Bundeskartellamt

Sektoruntersuchung Smart-TVs

Bericht

Juli 2020

Sektoruntersuchung Smart-TVs
Bericht gemäß § 32e GWB
Az. V-22/17
Juli 2020

Kontakt
Bundeskartellamt
Beschlussabteilung Wettbewerbs- und Verbraucherschutz
Kaiser-Friedrich-Straße 16
53113 Bonn
poststelle@bundeskartellamt.bund.de
www.bundeskartellamt.de

Vorbemerkung

Die Beschlussabteilung Verbraucherschutz des Bundeskartellamts hat im Dezember 2017 eine verbraucherrechtliche Sektoruntersuchung nach § 32e Abs. 5 GWB[1] im Wirtschaftszweig Smart-TVs eingeleitet.[2] Sektoruntersuchungen richten sich nicht gegen bestimmte Unternehmen, sondern dienen der Untersuchung eines Wirtschaftszweigs im Hinblick auf mögliche verbraucherrechtliche Verstöße. Vorausgegangen war die erstmalige Übertragung von Kompetenzen im Bereich des Verbraucherschutzes auf das Bundeskartellamt mit der im Juni 2017 in Kraft getretenen 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen.[3]

Auf die Regelung des § 32e Abs. 6 GWB über den ausgeschlossenen Aufwendungsersatz im Falle einer Abmahnung nach § 12 Abs. 1 Satz 2 UWG[4] wird hingewiesen.

---

1 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bek. v. 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Art. 1 des Gesetzes v. 25.05.2020 (BGBl. I S. 1067) - GWB.

2 S. Pressemitteilung vom 13.12.2017, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/13_12_2017_SU_SmartTV.html?nn=3591568. **Soweit nicht anders angegeben, ist Stand sämtlicher Internetquellen der 24.06.2020.**

3 S. Pressemitteilung vom 12.06.2017, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/12_06_2017_Abteilung%20V.pdf?__blob=publicationFile&v=2).

4 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bek. v. 03.03.2010 (BGBl. I S. 254), zuletzt geändert durch Art. 5 des Gesetzes v. 18.04.2019 (BGBl. I S. 466) – UWG.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

A. Zusammenfassung

Smart-TVs stehen mit ihrer Anbindung an das Internet stellvertretend für viele Geräte des sog. Internet der Dinge (*Internet of Things*, IoT). Gegenstände des Alltags oder Maschinen in der Industrie werden über das Internet vernetzt und können miteinander kommunizieren. Auch mit einem Smart-Fernsehgerät können die Verbraucher[5] – anders als bei herkömmlichen Fernsehgeräten – im Internet surfen. Sie können ferner soziale Netzwerke und Apps nutzen und auch Speichermedien und Medienzuspieler verwenden. Smart-TVs verfügen zusätzlich über den sog. Roten Knopf (*Red-Button*-Funktion). Über diese rote Taste auf der Fernbedienung kann der Fernsehzuschauer die HbbTV-Funktion aktivieren, über die er auf Mediatheken zugreifen sowie Zusatzinfos oder aktuelle Nachrichten abrufen kann.

Je mehr smarte Geräte die Verbraucher einsetzen, desto umfassender ist ihr digitaler Fingerabdruck. Die Empfänger ihrer Daten können diesen geschäftlich für sich nutzen. Smart-TVs standen immer wieder im Verdacht, dass Verbraucher den Mehrwert der neuen Technik mit einer Verletzung ihrer Verbraucherrechte bezahlen müssen. So sind Verbraucher Datenschutzrisiken ausgesetzt, wenn Nutzerdaten ohne ausreichende Rechtsgrundlage verarbeitet werden. Auch auf Sicherheitsrisiken gab es zahlreiche Hinweise. Smart-TVs gehören zu den am weitesten verbreiteten Geräten des Internet der Dinge. Mutmaßliche Verbraucherschutzverstöße betreffen viele Menschen aller Bevölkerungsgruppen.

Vor diesem Hintergrund hat das Bundeskartellamt auf der Basis seiner verbraucherrechtlichen Kompetenzen im Dezember 2017 eine Sektoruntersuchung zu Smart-TVs eingeleitet. Zu dem untersuchten Wirtschaftszweig im Sinne von § 32e GWB zählen die Unternehmen, die in Deutschland Smart-TVs anbieten. Zumeist handelt es sich dabei um Unternehmen, die die Fernsehgeräte selbst herstellen und unter ihrer Marke in Verkehr bringen. Daneben gibt es auch Händler, die die Fernsehgeräte fertigen lassen und unter eigener Marke verkaufen. Smart-TVs stellen aber auch eine Plattform dar, über die verschiedene Diensteanbieter mit Verbrauchern unmittelbar oder mittelbar über den Hersteller eine Geschäftsbeziehung aufbauen können. Aufgrund dieses Netzes an Datenaustauschbeziehungen dürften sich Erkenntnisse aus der Sektoruntersuchung Smart-TV auch auf andere komplexe Geräte des Internets der Dinge übertragen lassen.

---

[5] Aus Gründen der besseren Lesbarkeit wird im gesamten Text auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für jedes Geschlecht.

Mit der Sektoruntersuchung Smart-TVs zielt das Bundeskartellamt zunächst darauf ab, Transparenz darüber herzustellen, inwieweit auch Smart-TVs Teil des Geschäfts mit den Daten sind oder werden können. Wenn Verbraucher internetfähige Geräte nutzen, ist dies mit dem Einstieg in ein regelrechtes Karussell des Datengeschäfts vergleichbar, das sie nicht mehr anhalten und aus dem sie nicht mehr aussteigen können. Ziel dieser Sektoruntersuchung ist es des Weiteren, die Verarbeitung von personenbezogenen Daten der Verbraucher aufzuklären. Damit einhergehende rechtswidrige Datenverarbeitungen sollen aufgedeckt sowie Rechtsdurchsetzungsdefizite und Schutzlücken im geltenden Recht offengelegt werden. Im Fokus der Untersuchung stehen die Datenschutzprobleme, die für den Verbraucher ab Inbetriebnahme eines Smart-TV auftreten (siehe zu den Zielen der Sektoruntersuchung im Einzelnen Kapitel B.).

Das Bundeskartellamt hat seine Erkenntnisse im Wesentlichen aus zwei schriftlichen Befragungsrunden gewonnen. Die erste Befragungsrunde richtete sich an 32 Unternehmen und diente in erster Linie der Aufklärung der Marktstrukturen und Marktverhältnisse. Besonderes Augenmerk lag auf den Datenflüssen zwischen dem Verbraucher und den Herstellern von Smart-TVs sowie deren Lieferanten von Software für die smarte TV-Plattform. In die Auswertung der Struktur-Befragung sind Antworten von 21 Herstellern eingeflossen.[6] Darunter sind alle in der Öffentlichkeit bekannten Smart-TV-Hersteller. Die Unternehmen vereinen nahezu 100 % des Smart-TV-Absatzes (nach Stückzahlen) in Deutschland auf sich. In der zweiten Befragungsrunde hat das Bundeskartellamt diesen 21 Unternehmen detaillierte Fragen insbesondere zu Datenschutz und Sicherheit bei der Verwendung von Software, Datenflüssen und Vertragsbeziehungen gestellt. Parallel dazu führte das Bundeskartellamt während der gesamten Untersuchung mehrere Gespräche mit Marktteilnehmern. Zusätzlich zu solchen für Sektoruntersuchungen üblichen Ermittlungsschritten hat das Bundeskartellamt weitere speziell für die Untersuchung konzipierte Ermittlungsmethoden angewendet (siehe zum Gang der Ermittlungen im Einzelnen Kapitel C.).

Smart-TVs sind in den letzten Jahren zur Standardausstattung in den deutschen TV-Haushalten avanciert. Vor allem, wenn die Verbraucher länger vor dem Bildschirm verweilen, ist nach wie vor

6 Die Antworten von insgesamt 10 Unternehmen ergaben, dass sie in Deutschland entweder keine Smart-TVs (mehr) vertreiben oder einen Vertrieb bisher lediglich geplant hatten.

der Fernseher die unangefochtene Nummer eins unter den Geräten für die Wiedergabe von Bewegtbild-Inhalten.[7] Die Märkte für Smart-TVs und andere smarte Geräte dürften sich noch dynamischer entwickeln, sobald die technische Entwicklung erweiterte Netzkapazitäten mit sich bringen wird. Von diesem Prozess werden nicht nur die Hersteller von Smart-TVs als Betreiber der zentralen Plattform-Infrastruktur des Smart-TVs, d. h. des Betriebssystems, TV-Portals oder App-Stores profitieren. Am Funktionieren des Smart-TVs sind weitere Unternehmen beteiligt, auch wenn sie vom untersuchten Wirtschaftszweig nicht umfasst sind. Dazu zählen HbbTV-Anbieter, selbstständige Portalbetreiber, App-Store-Betreiber, App-Anbieter und Betreiber von Empfehlungsdiensten. Eine zentrale Rolle nehmen dabei Apps der bekannten Streaming-Anbieter ein, die auf den Smart-TVs häufig bereits vorinstalliert sind.

Die Plattformteilnehmer haben vielfältige technische Möglichkeiten, über Smart-TVs das Verhalten der Verbraucher nachzuvollziehen. So können etwa das generelle Fernsehverhalten einer Person, ihre App-Nutzung, ihr Surf- und Klickverhalten oder auch biometrische Daten wie Stimme oder Cursorbewegungen sowie die im Einzelnen über den Fernseher abgespielten Inhalte erfasst und ausgewertet werden. Solche Daten lassen sich anhand eindeutiger Identifikatoren mit anderweitig bereits vorhandenen oder öffentlich verfügbaren personenbezogenen Daten zusammenführen. Beim Login in ein Nutzerkonto ist die Identifizierung einer Person besonders einfach und ermöglicht die Erweiterung eines Profils um Daten, die der Nutzer selbst über sich preisgibt sowie um Daten aus Drittquellen, die z. B. ebenfalls den Nutzernamen enthalten. Wirtschaftlich gesehen besteht ein starker Anreiz, die gesammelten Nutzerdaten (auch) für Werbezwecke zu verwenden, da so beim Werbungsempfänger eine erhöhte Aufmerksamkeit und entsprechend höhere Umsätze erreicht werden können. Je mehr werberelevante Daten über eine Person vorliegen (z. B. Interessen, Alter, Einkommen), desto lukrativer wird sie für die Werbewirtschaft, da sie sich Werbezielgruppen besser zuordnen lässt und auch für eine größere Anzahl maßgeschneiderter Werbekampagnen in Betracht kommt. Der Werbungsempfänger erhält so „passgenauere“ und für ihn mutmaßlich interessantere Werbung. Allerdings werden immer genauere Nutzerprofile gebildet, die den Einzelnen und sein Umfeld zunehmend berechenbar machen. Da ein großer

---

7 Vgl. *gfu Studie 2019 Einschätzungen der Konsumenten* (gfu.de, 10.07.2019), abrufbar unter https://gfu.de/gfu-studie-2019-einschaetzungen-der-konsumenten/ sowie gfu Consumer & Home Electronics GmbH, *gfu Studie 2019: Erste Ergebnisse der repräsentativen Konsumenten-Befragung*, Pressemeldung vom 24.06.2019, abrufbar unter https://www.gfu.de/presseraum/uebersicht/gfu-studie-2019-erste-ergebnisse-der-repraesentativen-konsumenten-befragung/ und SevenOne Media GmbH, *Media Activity Guide 2019*, Kapitel 2, abrufbar unter https://www.sevenonemedia.de/documents/924471/1111769/Media+Activity+Guide+2019/040352cd-a958-6876-6541-93630deee1c7.

Teil der Verbraucher in Deutschland Vorbehalte gegen personalisierte Werbung hat, ist es besonders wichtig, dass über die Verarbeitung personenbezogener Daten transparent informiert wird. Die Verarbeitung personenbezogener Daten muss daher vermieden oder wenigstens minimiert werden können (siehe hierzu auch Kapitel D.).

Smart-TV-Hersteller stehen nicht anders als App-Anbieter, Online-Dienste und viele andere Akteure in der Pflicht, Verbraucherrechte beim Umgang mit den Nutzerdaten zu achten. Berührungspunkte gibt es hier insbesondere mit den einschlägigen Vorschriften der DSGVO[8], des UWG und des BGB[9]. Indessen sehen sich Verbraucher einer Reihe an Erschwernissen gegenüber, wenn sie einen Smart-TV erwerben und nutzen und gleichzeitig auf Datenschutz und Datensicherheit Wert legen. Eine Reihe von verbraucherrechtlichen Problemfeldern schränkt ihre Handlungsmöglichkeiten ein (siehe zu den Problemfeldern im Einzelnen Kapitel E.):

Transparente Verbraucherinformation

Das erste Problemfeld betrifft die klare und transparente Information der Verbraucher. Diverse Studien und Marktbeobachtungen haben ergeben, dass Verbraucher einerseits großen Wert darauf legen, dass ihre personenbezogenen Daten privat bleiben. Andererseits handeln sie in Situationen des täglichen Lebens überwiegend nicht datenschutzbewusst. Dieses als *Privacy Paradox* bezeichnete Phänomen lässt sich indessen maßgeblich dadurch erklären, dass der Verbraucher in datenschutzrelevanten Entscheidungssituationen wesentliche Informationen nicht erhält, sie nicht versteht oder sich deshalb nicht informiert, weil der Aufwand hierfür hoch und der erwartete Erkenntnisgewinn gering ist. Nicht selten spielt auch eine Rolle, dass es zu einer Akzeptanz von Datenschutzbestimmungen keine realistische Alternative gibt, will man ein bestimmtes Gerät oder eine Dienstleistung nutzen. Schließlich neigen Verbraucher dazu, kurzfristigen Nutzen höher zu bewerten als ggf. langfristig eintretende Risiken.

Die Datenschutzbestimmungen der in Deutschland im Bereich der Smart-TVs wesentlichen Akteure wiesen fast durch die Bank schwerwiegende Transparenzmängel auf. Die Datenschutzbestimmungen sind vor allem deshalb für die Verbraucher nicht nachvollziehbar, weil sie für eine Vielzahl von Diensten und Nutzungsprozessen gelten sollen. Die „one fits all"-Architektur der

---

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. EU Nr. L 119 v. 04.05.2016, S. 1 (kurz DSGVO).

9 Bürgerliches Gesetzbuch in der Fassung der Bek. v. 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 1 des Gesetzes v. 19.03.2020 (BGBl. I S. 541) – BGB.

meisten Datenschutzbestimmungen führt insbesondere dazu, dass die Verbraucher nicht zuverlässig erfahren,

- welche konkreten personenbezogenen Daten überhaupt erhoben werden;
- welche Datenverarbeitungen ausgelöst werden, wenn bestimmte Funktionen genutzt werden;
- zu welchen Zwecken welche personenbezogenen Daten verarbeitet werden;
- welche Rechtfertigung für die Verarbeitung welcher konkreten personenbezogenen Daten besteht;
- wie lange welche personenbezogenen Daten gespeichert werden;
- wer außer dem Verantwortlichen noch in den Besitz der erhobenen Daten gelangt.

Für die Verbraucher ist es somit kaum möglich, eine Strategie zu verfolgen, bei der sie möglichst wenige oder nur weniger private personenbezogene Daten preisgeben oder zumindest deren Verbreitung oder Speicherdauer minimieren. Es ist erkennbar, dass Datenschutzbestimmungen primär mit dem Ziel *förmlicher* DSGVO-Konformität konzipiert wurden. So finden sich in den Datenschutzbestimmungen zumeist Ausführungen zu den einschlägigen DSGVO-Normen. Diese enthalten jedoch in vielen Fällen keine Angaben, mit denen der Verbraucher in der Praxis etwas anfangen kann. Insbesondere Pauschalierungen führen dazu, dass Datenschutzbestimmungen erheblich an Informationsgehalt einbüßen. Dies führt sehr häufig zu Verstößen gegen die DSGVO. Verbraucher, die Verbraucherinformationen wie Datenschutzbestimmungen nicht durchlesen, verhalten sich somit durchaus rational. Die Lektüre ist zeitlich aufwendig, bringt aber zumeist keinen echten Erkenntnisgewinn mit sich. Allenfalls bei gesonderten Einwilligungsersuchen wird der Verbraucher vor eine echte Wahl gestellt (siehe hierzu E. II.).

Zeitpunkt der Verbraucherinformation

Als weiteres verbraucherrechtliches Problemfeld haben die Ermittlungen den Zeitpunkt der Verbraucherinformation identifiziert. Unter Transparenz- und Verbraucherschutzgesichtspunkten ist es wünschenswert, dass alle für die Verbraucher wichtigen Informationen bereits vor dem Kauf verfügbar sind. Andernfalls können sich die Verbraucher kein umfassendes Bild von dem gewünschten Produkt machen.

Das insoweit einschlägige Lauterkeitsrecht stellt jedoch nicht notwendigerweise auf die Vollständigkeit von Verbraucherinformationen ab. Unlauter handelt vielmehr, wer unter Berücksichtigung aller Umstände dem Verbraucher eine wesentliche Information vorenthält, die dieser benötigt, um eine informierte geschäftliche Entscheidung zu treffen. Zudem muss das Vorenthalten dieser Information geeignet sein, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Werden bestimmte Informationen trotz objektiver Wichtig-

keit vom angemessen gut unterrichteten und angemessen aufmerksamen und kritischen Verbraucher typischerweise nicht mit spürbarer Gewichtung in seinen Entscheidungsprozess einbezogen, so kann das Lauterkeitsrecht bei solchen Marktgegebenheiten wenig Abhilfe schaffen. Es besteht etwa keine lauterkeitsrechtliche Pflicht, sämtliche Datenschutzbestimmungen oder Allgemeine Geschäftsbedingungen schon vor dem Kauf zur Verfügung zu stellen, die erst bei der späteren Nutzung eines Smart-TVs relevant werden. Anders fällt hingegen die rechtliche Beurteilung aus, soweit der Verbraucher den gekauften Smart-TV nicht „out of the box" für alle wesentlichen Verwendungen nutzen kann, ohne dass er – beim Ersteinrichtungsprozess oder ggf. auch zu einem späteren Zeitpunkt – in wesentlichem Umfang personenbezogene Daten preisgeben muss (insbesondere durch das Erfordernis eines Nutzerkontos). Wird hierüber nicht bereits vor dem Kauf informiert, so liegt ein Verstoß gegen Lauterkeitsrecht vor (siehe hierzu E. III.).

Praxis der Datenverarbeitung

Hinsichtlich der Rechtmäßigkeit der Datenverarbeitungsvorgänge stellten sich im Rahmen der Untersuchung diverse Fragen.

