sicherheit der personenbezogenen Daten ist außerdem von Relevanz, inwieweit sie verschlüsselt sind und wo die Daten übertragen und gespeichert werden. Zahlreiche Schnittstellen machen dabei grundsätzlich angreifbar. Wenn ein Nutzer die mit dem Produkt erhobenen personenbezogenen Daten mit seinem Kundenkonto synchronisiert, erfolgt eine Übertragung dieser Daten an den Server des Herstellers. Hierhin werden Daten nicht nur übertragen, sondern auch (für einen langen Zeitraum) gespei-

---

218 Vgl. Telecom Handel (2020): Apple verschiebt Maßnahmen für mehr Privatsphäre. 04.09.2020, elektronisch verfügbar unter: https://www.telecom-handel.de/consumer-communications/apple/apple-verschiebt-massnahmen-privatsphaere-2572630.html?utm_source=th_nl&utm_campaign=Etappensieg_f%c3%bcr_Nokia_im_Mobilfunk-Patentstreit_mit_Daimler_07092020&utm_medium=email.

219 Siehe z. B. https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/wearables-und-fitness-apps-datenschutzrisiko/.

220 Vgl. z. B. 2017: Die Verbraucherzentrale NRW hatte sechs Anbieter (Garmin, Fitbit, Technaxx, Jawbone, Striiv und Apple) wegen Verstößen gegen Datenschutzbestimmungen abgemahnt. Garmin, Fitbit, Striiv und Technaxx haben eine Unterlassungserklärung abgegeben. Apple wurde verklagt. Elektronisch verfügbar unter: https://www.verbraucherzentrale.de/marktbeobachtung/wearables-fitnessapps-und-das-recht-auf-auskunft-ein-praxistest-41429.

chert.[221] Der Standort dieser Server und die Zugriffsmöglichkeiten für Dritte sind oft nicht transparent.

Selbst wenn Hersteller den Serverstandort und die von ihnen getroffenen Schutzvorkehrungen gegenüber missbräuchlichen Zugriff durch Dritte darlegen, bleiben Unsicherheiten. Typischerweise arbeiten Hersteller mit anderen Dienstleistern zusammen („autorisierte Dritte“) , denen Zugriff auf die Daten ermöglicht werden muss. Dies ist z. B. zum Zwecke der Lieferung, des Kundendiensts oder der Überprüfung von Bankdaten erforderlich. Häufig geht damit auch die internationale Übermittlung von personenbezogenen Daten einher. Es ist dabei nicht ausgeschlossen, dass Daten in Ländern außerhalb der EU gelangen, in denen keine oder andere Datenschutzgesetze bestehen. Zudem kann es passieren, dass Herstellern gesetzlich gezwungen werden, personenbezogene Daten Behörden oder Strafverfolgungs-/Justizbehörden offenzulegen.

Führende Hersteller von Wearables bieten in der Regel eine höhere IT-Sicherheit als die große Gruppe kleinerer Nischenanbieter, die häufig im Ausland agiert. Auch Tests von IoT-Produkten belegen IT-Sicherheits-Lücken von Wearables.[222] Diese wurden teilweise nachgebessert oder führten dazu, dass deutsche Vertriebspartner unsichere Produkte nicht mehr vermarktet haben. Allerdings haben deutsche Nutzer weiterhin Zugang zu zahlreichen Wearables mit niedrigem IT-Sicherheitsniveau über globale Portale wie z. B. Gearbest[223] oder Alibaba.

Verbraucherschutz

Verbraucher können aus einer zunehmenden Produkt- und Anbietervielfalt ihren persönlichen Präferenzen entsprechende Wearables wählen. Die typischerweise einfachen Preismodelle, die in der Regel nur Anschaffungskosten umfassen, ermöglichen einen relativ guten Produktvergleich anhand der bereitgestellten Funktionen.

Aus Verbraucherschutzsicht kritisch zu sehen sind Wearables dann, wenn sie eine direkte **Telefoniefunktion** umfassen – nicht wegen der Telefonie an sich, sondern wegen der mit deren Ausgestaltung verbundenen Kritikpunkten. Dies betrifft zum einen (bewusst eingeführte) **Nutzungseinschränkungen** führender Wearables-Anbieter und zum anderen **unerlaubte Abhörfunktionen** bei Kinder-Smartwatches.