Hersteller von Smart-TVs und Diensteanbieter können eine Verarbeitung personenbezogener Nutzerdaten im Wesentlichen auf dreierlei Weise rechtfertigen: Wenn die Daten für den mit dem Nutzer abgeschlossenen Vertrag erforderlich sind, wenn berechtigte Interessen vorliegen, die mindestens ebenso schwer wiegen wie diejenigen der betroffenen Person oder wenn diese eingewilligt hat. Von den einschlägigen Rechtsgrundlagen machen die befragten Unternehmen in unterschiedlichem Ausmaß Gebrauch. Soweit für Datenverarbeitungen berechtigte Interessen angeführt werden, bestehen regelmäßig erhebliche Zweifel an der Rechtmäßigkeit. Eine Auseinandersetzung mit den Interessen der von der Datenverarbeitung betroffenen Personen findet nicht erkennbar statt. Darüber hinaus führen die Unternehmen als ein berechtigtes Interesse zumeist die Verbesserung des eigenen Produkts bzw. der eigenen Dienstleistung ins Feld. Dabei wird jedoch nicht erkennbar, worin diese Verbesserung besteht, weshalb diese nicht im Wesentlichen ebenso gut mit anonymisierten Daten erreicht werden kann oder welche der verarbeiteten Daten für diese Verbesserung überhaupt herangezogen werden. Eine Verarbeitung personenbezogener Daten zu Werbezwecken wird in der Regel nicht als berechtigtes Interesse deklariert, sondern von der Einwilligung des Nutzers abhängig gemacht. Dies ist insofern sinnvoll, als eine Abwägung der berührten Interessen jedenfalls bei bezahlten Produkten im Regelfall zuungunsten des datenverarbeitenden Unternehmens ausgehen würde. Das Einholen einer Einwilligung stellt in solchen Fällen zudem unter Transparenzgesichtspunkten die deutlich vorzugswürdige Variante dar. Eine wirksame Einwilligung scheitert dabei zumeist nicht am Vorliegen einer Drucksituation. Hingegen fehlt es den Einwilligungsersuchen praktisch durchgängig an einer Darstellung aller wesentlichen Angaben, die der Nutzer für eine informierte Einwilligung benötigen würde.

Nutzermenüs sind häufig nicht neutral ausgestaltet, sondern lenken den Nutzer in Richtung bestimmter Auswahlentscheidungen, die mit einer umfangreicheren Verarbeitung personenbezogener Daten einhergehen. Die Zulässigkeit eines solchen Vorgehens („Digital Nudging“) lässt sich zwar grundsätzlich durchaus nach geltendem Recht, insbesondere dem Datenschutz- und Lauterkeitsrecht, beurteilen. Einschlägige Behörden- oder Gerichtsentscheidungen, die als Orientierungspunkte dienen könnten, sind jedoch bislang Mangelware.

In Einzelfällen, in denen eine gemeinsame Verantwortlichkeit i. S. d. Datenschutzrechts vorliegt, verstoßen TV-Portal-Betreiber und App-Anbieter gegen die Vorgaben der DSGVO, wonach sie Regelungen zur gemeinsamen Verantwortlichkeit treffen müssen. Hinzu kommen ggf. Verstöße gegen Informations- und Transparenzpflichten der DSGVO, da für etwaige Versäumnisse beide Verantwortliche gleichermaßen einstehen müssen. Nach Auffassung des Bundeskartellamts besteht allerdings im Regelfall keine datenschutzrechtliche Verantwortung des TV-Portal-Betreibers. Eine weiter gehende Auslegung des Verantwortlichenbegriffs durch den EuGH in der Zukunft erscheint jedoch nicht ausgeschlossen. Die Tatsache, dass womöglich ein Akteur – ohne selbst Verantwortlicher zu sein – einen DSGVO-widrigen Zugriff auf personenbezogene Nutzerdaten ermöglicht, kann zwar nach den Grundsätzen der Störerhaftung betrachtet werden. Vermutlich wird es jedoch noch eine geraume Zeit dauern, bis sich zu dieser Problematik eine gefestigte Rechtsprechung herausgebildet haben wird. Eine behördliche Durchsetzung in diesem Bereich dürfte jedenfalls mangels einschlägiger Eingriffsbefugnisse grundsätzlich nicht möglich sein (siehe hierzu E. V.).

Binnenorganisation in Datenschutzfragen

Die Ermittlungen erstreckten sich auch auf die Binnenorganisation der Smart-TV-Anbieter in Datenschutzfragen. Einige der untersuchten Unternehmen speichern selbst keine personenbezogenen Daten und unterliegen insoweit nicht den Pflichten der DSGVO und des BDSG[10]. Die übrigen Unternehmen kommen ihren in der DSGVO ausdrücklich niedergelegten internen Datenschutz-Organisationspflichten im Wesentlichen nach. Insoweit gibt es nur vereinzelt kleinere Kritikpunkte (siehe hierzu E. VI.).

Nachhaltigkeit der Produktpflege

Nachdem das Bayerische Landesamt für Datenschutzaufsicht noch im Jahr 2015 erhebliche Datensicherheitsmängel bei Smart-TVs ermittelt hatte, ist aktuell ein Bemühen der Hersteller um ein

10 Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), geändert durch Art. 12 des Gesetzes . 20.11.2019 (BGBl. I S. 1626) – BDSG.

hohes Datensicherheitsniveau erkennbar. Der Aufwand für Sicherungsmaßnahmen ist dabei durchaus unterschiedlich.

Bei etlichen Herstellern ist keinesfalls gesichert, dass der Sicherheitsstandard der Geräte bei Inverkehrbringen auch in den Folgejahren durch Software-Aktualisierungen aufrechterhalten wird. Bislang veröffentlicht kein Hersteller verbindliche Angaben dazu, wie lange seine Produkte mit Sicherheits-Patches versehen werden. Dieses Problem betrifft andere IoT-Geräte und insbesondere Smartphones in gleicher Weise.

Für den Kunden ist die Information, ob und ggf. bis zu mindestens welchem Zeitpunkt ein Gerät Sicherheits-Updates erhält, unerlässlich, um einschätzen zu können, wie lange eine uneingeschränkte Verwendung des Geräts gefahrlos möglich ist. Wenn der Kunde dies nicht weiß, fällt es ihm auch schwerer, die Angemessenheit des Kaufpreises zu beurteilen.

Nach aktueller Rechtslage sind jedoch keine belastbaren rechtlichen Ansprüche gegen Smart-TV-Hersteller oder Verkäufer auf Bereitstellung von Software-Sicherheitsupdates ersichtlich.

Das Gewährleistungsrecht ist darauf ausgerichtet, die Mangelfreiheit nur für den Zeitpunkt des Gefahrübergangs der Kaufsache sicherzustellen. Ob die Umsetzung der Warenkaufrichtlinie für den Verbraucher in diesem Punkt spürbare Verbesserungen erbringen wird, bleibt abzuwarten. Auch die Regelungen zu verpflichtenden Verbraucherinformationen helfen den Käufern von Smart-TVs nicht weiter; jedenfalls bei den aktuellen Gegebenheiten dürfte dem Verkäufer nicht zuzumuten sein, sich jeweils aktuelle Informationen über vorgesehene oder nicht vorgesehene Software-Aktualisierungen für die angebotenen Produktpalette zu besorgen und diese dem Kaufinteressenten zu präsentieren.

Die DSGVO fordert zwar grundsätzlich die Datensicherheit bei Datenverarbeitungsvorgängen ein. Eine Pflicht zu Software-Sicherheitsupdates ist aber nicht explizit vorgesehen und könnte sich erst über eine Fortentwicklung der Rechtsprechung herausbilden. Ansätze hierzu sind bislang nicht erkennbar. Hinzu kommt, dass nicht immer gewährleistet ist, dass Software-Sicherheitslücken überhaupt vom (verantwortlichen) datenverarbeitenden Unternehmen behoben werden können.

Aus den Vorschriften des Lauterkeitsrechts in ihrer derzeitigen Fassung lässt sich ebenfalls kein Anspruch des Verbrauchers auf die Bereitstellung von Updates ableiten. Ein solcher Update-Anspruch gegen den Hersteller ist aufgrund der schwierigen Dreieckskonstellation Hersteller – Verbraucher – Dritter als Täter der Rechtsgutverletzung kaum zu begründen. Zum einen würde die eigentliche Rechtsgutverletzung von einer Person begangen, mit der der Hersteller als An-

spruchsgegner in keinerlei Geschäftsbeziehung steht. Zum anderen wird die Rechtsgutverletzung typischerweise durch nicht näher bestimmbare Dritte begangen. Sie ist daher i. d. R. nicht einmal in Umrissen absehbar und eine konkret bevorstehende Rechtsgutverletzung somit nicht nachweisbar.

Nach Produkthaftungsrecht besteht eine Haftung des Herstellers nur bei Schäden an Körper, Gesundheit oder Sachen, mit Ausnahme der vertriebenen Sache selbst. Im allgemeinen Deliktsrecht besteht wie im Lauterkeitsrecht die Schwierigkeit, dass eine bevorstehende Gefährdung konkret nachgewiesen werden müsste. Einem subjektivrechtlichen Anspruch auf Sicherheits-Updates steht zudem entgegen, dass der Kläger keine Gefährdung mehr behaupten kann, sobald er selbst die Gefährdung bereits erkannt hat.

Eine auf Lauterkeitsrecht fußende, gegenüber dem Verbraucher bestehende Informationspflicht des Herstellers über Updates erscheint hingegen nicht ausgeschlossen. Praktische Schwierigkeiten ergeben sich aber aus dem Erfordernis, dass der Verbraucher durch die unterbliebene Information zu einer geschäftlichen Entscheidung veranlasst worden sein müsste, die er andernfalls nicht getroffen hätte. Auch müsste sich erst noch eine Rechtsprechung dazu herausbilden, für welchen Zeitraum Update-Informationen bereitgestellt werden müssten und ob und ggf. unter welchen Umständen eine entsprechende Verbrauchererwartung hinsichtlich der gesamten Produktpalette oder nur einzelner Geräte(kategorien) besteht. Da das Lauterkeitsrecht dem einzelnen Verbraucher keine rechtlichen Durchsetzungsmöglichkeiten an die Hand gibt, müssten insoweit Verbraucherverbände tätig werden.

Soweit im Rahmen der Sektoruntersuchung Herstellergarantien vorgelegt wurden, greifen diese auch bei Softwaremängeln ein, wenn sich nicht aus der Garantieerklärung eindeutig etwas anderes ergibt. Allerdings decken die Garantien nur solche Mängel ab, die bereits im Zeitpunkt des Gefahrübergangs auf den Verbraucher bestanden. Kein Unternehmen gewährte eine Haltbarkeitsgarantie. Mitunter waren die Garantien insofern nicht fehlerfrei, als sie nicht auf die vollständige Geltung des Gewährleistungsrechts hinwiesen oder dieses sogar einzuschränken vorgaben.

Die Nichtlöschbarkeit von Apps stellt grundsätzlich ein weniger großes Problem dar als bei Smartphones. Auch bei Smart-TVs können hierdurch jedoch Sicherheitsprobleme entstehen. Apps sind bei manchen Herstellern löschbar, bei anderen hingegen nicht. Das zeigt, dass es durchaus technisch machbar wäre, dem Verbraucher die Entscheidung zu überlassen, welche Apps er auf seinem Fernsehgerät haben möchte. Ein Rechtsverstoß ist mit der Vorinstallation nicht löschbarer Apps – jedenfalls bei dem festgestellten Ausmaß an Vorinstallationen – jedoch nicht verbunden (s. hierzu E. VII.).

Sonstige Problemfelder

Die Sektoruntersuchung hat schließlich einige Rechtsverstöße zutage gefördert, die zwar nicht die gesamte Branche betreffen, aber gleichwohl bemerkenswert sind. Neben fehlerhaften Garantieerklärungen und Haftungsfreizeichnungen ist hier das unaufgeforderte Einspielen von Werbeeinblendungen hervorzuheben. Aufgrund generell vermehrten Einsatzes personalisierter Werbung steht zu befürchten, dass solche unaufgeforderte Werbeeinblendungen im TV-Portal zunehmen werden. Werbung zu schalten, ohne dass der Verbraucher hierauf bereits beim Kauf des Fernsehers hingewiesen worden wäre bzw. diese Funktion deaktivieren kann, ist nach Auffassung des Bundeskartellamts unzulässig (siehe hierzu E. VIII.).

Die Sektoruntersuchung hat auch Erkenntnisse zur Durchsetzung der Verbraucherrechte und zu entsprechenden Verbesserungsmöglichkeiten erbracht (siehe hierzu im Einzelnen Kapitel F.):

Den Verbrauchern fällt es im digitalen Alltag schwer, ihre Rechte durchsetzen. Sie können Rechtsverstöße bei komplexen Sachverhalten, insbesondere wenn Geschäftsgeheimnisse der Unternehmen betroffen sind, vor den Zivilgerichten kaum selbst nachweisen. Auch die bewährte Rechtsdurchsetzung durch die Verbände stößt hier an Grenzen. Ohne behördliche Mittel erscheinen der Personenbezug und der Weg der Daten in vielen Fallgestaltungen kaum gerichtsfest nachweisbar zu sein. Die derzeitige behördliche Rechtsdurchsetzung ist aber entweder nicht effektiv genug (Datenschutzrecht) oder fehlt völlig (Lauterkeits- und bürgerliches Recht). Bemühungen des Bundeskartellamts, zumindest ergänzende Eingriffskompetenzen im Rahmen der 10. GWB-Novelle zu erhalten,[11] sind erfolglos geblieben.

Datenschutzqualität muss künftig als Wettbewerbsparameter wahrgenommen werden, wenn Datenschutz mehr Breitenwirkung entfalten soll. Die Nachfrage nach datenschutzfreundlichen Smart-TVs wird erst entstehen können, wenn den Verbrauchern die notwendigen Informationen über die stattfindenden Datenverabeitungen vor der Kaufentscheidung zugänglich sind. Sie müssen in die Fairness des Anbieters nach Vertragsabschluss vertrauen können. Hersteller werden erst dann in Datenschutz investieren und dies verständlich kommunizieren oder sogar bewerben, wenn die Verbraucher Datensparsamkeit, Datenschutzkonformität und Datensicherheit als Qualitätsmerkmal ihrer Produkte wünschen. Datenschutz könnte dann zum Wettbewerbsvorteil von Anbietern werden. Entscheider, Unternehmen und Wissenschaft stehen in der Verantwortung, die notwendigen Voraussetzungen für informierte Entscheidungen der Verbraucher zu schaffen

---

11 Vgl. *Bundeskartellamt*, Stellungnahme des Bundeskartellamts zum Referentenentwurf zur 10. GWB-Novelle vom 25.02.2020, S. 25, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Stellungnahmen/Referentenentwurf_10_GWB_Novelle.html.

bzw. den Handlungsrahmen zu verbessern. Lösungsansätze sollten sich dabei in erster Linie auf innovative Wege der Informationsvermittlung konzentrieren. Dem Verbraucher kann so zu mehr Datensouveränität verholfen werden, ohne die dynamische Entwicklung der Digitalwirtschaft unnötig zu beeinträchtigen.

Sobald auf europäischer bzw. nationaler Ebene die nach der DSGVO vorgesehenen strukturellen Voraussetzungen gegeben sind, können die Unternehmen bei ihren Produktdarstellungen Zertifikate und/oder standardisierte Bildsymbole verwenden. Solche und ggf. weitere visuelle Informationsinstrumente sollten Unternehmen zunächst auf der Basis von Selbstverpflichtungen in der Werbung, im Verkaufsprozess und bei der Nutzerführung verwenden. Nur falls sich eine Verwendung der genannten Instrumente im Markt nicht etablieren sollte, wäre ein Eingreifen des Gesetzgebers zu erwägen.

Das Bundeskartellamt empfiehlt deshalb, in Anknüpfung an den vorliegenden Bericht,

- das Bewusstsein der Verbraucher für die extensiven Datenverarbeitungsmöglichkeiten von Smart-TVs und IoT-Geräten insgesamt weiter zu schärfen,
- Haftungsfragen beim Zusammenspiel der verschiedenen Akteure im IoT-Bereich gesetzgeberisch zu klären und einen Anspruch des Verbrauchers auf Software-Updates durch den Hersteller gesetzlich zu verankern,
- auf die Ergänzung bestehender Transparenzanforderungen durch aussagekräftige, einfach zu erfassende und bereits vor dem Kauf verfügbare Datenschutzinformationen hinzuwirken, die dem Verbraucher ermöglichen, den Weg preisgegebener Daten konkret nachzuvollziehen,
- dem Verbraucher die Möglichkeit an die Hand zu geben, Verarbeitungen seiner personenbezogenen Daten tagesaktuell effektiv nachzuvollziehen, anzupassen und ggf. zu beenden,
- durch Kennzeichnung und neue Technologien Datenschutzqualität als Wettbewerbsparameter zu etablieren und
- die Verwendung visueller Informationsinstrumente durch die Smart-TV-Anbieter voranzutreiben und dafür die gesetzlich bereitgestellten Akkreditierungs- und Zertifizierungsverfahren abzuschließen.

Mit dem vorliegenden Bericht leistet das Bundeskartellamt einen Beitrag zu mehr Transparenz bei Datenverarbeitungen durch Smart-TVs. Ein bewussterer Umgang der Verbraucher mit Smart-TVs bzw. IoT-Geräten im Allgemeinen sollte auf alle Fälle gefördert werden. Um das Bewusstsein und den Informationsstand der Verbraucher zu verbessern, aber auch den Marktmechanismus zu stärken und so dem Datenschutz zu mehr Breitenwirkung zu verhelfen, sollten die in diesem Bericht dargestellten Anregungen aufgegriffen werden.

TIPPS FÜR VERBRAUCHER BEI KAUF UND NUTZUNG VON SMART-TVs:

- ► Beachten Sie, dass beim Kauf älterer TV-Modelle ggf. nicht mehr oder nur noch für eine geringe Zeitspanne mit einer aktiven Produktunterstützung durch den Hersteller zu rechnen ist.

- ► Prüfen Sie, soweit möglich, vor dem Kauf, ob der Hersteller eine Garantie anbietet und inwieweit diese auch Softwarefehler mit einschließt.

- ► Bringen Sie, soweit möglich, vor dem Kauf in Erfahrung, ob der Hersteller in der Vergangenheit seine TV-Modelle zuverlässig und längerfristig mit Software-Updates versorgt hat.

- ► Smart-TVs sind im Auslieferungszustand häufig nicht datensparsam voreingestellt; beachten Sie dies bei der Ersteinrichtung und weiteren Nutzung.

- ► Prüfen Sie bei der Ersteinrichtung des Smart-TVs und auch sonst sorgfältig, ob die auf dem Bildschirm hervorgehoben angezeigten Auswahloptionen tatsächlich Ihren Bedürfnissen und Interessen entsprechen.

- ► Sie können Einwilligungen in die Verarbeitung Ihrer personenbezogenen Daten meist verweigern, etwa bei dem Empfehlungsdienst *Samba TV*. Machen Sie von dieser Möglichkeit Gebrauch, lassen sich solche Einwilligungen im tatsächlichen Bedarfsfall später immer noch nachholen.

- ► Führen Sie regelmäßig Sicherheitsupdates durch.

- ► Deinstallieren Sie nicht benötigte Apps, soweit dies möglich ist; jede App stellt ein potentielles Sicherheitsrisiko dar, insbesondere, wenn sie nicht (mehr) aktualisiert wird.

- ► Sie können nicht davon ausgehen, dass die Software Ihres Smart-TVs auch nach Jahren noch sicher ist. Falls sich Ihre Gerätesoftware nicht mehr aktualisieren lässt, erwägen Sie die Trennung Ihres Smart-TVs vom Internet und den Kauf eines externen Zuspielgeräts zur Nutzung von Smartfunktionen.

B. Einleitung

Fernsehgeräte erfreuen sich seit den 1960er-Jahren großer Wertschätzung bei den Verbrauchern. War zu Beginn der 1950er-Jahre noch der Rundfunk das alleinige Medium zur Information und Unterhaltung der Bevölkerung, hatte sich das Fernsehen bereits eine Dekade später zum weltweit verbreiteten Massenmedium entwickelt.[12] In den letzten 10 Jahren hat die Digitalisierung diverse internetfähige Geräte als neue Konkurrenten des Fernsehers hervorgebracht. Smartphone, Tablet & Co. haben die Gewohnheiten der Menschen bei der Nutzung von Medien verändert. Informationen und Unterhaltung sind ortsungebunden und ohne feste Programmzeiten ständig verfügbar. Die Wertschätzung für das Fernsehgerät ist bei den Verbrauchern aber nach wie vor ungebrochen.

Das Fernsehgerät selbst hat ebenfalls eine Wandlung vollzogen. Gehörten Fernsehgeräte vormals zur Kategorie der Offline-Geräte, ist dies bei Smart-TVs[13] anders. Smarte Fernsehgeräte können heute mehr als nur Rundfunksignale empfangen. Der Verbraucher kann mit seinem Smart-Fernsehgerät auch im Internet surfen und z. B. Videos über Mediatheken abrufen sowie soziale Netzwerke und Apps[14] nutzen. Ein smartes Fernsehgerät besitzt – wie ein internetfähiger Computer – ein Betriebssystem. Mit dem Smart-TV können also auch Speicherkarten, USB-Sticks oder digitale Medienzuspieler (Blu-Ray-Player, DVD, Spielekonsolen, Set-Top-Boxen) genutzt werden. Smart-TVs verfügen zusätzlich über den sog. Roten Knopf (Red-Button-Funktion). Über diese rote Taste auf der Fernbedienung gelangt der Fernsehzuschauer zum *Hybrid Broadcast Broadband TV* (HbbTV). Diese Funktion ermöglicht es, Internetinhalte mit dem (traditionellen) Fernsehen zu verbinden.[15] HbbTV bietet dem Verbraucher programmabhängige Funktionen, wie beispielsweise die Anzeige von Live-Informationen aus dem Internet, angepasste

---

12 Vgl. *Kurze Geschichte des Fernsehens* (Zeit Online, 28.12.2006), abrufbar unter https://www.zeit.de/2007/01/Kurze_Geschichte_des_Fernsehens.

13 Englisch „smart“ = „schlau“ oder „intelligent“.

14 Damit ist eine Anwendungssoftware gemeint, also ein ausführbares Programm, das eine Funktion erfüllt, aber nicht relevant für das Funktionieren eines Systems selbst ist. Auf diese Weise wird der Funktionsumfang eines Gerätes erweitert, etwa durch Browser-Apps, Spiele-Apps, Navigations-Apps usw.

15 S. etwa *Eichfelder*, HbbTV – was ist das? (chip.de, 25.10.2018), abrufbar unter https://praxistipps.chip.de/hbbtv-was-ist-das_27293.

Werbung, direkte Unterstützung beim Kauf von Teleshopping-Produkten oder auch senderabhängige Mediatheken.[16]

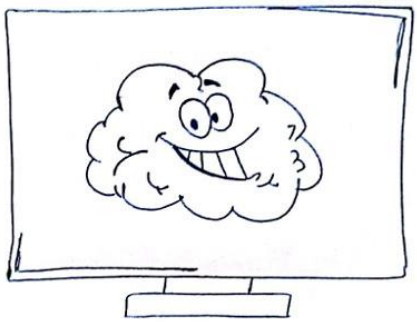


Abbildung 1: Smart-TV[17]

I. Warum eine Sektoruntersuchung zu Smart-TVs?

Mit ihrer Anbindung an das Internet stehen Smart-TVs stellvertretend für viele Geräte des sog. **Internet der Dinge (Internet of Things, IoT)**. Gegenstände des Alltags oder Maschinen in der Industrie werden über das Internet vernetzt. Die Geräte bekommen eine eindeutige Identität (Adresse) im Netzwerk, können über das Internet kommunizieren und Aufgaben voll automatisiert ausführen. Das Internet der Dinge ist im Alltag der Menschen längst angekommen. Viele Verbraucher verwenden neben Smartphones und Smart-TVs diverse Smart-Home-Technologien für Alltagsgegenstände, wie z. B. Lampen oder Jalousien. Die Entwicklung der Märkte für smarte Geräte dürfte sich weiter beschleunigen, wenn die flächendeckende Verbreitung des Mobilfunkstandards 5G voranschreitet und sich die Netzkapazitäten erhöhen. Industrie und Verbraucher werden von der neuen Technik profitieren.

Wenn Verbraucher ihren Alltag mit smarten Geräte organisieren und gestalten, nehmen viele von ihnen unbewusst in Kauf, dass ihre Handlungen und Gewohnheiten datenmäßig erfasst werden. Je mehr smarte Geräte ein Verbraucher einsetzt, desto umfassender ist sein digitaler Fingerabdruck, den die Empfänger seiner Daten kommerziell nutzen können. Hierbei besteht die Gefahr, dass der Verbraucher den Mehrwert der neuen Technik mit einer **Verletzung seiner Verbraucherrechte** bezahlt.

---

16 Vgl. *Ghiglieri*, Smart TV Privacy Risks and Protection Measures, 28.02.2017, S. V; abrufbar unter http://tuprints.ulb.tu-darmstadt.de/6187/1/DissertationMarcoGhiglieri_v2.pdf.

17 Bildnachweis: *Levent-Levi* – CC BY 2.0.

Das Bundeskartellamt ist in Internetforen und Medienberichten sowie in einem Zivilrechtsstreit auf zahlreiche **Hinweise** gestoßen, dass Verbraucher bei der Nutzung eines Smart-TVs nicht ausreichend geschützt sein könnten. Zudem wurde von mehreren Seiten der Verdacht geäußert, dass **Nutzerdaten ohne ausreichende Rechtsgrundlage** erhoben werden. So hatte das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bereits im Jahr 2015 diverse Smart-TVs untersucht und dabei Datenschutz- und Datensicherheitslücken entdeckt.[18]

Ähnliche Beobachtungen hatte auch die Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) gemacht. Die VZ NRW hatte gegen *Samsung*, einen führenden Smart-TV-Hersteller, geklagt[19] und insbesondere diverse in Allgemeinen Geschäftsbedingungen (AGB) enthaltene Klauseln angegriffen, welche die Übertragung von Daten an den Hersteller oder Dritte regeln.

Es gab zudem Hinweise, dass Smart-TV-Geräte für den Verbraucher **Sicherheitsrisiken im Hinblick auf Fremdzugriffe** bergen können. So hatte WikiLeaks über von CIA und MI5 ausgenutzte Sicherheitslücken von Smart-TVs[20] berichtet. Im Dezember 2017 verfasste der Sicherheitsdienstleister *AV-Comparatives* einen Bericht über Smart-TVs und beschrieb erhebliche Sicherheitslücken. Beispielsweise bestand laut *AV-Comparatives* für Angreifer die Möglichkeit, über manipulierte Firmware-Updates die Kontrolle über den gesamten Smart-TV zu erlangen.[21]

Das Bundeskartellamt hat daher im Dezember 2017 eine **Sektoruntersuchung** Smart-TVs eingeleitet. Es hatte mit Inkrafttreten der 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen im Juni 2017 erstmals Kompetenzen im Bereich des Verbraucherschutzes erhalten und kann seitdem u. a. verbraucherrechtliche Sektoruntersuchungen durchführen (§ 32e Abs. 5 GWB). Vo-

---

18 S. hierzu die Pressemeldung des BayLDA vom 27.02.2015, abrufbar unter https://www.lda.bayern.de/media/pm2015_02.pdf. Auf Basis der Untersuchung des BayLDA wurde vom *Düsseldorfer Kreis* eine Orientierungshilfe herausgegeben, S. *Düsseldorfer Kreis*, Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste, September 2015, abrufbar unter https://www.lda.bayern.de/media/oh_smarttv.pdf.

19 LG Frankfurt, Urteil vom 10.06.2016, Az. 2-3 O 364/15 – *VZ NRW/Samsung*, sowie nachgehend (jedoch nicht mehr zur Frage der AGB) OLG Frankfurt, Urteil vom 05.10.2017, Az. 6 U 141/16.

20 S. *Wikileaks*, Vault 7: CIA Hacking Tools Revealed, Pressemitteilung von *wikileaks* vom 07.03.2017, abrufbar unter https://wikileaks.org/ciav7p1/.

21 S. *AV-Comparatives*, AV-Comparatives & sigma star gmbh discovers security flaws in firmware used by 30+ popular TV brands, including *Medion*, Pressemitteilung von *AV Comparatives* vom 27.12.2017, abrufbar unter https://www.av-comparatives.org/wp-content/uploads/2018/02/avc_sigma_Medion_201802.pdf. *Medion* hat die damals festgestellte Sicherheitslücke zwischenzeitlich geschlossen.

raussetzung dafür ist der begründete Verdacht auf erhebliche, dauerhafte oder wiederholte Verstöße gegen verbraucherrechtliche Vorschriften, die nach ihrer Art oder ihrem Umfang die Interessen einer Vielzahl von Verbraucherinnen und Verbrauchern beeinträchtigen.

Entsprechende Verdachtsmomente zeigten sich auch noch während der Durchführung der Sektoruntersuchung. So stellte das britische Verbrauchermagazin *Which?* im Juni 2018 fest, dass während einer nur viertelstündigen Nutzung von Apps und Diensten auf einem Smart-TV Daten an über 700 Internetadressen gesendet wurden.[22] Eine im November 2018 veröffentlichte Untersuchung des c't Magazins zeigte, dass TV-Anstalten über den HbbTV-Datenverkehr Nutzerdaten erhalten, ohne hierüber vorab angemessen zu informieren. Ferner sollte Berichten zufolge die auf vielen Smart-TVs vorinstallierte Software *Samba TV* in großem Umfang Daten der Nutzer ohne deren Kenntnis erheben und verwerten.[23]

Neben den Datenschutzproblemen und Sicherheitsrisiken sprachen aus Sicht des Bundeskartellamts **weitere Gründe** dafür, gerade Smart-TVs in einer Sektoruntersuchung zum Themenkreis IoT und Verbraucherrecht zu untersuchen.

Zum einen gehören Smart-TVs zu den am **weitesten verbreiteten Geräten des Internet der Dinge**, die von allen Bevölkerungs- und Altersgruppen genutzt werden. Es handelt sich nicht etwa nur um Nischenprodukte für besonders technikaffine Menschen. Smart-TVs genießen bei den Verbrauchern eine hohe Wertschätzung. Ihr Anteil an den Fernseherverkäufen hat immer stärker zugenommen, so dass mittlerweile in Deutschland acht von zehn verkauften Fernsehern[24] Smartfunktionen aufweisen und deutlich mehr als die Hälfte[25] der Haushalte einen Smart-TV besitzen.

---

22 Vgl. *Laughlin*, Your home is watching you, Which? Magazine Juni 2018, S. 22.

23 S. z. B. *Maheshwari*, How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight (nytimes.com, 05.07.2018), abrufbar unter https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html; *Wenn Millionen fernsehen, schaut Samba TV mit* (Spiegel.de, 06.07.2018), abrufbar unter https://www.spiegel.de/netzwelt/gadgets/smart-tvs-mit-samba-tv-denn-wir-wissen-genau-was-sie-gucken-a-1217072.html.

24 S. *Smart Media – Zahlen, Fakten, News* (tv-plattform.de, undatiert), abrufbar unter https://www.tv-plattform.de/de/service/thema/thema-smart-media.

25 56,2 % lt. *Kantar/die medienanstalten*, VIDEO Digitalisierungsbericht 2019, S. 32, abrufbar unter https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Digibericht_Video_19/Medienanstalten_Chartreport_Digitalisierungsbericht_Video_2019_web.pdf. Die Studie *Goldbach*, Rising Star Smart TV – Neue Möglichkeiten in einer digitalen Welt, S. 6, abrufbar unter https://cdn.goldbach.com/bankai/uploads/goldbach-smart-tv-dach-studie-2019-2.pdf kommt für Deutschland, Österreich und die Schweiz sogar auf einen Haushaltsanteil von 80 %.

Daraus ergibt sich, dass auch mutmaßliche Verbraucherschutzverstöße und etwaige Durchsetzungsdefizite viele Menschen aller Bevölkerungsgruppen betreffen.

Zum anderen hat sich das Bundeskartellamt für eine Untersuchung smarter Fernseher entschieden, da diese eine **Plattform** darstellen, über die verschiedene Diensteanbieter und Verbraucher unmittelbar oder mittelbar über den Hersteller eine Geschäftsbeziehung aufbauen können. Der Hersteller des Smart-TVs tritt somit im Regelfall nicht nur als Produzent der „Hardware“ Fernseher in Erscheinung, sondern ist beim Betrieb eines Smart-TVs auch Anbieter und / oder Plattformanbieter für Dienste. Zum Funktionieren eines „Smart-TV“ tragen weitere Unternehmen bei, die zwar nicht zum untersuchten Wirtschaftszweig zählen, die aber neben dem Hersteller weitere Funktionen des Smart-TVs ermöglichen, wie Anbieter des Betriebssystems, HbbTV-Anbieter, selbstständige TV-Portale, App-Anbieter und andere Dienstebetreiber. Aufgrund dieses Netzes an kommerziellen Datenaustauschbeziehungen dürften sich Erkenntnisse aus dieser Sektoruntersuchung auch auf andere komplexe Geräte des Internets der Dinge übertragen lassen.

Mit der Sektoruntersuchung Smart-TV möchte das Bundeskartellamt die Verbraucher zunächst über den Umgang der Smart-TV-Anbieter mit ihren Daten aufklären und für den Schutz ihrer Daten sensibilisieren. Das Bundeskartellamt wird zugleich für Entscheider, Unternehmen und Verbraucher **Empfehlungen** formulieren, wie die aufgedeckten Missstände behoben und Verbraucher besser geschützt werden können. Individuelle Verfahren gegen Unternehmen führen – wie es sich für den Schutz des Wettbewerbs seit mehr als 60 Jahren bewährt hat – darf das Bundeskartellamt im Verbraucherschutz nach aktueller Gesetzeslage bislang nicht.

II. Untersuchungsgegenstand

Wie die aktuelle Diskussion in der Verbraucherschutzpraxis zeigt, fällt es den Verbrauchern **im digitalen Alltag** schwer, ihre Rechte durchzusetzen. Sie können Rechtsverstöße bei komplexen Sachverhalten, insbesondere wenn Geschäftsgeheimnisse der Unternehmen betroffen sind, vor den Zivilgerichten kaum selbst nachweisen. Sie verzichten in der Regel darauf, ihren Schaden geltend zu machen. Aus ihrer Sicht sind Kosten und Aufwand der Rechtsverfolgung höher als die hieraus zu erwartenden Vorteile (sog. rationale Apathie). Ohne behördliche Mittel erscheinen der Personenbezug und der Weg der Daten in vielen Fallgestaltungen kaum gerichtsfest nachweisbar zu sein. Gleichzeitig ist das öffentliche Interesse daran hoch. Viele smarte Geräte, wie z. B. Smart-TVs, sind Alltagsprodukte, die Verbraucher vor allem privat nutzen.

Das Bundeskartellamt hat die **Sektoruntersuchung** Smart-TVs eingeleitet, um über die Verarbeitung von personenbezogenen Daten der Verbraucher, ihren Weg und ihre kommerzielle Ver-

wendung aufzuklären sowie möglichen Datenmissbrauch in diesem Zusammenhang aufzudecken. In rechtlicher Hinsicht geht es insbesondere um die Beachtung des Datenschutzrechts, des Lauterkeits- und bürgerlichen Rechts und die Gewährleistung von Datensicherheit gegenüber Verbrauchern. Im Fokus der Untersuchung stehen die Datenschutzprobleme, die für den Verbraucher ab Inbetriebnahme eines Smart-TV auftreten.

Die Nutzung mit dem Internet verbundener Geräte kann für den Verbraucher mit dem Einstieg in ein regelrechtes **Karussell des Datengeschäfts** verbunden sein, das sie nicht mehr anhalten und aus dem sie nicht mehr aussteigen können. Sind personenbezogene Nutzerdaten erst einmal abgeflossen, können Verbraucher kaum noch beeinflussen, was mit ihren Daten geschieht. Daten können unbemerkt erfasst, zusammengeführt und für Profilbildung, Scoring und hierauf basierende personalisierte Angebote verwendet werden. Eine solche Profilbildung kann zumindest unter bestimmten Gesichtspunkten von Verbrauchern erwünscht sein, z. B. wenn sie für sich passgenaue Angebote erhalten möchten. Eine Profilbildung kann aber auch dazu führen, dass die über eine Person gespeicherten Daten zu deren Nachteil genutzt werden. Dies können z. B. mögliche Schwierigkeiten bei der Arbeitssuche oder beim Versicherungsabschluss sein. Im äußersten Fall ist auch Erpressbarkeit[26] vorstellbar, wenn Verbrauchern mit der Veröffentlichung intimer Daten oder Vorlieben gedroht werden kann. Die Sektoruntersuchung Smart-TVs soll aufklären, inwieweit auch Smart-TVs Teil des Geschäfts mit den Daten sind oder werden können. Dies ist bei einem Smart-TV deshalb besonders virulent, weil sich die Verbraucher nach dem Kauf in einem Dilemma befinden können. Lehnen sie Nutzungsbedingungen ab bzw. verweigern sie die Einwilligung in bestimmte Datenübertragungen, müssen sie befürchten, das Gerät nicht oder nicht im vorgesehenen Umfang verwenden zu können. Eine Rückgabe des Geräts ist rechtlich nicht ohne Weiteres möglich und praktisch mit hohem Aufwand verbunden. Der Verbraucher kann auch nicht unbedingt davon ausgehen, dass Alternativprodukte ein höheres Datenschutzniveau garantieren.

Die Branche Smart-TVs steht hierbei nur stellvertretend für eine Vielzahl anderer technischer Geräte, bei denen sich die Frage rechtswidriger Datenverarbeitungen (z. B. aufgrund unfreiwilliger Einwilligungen) gleichermaßen stellt.