Mit eSIM ausgestattete Premium-Smartwatches führender Anbieter sind mit Nutzungseinschränkungen verbunden, die der Verbraucher beim Erwerb ggf. nicht vollumfänglich überblicken kann. Bisher gibt es mit ausgewählten Modellen der Apple Watch und der Samsung Galaxy Watch zwar nur wenige Angebote im Markt, die jedoch aufgrund der führenden Rolle ihrer Anbieter relativ stark verbreitet sind.

---

221 Bei Withings z. B. so lange bis der Nutzer deren Löschung verlangt.

222 Vgl. z. B. Smartwatch Vidimensio, elektronisch verfügbar unter: https://www.heise.de/newsticker/meldung/Vidimensio-Smartwatches-Der-Sicherheits-Alptraum-geht-weiter-4359967.html.

223 Zum Beispiel SMA-Watch-M2, elektronisch verfügbar unter: https://www.gearbest.com/smart-watch-phone/pp_009803002470.html.

- Zunächst einmal beschränken die beiden Premium-Modelle Apple Watch und Samsung Galaxy Watch die Auswahl möglicher Anbieter auf die drei Mobilfunknetzbetreiber. Drillisch ist für die Samsung Galaxy Watch ebenfalls wählbar, für die Apple Watch hingegen nicht. Es handelt sich dabei um bewusste Eingrenzungen durch die Wearables-Hersteller.

- Die Preisgestaltung der für die Nutzung der Mobiltelefonie in einem Wearable erforderlichen Konnektivität ist dabei im Detail nur schwierig zu durchschauen. Grundsätzlich ist ein neuer Mobilfunkvertrag oder eine Erweiterung des bestehenden Vertrags erforderlich. Die Nutzung eines bestehenden Vertrags ist i.d.R. durch Buchung einer MultiSIM[224] möglich, die mit Kosten in Höhe von mindestens 5 Euro pro Monat verbunden ist. Bei einigen Verträgen ist die Multi-SIM nicht zubuchbar, so gibt es einen Tarif der Telekom (MagentaMobil XL Premium), in dem zwei MultiSIMs kostenlos inklusive sind.[225] Bei Vodafone fallen für einige Tarife zusätzlich 5 Euro, für andere 10 Euro für die zusätzlich gebuchte SIM an. Zudem werden einige Vertragsarten, z. B. Prepaid-Verträge und nicht näher spezifizierte „ältere Verträge“ ausgeschlossen.

- Für die Apple Watch gilt darüber hinaus, dass zwingend der gleiche Mobilfunkbetreiber wie für das iPhone genutzt werden muss. Abgesehen davon, dass dies die Wahlmöglichkeiten weiter begrenzt, ist auch die Nutzung der Telefoniefunktion ggf. gar nicht möglich ohne den Anbieter für das Smartphone zu wechseln. Dies gilt z. B. wenn für das Smartphone ein Diensteanbieter genutzt wird oder wenn Prepaidkarten eingesetzt werden.[226]

- Darüber hinaus sind mit der Apple Watch weder Roaming noch GSM-Verbindungen möglich.

Auch Kinder-Smartwatches mit Telefoniefunktion sind teilweise mit verbraucherschutzrechtlichen Problemen behaftet, die sich jedoch von denen der Premium-Modelle unterscheiden. Sie verfügen typischerweise über eine eingeschränkte Telefoniefunktion und weitere Funktionalitäten wie eine Ortungsfunktion, die den Eltern Kontrollmöglichkeiten zum Schutz ihrer Kinder bieten sollen. Zwar gibt es auch hier einige Smartwatches, die

---

224 Die Multi-SIM, eine zusätzlich zum bestehenden Vertrag zu beziehende SIM-Karte bzw. SIM-Profil, bietet dem Verbraucher die Möglichkeit, unter einer Rufnummer auf mehreren Geräten erreichbar zu sein. Siehe https://www.telekom.de/unterwegs/tarife-und-optionen/multisim.