Das Bundeskartellamt hat für die Sektoruntersuchung seine **bewährten Ermittlungsbefugnisse wie das Auskunfts- und Herausgabeverlangen** genutzt. Die Ermittlungen des Bundeskartellamts werden im Anschluss an diese Einleitung in Kapitel C. ausführlich beschrieben. Danach

---

26 Prominentes Beispiel: der sog. *Ashley Madison data breach*, s.: https://en.wikipedia.org/wiki/Ashley_Madison_data_breach.

werden in Kapitel D. die Funktionsweise eines smarten Fernsehgeräts, die Branchenteilnehmer und die wirtschaftliche Entwicklung des Sektors, die am Funktionieren eines Smart-TV beteiligten Akteure sowie die Rolle der Geräte im Geschäft mit den Daten geschildert. Kapitel E. ist den „verbraucherrechtlichen Problemfeldern“ gewidmet. Hier werden die Ermittlungsergebnisse dargestellt und rechtlich eingeordnet. Schwerpunktfragen, die hier behandelt werden, sind: Werden personenbezogene Daten beim Betrieb des Smart-TVs verarbeitet? Dürfen die Daten überhaupt erhoben oder verwendet werden? Werden die einschlägigen Datenschutzregelungen eingehalten? Welche Maßnahmen werden getroffen, um die rechtlichen Verpflichtungen, die sich insbesondere aus der DSGVO ergeben, zu erfüllen? In Kapitel E. hinterfragt das Bundeskartellamt außerdem, ob und inwieweit die Smart-TV-Branche **nachhaltige Produktpflege** betreibt: Welche Sicherheitsvorkehrungen treffen Smart-TV-Hersteller, um die Verbraucher vor Hackerangriffen oder anderen Sicherheitsrisiken zu schützen? Wird die Gerätesoftware regelmäßig aktualisiert? Kann das Gerät auch in fünf Jahren noch risikolos genutzt werden?

Der Bericht endet mit einer Darstellung des rechtspolitischen Handlungsbedarfs in Kapitel F. Zum einen werden die im Zuge der Untersuchung deutlich gewordenen Rechtsdurchsetzungsdefizite und Schutzlücken im geltenden Recht dargelegt. Zum anderen wird beleuchtet, inwieweit Datenschutzqualität künftig als Wettbewerbsparameter eingesetzt werden und dem Datenschutz zu mehr Breitenwirkung verhelfen kann. Eine innovative Informationsvermittlung ermöglicht dabei mehr Datensouveränität, ohne die dynamische Entwicklung der Digitalwirtschaft unangemessen zu beeinträchtigen. Auf dieser Grundlage werden schließlich Handlungsempfehlungen für Entscheider, Unternehmen und Wissenschaft ausgesprochen.

C. Ermittlungen

Nach dem GWB kann das Bundeskartellamt im Rahmen einer verbraucherrechtlichen Sektoruntersuchung alle Ermittlungen führen und alle Beweise erheben, die erforderlich sind, mit Ausnahme von Nachprüfungen, Durchsuchungen und Beschlagnahmen (§ 57 Abs. 1, § 32e Abs. 4 GWB). Insbesondere kann das Bundeskartellamt von Unternehmen und Vereinigungen von Unternehmen mit Sitz in Deutschland Auskünfte über ihre wirtschaftlichen Verhältnisse und die Herausgabe von Unterlagen verlangen (§ 59 Abs. 1, § 32e Abs. 4 GWB). Die Unternehmen sind zur wahrheitsgemäßen und rechtzeitigen Auskunftserteilung verpflichtet. Tun Sie dies nicht, kann das Bundeskartellamt zu Zwangsgeldern oder Geldbußen greifen. Die Unternehmen können die Auskunft auch nicht unter Hinweis auf Betriebs- und Geschäftsgeheimnisse verweigern.

Datenschutzbehörden und andere Institutionen haben im Bereich der Smart-TVs bereits Erkenntnisse gesammelt und publiziert. Das Bundeskartellamt hat seine Ermittlungsbefugnisse nun insbesondere eingesetzt, um weitere Problemsachverhalte zu beleuchten, die auch auf dem Zivilrechtsweg nicht oder nur schwer aufzuklären wären.

Die Ermittlungen zielten nicht darauf ab, endgültig gerichtsfest festzustellen, ob ein bestimmtes Verhalten eines Unternehmens einen Verstoß gegen verbraucherrechtliche Vorschriften und dabei insbesondere gegen Datenschutzbestimmungen darstellt. Denn für die Feststellung konkreter Rechtsverstöße im Einzelfall wäre der individuelle, unternehmensspezifische Sachverhalt einschließlich der Beziehungen zu Softwareanbietern und Dienstleistungen auszuermitteln. Dies würde aber die gegenwärtigen Befugnisse des Bundeskartellamts im Verbraucherrecht überdehnen, die nach dem Willen des Gesetzgebers konkrete Eingriffsbefugnisse nicht umfassen.

Das Bundeskartellamt hat seine Erkenntnisse im Wesentlichen aus zwei schriftlichen Befragungsrunden gewonnen. Die erste Befragungsrunde („Struktur-Befragung“, dazu unten I.) richtete sich an 32 Unternehmen und diente in erster Linie der Aufklärung der Marktstrukturen und -verhältnisse. In der zweiten Befragungsrunde („Detail-Befragung“, dazu unten II.) hat das Bundeskartellamt 21 Unternehmen detaillierte Fragen insbesondere zu Software, Datenflüssen und Vertragsbeziehungen gestellt. Nach Auswertung der Ergebnisse der Detail-Befragung hat das Bundeskartellamt im Juli 2019 begonnen, fehlende oder unklare Antworten aufzuklären sowie fehlende oder unverständliche Dokumente bei den Herstellern erneut anzufordern („Nacherhebung“). Teilweise musste mehrfach nachgefasst werden. Die letzten Antworten hat das Bundeskartellamt im November 2019 erhalten.

Parallel dazu führte das Bundeskartellamt während der gesamten Untersuchung mehrere Gespräche mit Marktteilnehmern (dazu unten III.).

Zusätzlich zu solchen für Sektoruntersuchungen üblichen Ermittlungsschritten hat das Bundeskartellamt weitere speziell für die Untersuchung konzipierte Ermittlungsmethoden angewendet (dazu unten IV.).

Hinweis

Im Rahmen der Sektoruntersuchung wurden nur Hersteller von Fernsehgeräten formell befragt. Soweit dieser Bericht Aussagen zu anderen Akteuren, wie z. B. Betriebssystem- bzw. TV-Portal-Anbietern (insb. *Google*, *Foxxum*, *Netrange*, *Samba TV* o. a.) enthält, beruhen diese nicht auf Angaben der Unternehmen selbst, sondern auf Informationen, die das Bundekartellamt von Fernseherherstellern erhalten oder selbst recherchiert hat.

I. Struktur-Befragung

Der erste Fragebogen diente der Aufklärung der Marktstrukturen und -verhältnisse. Das Bundeskartellamt hat z. B. ermittelt, welche Hersteller in welchem Umfang und unter welchen Marken Smart-TVs in Deutschland verkaufen, welche Software auf Smart-TVs vorinstalliert wird und mit welchen Zulieferern Geschäftsbeziehungen bestehen sowie wer hierbei jeweils Vertragspartner des Verbrauchers ist. Darüber hinaus hat das Bundeskartellamt von den Unternehmen, Datenschutzbestimmungen und sämtliche Allgemeine Geschäftsbedingungen angefordert, die im Verhältnis zum Endverbraucher Verwendung finden.

1. Auswahl der zu befragenden Unternehmen

In der Struktur-Befragung sollten möglichst alle Hersteller erfasst werden, deren Smart-TVs in Deutschland vertrieben werden. Zugrunde gelegt wurde dabei der weite Herstellerbegriff des Produkthaftungsgesetzes. Gemäß § 4 ProdHaftG[27] ist Hersteller nicht nur, wer das Endprodukt hergestellt hat, sondern insbesondere auch, wer sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt. Erfasst wurden so beispielsweise auch Handelsketten, die Fernsehgeräte zumeist in Asien herstellen lassen und anschließend unter einer Eigenmarke in den Verkehr bringen. Das Bundeskartellamt bezog auch das Angebot diverser Online-Händler und Shoppingportale in die Untersuchung ein. Ermittelt wurden schließlich 32 Unternehmen, die entweder in der Vergangenheit Smart-TVs vertrieben hatten oder bei denen es zumindest nicht ausgeschlossen schien, dass sie Smart-TVs in ihrem Produktportfolio führen.

Das Bundeskartellamt geht davon aus, dass die Erhebung nahezu lückenlos war und allenfalls Kleinsthersteller oder ausschließlich im Ausland ansässige Unternehmen mit sehr geringen Stückzahlen nicht befragt wurden.

2. Durchführung der Befragung

Die ausgewählten Unternehmen erhielten zwischen Mai und Juli 2018 ein Auskunftsersuchen mit Fragebogen. Den Versandzeitpunkt der Struktur-Befragung wählte das Bundeskartellamt so, dass die DSGVO für die Beantwortung bereits einschlägig war. Ein Unternehmen mit Sitz im europäischen Ausland ohne feststellbare Marktaktivitäten und mit mutmaßlich vernachlässigbaren Absatzzahlen in Deutschland hat nicht geantwortet. 31 Unternehmen haben den Fragebogen beantwortet und bis Ende November 2018 an das Bundeskartellamt zurückgesandt. Die internationalen Konzernstrukturen vieler befragter Unternehmen machten die Einbeziehung nicht in

---

27 Gesetz über die Haftung für fehlerhafte Produkte v. 15.12.1989 (BGBl. I S. 2198), zuletzt geändert durch Art. 5 des Gesetzes v. 17.07.2017 (BGBl. I S. 2421) – Produkthaftungsgesetz (ProdHaftG)

Deutschland bzw. nicht in Europa ansässiger Unternehmenseinheiten notwendig. Hier kam es mitunter zu Missverständnissen und Verzögerungen bei der Beantwortung des versandten Fragebogens.

Die Antworten von insgesamt 10 Unternehmen ergaben, dass sie in Deutschland entweder keine Smart-TVs (mehr) vertreiben oder einen Vertrieb bisher lediglich geplant hatten. Daher wurden diese Unternehmen nicht weiter befragt. In die Auswertung der Struktur-Befragung sind Antworten von 21 Herstellern eingeflossen. Darunter sind alle in der Öffentlichkeit bekannten Smart-TV-Hersteller. Die Unternehmen vereinten im Jahr 2018 nahezu 100 % des Smart-TV-Absatzes (nach Stückzahlen) in Deutschland auf sich. Das Bundeskartellamt konnte die Auswertung der Struktur-Befragung somit auf eine solide Datenbasis stützen.

Durch diese breit angelegte Befragung gewann das Bundeskartellamt einen umfassenden Überblick über die Struktur und die Absatzstärke des Wirtschaftszweigs einschließlich aller Beteiligten an der Plattform Smart-TV. Besonderes Augenmerk lag auf den Datenflüssen zwischen dem Verbraucher und den Herstellern von Smart-TVs sowie deren Lieferanten von Software für die smarte TV-Plattform. Dazu zählen z. B. mögliche Zulieferer des Betriebssystems, des Standard-Internetbrowsers, des HbbTV-Standardbrowsers, des Elektronischen Programmführers (EPG) und, sofern vorhanden, des Sprachassistenten der Smart-TVs. Auch nach möglichen Datenflüssen zwischen Verbraucher, Smart-TV-Herstellern und externen App-Entwicklern wurde ausführlich gefragt. Die Ergebnisse der Struktur-Befragung sind insbesondere in Kapitel D., aber auch Kapitel E. dieses Abschlussberichts eingeflossen.

II. Detail-Befragung

Auf der Grundlage der Antworten aus der Struktur-Befragung und weiterer Ermittlungsergebnisse hat das Bundeskartellamt in einer zweiten Befragungsrunde weitere Auskünfte von einer kleineren Auswahl an Herstellern verlangt. Ziel der Befragung war es, detaillierte Erkenntnisse vor allem zum Datenschutz bei der Verwendung von Software, zur nachhaltigen Produktpflege und zur Compliance zu gewinnen.

1. Auswahl der zu befragenden Unternehmen

Bei der Detail-Befragung hat das Bundeskartellamt detaillierte Auskünfte von den 21 Unternehmen verlangt, die es zuvor als am Markt aktive Hersteller von Smart-TVs identifiziert hatte.

12 dieser Unternehmen, deren Absatz in Deutschland unter 50.000 Smart-TVs[28] lag und deren mengenmäßiger gemeinsamer Marktanteil sich auf weniger als 3 %[29] belief, waren von der Beantwortung besonders umfangreicher Fragen zu vorinstallierter Software freigestellt. Aus Sicht des Bundeskartellamts war auch ohne die betreffenden Angaben ein hinreichend repräsentatives Bild der Branche gewährleistet.

Die Unternehmen mussten nicht nur den Fragebogen beantworten, sondern auch die Dokumente beifügen, auf welche sich ihre Antworten bezogen, beispielsweise Allgemeine Geschäftsbedingungen, Datenschutz-, Nutzungs- und/oder Garantiebestimmungen. Das Bundeskartellamt konnte so die Angaben der Unternehmen nachprüfen sowie untersuchen, ob die entsprechenden Bestimmungen für die Verbraucher zugänglich und verständlich sind.

2. Durchführung der Befragung

Das Bundeskartellamt hat die Befragung mittels eines förmlichen Auskunftsverlangens auf der Grundlage von § 59 GWB durchgeführt, welches Ende November 2018 versandt wurde. Die Auswertung begann im Februar 2019. Wie bereits im Rahmen der Struktur-Befragung gestaltete sich die Einholung der relevanten Informationen mitunter schwierig. Es wurden zahlreiche Fristverlängerungen gewährt. Gegenüber einem Unternehmen musste das Bundeskartellamt ein Zwangsgeld androhen und schließlich festsetzen, bevor dieses die erforderlichen Angaben machte. Nach Auswertung der Ergebnisse der Detail-Befragung begann das Bundeskartellamt im Juli 2019, fehlende oder unklare Antworten sowie fehlende oder unverständliche Dokumente bei den Herstellern erneut anzufordern („Nacherhebung“). Teilweise musste mehrfach nachgefasst werden. Die letzten Angaben zu den versendeten Fragebögen hat das Bundeskartellamt im November 2019 erhalten.

Durch die Detail-Befragung hat das Bundeskartellamt wertvolle Erkenntnisse zu wichtigen Themengebieten erhalten. Schwerpunkt der Befragung war der Datenschutz bei der Verwendung von Software (z. B. Betriebssystem, HbbTV-Standardbrowser etc.) für Smart-TVs. Kapitel E. des vorliegenden Abschlussberichts basiert ganz überwiegend auf den Informationen, die das Bundeskartellamt in der Detail-Befragung erhoben hat. Für die Datensicherheit ist auch wichtig, dass die Software, die die Verbraucher verwenden, gut geschützt ist. Mehrere Fragen richteten sich darauf, welchen Aufwand die Hersteller betreiben, um Verbraucher vor Softwaremängeln zu schützen und inwieweit diese im Schadensfall abgesichert ist. Das Bundeskartellamt hat sich auch mit den Maßnahmen der Unternehmen zur Erfüllung ihren rechtlichen Verpflichtungen

---

28 Nach Absatzzahlen entspricht dies in etwa einem Marktanteil in Deutschland von 1 %.

29 Bezugsjahr 2017, gemessen an Absatzzahlen in Deutschland.

(Compliance), die sich insbesondere aus der DSGVO ergeben, befasst. Schließlich hat das Bundeskartellamt die Smart-TV-Hersteller auch nach den Beziehungen zu den anderen Akteuren befragt, da gerade an diese Datenübermittlungen zu erwarten sind.

III. Gespräche mit Marktteilnehmern und Experten

In allen Phasen der Sektoruntersuchung hat das Bundeskartellamt Gespräche mit Marktteilnehmern und Experten geführt. Dies waren vor allem Smart-TV-Hersteller, aber auch andere mit der Thematik vertraute Institutionen und Verbände. Die Gespräche fanden vor Ort im Bundeskartellamt, bei den Institutionen bzw. Verbänden oder telefonisch statt. Auf diese Weise konnte das Bundeskartellamt zahlreiche zusätzliche Erkenntnisse und Hintergrundinformationen über die verbraucherrechtlichen Problemfelder und technischen Gegebenheiten bei Smart-TVs gewinnen.

Vor Einleitung der Sektoruntersuchung konsultierte das Bundeskartellamt andere Behörden, um mögliche thematische Überschneidungen zu identifizieren. Inhaltliche Überschneidungen mit diesen Behörden bestanden, wenn überhaupt, nur in geringem Ausmaß. Die Rückmeldung der Behörden zur geplanten Sektoruntersuchung war durchweg positiv.

Während der Vorbereitung der Fragebögen führte das Bundeskartellamt Vorklärungsgespräche mit verschiedenen Smart-TV-Herstellern (*Vestel*, *Samsung*, *Loewe* und *TechniSat*). Außerdem stand das Bundeskartellamt in Kontakt mit der Verbraucherzentrale Nordrhein-Westfalen, um verbraucherrechtliche Fragen bei Smart-TVs zu diskutieren.

Im März 2019 traf sich das Bundeskartellamt mit Vertretern des Forschungskonsortiums des Projekts „Datenschutzscanner-App Privacy Guard“. Dieses vom Bundesministerium für Bildung und Forschung finanzierte Projekt soll Verbrauchern ermöglichen, „selbstbestimmt über Datennutzungsvorgänge in Smartphone-Apps zu entscheiden“[30]. Der Fokus des Forschungsvorhabens lag zwar auf mobilen Smartphone-Apps. Es bestanden aber durchaus vergleichbare Problemstellungen bei Smart-TVs, insbesondere bei der rechtlichen Bewertung von Datenschutzbestimmungen.

Darüber hinaus wurde im März 2019 im Bundeskartellamt in einem mehrtägigen Workshop in Zusammenarbeit mit den Experten des TÜV Rheinland i-sec GmbH (TÜV Rheinland) ein wesentlicher Teil eines Prüfkonzepts für Smart-TVs erarbeitet. Anhand des Prüfkatalogs sollte untersucht werden können, ob smarte Fernsehgeräte den Datenschutz- und Datensicherheitsvorgaben der DSGVO entsprechen. Die Prüfung bezog sich sowohl auf die Datenschutzbestimmungen

30 *Bundesministerium für Bildung und Forschung*, Das Projekt Datenschutzscanner by PrivacyGuard, abrufbar unter https://datenschutz-scanner.de/das-projekt.html.

an sich als auch auf die technische Seite eines Smart-TVs. Das umfangreiche Prüfprogramm ist indessen auf Verfahren in Einzelfällen zugeschnitten und nur ausschnittsweise geeignet für die Analyse der Gesamtbranche, wie sie Gegenstand der vorliegenden Sektoruntersuchung ist. Würden dem Bundeskartellamt verbraucherrechtliche Eingriffsbefugnisse zustehen, könnte der Prüfkatalog eine Subsumtionsgrundlage bei möglichen Verwaltungsverfahren gegen einzelne Hersteller, ggf. sogar eine Grundlage für verbindliche Zusagen der Hersteller sein.

IV. Experiment Smart-TV-Ersteinrichtung

Idealerweise sollten Smart-TV-Nutzer stets sämtliche Nutzungsbedingungen und Datenschutzbestimmungen[31] lesen, die ihnen im Verlauf der Ersteinrichtung und bei der Verwendung von Apps etc. zur Kenntnis oder zur Zustimmung angezeigt werden. Dass dies in der Praxis oftmals nicht der Fall ist, bestätigen zumeist eigene Erfahrungen. Dies kann zum einen daran liegen, dass Nutzungsbedingungen und Datenschutzbestimmungen zu umfangreich, schlecht verständlich und/oder lückenhaft sind. Zum anderen sind entscheidende Textpassagen nicht immer problemlos auffindbar.

Das Bundeskartellamt hat im Januar und Februar 2019 ein hausinternes Experiment durchgeführt. Ziel dieses Experiments war es, festzustellen, ob der durchschnittliche Verbraucher alle Nutzungsbedingungen und Datenschutzbestimmungen, die ihm bei der Ersteinrichtung eines Smart-TVs zur Kenntnis oder zur Zustimmung angezeigt werden, tatsächlich finden und verstehen kann. Außerdem sollte erfasst werden, wieviel Zeit für die Ersteinrichtung durchschnittlich benötigt wird.

Jedem Teilnehmer des Experiments wurde in einem geschlossenen Raum ein Smart-TV eines bekannten Herstellers zur Ersteinrichtung mit dem Betriebssystem *Android* zur Verfügung gestellt. Dieser smarte Fernseher war auf Werkseinstellungen zurückgesetzt und mit dem Internet verbunden. Der weitere Ablauf gestaltete sich für jeden Probanden wie folgt: Der Leiter des Experiments schaltete den Smart-TV ein und gab dem Probanden eine kurze Einweisung in die Bedienung des Geräts. Hiermit sollte verhindert werden, dass fehlende technische Kenntnisse die Ersteinrichtung verzögern und das Ergebnis beeinflussen. Jeder Teilnehmer wurde anschließend vom Versuchsleiter aufgefordert, die Ersteinrichtung des Smart-TVs durchzuführen. Dabei sollte der Teilnehmer sämtliche Datenschutzbestimmungen und Nutzungsbedingungen in der aktuell gültigen Version lesen, die ihm währenddessen zur Kenntnis oder zur Zustimmung angezeigt

---

31 In diesem Bericht wird grundsätzlich der Begriff „Datenschutzbestimmungen“ verwendet. Nur soweit Datenschutzbestimmungen eines bestimmten Unternehmens in Bezug genommen werden, wird die von diesem Unternehmen gewählte Bezeichnung verwendet.

wurden. Jeder Teilnehmer sollte den Smart-TV so einrichten, dass während des späteren Betriebs so wenige Daten wie möglich an den TV-Hersteller oder Dritte weitergegeben werden. Um die Ersteinrichtung abschließen zu können, mussten die Probanden den Nutzungsbedingungen und der Datenschutzerklärung von *Google* zustimmen.

Im Anschluss an das Experiment beantwortete jeder Teilnehmer einen Fragebogen. Dieser enthielt sowohl allgemeine Fragen zur Ersteinrichtung als auch inhaltliche Fragen zu den wesentlichen Teilen der Datenschutzbestimmungen und Nutzungsbedingungen. Abschließend überprüfte der Leiter des Experiments anhand der Einstellungen des smarten Fernsehers, ob der jeweilige Teilnehmer alle möglichen Datenübertragungen deaktiviert hatte.

Für das Experiment wurden per Zufallsgenerator 20 Personen aus der Gesamtmenge der Mitarbeiter des Bundeskartellamts ausgewählt, wovon jeweils fünf auf die verschiedenen Laufbahngruppen des öffentlichen Dienstes entfielen. Die ausgewählte Personengruppe ist für die Bevölkerung der Bundesrepublik Deutschland nicht repräsentativ. Nicht repräsentativ ist das Experiment auch insoweit, als ein vollständiges Ignorieren und „Wegklicken“ der vorgelegten Verbrauchertexte nicht als Option vorgesehen war. Der durchschnittliche Zeitaufwand der Mitarbeiter des Bundeskartellamts für die Einrichtung des Smart-TVs in diesem Experiment dürfte daher deutlich über der durchschnittlichen Bearbeitungsdauer der Gesamtbevölkerung liegen.

D. Marktüberblick Smart-TVs

Im Folgenden werden die technischen Besonderheiten eines Smart-TV-Gerätes, die Entwicklung des Smart-TV-Markts sowie die wichtigsten Marktteilnehmer und sonstigen Akteure, die zum Funktionieren eines Smart-TV beitragen, dargestellt. Im Anschluss hieran wird die Rolle der Geräte beim Geschäft mit den Daten beleuchtet. Wie in vielen digitalen Wirtschaftsbereichen ist auch bei Smart-TVs eine hohe Dynamik zu verzeichnen. Die nachfolgende Beschreibung gibt den Stand der Erkenntnisse zum Untersuchungszeitpunkt wieder.

I. Was unterscheidet Smart-TVs von herkömmlichen Fernsehgeräten?

Fernsehgeräte empfangen Programme über Kabel, Satellit oder auch terrestrisch (DVB-T). Bei einem smarten Fernseher können darüber hinaus Informationen über das Internet bezogen werden. Besitzt ein Verbraucher einen Internetanschluss mit ausreichender Bandbreite, kann er mit seinem Fernsehgerät im Internet surfen und alle damit verbundenen Vorteile nutzen. Er kann zum Beispiel Videos über Mediatheken abrufen und sich in sozialen Netzwerken bewegen. Ebenso wie bei internetfähigen Computern ist auf dem smarten Fernsehgerät ein Betriebssystem installiert, welches in der Regel die Nutzung von Apps ermöglicht. Darüber hinaus kann der Smart-TV auf externe Datenquellen wie z. B. Speicherkarten, USB-Sticks oder digitale Medienzuspieler (Blu-Ray/DVD-Player, Spielekonsolen, Set-Top-Boxen) zugreifen.

Smart-TVs verfügen über einen Browser[32] für das hybride Fernsehen (HbbTV). Beim hybriden Fernsehen werden die bislang getrennten Übertragungswege Fernsehsignal und Internet kombiniert. Dabei werden für die Übertragung von Inhalten sowohl das Rundfunksignal (*Broadcasting*) als auch das Breitbandinternet (*Broadband*) genutzt. Der Verbraucher kann auf diese Weise wesentlich mehr Informationen als bei herkömmlichen Fernsehgeräten abrufen. Die Informationen werden in Echtzeit aktualisiert und können an seine persönlichen Bedürfnisse angepasst werden. Wählt der Verbraucher z. B. einen Sender oder eine Sendung aus, bietet der Smart-TV weitere Informationen zum Film aus dem Internet an. Auf Wunsch kann der Verbraucher diese sofort am Gerät aufrufen. Umgangssprachlich wird die Funktion auch *Red-Button*-Funktion genannt, da sie oftmals über eine rote Auswahltaste auf der Fernbedienung angesteuert wird.

Außerdem kann sich der Nutzer, ähnlich wie beim Videotext, über den elektronischen Programmführer (*Electronic Program Guide*, kurz „EPG“) – einer elektronischen Fernsehzeitung – über das Fernsehprogramm informieren und z. B. Aufnahmen programmieren oder Sendungen vormerken. Viele smarte Fernseher können auch über einen Sprachassistenten gesteuert werden.

In die Sektoruntersuchung nicht einbezogen wurden externe Geräte, die ein Fernsehgerät zu einem Smart-TV machen können, z. B. Settop-Boxen wie *Amazon-Fire-TV* oder *Apple-TV* oder Satellitenempfänger oder Blu-Ray-Player mit Smartfunktionen. Zwar stellen sich hier durchaus vergleichbare rechtliche Fragen. Diese Geräte sind aber – was ihren Leistungsumfang angeht – deutlich heterogener als Smart-TVs und unter den Verbrauchern weniger weit verbreitet. Das Bundeskartellamt hat daher von einer Untersuchung dieser Geräte abgesehen.

II. Marktentwicklung

Hybride TV-Geräte, die neben dem Rundfunkempfang zusätzlich eine Internetverbindung und optimierte Darstellung von Internet-Diensten auf dem TV-Bildschirm ermöglichen, sind seit 2009 auf dem deutschen Markt erhältlich.[33] Im Zuge der nahezu flächendeckenden Verfügbarkeit von immer leistungsstärkeren Internetanschlüssen haben Smart-TVs einen immer größeren Marktanteil am gesamten TV-Absatz in Deutschland erlangt. Wesentlich für die Verbreitung der Smart-TVs war die Entwicklung und Verbreitung des HbbTV-Standards. Dieser geht auf eine Initiative verschiedener Unternehmen – darunter TV-Hersteller, Satellitenbetreiber und Rundfunkanstalten – zurück. Die HbbTV-Spezifikation wurde Ende 2009 beim Europäischen Institut für Telekommunikationsnormen (ETSI) eingereicht und im Juni 2010 unter der Referenznummer ETSI TS 102

---

32 Dieser Browser ist für den Nutzer nicht unbedingt als solcher erkennbar, da er in der Regel nicht in Form einer separaten App o. Ä. auf der Benutzeroberfläche des Fernsehers angezeigt wird.

33 Vgl. *Deutsche TV-Plattform*, Marktanalyse Smart-TV, Mai 2014, S. 5.

796 in einer ersten Version publiziert.[34] Seit 2010 bieten alle großen Anbietergruppen des werbefinanzierten Privatfernsehens und des öffentlich-rechtlichen Fernsehens (ARD, ZDF, RTL und Pro7/Sat1) HbbTV-Dienste an. Mit über 90 % unterstützt der Großteil der 2018 abgesetzten smarten Geräte den Standard HbbTV.[35]

Smart-TVs sind in den letzten Jahren zur Standardausstattung in den deutschen TV-Haushalten avanciert. Im Jahr 2019 besaßen rund 56 % aller Haushalte in Deutschland ein Smart-TV-Gerät.[36] Insgesamt wurden laut *TV-Plattform* auf Basis von Daten von *GfK Retail & Technology* seit 2011 in Deutschland knapp 36 Millionen Smart-TVs verkauft.[37] Der Anteil der Smart-TVs am gesamten TV-Absatz in Deutschland steigt beständig und betrug nach Angaben von *Statista* und *TV-Plattform* basierend auf einer Studie der *GfK Retail & Technology* 80 % in den ersten drei Quartalen 2019.[38]

Nach Angaben der *gfu Consumer & Home Electronics GmbH* finden auch die smarten Funktionen immer mehr Verwendung. Nutzten im Jahr 2017 nur 56 % der Befragten die Möglichkeiten ihres smarten Fernsehers, waren es im Jahr 2019 bereits 67 % – in der Altersgruppe der 16- bis 39-Jährigen sogar 80 %.[39] In der *gfu*-Studie wurden die Probanden ferner nach den bevorzugten Geräten für die Wiedergabe von Bewegtbild-Inhalten gefragt. Geht es um die Wiedergabe von *Video-on-demand* (84 %) und die Mediatheken der TV-Sender (82 %) dominiert eindeutig der Fernseher. Für Videoportale wie zum Beispiel *YouTube* liegt zwar das Smartphone vorn (36 %), für die Wiedergabe von *Video-on-demand* und Inhalten der Mediatheken wird dieses hingegen nur zu jeweils vier Prozent genutzt. Vor allem bei längerer Verweildauer ist also – trotz deutlichen

---

34 S. hierzu *Deutsche TV-Plattform*, Marktanalyse Smart-TV, Mai 2014, S. 7, abrufbar unter https://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_de.pdf.

35 S. *Smart Media – Zahlen, Fakten, News* (tv-plattform.de, undatiert), abrufbar unter https://www.tv-plattform.de/de/service/thema/thema-smart-media.

36 S. Fn. 25.

37 S. *Smart Media – Zahlen, Fakten, News* (tv-plattform.de, undatiert), abrufbar unter https://www.tv-plattform.de/de/service/thema/thema-smart-media.

38 Ebenda. Der Umsatzanteil von Smart-TVs an Gesamtumsatz von TV-Geräten in Deutschland liegt noch deutlich darüber und betrug etwa ersten Halbjahr 2018 91%, s. *Weltweiter TV-Markt wächst* (marktforschung.de, 03.09.2018), abrufbar unter https://www.marktforschung.de/wissen/datenschutz/marktforschung/weltweiter-tv-markt-waechst/.

39 Vgl. *gfu Studie 2019 Einschätzungen der Konsumenten* (gfu.de, 10.07.2019), abrufbar unter https://gfu.de/gfu-studie-2019-einschaetzungen-der-konsumenten/.

Rückgangs des linearen Fernsehens – nach wie vor der Fernseher die unangefochtene Nummer eins unter den Geräten für die Wiedergabe von Bewegtbild-Inhalten. [40]

Die Märkte für Smart-TVs und andere smarte Geräte dürften sich zukünftig noch dynamischer entwickeln. Gegenstände des Alltags oder Maschinen in der Industrie werden über das Internet vernetzt. Die Geräte erhalten eine eindeutige Identität (Adresse) im Netzwerk und werden zu Datenverarbeitung und -kommunikation befähigt. So sind sie in der Lage, über das Internet zu kommunizieren und Aufgaben voll automatisiert auszuführen. Das Internet der Dinge ist im Alltag der Menschen längst angekommen. Viele Verbraucher benutzen neben Smartphones und Smart-TVs diverse Smart-Home-Technologien für Alltagsgegenstände. So können etwa Lampen, Thermostate, Jalousien oder Kühlschränke über das Internet gesteuert werden.

Begünstigt wird die Entwicklung des Internets der Dinge auch durch die Einführung des Mobilfunkstandards 5G, welche insbesondere erweiterte Netzkapazitäten mit sich bringen wird.[41] Mit dem Mobilfunkstandard 5G kann das Funksignal mit einer geringeren Verzögerungszeit (sog. Latenzzeit) übertragen werden. Smarte Geräte werden so in Echtzeit miteinander kommunizieren können. Mit der Diffusion der neuen Technik dürfte die Entwicklung der Märkte für smarte Geräte weiter an Fahrt aufnehmen.

III. Branche

Zu dem untersuchten Wirtschaftszweig im Sinne von § 32e GWB zählen die Unternehmen, die in Deutschland Smart-TVs anbieten. Zumeist handelt es sich dabei um Unternehmen, die die Fernsehgeräte selbst herstellen und unter ihrer Marke in Verkehr bringen. Daneben gibt es auch Händler, die die Fernsehgeräte fertigen lassen und unter eigener Marke verkaufen. Der Hersteller des Smart-TVs tritt dabei im Regelfall nicht nur als Produzent der Hardware „Fernsehgerät“ in Erscheinung, sondern kann auch Anbieter für Dienste sein oder die entsprechende Plattform be-

---

40 Vgl. *gfu Studie 2019 Einschätzungen der Konsumenten* (gfu.de, 10.07.2019), abrufbar unter https://gfu.de/gfu-studie-2019-einschaetzungen-der-konsumenten/ sowie gfu Consumer & Home Electronics GmbH, *gfu Studie 2019: Erste Ergebnisse der repräsentativen Konsumenten-Befragung*, Pressemeldung vom 24.06.2019, abrufbar unter https://www.gfu.de/presseraum/uebersicht/gfu-studie-2019-erste-ergebnisse-der-repraesentativen-konsumenten-befragung/ und SevenOne Media GmbH, *Media Activity Guide 2019*, Kapitel 2, abrufbar unter https://www.sevenonemedia.de/documents/924471/1111769/Media+Activity+Guide+2019/040352cd-a958-6876-6541-93630deee1c7.

41 Vgl. *Bundesnetzagentur*, Bundesnetzagentur teilt 5G-Frequenzen aus Versteigerung zu, Pressemitteilung der Bundesnetzagentur vom 04.09.2019, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2019/20190904_5G_Zuteilung.html.

reitstellen. Das Bundeskartellamt hat bei der Erstbefragung insgesamt 21 Unternehmen identifiziert, deren Smart-TVs 2017 in Deutschland vertrieben wurden. Geräte dieser Hersteller deckten im Referenzjahr 2017 nahezu 100 % des Smart-TV-Absatzes in Deutschland ab, welcher nach Angaben der Unternehmen insgesamt rd. 5,2 Mio. Stück betrug. Marktführer war *Samsung* mit einem Marktanteil von ca. 30 bis 35 %. Die Marktanteile lassen sich der folgenden Tabelle entnehmen:

Hersteller	**Wichtigste Marke(n)**	**Marktanteil 2017 nach Stückzahlen**
Samsung	*Samsung*	30 – 35 %
Panasonic	*Panasonic*	10 – 15 %
Sony	*Sony (Bravia)*	10 – 15 %
Vestel	*JVC, Hitachi, Telefunken, Toshiba*	10 – 15 %
Arçelik	*Grundig*	5 – 10 %
LG	*LG*	5 – 10 %
TP Vision	*Philips*	5 – 10 %
Sonstige		< 5 %

Tabelle 1: Marktanteile Smart-TVs in Deutschland 2017 nach Stückzahlen[42]

Über die Smart-TV-Anbieter hinaus sind weitere Unternehmen am Funktionieren des Smart-TVs beteiligt, auch wenn sie vom untersuchten Wirtschaftszweig nicht umfasst sind. Dazu zählen insbesondere HbbTV-Anbieter, selbstständige Portalbetreiber, App-Anbieter und Betreiber von Empfehlungsdiensten[43].

[42] Die Sortierung innerhalb der identischen Spannenangaben erfolgte alphabetisch und lässt keinen Rückschluss auf die Anzahl abgesetzter Fernsehgeräte zu.

[43] Empfehlungsdienste sind Dienstleister, die dem Verbraucher Angebote oder Empfehlungen für weitere Fernsehsendungen machen; mitunter basieren diese Empfehlungen auf der Analyse des bisherigen Nutzerverhaltens, vgl. *Düsseldorfer Kreis*, Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste, September 2015, S. 11, abrufbar unter https://www.lda.bayern.de/media/oh_smarttv.pdf.

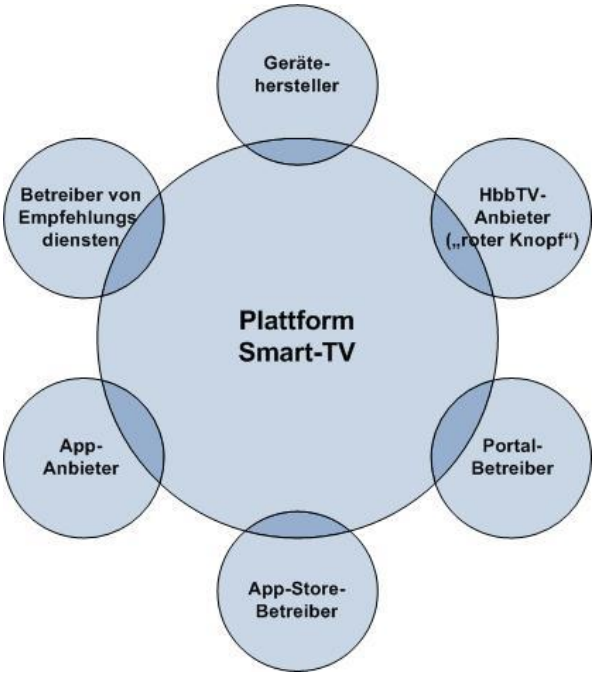


Abbildung 2: Akteure des Smart-TVs[44]

Will man sich ein Bild von der Datenerhebung mittels Smart-TV machen, so darf diese Vielzahl von Akteuren, die jeweils eigene Leistungen erbringen und im Zusammenhang damit Daten der Nutzer erheben, nicht außer Acht gelassen werden.