225 Vgl. https://www.telekom.de/unterwegs/tarife-und-optionen/multisim und *„Für die Nutzung von eSIM Smartwatches im Mobilfunkmodus ist die Zubuchung einer MultiSIM mit einem monatlichen Grundpreis von 4,95 € zu einem bestehenden Mobilfunkvertrag in einem MagentaMobil Tarif der Telekom Deutschland GmbH erforderlich. Im Tarif MagentaMobil XL beträgt der monatliche Grundpreis der MultiSIM 29,95 € (bei reiner Smartwatch Nutzung mit dem zubuchbaren MultiSIM XL Smartwatch Vorteil 4,95 €).“*, elektronisch verfügbar unter: https://www.telekom.de/hilfe/downloads/esim-profil-apple-watch.pdf.

226 Vgl. z. B. Apple Support*: „Dein iPhone und deine Apple Watch müssen denselben Mobilfunkanbieter nutzen.“*, *„Mobiles Roaming wird außerhalb des Netzabdeckungsbereichs deines Mobilfunkanbieters nicht unterstützt.,* “*Prepaidkarten und einige ältere Verträge werden derzeit nicht unterstützt. Um sicherzustellen, dass dein Konto qualifiziert ist, kontaktiere deinen Mobilfunkanbieter*.“, elektronisch verfügbar unter: https://support.apple.com/de-de/HT207578.

fest an einen Anbieter gebunden sind, der Grund liegt hier jedoch weniger in einer bewussten Einschränkung der Anbieterwahl, sondern im Produktdesign. So spricht vieles dafür, dass diese Produkte aufgrund funktionaler Aspekte gemeinsam mit einem Netzbetreiber entwickelt wurden. Zudem handelt es sich bei ihnen um Modelle, die in vergleichsweise geringer Stückzahl vertrieben werden und keinesfalls die Marktposition der Apple Watch oder der Samsung Galaxy Watch erlangen (z. B. xplora Kindersmartwatch im Netz der Deutschen Telekom).

Das verbraucherschutzrechtliche Hauptproblem im Bereich der Kinder-Smartwatches liegt vielmehr in unerlaubten Abhörmöglichkeiten einiger Modelle. Diese werden typischerweise realisiert, indem in der zugehörigen App eine sog. „Monitorrufnummer" eingegeben wird. Das Mikrofon in der Uhr wird dabei durch eine in der App hinterlegte Telefonnummer (oder per SMS) aktiviert. Die Eingabe der Telefonnummer dient dann nicht dem Tätigen eines Anrufs, sondern dem Mithören von Stimmen und Geräuschen. Der Träger der Uhr kann dabei nicht erkennen, dass gerade mitgehört wird. Teils werden diese Funktionen als „voice monitoring", „Babyphonefunktion" oder „one-way conversation" vermarktet. Damit wird das Smartphone zu einer verbotenen Sendeanlage nach § 90 TKG, die in einen Gegenstand des täglichen Gebrauch integriert ist und ohne Zustimmung des Trägers ein unbemerktes Abhören ermöglicht.[227]

Aufgrund der zunehmenden Anzahl an Anbietern und Produktvarianten nimmt die Transparenz im Markt immer stärker ab und Verbraucher können bestehende Produkte schwieriger miteinander vergleichen. Über die Vielzahl an Online-Vertriebskanälen können Verbraucher auch unwissentlich an Produkte gelangen, die Anforderungen an Datenschutz, Verbraucherschutz und IT-Sicherheit nicht entsprechen. Mit dem Besitz von Produkten, die eine unerlaubte Abhörfunktion umfassen, machen sich Verbraucher jedoch strafbar.

Wettbewerbliche Aspekte

Im global geprägten Wearables-Bereich, der durch **relativ niedrige Markteintrittsbarrieren** geprägt ist, hat sich ein **vielfältiges Anbieterspektrum** herausgebildet. Führende IT- und Internetkonzerne spielen jedoch eine herausragende Rolle, die in wettbewerblicher Hinsicht kritisch zu sehen ist. Sie kann sich in vielfacher Hinsicht auswirken und manifestiert sich u.a. in der Tendenz zu geschlossenen Ökosystemen und in Gatekeeper-Rollen, die auch nachgelagerte Märkte betreffen.