Zunächst sind dies die Betreiber der zentralen Plattform-Infrastruktur des Smart-TVs, d. h. des Betriebssystems, TV-Portals und ggf. App-Stores. Vielfach handelt es sich dabei um die – im Zentrum der Untersuchung stehenden – Hersteller von Smart-TVs. Denn wie bereits dargestellt, beschränken sich viele Hersteller nicht auf die Produktion der Hardware, sondern installieren und betreiben auch selbst die IT-Plattform des Smart-TVs und erheben dabei Daten der Nutzer. Die Ermittlungen des Bundeskartellamts haben ergeben, dass die meisten Hersteller auf ihren Smart-TVs *Linux*-basierte Betriebssysteme installieren. Es gibt jedoch auch Unternehmen, die auf Systemsoftware Dritter, insbesondere *Android TV* von *Google*, zurückgreifen oder bei denen die Funktion des TV-Portals von Drittanbietern wie *Netrange* oder *Foxxum* bereitgestellt wird. In diesen Fällen findet eine Datenverarbeitung regelmäßig durch diese Dritten statt. Mitunter wird für die Speicherung von Daten auch auf Cloud-Dienstleister wie *Amazon Web Services* zurückgegriffen. Der Betreiber des App-Stores ist im Regelfall identisch mit dem Portalbetreiber.

Neben den Betreibern der Smart-TV-Plattform stehen die zahlreichen Apps und Programme im Blickpunkt, die auf dieser Plattform laufen. Eine zentrale Rolle nehmen dabei Apps der bekannten Streaming-Anbieter (*Netflix*, *Amazon Prime Video*, *Maxdome*, *Rakuten TV* u. a.) ein, die auf den

44 Eigene Darstellung in Anlehnung an die Darstellung in der Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste (s. vorhergehende Fußnote), S. 9.

Smart-TVs häufig bereits vorinstalliert sind. Diese haben jeweils eine eigene Beziehung zu den Nutzern, in der Leistungen erbracht und Daten erhoben werden. Daneben gibt es Programme mit übergreifenden Funktionalitäten wie der Anzeige von Programmempfehlungen. Zu nennen ist insoweit insbesondere der Empfehlungsdienst *Samba TV*, der nach eigener Aussage in Deutschland auf nahezu allen Smart-TVs mit Ausnahme der *Samsung*-Geräte präsent ist.[45]

Ferner können von Fernsehsendern mit HbbTV-Angebot (siehe unter D. I., S. 26) personenbezogene Daten erhoben werden. Da bei der Aktivierung von HbbTV neben der Übertragung von Inhalten über das Rundfunksignal auch eine Internetverbindung hergestellt wird, ist nicht nur die Nutzung zusätzlicher Inhalte und Funktionen sondern auch ein „Rückfluss" von Daten an die jeweiligen Fernsehsender oder Dritte möglich. An die Stelle des einseitigen „Sendens" von Fernsehprogrammen tritt damit eine wechselseitige Kommunikation.

Das Gesamtbild ist vorrangig dadurch geprägt, dass jeder Akteur selbst Nutzerdaten sammelt und für eigene Zwecke verwendet („first-party data"). Eine „Weitergabe" der Daten findet eher ausnahmsweise bzw. nur in aggregierter Form (z. B. Aufrufzahlen) statt. Ausnahmen bestehen etwa, soweit individuelle Daten zu Abrechnungszwecken erforderlich sind oder soweit Dritt-Dienstleister (z. B. Cloud-Anbieter) eingeschaltet werden. Daten werden von den Unternehmen häufig auch als Geschäftsgeheimnis angesehen, das es zu schützen gilt. Beispielsweise haben Anbieter von *Video-on-demand* kein Interesse daran, dass potentielle Wettbewerber an genaue Daten über das In-App-Nutzerverhalten gelangen. Was „in" den Apps passiert, kann regelmäßig nur der App-Anbieter verfolgen oder Dritte mit seinem Einverständnis; die Smart-TV-Hersteller haben hiervon nach eigenen Angaben keine Kenntnis.[46] Vertragliche Regelungen sehen z. B. vor, dass sie zwar die Zahl der Aufrufe und die Nutzungsdauer einer App erfassen dürfen, nicht aber die dort abgerufenen Inhalte.

Die im Einzelnen erbrachten Beiträge sind vielgestaltig und komplex. Das Zusammenspiel einer Vielzahl von Akteuren wirft etliche verbraucherrechtlich relevante Fragen auf – insbesondere danach, wann und welche personenbezogenen Daten bei Nutzung der unterschiedlichen Angebote fließen, wer diese Daten zu welchen Zwecken erhält, ob eine Erlaubnis für das Erheben und die weitere Verwendung der Daten besteht, ob die einschlägigen Datenschutzregelungen eingehalten werden und inwieweit technisch-organisatorische Maßnahmen dem jeweiligen Schutzbedarf entsprechen.[47]

---

45 Interview mit *Carsten Schüler*, Managing Director Germany in ADZINE – Magazin für Online Marketing, 26.11.2019, abzurufen unter: https://www.adzine.de/2019/11/*Targeting*-mit-tv-nutzungsdaten-smart-tvs-als-bruecke-ins-digitale/.

46 Hierzu ausführlich unter E. V. 3. a) aa), S. 152.

47 Vgl. *Düsseldorfer Kreis*, Orientierungshilfe Smart-TV, September 2015, S. 4, abrufbar unter https://www.lda.bayern.de/media/oh_smarttv.pdf.

IV. Das Geschäft mit den Daten

Während in Bezug auf mobile Endgeräte mittlerweile eine gesteigerte Sensibilität für die teils extensive Datenverarbeitung besteht, stehen entsprechende Möglichkeiten bei Smart-TVs bislang weniger im Fokus der öffentlichen Aufmerksamkeit und Diskussion. Dabei ermöglichen viele Smart-TVs von ihrer technischen Ausrüstung und der Reichweite ihrer Datenschutzbestimmungen her eine weitgehende Verarbeitung von Nutzerdaten einschließlich des TV-Nutzungsverhaltens für die unterschiedlichsten Zwecke – auch wenn dieses Potenzial heute praktisch noch nicht voll ausgeschöpft wird. Da ein Smart-TV durch die Verbindung mit dem Internet über einen „Rückkanal“ verfügt, stehen dem Verbraucher zunächst zahlreiche zusätzliche Nutzungsmöglichkeiten zur Verfügung. Die Kehrseite ist, dass mit dieser Nutzung, oder sogar unabhängig von ihr, in erheblichem Umfang Daten abfließen können, die Auskunft über das Verhalten des Verbrauchers geben und für verschiedene kommerzielle Zwecke genutzt werden können.

1. Welche Daten werden erhoben? – Kategorien von erhobenen Daten

Die Analyse der von den Herstellern aufgeführten Datenverarbeitungen ergab, dass über die vorinstallierte systemnahe Software vor allem gerätebezogene Daten erhoben wurden (IP-Adresse, Geräte-ID(s), MAC-Adresse, Gerätestandort, individuelle Gerätekonfiguration, verbundene Geräte, installierte Apps etc.), nur in Einzelfällen wurden Nutzungsdaten verarbeitet, was nach Angaben der Hersteller zu Zwecken der Statistik bzw. Weiterentwicklung der Software dient. Hingegen übermittelten Zusatzdienste, also insbesondere Sprachassistenten und Empfehlungsdienste, in beachtlichem Umfang Nutzungsdaten, insbesondere auch solche aus automatisierter Inhaltserkennung (ACR); Sprachassistenten erhielten naturgemäß auch Stimmdaten der Nutzer.

Im Allgemeinen lassen sich die im Zusammenhang mit dem Betrieb eines Smart-TVs verarbeiteten Nutzerdaten in drei Kategorien einordnen: Basisdaten, vom Nutzer selbst eingegeben Daten sowie Daten über sein TV-Nutzungsverhalten. Die technischen Instrumente, mit denen die Daten verarbeitet werden, unterscheiden sich dabei jeweils. Im Einzelnen:

a) „Basisdaten“

Als Basisdaten werden hier solche Daten bezeichnet, die grundlegende Informationen zur Identifikation des Geräts, seiner Eigenschaften (z. B. installierte Software-Versionen) und seines „Standorts“ enthalten, und die auch erhoben und verarbeitet werden, wenn der Nutzer sich nicht bei einem Smart-TV-Dienst registriert.

Eine besondere Rolle spielen insoweit sog. **Identifikatoren**, also Merkmale, die die eindeutige Identifizierung eines Smart-TVs (oder anderen IoT-Geräts) erlauben. Hierzu zählen etwa eine

eindeutige Gerätenummer, die MAC-Adresse[48] des Smart-TVs oder eine dem Gerät fest zugeordnete Werbe-ID. Der Hauptzweck solcher Identifikatoren und insbesondere von Werbe-IDs besteht darin, es Unternehmen (z. B. Werbetreibenden) zu ermöglichen, Daten über das Nutzerverhalten von verschiedenen Anwendungen und Aufrufe von Websites zu einem umfassenden Profil zu verknüpfen. Gelingt es Werbetreibenden, solche gerätespezifischen Profile mit anderweitig gesammelten nutzerspezifischen Daten zusammenzuführen (z. B. durch sog. *ID Syncing*), kann ein feinkörniges und intimes Bild der Aktivitäten, Interessen, Verhaltensweisen und Routinen der Nutzer gezeichnet werden.

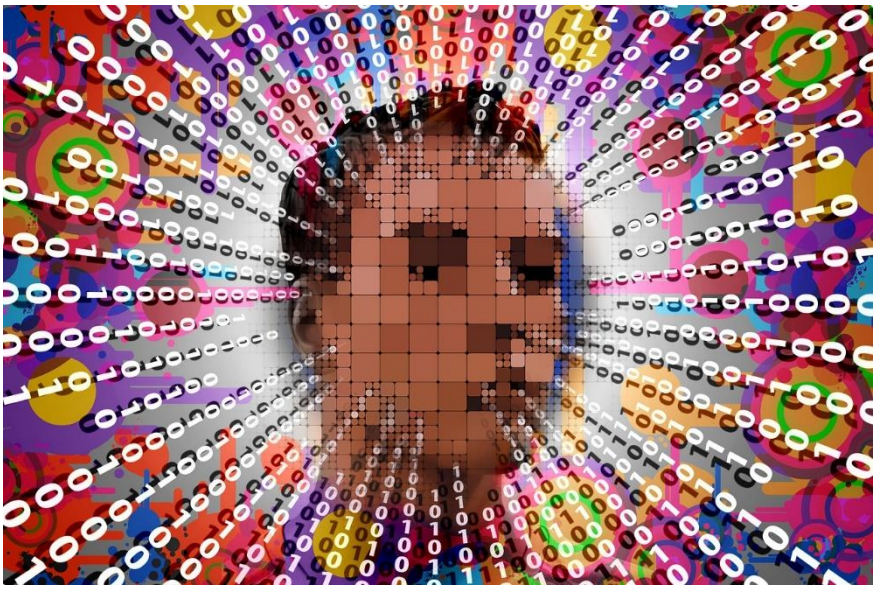


Abbildung 3: Aus Einzeldaten werden Profile[49]

Im Rahmen der Sektoruntersuchung machten die Unternehmen Ausführungen dazu, ob und über welche Art von Identifikatoren ihre Smart-TVs verfügen und ob diese vom Nutzer geändert werden können. Zusätzlich mussten die Unternehmen angeben, wer diese Identifikatoren erhält. Die Smart-TVs aller insoweit befragten Unternehmen[50] verfügten über Identifikatoren, die vom durchschnittlichen Verbraucher nicht geändert werden können. Hierzu zählten bei allen Unternehmen die Seriennummer des Smart-TVs sowie die MAC-Adresse. Neben diesen zwei Identifikatoren

48 *Wikipedia*, MAC-Adresse: Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die als eindeutiger Identifikator des Geräts in einem Rechnernetz dient.

49 Bildnachweis: *geralt*/*pixabay*.

50 Im Zuge der ausführlichen Befragung zum Schwerpunktthema Datenschutz waren nur die 12 größten Smart-TV-Hersteller zu einer detaillierten Auskunft bezüglich der verwendeten Identifikatoren verpflichtet.

verfügten die Smart-TVs im Durchschnitt über zwei weitere nicht änderbare Identifikatoren. Insgesamt lag die durchschnittliche Anzahl bei über 5 Identifikatoren pro Smart-TV. Von diesen waren über 80% nicht oder nicht ohne Expertenwissen änderbar. Ein Hersteller verwendete insgesamt 14 Identifikatoren. Darauf folgten ein Unternehmen mit 8 sowie drei weitere mit jeweils 7 Identifikatoren.

Eine größere Anzahl an Identifikatoren muss nicht zwingend mit einer insgesamt häufigeren Übermittlung von Identifikatoren oder anderen Nutzerdaten an Dritte einhergehen. Sie dürfte aber in jedem Fall erweiterte Möglichkeiten identifizierender Datentransfers eröffnen. Dies gilt umso mehr, als identifizierende Cookies in ihrer Bedeutung tendenziell abnehmen, da sie vom Nutzer immer effektiver geblockt werden können.[51] So gaben die meisten befragten Unternehmen auch an, dass der Nutzer Cookies blockieren kann; eine Löschung ist fast immer möglich. Erfolgt eine Nutzeridentifizierung hingegen über *HTML5 Local Storage*[52], kann der Nutzer die so erfassten Daten nach Angabe der Unternehmen auf seinem Smart-TV in der Regel weder einsehen noch einfach löschen.

Eine Zuordnung von Identifikatoren zu einer bestimmten Person ist spätestens in dem Zeitpunkt möglich, in dem sich die Person, deren ID vom Datenempfänger ausgelesen wird, mit Klarnamen, E-Mail- oder postalischer Adresse an irgendeiner Stelle im Internet registriert.[53]

---

51 S. dazu *Schutzmann*, Antworten auf das Cookie-Sterben (internetworld.de, 23.10.2019), abrufbar unter https://www.internetworld.de/technik/cookie/antworten-cookie-sterben-1774771.html; *The ad industry continues its quest toward fewer cookies and more consistent user IDs* (martechtoday.com, 17.01.2019), abrufbar unter https://martechtoday.com/the-ad-industry-continues-its-quest-toward-fewer-cookies-and-more-consistent-user-ids-229754. Bei Smart-TVs gestaltet sich das Blockieren von Cookies und anderen Tracking-Tools indessen oftmals schwerer als bei Browsern, die auf dem PC oder Laptop verwendet werden.

52 Die fünfte Fassung der Programmiersprache HTML (HTML5) erlaubt es, Daten auch unabhängig von Cookies über den Browser lokal auf dem Gerät des Nutzers zu speichern, entweder für die Dauer einer Sitzung (*Session Storage*) oder auch dauerhaft über das Beenden der Sitzung hinweg (*Local Storage*).

53 S. *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, März 2019, S. 15, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

b) Vom Nutzer eingegebene Daten

Eine weitergehende Datenverarbeitung findet statt, wenn der Nutzer sich zu bestimmten Diensten oder Apps anmeldet. Hier sind von dem Nutzer aktiv Daten einzugeben (Kontaktdaten, Geburtsdatum, Bankdaten etc.), die für die jeweilige Dienstleistung erforderlich sein aber unter Umständen auch für andere Zwecke verwendet werden können.

Eine besondere Form der an Hersteller aktiv „hingegebenen" Daten sind Sprachinformationen, wie sie bei der Nutzung von Spracherkennungsdiensten anfallen.

c) Daten über das TV-Nutzungsverhalten

Eine weitergehende Datenverarbeitung kann aber auch stattfinden, ohne dass der Nutzer aktiv und bewusst Daten eingibt, und zwar insbesondere dadurch, dass eine automatisierte Aufzeichnung und Analyse seines TV-Nutzungsverhaltens vorgenommen wird. Es handelt sich also um Daten, die aus der beobachteten Interaktion des Verbrauchers mit dem Smart-TV resultieren.

Diese Datenverarbeitung kann hinsichtlich Tiefe und Umfang unterschiedliche Formen annehmen. So gibt es zunächst Instrumente zur Erhebung anonymisierter statistischer Daten, die etwa zur Reichweitenmessung oder sonstigen Analysezwecken verwendet werden. Den Umgang mit anonymisierten Daten braucht der jeweilige Verantwortliche nicht in seinen Datenschutzbestimmungen anzugeben, da aus der Verwendung dieser Daten kein Eingriff in Rechte einer einzelnen Person resultiert.

Darüber hinaus können individuelle Daten zur Interaktion mit Programmen oder Apps erhoben werden. So werden unter Umständen die Aufrufzeiten, Verweildauer, abgerufene Inhalte oder auch die Bewegung des Cursors aufgezeichnet. Auch Stimmdaten[54] werden ggf. erfasst.[55] Noch weitergehend zeigt die Untersuchung, dass manche Akteure über technische Möglichkeiten und Regelwerke verfügen, die es vorsehen, das gesamte TV-Nutzungsverhalten mit Bezug zum konkreten Nutzer verfolgen zu können.

Hinweise hierauf finden sich in den Datenschutzbestimmungen der Smart-TV-Hersteller (bzw. TV-Portal-Betreiber). So sehen Datenschutzbestimmungen verschiedener Hersteller, die selbst die Plattform-Infrastruktur des Smart-TVs betreiben, vor, den TV-Nutzungsverlauf mittels auto-

---

54 S. *Google*, Datenschutzerklärung – Daten, die wir bei der Nutzung unserer Dienste erheben – Ihre Aktivitäten.

55 Bei Stimmdaten handelt es sich ebenso wie bei Cursorbewegungen um sog. biometrische Daten. Biometrische Daten erlauben eine Personenerkennung von Individuen, die auf ihren Verhaltens- und biologischen Charakteristika basiert. Die Verarbeitung biometrischer Daten bedarf stets der Einwilligung durch die betroffene Person, S. Art. 9 Abs. 2 lit. a) DSGVO.

matisierter Inhaltserkennung (*Automatic Content Recognition*, *ACR*) zu verfolgen. ACR bezeichnet die Fähigkeit einer Smart-TV-App oder sonstiger Smart-TV-Software, einen Inhalt (z. B. Audio- oder Videosignal), der auf einem an das Internet angeschlossenen Gerät (hier: dem Smart-TV) wiedergegeben wird, anhand der einzigartigen Merkmale des Inhalts mit einer hierauf spezialisierten Datenbank abzugleichen und zu identifizieren. So heißt es in der „Samsung Datenschutzrichtlinie – Ergänzung für Smart-TV“:

> „[…] Damit wir Ihnen ein auf Sie zugeschnittenes Smart TV Erlebnis bieten können, sind einige unserer Funktionen und Dienste auf Ihren TV-Anzeigeverlauf und Ihre Smart TV-Nutzungsinformationen angewiesen.“ [56]

sowie

> „Wir erfassen Ihre Historie der gesehenen Sendungen zusammen mit der TV-Gerätekennung (einschließlich der personalisierten Service-ID bzw. „PSID“) und der IP-Adresse. Die Historie der gesehenen Sendungen enthält Informationen über:
>
> - Netze, Sender, besuchte Webseiten und auf dem Smart TV gesehene Sendungen sowie
> - die dafür aufgewendete Zeit.
>
> Wir verwenden zur Erhebung dieser Daten die Automatische Inhaltserkennung (ACR) und andere Technologien. Dabei überträgt Ihr Smart TV Audio- und Videoausschnitte oder Informationen des TV-Tuners, um die gesehenen Sendungen festzustellen. Wenn Sie den Anzeigeinformationsdiensten zustimmen, ermöglicht ACR unseren Smart TVs die Generierung einer eindeutigen Videosignatur von Fernsehbildern, um festzustellen, ob die Videosignatur von einem Fernsehprogramm, Video-On-Demand-Titeln, linearer Fernsehwerbung oder Videospielen stammt. […].“[57]

Eine Verfolgung des TV-Nutzungsverlaufs mittels ACR kann auch durch auf dem Smart-TV installierte Drittprogramme erfolgen. So verwendet der Empfehlungsdienst *Samba TV* nach eigenen Angaben ACR-Technologie, die in Echtzeit (mittels *Fingerprinting*) Bilder erkennt, die auf

---

56 *Samsung*, Datenschutzrichtlinie – Ergänzung für Smart-TV, unter *Was sind Anzeigeinformationsdienste?*

57 *Samsung*, Datenschutzrichtlinie – Ergänzung für Smart-TV, unter *Was sind Anzeigeinformationsdienste? – Welche Daten erfassen wir?*

dem Bildschirm laufen, auch im Rahmen von Streamingdiensten und Konsolennutzung, und kann dadurch Zielgruppen auf Basis der ermittelten Interessen erstellen.[58]

In der Datenschutzrichtlinie von *Samba TV*[59] heißt es unter „Informationen zu den von Ihnen gesehenen Inhalten“:

> „Wir erhalten Informationen über den Inhalt, den Sie sehen oder mit dem Sie über ein Smart TV interagieren, das unsere Smart TV-Dienste integriert oder über Smart TV-Apps […]“.[60]

Zu den Smart TV-Diensten wird das wie folgt konkretisiert:

> „Wenn Sie sich für unsere Smart TV-Dienste anmelden, können wir den Inhalt erkennen, der über Ihr Fernsehgerät wiedergegeben wird. Bitte beachten sie, dass wir nur öffentliche Inhalte, wie etwa bestimmte Sendungen und Filme, erkennen können. Wir werden nicht wissen, wenn Sie beispielsweise Heimvideos anschauen.“

Schließlich ist eine Verfolgung des Nutzungsverhaltens bei Aktivierung von HbbTV auch für die jeweiligen **Fernsehsender bzw.** übergreifend für die großen **Sendergruppen** mit einer Vielzahl von Programmen möglich. Dies kann über anonymisierte Reichweitenmessung hinaus auch für Profilbildung und gezielte Werbung genutzt werden.

Zumeist besteht die Möglichkeit, die Verarbeitung solcher Nutzungsdaten – sei es durch Hersteller, Fernsehsender oder andere Dritte wie z. B. Empfehlungsdiensteanbieter – vorab zu verweigern oder nachträglich in den Einstellungen des Fernsehers abzuschalten.[61]

---

58 Interview mit Carsten Schüler, Managing Director Germany (ADZINE – Magazin für Online Marketing, 26.11.2019), abrufbar unter https://www.adzine.de/2019/11/targeting-mit-tv-nutzungsdaten-smart-tvs-als-bruecke-ins-digitale/.

59 Stand: 28.10.2018.

60 Im Internet abrufbar ist nur eine neuere englischsprachige Fassung: https://samba.tv/legal/privacy-policy/.

61 S. dazu etwa *Samsung*, Globale Datenschutzrichtlinie – Datenschutzhinweis zu Anzeigeinformationsdiensten, unter *Was sind Anzeigeinformationsdienste?*: „[…] Sie können Ihre Einwilligung jederzeit im Einstellungsmenü […] widerrufen; in diesem Fall wird die Historie der gesehenen Sendungen nicht mehr für diese bestimmte Funktion oder diesen Zweck verarbeitet.“

2. Wozu werden Daten erhoben? – Wirtschaftliche Zwecke der Datenerhebung

Die von den verschiedenen Akteuren erhobenen Daten können über ganz konkrete Erfordernisse der Leistungserbringung hinaus für verschiedene weitergehende wirtschaftliche Zwecke verwendet werden.[62]

So können Erkenntnisse aus der Datenanalyse für die **Produktweiterentwicklung** verwendet werden. Dies kann das Erkennen von Fehlern und technischen Problemen, aber etwa auch Anpassungen der Benutzeroberfläche umfassen, z. B. im Hinblick auf die Menüführung. Ein wichtiger Gesichtspunkt ist insoweit auch die **Personalisierung des Angebots**, indem etwa App- oder Filmempfehlungen auf Grundlage der bisherigen Nutzung und Sehgewohnheiten und der daraus „errechneten" Interessen des Nutzers abgegeben werden können. Auch kann die Bedienung durch Funktionen wie Auto-Vervollständigen oder Anzeige häufig besuchter Seiten erleichtert werden.

Daten können aber auch für die Steuerung von Marketing und Vertrieb von Bedeutung sein. Insoweit kann z. B. von Interesse sein, wo der Smart-TV steht, welche Apps der Nutzer installiert hat oder welche Fernsehprogramme er gerne sieht. In diesem Zusammenhang erlangen die Daten aus dem TV-Nutzungsverhalten für das Angebot **zielgerichteter Werbung („targeted advertising")** zunehmend an Bedeutung. Hierunter versteht man Werbung, die auf bestimmte Nutzergruppen und deren Interessen oder Eigenschaften ausgerichtet ist.

Zielgerichtete Werbung hat in den vergangenen Jahren enorm an Bedeutung gewonnen. Zum einen lassen sich durch zielgerichtete Werbung Streuverluste minimieren. So werden beispielsweise Produkte mit einer jugendlichen Zielgruppe Rentnern erst gar nicht zum Kauf angeboten (und umgekehrt). Zum anderen liegt die Resonanz bei den Werbungsempfängern im Durchschnitt deutlich höher als bei konventioneller Werbung. Der genaue Mehrwert zielgerichteter Werbung lässt sich nur schwer beziffern, was auch daran liegen mag, dass dieser u. a. maßgeblich vom Zuschnitt der Werbekampagne und dem Detailgrad des Zielkundenprofils abhängen dürfte. Studien legen jedoch nahe, dass zielgerichtete Werbung spürbar mehr Umsatz generiert als nichtzielgerichtete Werbung.[63] Unstreitig ist jedenfalls, dass Unternehmen immer größere Summen für

---

62 Vgl. generell zur Bedeutung von Daten für die wirtschaftliche Aktivität: *Bundeskartellamt und Autorité de la Concurrence*, Competition Law and Data, Mai 2016, S. 8, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html.

63 *Farahat/Bailey*, How Effective is Targeted Advertising?, 2012, abrufbar unter https://www2012.universite-lyon.fr/proceedings/proceedings/p111.pdf, stellen um 79 % erhöhte Suchanfragen nach dem Ansehen zielgerichteter Werbung (gegenüber nicht gezielt ausgespielter Werbung) fest, die Autoren berücksichtigen dabei den sog. *Selection Bias*, d. h., dass Angehörige der angesprochenen Werbezielgruppe sich auch unabhängig von der Werbung stärker für ein bestimmtes Produkt interessieren bzw. dieses häufiger kaufen.

zielgerichtete Werbung ausgeben. Je nach Quelle differiert der geschätzte Anteil der auf *Behavioural Targeting* beruhenden Werbung an den gesamten Werbeausgaben für digitale Bildschirmwerbung[64] teils erheblich.[65] Unstreitig ist, jedoch, dass er mit hohen Wachstumsraten beständig ansteigt.[66]

Die aus dem Bereich der Online-Werbung bekannten Instrumente werden mithin auch immer interessanter für die Daten aus der Nutzung des Smart-TVs. Dies kann unterschiedliche Ausprägungen haben, je nachdem wo die Werbung geschaltet wird:

a) Werbung im TV-Portal

In Deutschland bisher nur vereinzelt anzutreffen ist die **Werbung im TV-Portal (Startbildschirm/Homescreen des Smart-TV)** selbst, z. B. über Display- oder Video-Werbeflächen (s. dazu E. VIII.1., S. 212). Wenn diese angeklickt werden, können sie zu einem Full-Screen-Video erweitert werden oder den Nutzer auf eine Internetseite des Werbetreibenden weiterleiten.

Ein Vorreiter ist insoweit „Samsung Ads“, die seit Mitte 2018 und in jüngerer Zeit in Europa verstärkt angeboten werden. Samsung verfügt nach eigenen Angaben über 30 Millionen für Anzeigen aktivierte Smart-TVs im Vereinigten Königreich, Frankreich, Deutschland, Italien, Spanien und Russland.[67]

---

64 Mit digitaler Bildschirmwerbung (im Englischen „Digital display advertising“) ist hier jegliche Werbung gemeint, die per Internet auf Bildschirmen ausgespielt wird (Computer, Tablet, Smartphone etc.), s. dazu *eMarketer*, Programmatic Digital Display Ad Spending – Executive Summary (21.11.2019), abrufbar unter https://www.emarketer.com/content/germany-programmatic-digital-display-ad-spending.

65 *Statista* ermittelt für 2020 einen Anteil am Markt für Bildschirmwerbung von ca. 74 %, S. *Statista*, Statista Digital Market Outlook, Oktober 2019, abrufbar unter https://de.statista.com/statistik/daten/studie/831081/umfrage/umsatzanteil-von-programmatic-advertising-im-markt-fuer-digitale-werbung-in-deutschland/; *eMarketer* prognostiziert für programmatische Display-Werbung in Deutschland einen Anteil von rund 82 % im Jahr 2020, S. *eMarketer*, Programmatic Digital Display Ad Spending – Executive Summary (vorhergehende Fußnote). Deutlich vorsichtiger (rund 47 %): *Pfannenmüller*, Warum Deutschland beim Programmatic Advertising hinterherhinkt (wuv.de, 20.11.2018, abrufbar unter https://www.wuv.de/tech/warum_deutschland_beim_programmatic_advertising_hinterherhinkt. Es ist auch nicht auszuschließen, dass hier bei Marktdefinition und Berechnungsgrundlagen Unterschiede bestehen.

66 Unklar ist, inwieweit die Inhalteanbieter, die die Werbung anzeigen, von den erhöhten Werbeumsätzen profitieren, s. dazu *Marotta/Abhishek/Acquisti*, Online Tracking and Publishers' Revenues: An Empirical Analysis, Mai 2019, abrufbar unter https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

67 Vgl. die Darstellung unter https://www.samsung.com/de/business/samsungads/.

Grundlage der zielgerichteten Werbung ist die bereits oben (S. 37 ff.) erwähnte automatische Inhalteerkennung (ACR), mittels derer das Nutzungsverhalten über Fernsehkanäle und -programme, sonstige Gerätenutzung bis hin zur Nutzung von angeschlossenen Set-Top-Boxen und Spielekonsolen hinweg verfolgt werden kann. Dies ermöglicht es beispielsweise, Haushalte zu identifizieren und anzusprechen, die eine Werbekampagne im klassischen linearen Fernsehen nicht gesehen haben. Es können zudem gezielt Nutzergruppen angesprochen werden, die kaum oder nie lineares werbefinanziertes Fernsehen sehen. Ein *Targeting* ist aber auch nach den Inhalten des linearen TV-Sehverhaltens (z. B. Ansprache von Fussballfans), des generellen App-Nutzungsverhaltens, der Gaming-Vorlieben auf angeschlossenen Konsolen und nach Kriterien wie TV-Typ, Internet-Provider, Postleitzahl etc. möglich.[68] So kann die Werbung für eine Fernsehshow etwa an Nutzer gerichtet werden, die sich grundsätzlich für Spielshows interessieren, die beworbene Show aber bisher noch nicht gesehen haben.

Die Möglichkeit zielgerichteter Werbung wird insbesondere in den Datenschutzbedingungen von *Samsung*, *LG* und *TP Vision* explizit angesprochen.

Wo Hersteller Drittanbieter zum Betrieb des TV-Portals oder App-Stores einschalten, ist die Möglichkeit, Werbung auf den Benutzeroberflächen zu schalten, Teil der vertraglichen Vereinbarung. Dabei wird dies teilweise ausdrücklich als Teil der Vergütung geregelt, d. h. wenn der Hersteller weniger Werbung wünscht, steigen die Lizenzentgelte für das Drittprogramm.

b) Addressable TV

Ein wachsender Markt ist auch das Angebot von **adressierter Werbung im TV-Programm (*Addressable TV*)**. Auf Basis des HbbTV-Standards kann (unabhängig vom Endgerät) auf den konkreten Nutzer/Haushalt abgestimmte Werbung in das lineare TV-Programm eingespielt werden – als Teilüberblendung des Programms beim Umschalten („SwitchIn“) oder (bei Geräten mit neuerem HbbTV-Standard) durch Überblenden eines klassischen linearen TV Spots. Bei einem Anklicken der Werbung durch den Nutzer kann dieser auf eine Website des Werbetreibenden weitergeleitet werden.

Es werden von den Vermarktungsgesellschaften der HbbTV-Sender verschiedene Möglichkeiten des *Targeting* angeboten: Bestimmte Geräte können mit technischem *Targeting* angesprochen werden. Mit einem IP-basierten *Targeting* kann Werbung in bestimmten Regionen oder Städten ausgespielt werden. In einem Beispielsfall ermöglichte dies den Instituten der Volksbanken/Raiffeisenbanken-Gruppe, eigenständig Werbespots mit eigenem Logo nur im jeweiligen regionalen

---

[68] Vgl. die Darstellung bei dem Werbevermarkter *Goldbach*, abzurufen unter https://goldbach.com/de/de/advertiser/smart-tv/samsung-ads.

Geschäftsgebiet auszuspielen.[69] Mit einem *TV Spot Re-Targeting* können Zuschauer gezielt angesprochen werden, die einen linearen Werbespot gesehen oder gerade nicht gesehen haben. Mit *Audience-Targeting* (in Verbindung mit AGF/GFK-Paneldaten[70]) oder *Behavioral targeting* (Cookie-basiert) können gezielt bestimmte Zuschauergruppen angesprochen werden (Familien, Senioren, weibliche Singles etc.).[71] Um eine „personalisierte Ansprache" zu ermöglichen, kann auch eine Zusammenführung mit pseudonymisierten Daten aus anderen Quellen erfolgen.[72]

Mittlerweise besteht sogar die Möglichkeit, bestimmte Elemente einer Fernsehsendung mit Werbung zu überblenden. So kann etwa die Bandenwerbung bei Sportübertragungen auf bestimmte Zuschauergruppen zugeschnitten werden, was insbesondere bei der Vermarktung von Live-Übertragungen von Fußballspielen auf verschiedenen internationalen Märkten bereits genutzt wird.[73]

---

69 Vgl. *smartclip,* smartclip und VR-NetWorld ermöglichen Addressable TV-Display-Werbung für alle Volksbanken Raiffeisenbanken in Deutschland, Pressemitteilung von *smartclip* vom 28.10.2019, abrufbar unter https://www.smartclip.com/de/node/972.

70 Mit dem Fernsehpanel wird die Fernsehnutzung eines repräsentativen Panels von über 5.000 Haushalten tagesaktuell elektronisch erfasst und durch eine jährliche schriftliche Strukturerhebung ergänzt, vgl. https://www.agf.de/forschung/methode/fernsehpanel/.

71 Vgl. Präsentation „Basisinformationen (Markt, Nutzung und Werbeprodukte)" der (*SevenOne Media*, März 2020), abrufbar unter https://www.sevenonemedia.de/addressable-tv/basisinformation.

72 Vgl. *smartclip*, Personalisierte TV-Werbung: smartclip und AZ Direct bieten datenschutzkonforme Daten, Know-how und Technologie für Addressable TV in Echtzeit, Pressemitteilung von *smartclip* vom 30.01.2019, abrufbar unter https://www.smartclip.com/news-media/personalisierte-tv-werbung-smartclip-und-az-direct-bieten-datenschutzkonforme-daten-know.

73 S. etwa *Positive Reaktionen auf die virtuelle Bande* (bvb.de, nicht datiert), abrufbar unter https://www.bvb.de/News/Uebersicht/Positive-Reaktionen-auf-virtuelle-Bande; *Man United and others to take perimeter boards to the next level through AR* (digitalsport.co, 26.09.2017), abrufbar unter https://digitalsport.co/man-united-and-others-to-take-perimeter-boards-to-the-next-level-through-ar; Webseite des Anbieters ADI: https://www.adi.tv/sales/markets/sport (im Abschnitt *Virtual Hybrid digiBOARD*).

Abbildung 4: Addressable TV ermöglicht individuelle Werbeansprache[74]

c) Crossmediale Werbung

Jenseits des Smart-TVs selbst können die Daten aus dem Nutzungsverhalten auch für adressierte Werbung auf anderen digitalen Geräten, d. h. Smartphone, Tablet oder Desktop („second screen“) genutzt werden. Dies ist attraktiv, weil ein hoher Anteil der TV-Zuschauer heute parallel im Internet surft.[75]

So erstellt *Samba TV* mittels der automatisierten Inhaltserkennung Zielgruppen auf Basis der Interessen (etwa „Fußballfan“ oder „Nutzer von Streamingdiensten“) und nutzt diese zur passgenauen Werbeansprache auf anderen Geräten. Die Zuordnung der anderen Geräte erfolgt dabei über das WLAN, in dem häufig neben dem Fernseher auch Smartphone oder Tablet angemeldet sind. Mit dieser Verbindung können dann z. B. TV-Kampagnen komplementiert werden, etwa mit einem *Re-Targeting* auf einen TV-Spot, den ein Nutzer gesehen oder gerade nicht gesehen hat.[76]

---

74 Bildnachweis/Quelle: *Experian*, White Paper Addressable TV, S. 9, abrufbar unter https://www.experian.com/assets/marketing-services/white-papers/audience-iq-addressable-tv-wp.pdf.

75 Laut einer *forsa*-Umfrage surften im Jahr 2019 In Deutschland 42 % der 14- bis 49-Jährigen während des Fernsehens häufig parallel im Internet, 18 % manchmal, 16 % selten; Quelle: *SevenOne Media*, Media Activity Guide 2019 – Trends in der Mediennutzung, S. 33, abrufbar unter https://indd.adobe.com/view/38e7b77a-ef71-4562-9d73-e5e9ab0f15ca.

76 Interview mit *Carsten Schüler*, Managing Director Germany in (ADZINE – Magazin für Online Marketing, 26.11.2019), abrufbar unter https://www.adzine.de/2019/11/targeting-mit-tv-nutzungsdaten-smart-tvs-als-bruecke-ins-digitale/https://www.adzine.de/2019/11/Targeting-mit-tv-nutzungsdaten-smart-tvs-als-bruecke-ins-digitale/.

Auch der Anbieter *Inscape* weist in seiner Datenschutzerklärung darauf hin, dass die Daten aus dem Anzeigeverlauf von Dritten nicht nur für Werbung auf dem Bildschirm des Smart-TVs sondern auch für Werbung auf anderen digitalen Geräten mit derselben IP-Adresse verwendet werden können.[77]

Die Werbung auf Drittgeräten kann auch mit adressierter TV-Werbung kombiniert werden. So haben Vermarkter der Fernsehsender zumindest in Einzelprojekten bereits mittels einer sogenannten „Cross-Device-Bridge" adressierte Fernsehwerbung mit Video- oder Displaywerbung auf weiteren Geräten im Haushalt ergänzt.[78]

Diese Beispiele zeigen, dass durchaus erhebliche wirtschaftliche Anreize zu einer umfassenden Erhebung von Nutzerdaten bestehen und die Datenschutzerklärungen der Hersteller oder mit ihnen kooperierender Drittanbieter vielfach bereits Bestimmungen auch für die Erfassung des TV-Nutzungsverhaltens vorsehen.