Alle globalen ITK-Hersteller, die Wearables im Rahmen eines breiten Produktportfolios vermarkten (z. B. Huawei, Xiaomi, Samsung, Apple), streben die Entwicklung von Öko-

227 Vgl. Hierzu auch Bundesnetzagentur: Hinweise zu einzelnen Produktkategorien, elektronisch verfügbar unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/MissbrauchSendeanlagen/HinweiseProduktkategorien/hinweiseproduktkategorien-node.html.

systemen mit einer steigenden Anzahl an vernetzten Geräten und zugehörigen Diensten über eine einzige Plattform an.

Besonders stark fortgeschritten ist dabei **Apple**: Die Apple Watch bildet Teil des geschlossenen **Ökosystems**, das Apple in den vergangenen Jahren rund um seine breite Hard- und Software-Produktpalette geschaffen hat. Hier gibt es massive Lock-In-Effekte. So ist die Apple Watch ausschließlich dann nutzbar, wenn der Besitzer gleichzeitig über ein iPhone verfügt. Selbst rudimentäre Funktionen der Apple Watch können über andere Smartphones nicht genutzt werden. Apple Watch-Nutzer können Apps nur im App Store kaufen. Die auf der Apple Watch genutzten Apps müssen gleichzeitig auch auf dem iPhone installiert sein. An den Umsätzen der Apps erhält Apple einen Anteil in Höhe von 15-30 %. Der Umgang von Apple mit den App-Entwicklern in seinem App-Store – insbesondere mit denjenigen, die im Wettbewerb zu Apples eigenen Apps stehen - ist gegenwärtig auch Gegenstand von kartellrechtlichen Untersuchungen der Europäischen Kommission.[228] Der Vorwurf lautet, dass die Geschäftsbedingungen von Apple den Wettbewerb verfälschen, die Auswahl für Verbraucher reduzieren und Apple die Rolle eines „Gatekeepers“ ausnutzt. Dabei geht es auch um Auswirkungen von Apples Regelungen auf Wettbewerb in den Bereichen Musik-Streaming und E-Books/Hörbücher – beides Anwendungen die über die Apple Watch besonders stark genutzt werden.

Ein weiterer wettbewerbsrelevanter Aspekt besteht darin, dass Apple bei seiner Apple Watch **Einfluss auf die Mobilfunkbetreiber-Auswahl** nimmt, die auf die drei deutschen Netzbetreiber (sog. „unterstützte Anbieter“ von Apple[229]) beschränkt ist.[230]

Auch in Bezug auf Google gibt es im Zusammenhang mit dem Wearables-Markt wettbewerbsrechtliche Bedenken. Google ist zwar bisher kein bedeutender Anbieter in diesem Segment, hat jedoch den Aufkauf von Fitbit angekündigt. Der US-amerikanische Pionier im Wearables-Markt würde es Google ermöglichen, im Bereich der Online-Werbung noch mehr Macht zu erlangen. Die EU-Kommission hat daher eine eingehende Prüfung nach der EU Fusionskontrollverordnung eingeleitet, die bis Ende 2020 abgeschlossen sein soll (siehe Tabelle A-12).

---

228 Die Dauer des kartellrechtlichen Untersuchung ist offen, siehe zu Details Europäische Kommission (2020): Kartellrecht: Kommission leitet Untersuchung von Apples App-Store-Regeln ein, Pressemitteilung vom 16. Juni 2020, elektronisch verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1073.

229 Anbieterliste weltweit für die Apple Watch Series 6 elektronisch verfügbar unter: https://www.apple.com/de/watch/cellular/#table-series-6.

230 Bei der Samsung Galaxy Watch ist neben den Netzbetreibern auch Drillisch als Anbieter wählbar.

Tabelle A-12: Übernahme von Fitbit durch Google: EU-Kommission Prüfverfahren in Bezug auf den Markt für Onlinewerbung (Stand: September 2020)

November 2019	▪ Google gibt Pläne zur Übernahme von Fitbit (US-amerikanischer Hersteller von Wearables und smarten Waagen, Pionier, gegründet 2007) bekannt.
Juni 2020	▪ Zusammenschluss Google/Fitbit wird bei der EU-Kommission zur Genehmigung angemeldet. ▪ Im Vorprüfverfahren äußert die Kommission vorläufige wettbewerbsrechtliche Bedenken mit Blick auf die weitere Festigung der Marktposition von Google auf den Märkten für Online-Werbung, die sich hauptsächlich aus den erweiterten Möglichkeiten zur Personalisierung von Werbeanzeigen ergeben würden.
Juli 2020	▪ Google reagiert auf Bedenken der Kommission zur Auswirkungen der Übernahme mit einem Verpflichtungsangebot, die über Wearables erhobene Daten getrennt von den übrigen Datensätzen von Google aufzubewahren („Datensilo“).
August 2020	▪ Einleitung eines eingehenden Prüfverfahrens[231] der EU-Kommission in Bezug auf den angemeldeten Zusammenschluss. Die Prüfung erfolgt in enger Zusammenarbeit mit weltweiten Wettbewerbsbehörden und mit dem Europäischen Datenschutzausschuss.
Dezember 2020	▪ Entscheidung der EU-Kommission geplant (9.12.2020)

Quelle: EU-Kommission.[232]

231 Sog. Prüfverfahren (Phase II), nachdem nach Anmeldung der Übernahme bereits ein Vorprüfverfahren (Phase I) des Vorhabens stattgefunden hat.

232 Vgl. Europäische Kommission (2020): Fusionskontrolle: Kommission leitet eingehende Untersuchung der geplanten Übernahme von Fitbit durch Google ein, Pressemitteilung vom 04.08.2020, elektronisch verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1446.

Als "Diskussionsbeiträge" des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste sind zuletzt erschienen:

Nr. 394: Rolf Schwab:

Stand und Perspektiven von LTE in Deutschland, Dezember 2014

Nr. 395: Christian M. Bender, Alex Kalevi Dieke, Petra Junk, Antonia Niederprüm:

Produktive Effizienz von Postdienstleistern, November 2014

Nr. 396: Petra Junk, Sonja Thiele:

Methoden für Verbraucherbefragungen zur Ermittlung des Bedarfs nach Post-Universaldienst, Dezember 2014

Nr. 397: Stephan Schmitt, Matthias Wissner:

Analyse des Preissetzungsverhaltens der Netzbetreiber im Zähl- und Messwesen , März 2015

Nr. 398: Annette Hillebrand, Martin Zauner:

Qualitätsindikatoren im Brief- und Paketmarkt , Mai 2015

Nr. 399: Stephan Schmitt, Marcus Stronzik:

Die Rolle des generellen X-Faktors in verschiedenen Regulierungsregimen, Juli 2015

Nr. 400: Franz Büllingen, Solveig Börnsen:

Marktorganisation und Marktrealität von Machine-to-Machine-Kommunikation mit Blick auf Industrie 4.0 und die Vergabe von IPv6-Nummern, August 2015

Nr. 401: Lorenz Nett, Stefano Lucidi, Ulrich Stumpf:

Ein Benchmark neuer Ansätze für eine innovative Ausgestaltung von Frequenzgebühren und Implikationen für Deutschland, November 2015

Nr. 402: Christian M. Bender, Alex Kalevi Dieke, Petra Junk:

Zur Marktabgrenzung bei Kurier-, Paket- und Expressdiensten, November 2015

Nr. 403: J. Scott Marcus, Christin Gries, Christian Wernick, Imme Philbeck:

Entwicklungen im internationalen Mobile Roaming unter besonderer Berücksichtigung struktureller Lösungen, Januar 2016

Nr. 404: Karl-Heinz Neumann. Stephan Schmitt, Rolf Schwab unter Mitarbeit von Marcus Stronzik:

Die Bedeutung von TAL-Preisen für den Aufbau von NGA, März 2016

Nr. 405: Caroline Held, Gabriele Kulenkampff, Thomas Plückebaum:

Entgelte für den Netzzugang zu staatlich geförderter Breitband-Infrastruktur, März 2016

Nr. 406: Stephan Schmitt, Matthias Wissner:

Kapazitätsmechanismen – Internationale Erfahrungen, April 2016

Nr. 407: Annette Hillebrand, Petra Junk:

Paketshops im Wettbewerb, April 2016

Nr. 408: Tseveen Gantumur, Iris Henseler-Unger, Karl-Heinz Neumann:

Wohlfahrtsökonomische Effekte einer Pure LRIC - Regulierung von Terminierungsentgelten, Mai 2016

Nr. 409: René Arnold, Christian Hildebrandt, Martin Waldburger:

Der Markt für Over-The-Top Dienste in Deutschland, Juni 2016

Nr. 410: Christian Hildebrandt, Lorenz Nett:

Die Marktanalyse im Kontext von mehrseitigen Online-Plattformen, Juni 2016

Nr. 411: Tseveen Gantumur, Ulrich Stumpf:

NGA-Infrastrukturen, Märkte und Regulierungsregime in ausgewählten Ländern, Juni 2016

Nr. 412: Alex Dieke, Antonia Niederprüm, Sonja Thiele:

UPU-Endvergütungen und internationaler E-Commerce, September 2016
(in deutscher und englischer Sprache verfügbar)

Nr. 413: Sebastian Tenbrock, René Arnold:

Die Bedeutung von Telekommunikation in intelligent vernetzten PKW, Oktober 2016

Nr. 414: Christian Hildebrandt, René Arnold:

Big Data und OTT-Geschäftsmodelle sowie daraus resultierende Wettbewerbsprobleme und Herausforderungen bei Datenschutz und Verbraucherschutz, November 2016

Nr. 415: J. Scott Marcus, Christian Wernick:

Ansätze zur Messung der Performance im Best-Effort-Internet, November 2016

Nr. 416: Lorenz Nett, Christian Hildebrandt:

Marktabgrenzung und Marktmacht bei OTT-0 und OTT-1-Diensten, Eine Projektskizze am Beispiel von Instant-Messenger-Diensten, Januar 2017

Nr. 417: Peter Kroon:

Maßnahmen zur Verhinderung von Preis-Kosten-Scheren für NGA-basierte Dienste, Juni 2017

Nr. 419: Stefano Lucidi:

Analyse marktstruktureller Kriterien und Diskussion regulatorischer Handlungsoptionen bei engen Oligopolen, April 2017

Nr. 420: J. Scott Marcus, Christian Wernick, Tseveen Gantumur, Christin Gries:

Ökonomische Chancen und Risiken einer weitreichenden Harmonisierung und Zentralisierung der TK-Regulierung in Europa, Juni 2017

Nr. 421: Lorenz Nett:

Incentive Auctions als ein neues Instrument des Frequenzmanagements, Juli 2017

Nr. 422: Christin Gries, Christian Wernick:

Bedeutung der embedded SIM (eSIM) für Wettbewerb und Verbraucher im Mobilfunkmarkt, August 2017

Nr. 423: Fabian Queder, Nicole Angenendt, Christian Wernick:

Bedeutung und Entwicklungsperspektiven von öffentlichen WLAN-Netzen in Deutschland, Dezember 2017

Nr. 424: Stefano Lucidi, Bernd Sörries, Sonja Thiele:

Wirksamkeit sektorspezifischer Verbraucherschutzregelungen in Deutschland, Januar 2018

Nr. 425: Bernd Sörries, Lorenz Nett:

Frequenzpolitische Herausforderungen durch das Internet der Dinge - künftiger Frequenzbedarf durch M2M-Kommunikation und frequenzpolitische Handlungsempfehlungen, März 2018

Nr. 426: Saskja Schäfer, Gabriele Kulenkampff, Thomas Plückebaum unter Mitarbeit von Stephan Schmitt:

Zugang zu gebäudeinterner Infrastruktur und adäquate Bepreisung, April 2018

Nr. 427: Christian Hildebrandt, René Arnold:

Marktbeobachtung in der digitalen Wirtschaft – Ein Modell zur Analyse von Online-Plattformen, Mai 2018

Nr. 428: Christin Gries, Christian Wernick:

Treiber und Hemmnisse für kommerziell verhandelten Zugang zu alternativen FTTB/H-Netzinfrastrukturen, Juli 2018

Nr. 429: Serpil Taş, René Arnold:

Breitbandinfrastrukturen und die künftige Nutzung von audiovisuellen Inhalten in Deutschland: Herausforderungen für Kapazitätsmanagement und Netzneutralität, August 2018

Nr. 430: Sebastian Tenbrock, Sonia Strube Martins, Christian Wernick, Fabian Queder, Iris Henseler-Unger:

Co-Invest Modelle zum Aufbau von neuen FTTB/H-Netzinfrastrukturen, August 2018

Nr. 431: Johanna Bott, Christian Hildebrandt, René Arnold:

Die Nutzung von Daten durch OTT-Dienste zur Abschöpfung von Aufmerksamkeit und Zahlungsbereitschaft: Implikationen für Daten- und Verbraucherschutz, Oktober 2018

Nr. 432: Petra Junk, Antonia Niederprüm:

Warenversand im Briefnetz, Oktober 2018

Nr. 433: Christian M. Bender, Annette Hillebrand:

Auswirkungen der Digitalisierung auf die Zustelllogistik, Oktober 2018

Nr. 434: Antonia Niederprüm:

Hybridpost in Deutschland, Oktober 2018

Nr. 436: Petra Junk:

Digitalisierung und Briefsubstitution: Erfahrungen in Europa und Schlussfolgerungen für Deutschland, Oktober 2018

Nr. 437: Peter Kroon, René Arnold:

Die Bedeutung von Interoperabilität in der digitalen Welt – Neue Herausforderungen in der interpersonellen Kommunikation, Dezember 2018

Nr. 438: Stefano Lucidi, Bernd Sörries:

Auswirkung von Bündelprodukten auf den Wettbewerb, März 2019

Nr. 439: Christian M. Bender, Sonja Thiele:

Der deutsche Postmarkt als Infrastruktur für europäischen E-Commerce, April 2019

Nr. 440: Serpil Taş, René Arnold:

Auswirkungen von OTT-1-Diensten auf das Kommunikationsverhalten – Eine nachfrageseitige Betrachtung, Juni 2019

Nr. 441: Serpil Taş, Christian Hildebrandt, René Arnold:

Sprachassistenten in Deutschland, Juni 2019

Nr. 442: Fabian Queder, Marcus Stronzik, Christian Wernick:

Auswirkungen des Infrastrukturwettbewerbs durch HFC-Netze auf Investitionen in FTTP-Infrastrukturen in Europa, Juni 2019

Nr. 443: Lorenz Nett, Bernd Sörries:

Infrastruktur-Sharing und 5G: Anforderungen an Regulierung, neue wettbewerbliche Konstellationen, Juli 2019

Nr. 444: Pirmin Puhl, Martin Lundborg:

Breitbandzugang über Satellit in Deutschland – Stand der Marktentwicklung und Entwicklungsperspektiven, Juli 2019

Nr. 445: Bernd Sörries, Marcus Stronzik, Sebastian Tenbrock, Christian Wernick, Matthias Wissner:

Die ökonomische Relevanz und Entwicklungsperspektiven von Blockchain: Analysen für den Telekommunikations- und Energiemarkt, August 2019

Nr. 446: Petra Junk, Julia Wielgosch:

City-Logistik für den Paketmarkt, August 2019

Nr. 447: Marcus Stronzik, Matthias Wissner:

Entwicklung des Effizienzvergleichs in Richtung Smart Grids, September 2019

Nr. 448: Christian M. Bender, Antonia Niederprüm:

Berichts- und Anzeigepflichten der Unternehmen und mögliche Weiterentwicklungen der zugrundeliegenden Rechtsnormen im Postbereich, September 2019

Nr. 449: Ahmed Elbanna unter Mitwirkung von Fabian Eltges:

5G Status Studie: Herausforderungen, Standardisierung, Netzarchitektur und geplante Netzentwicklung, Oktober 2019

Nr. 450: Stefano Lucidi, Bernd Sörries:

Internationale Vergleichsstudie bezüglich der Anwendung und Umsetzung des Nachbildbarkeitsansatzes, Dezember 2019

Nr. 451: Matthias Franken, Matthias Wissner, Bernd Sörries:

Entwicklung der funkbasierten Digitalisierung in der Industrie, Energiewirtschaft und Landwirtschaft und spezifische Frequenzbedarfe, Dezember 2019

Nr. 452: Bernd Sörries, Lorenz Nett:

Frequenzmanagement: Lokale/regionale Anwendungsfälle bei 5G für bundesweite Mobilfunknetzbetreiber sowie für regionale und lokale Betreiber unter besonderer Betrachtung der europäischen Länder sowie von China, Südkorea und den Vereinigten Staaten von Amerika, Dezember 2019

Nr. 453: Martin Lundborg, Christian Märkel, Lisa Schrade-Grytsenko, Peter Stamm:

Künstliche Intelligenz im Telekommunikationssektor – Bedeutung, Entwicklungsperspektiven und regulatorische Implikationen, Dezember 2019

Nr. 454: Fabian Eltges, Petra Junk:

Entwicklungstrends im Markt für Zeitungen und Zeitschriften, Dezember 2019

Nr. 455: Christin Gries, Julian Knips, Christian Wernick:

Mobilfunkgestützte M2M-Kommunikation in Deutschland – zukünftige Marktentwicklung und Nummerierungsbedarf, Dezember 2019

Nr. 456: Menessa Ricarda Braun, Christian Wernick, Thomas Plückebaum, Martin Ockenfels:

Parallele Glasfaserausbauten auf Basis von Mitverlegung und Mitnutzung gemäß DigiNetzG als Möglichkeiten zur Schaffung von Infrastrukturwettbewerb, Dezember 2019

Nr. 457: Thomas Plückebaum, Martin Ockenfels:

Kosten und andere Hemmnisse der Migration von Kupfer- auf Glasfasernetze, Februar 2020

Nr. 458: Andrea Liebe, Jonathan Lennartz, René Arnold:

Strategische Ausrichtung bedeutender Anbieter von Internetplattformen, Februar 2020

Nr. 459: Sebastian Tenbrock, Julian Knips, Christian Wernick:

Status quo der Abschaltung der Kupfernetzinfrastruktur in der EU, März 2020

Nr. 460: Stefano Lucidi, Martin Ockenfels, Bernd Sörries:

Anhaltspunkte für die Replizierbarkeit von NGA-Anschlüssen im Rahmen des Art. 61 Abs. 3 EKEK, März 2020

Nr. 461: Fabian Eltges, Gabriele Kulenkampff, Thomas Plückebaum, Desislava Sabeva:

SDN/NFV und ihre Auswirkungen auf die Kosten von Mobilfunk und Festnetz im regulatorischen Kontext, März 2020

Nr. 462: Lukas Wiewiorra, Andrea Liebe, Serpil Taş

Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz, Juni 2020

Nr. 463: Bernd Sörries, Lorenz Nett, Matthias Wissner

Die Negativauktion als ein Instrument zur Versorgung weißer Flecken mit Mobilfunkdiensten, Dezember 2020

Nr. 464: Sebastian Tenbrock, Christian Wernick:

Incumbents als Nachfrager von Vorleistungen auf FTTB/H-Netzen, Dezember 2020

Nr. 465: Marcus Stronzik, Gonzalo Zuloaga:

Empirische Untersuchung der FTTB/H-Ausbauaktivität im europäischen Vergleich, Dezember 2020

Nr. 466: Antonia Niederprüm mit Unterstützung von Gonzalo Zuloaga und Willem van Lienden:

Verbundproduktion im Zustellmarkt: Briefnetze mit Paketen oder Paketnetze mit Briefen?, Dezember 2020

Nr. 467: Serpil Taş, Lukas Wiewiorra (in Zusammenarbeit mit dem Weizenbaum-Institut):

Multihoming bei Plattformdiensten – Eine nachfrageseitige Betrachtung, Dezember 2020

Nr. 468: Menessa Ricarda Braun, Julian Knips, Christian Wernick:

Die Angebotsentwicklung auf dem deutschen Mobilfunkmarkt 2017-2020, Dezember 2020

Nr. 469: Isabel Gull, Lisa Schrade-Grytsenko, Martin Lundborg:

Cloud-Lösungen und KI-as-a-Service – Aktuelle und potenzielle Anwendungsszenarien und Marktentwicklungen, Dezember 2020

Nr. 470: Bernd Sörries, Matthias Franken, Dajan Baischew, Stefano Lucidi:

Einfluss von Versorgungsauflagen auf die Mobilfunkabdeckung in der EU, Dezember 2020

Nr. 471: Julian Knips, Christin Gries, Christian Wernick:

Consumer-IoT in Deutschland – Anwendungsbereiche und möglicher Regelungsbedarf, Dezember 2020

ISSN 1865-8997