Zusammenfassung

Smart-TVs bieten vielfältige technische Möglichkeiten, die es Unternehmen erlauben, das Verhalten des Nutzers nachzuvollziehen. So können etwa die Fernsehvorlieben einer Person, ihre App-Nutzung, ihr Surf- und/oder ihr Klickverhalten erfasst werden. Je nach Fernseher können auch Internetsuchen ausgewertet oder gar biometrische Daten wie Stimme oder Cursorbewegungen erhoben werden. Diese Daten lassen sich mit anderweitig bereits vorhandenen oder öffentlich verfügbaren personenbezogenen Daten zusammenführen. Dies kann insbesondere anhand eindeutiger geräte- oder nutzerbezogener Identifikatoren oder Cookies geschehen. Beim Login in ein Nutzerkonto ist die Identifizierung einer Person besonders einfach und ermöglicht die Erweiterung eines Profils um Daten, die der Nutzer selbst über sich preisgibt sowie um Daten aus Drittquellen, die z. B. ebenfalls den Nutzernamen enthalten.

Wirtschaftlich gesehen besteht ein starker Anreiz, die gesammelten Nutzerdaten (auch) für Werbezwecke zu verwenden, da so beim Werbungsempfänger eine erhöhte Aufmerksamkeit und entsprechend höhere Umsätze erreicht werden können. Je mehr werberelevante Daten über eine

77 Inscape, Datenschutzerklärung, Version vom April 2018, bis Ende März 2020 abrufbar unter https://www.inscapedata.eu/deutsche/datenschutz-bestimmungen; seit Anfang April 2020 Website nicht mehr erreichbar.

78 Vgl. *SevenOne Media*, HaushaltsTargeting-Premiere: SevenOne Media und PREX lassen für ING die Gattungsgrenzen zwischen TV und Digital verschwinden, Pressemitteilung *von SevenOne Media* vom 04.12.2018, abrufbar unter https://www.sevenonemedia.de/documents/924471/1130000/18-12-04_PM_Haushaltstargeting_ING_PREX/967e3fbe-4c0d-a991-8374-61c7fb341000.

Person vorliegen (z. B. Interessen, Alter, Einkommen), desto lukrativer wird sie für die Werbewirtschaft, da sie sich Werbezielgruppen besser zuordnen lässt und auch für eine größere Anzahl maßgeschneiderter Werbekampagnen in Betracht kommt.

Der Werbungsempfänger erhält so „passgenauere“ und für ihn mutmaßlich interessantere Werbung. Der Preis hierfür ist die Bildung immer genauerer Nutzerprofile, die den Einzelnen und sein Umfeld zunehmend berechenbar machen. Da ein großer Teil der Nutzer in Deutschland Vorbehalte gegen personalisierte Werbung hat[79], ist es besonders wichtig, dass über die Verarbeitung personenbezogener Daten transparent informiert wird und die realistische Möglichkeit besteht, die Verarbeitung personenbezogener Daten zu vermeiden oder jedenfalls zu minimieren. Maßstab hierfür sind insbesondere die einschlägigen Vorschriften der DSGVO, des UWG und des BGB, deren Einhaltung in dem vorliegenden Bericht beleuchtet wird.

E. Verbraucherrechtliche Problemfelder

Nachfolgend wird zunächst dargestellt, welcher rechtliche Rahmen beim Umgang mit Nutzerdaten vom Smart-TV-Anbieter zu beachten ist (dazu unten I.). Anschließend werden die Themen vertieft behandelt, die das Bundeskartellamt in diesem Zusammenhang aus Verbrauchersicht als vorrangig identifiziert hat (dazu unten II. bis VIII.). Im Einzelnen zählen dazu die Frage einer hinreichend klaren und transparenten Information der Verbraucher über die bei der Nutzung des Smart-TVs verarbeiteten Daten, der Zeitpunkt dieser Information, die Rechtmäßigkeit der Datenverarbeitung mittels Smart-TVs, die Binnenorganisation der Smart-TV-Anbieter in Datenschutzfragen, die Nachhaltigkeit der Produktpflege sowie sonstige Problemfelder wie etwa unaufgeforderte Werbeeinblendungen oder unzulässige Haftungsfreizeichnungen.

I. Der rechtliche Rahmen

Smart-TV-Hersteller stehen nicht anders als App-Anbieter, Online-Dienste und viele andere Akteure in der Pflicht, Verbraucherrechte beim Umgang mit den Nutzerdaten zu achten. Für die rechtliche Beurteilung entsprechender Fallkonstellationen stellt sich immer die Frage, ob die DSGVO Anwendung findet (dazu unter 1.). Weitere Verbraucherrechtsnormen, die von den Smart-TV-Anbietern in einzelnen Sachverhaltskonstellationen einzuhalten sind, sind dem Lauterkeitsrecht sowie dem bürgerlichen Recht zu entnehmen (dazu unter 2. und 3.).

---

79 Im Rahmen einer auf Deutschland bezogenen *PricewaterhouseCoopers*-Studie gaben 76 % der befragten Personen an, sie befürchteten, dass ihre gesammelten Daten bei personalisierter Werbung in falsche Hände geraten könnten, S. *PwC*, Personalisierte Werbung und E-Privacy – Bevölkerungsbefragung zu personalisierter Werbung, März 2019, S. 22; abrufbar unter https://www.pwc.de/de/technologie-medien-und-telekommunikation/bevoelkerungsbefragung-personalisierte-werbung.pdf.

1. Datenschutzgrundverordnung

Seit dem 25. Mai 2018 findet die DSGVO in Deutschland und der gesamten Europäischen Union Anwendung. Die DSGVO ist aktuell das für die Einordnung von Datenschutzverstößen mit Abstand wichtigste Regelwerk und bildet auch in den nachfolgenden Ausführungen den wesentlichen Prüfmaßstab in Datenschutzfragen.

Entscheidend für die Anwendbarkeit der DSGVO ist die „Verarbeitung" sog. „personenbezogener Daten". „Personenbezogene Daten" sind gem. Art. 4 Nr.1 DSGVO

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind".

Dabei genügt es bereits, wenn sich ein Datum potentiell einer natürlichen Person zuordnen lässt. Diese Person muss also nicht bestimmt sein; eine Bestimmbarkeit reicht aus. Eine Bestimmbarkeit ist auch dann zu bejahen, wenn sich ein Datum erst zu einem späteren Zeitpunkt einer Person zuzuordnen lässt, etwa aufgrund einer Zusammenführung mit anderen Daten.[80]

Eine **„Verarbeitung"** stellt gem. Art. 4 Nr. 2 DSGVO

> „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"

dar.

---

80 *Specht-Riemenschneider* weist in diesem Zusammenhang richtigerweise darauf hin, dass auch mutmaßlich belanglose Daten kombiniert mit anderen die Aussagekraft eines Persönlichkeitsprofils erhöhen, s. *Specht-Riemenschneider*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73, 77.

Bei IoT-Geräten ist die Schwelle der Verarbeitung personenbezogener Daten meist schnell erreicht. Hierfür genügt i. d. R. bereits die Übermittlung einer IP-Adresse.[81] Zudem werden regelmäßig Geräte- oder Personen-IDs übermittelt (s. dazu D. IV. 1. a), S. 33).

2. Gesetz gegen den unlauteren Wettbewerb

Die datenbezogenen Praktiken der Smart-TV-Anbieter müssen sich zudem an den Regeln des Gesetzes gegen den unlauteren Wettbewerb (UWG) messen lassen. Beim Absatz der Geräte und der späteren Verwendung der gesammelten Nutzerdaten kommen die Anbieter immer wieder in Situationen, in denen ihr Verhalten gegenüber den Nutzern als „geschäftliche Handlung“ im Sinne von § 2 Abs. 1 Nr. 1 UWG anzusehen ist. Dies ist vielfach der Fall, weil und soweit der Hersteller in direkter Beziehung zum Verbraucher steht, etwa als Betreiber eines Smart-TV-Portals bzw. App-Stores (siehe dazu E. V. 3. a) cc), S. 153) oder als Verantwortlicher für Werbung auf der Benutzeroberfläche des Smart-TVs (s. dazu E. VIII. 1., S. 212). Adressaten des UWG dürfen den Verbraucher nicht durch geschäftliche Handlungen – sei es aktives Tun oder Unterlassen – in die Irre führen (§§ 5, 5a UWG). Auch sind unzumutbare Belästigungen des Verbrauchers, die insbesondere durch unerwünschte Werbung geschehen können, unzulässig (§ 7 UWG). Denkbar sind auch Verstöße gegen die Verbrauchergeneralklausel des § 3 Abs. 2 UWG. Schließlich können Verletzungen bestimmter Normen außerhalb des UWG dem Rechtsbruch-Tatbestand des § 3a UWG unterfallen.

3. Einschlägige Vorschriften aus dem bürgerlichen Recht

Nicht zuletzt sind von den Smart-TV-Anbietern beim Umgang mit den Nutzerdaten auch eine Reihe von Bestimmungen des bürgerlichen Rechts einzuhalten. Zu nennen sind hier insbesondere die Vorschriften über allgemeine Geschäftsbedingungen der §§ 307 ff. BGB, das Gewährleistungsrecht (§ 434 ff. BGB) und Garantien (§ 479 BGB).

II. Transparente Verbraucherinformation

Angesichts der beschriebenen Anreize und Möglichkeiten einer umfänglichen Datenverarbeitung bei der Nutzung von Smart-TVs stellt sich die Frage, inwieweit die Rechte und Interessen der Verbraucher in der Praxis gewahrt werden. Eine zentrale Bedeutung kommt dabei dem Erfordernis einer transparenten Verbraucherinformation zu.

---

81 Da zumindest auch statische IP-Adressen übermittelt werden, spielt auch der Streit keine Rolle, ob es sich bei dynamischen IP-Adressen um personenbezogene Daten handelt.

Um den wirtschaftlichen Akteuren Spielraum zu belassen oder auch, um eine sich als zu starr erweisende Regulierung zu vermeiden, hat sich die Aufklärung des Verbrauchers als ein weit verbreitetes Konzept des Verbraucherschutzes etabliert.[82] Verbote, die sich im Einzelfall als zu unflexibel erweisen können, sind entbehrlich, soweit der Verbraucher souverän entscheiden kann, welchen Regeln seiner Vertragspartner er sich zu unterwerfen bereit ist und welchen nicht.

Gerade das Datenschutzrecht und das AGB-Recht stellen in weiten Teilen auf Kenntnisnahme oder Einwilligungen durch das jeweilige Gegenüber ab. Grundvoraussetzung ist dabei jeweils, dass der Betroffene eine Entscheidung in Ansehung aller wesentlichen Umstände trifft (siehe dazu E. V. 1. c) bb), S. 130).

Abbildung 5: Auf der Suche nach den wirklich relevanten Informationen[83]

1. Transparenz und *Privacy Paradox*

Mit der immer wichtigeren Rolle des Internets und der immer stärkeren Verrechtlichung vieler Bereiche wird der Verbraucher immer häufiger mit umfangreichen Geschäfts- oder Datenschutzbestimmungen konfrontiert. Dabei fällt auf, dass Verbraucher in Umfragen regelmäßig ein starkes Bedürfnis nach Privatsphäre ausdrücken, mit ihren privaten Daten in der Praxis aber sorglos umgehen. Dieser Widerspruch wird als *Privacy Paradox* bezeichnet. Einer Studie des Sinus-Instituts

---

82 Kritisch hierzu *Ben-Shahar* und *Schneider*, die den Ansatz für verfehlt halten, Unternehmen zur Offenlegung aller möglichen Verbraucherinformationen zu verpflichten, S. *Ben-Shahar / Schneider*, The Failure of Mandated Disclosure, University of Pennsylvania Law Review 159 (2011), S. 647 ff., abrufbar unter https://www.law.upenn.edu/journals/lawreview/articles/volume159/issue3/BenShahar-Schneider159U.Pa.L.Rev.647(2011).pdf.

83 Bildnachweis*: powerofforever/gettyimages*.

zufolge ist 93% der Deutschen der Schutz ihrer persönlichen Daten wichtig. Nur 1 % der Befragten war es überhaupt nicht wichtig, was mit ihren persönlichen Daten geschieht.[84] Gleichzeitig hat eine Studie der *Bitkom* aus dem Jahr 2018 ergeben, dass *WhatsApp* von 81% der Internetnutzer in Deutschland genutzt wird und damit der beliebteste Messengerdienst ist. Der als datenschutzfreundlicher angesehene Messengerdienst *Telegram* wird hingegen nur von 7% der Internetnutzer verwendet. *Threema*, ein Messengerdienst, der ganz ohne Angabe persönlicher Daten genutzt werden kann, kommt sogar lediglich auf einen Anteil von 4%.[85] Auch zahlreiche wissenschaftliche Studien weisen das *Privacy Paradox* nach.[86] Es ließe sich daher argumentieren, dass der Transparenz von Datenflüssen aufgrund des sorglosen Umgangs der Verbraucher mit ihren Daten keine wesentliche Bedeutung zukommt.

Im aktuellen wissenschaftlichen Diskurs findet sich indessen eine Vielzahl von (verhaltens-)ökonomischen Theorien, die das *Privacy Paradox* erklären können.[87] Ein wesentlicher Teil dieser Theorien beruht auf der Annahme, dass die Verbraucher die Entscheidung über die Preisgabe persönlicher Daten auf Basis einer Kosten-Nutzen-Analyse treffen. Diesen theoretischen Modellen gemeinsam ist, dass aus Verbrauchersicht am Ende der Kosten-Nutzen-Analyse (teilweise als „privacy calculus“ bezeichnet) die Vorteile der Datenpreisgabe die Risiken für die Privatsphäre überwiegen. Dafür, dass aus Verbrauchersicht sehr häufig die Vorteile der Datenpreisgabe zu überwiegen scheinen, gibt es wiederum verschiedene Erklärungsansätze: Im Gegensatz zu einer rein rationalen Kosten-Nutzen-Analyse, die nach objektiven Kriterien eine Nutzenmaximierung

---

84 *Sinus Institut/YouGov*, Studie zu Datenschutz: Mehrheit der Deutschen zweifelt an Datensicherheit (2018), abrufbar unter https://www.sinus-institut.de/veroeffentlichungen/meldungen/detail/news/ studie-zu-datenschutz-mehrheit-der-deutschen-zweifelt-an-datensicherheit/news-a/show/news-c/NewsItem/ .

85 *Bitkom*, Neun von zehn Internetnutzern verwenden Messenger (bitkom.org, 02.05.2018), abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html.

86 S. etwa *Norberg/Horne/Horne*, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 2007, 100 - 126, abrufbar unter https://onlinelibrary.wiley.com/doi/full/10.1111/j.1745-6606.2006.00070.x und *Spiekermann/Grossklags/Berendt*, E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, Proceedings of the 3rd ACM Conference on Electronic Commerce (Tampa, Florida; USA, Oct 14 – 17, 2001), EC ’01. ACM, New York, NY, USA, 38-47, abrufbar unter http://ec-wu.at/spiekermann/publications/inproceedings/E-privacy%20in%202nd%20Generation%20E-Commerce.pdf .

87 Ein Überblick findet sich bei *Barth/de Jong*, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics 2017, 1038 - 1058, abrufbar unter https://doi.org/10.1016/j.tele.2017.04.013.

anstrebt, kann die Entscheidungsfindung der Verbraucher durch verschiedene Arten von kognitiven Verzerrungen beeinflusst werden wie Zeitinkonsistenz, Verlust der Selbstkontrolle bei unmittelbarer Bedürfnisbefriedigung oder übertriebenen Optimismus. Diese Verzerrungen sind den Verbrauchern oftmals nicht bewusst, haben jedoch einen erheblichen Einfluss auf den Entscheidungsprozess. So haben verschiedene Studien gezeigt, dass Individuen kleine sofortige Gewinne gegenüber größeren zu einem späteren Zeitpunkt ausgezahlten Gewinnen bevorzugen.[88] Diese Gegenwartspräferenz kann dazu führen, dass der sofortige Nutzen einer Anwendung (App) stärker gewichtet wird als die sich möglicherweise später realisierenden Risiken der mit der Anwendung verbundenen Datenweitergabe. Hierzu trägt auch bei, dass der durchschnittliche Verbraucher im Jetztzeitpunkt weder die Dimension noch die Eintrittswahrscheinlichkeit einer Verletzung seiner Privatsphäre einschätzen kann.

Das *Privacy Paradox* lässt sich auch mit dem Konzept des sog. begrenzt rationalen Verhaltens („bounded rationality“) erklären. Dieses Konzept berücksichtigt, dass jedenfalls in komplexen Situationen Entscheidungen in der Regel unter bestimmten Einschränkungen getroffen werden müssen. Hierzu zählen insbesondere nur begrenzt verfügbare Informationen und zeitliche Zwänge. Dies führt dazu, dass Entscheidungen ohne abschließende Analyse aller Einflussfaktoren, z. B. auf der Basis von Erfahrungswerten oder Heuristiken, getroffen werden. Sie können dabei auch durch die Ausgestaltung der Entscheidungssituation, etwa die Verwendung von Voreinstellungen, beeinflusst werden.

In Rechnung zu stellen ist auch, dass Verbraucher oft auf sog. „Take-it-or-leave-it-choices“ stoßen, in denen ihre Wahlfreiheit nur darin besteht, ein Angebot – widerwillig[89] – mit unerwünschter Datenpreisgabe zu nutzen oder überhaupt nicht. Dies ist insbesondere dann problematisch, wenn ein Ausweichen auf alternative Angebote aufgrund fehlenden Wettbewerbs bei realistischer Einschätzung nicht möglich ist. Dies kann etwa der Fall sein, wenn ein Unternehmen – insbesondere aufgrund von Netzwerkeffekten – über Marktmacht verfügt. Es kann zudem ein Marktversagen vorliegen, soweit keine datenschutzfreundlichen Angebote am Markt verfügbar sind oder der Nut-

---

88 Vgl. grundlegend etwa *Thaler*, Some empirical evidence on dynamic inconsistency (Economics Letters 8 (1981), 201 – 207), abrufbar unter https://www.sciencedirect.com/science/article/pii/0165176581900677. Für den Bereich es E-Commerce vgl. *Acquisti*, Privacy in Electronic Commerce and the Economics of Immediate Gratification, abrufbar unter https://www.heinz.cmu.edu/%7Eacquisti/papers/privacy-gratification.pdf.

89 S. *Borgesius/Kruikemeier/Boerman/Helberger*, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, EDPL 2017, 1, abrufbar unter https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf.

zer das Datenschutzniveau einzelner konkurrierender Anbieter nicht oder jedenfalls nicht mit vertretbarem Aufwand in Erfahrung bringen kann.[90] Bei einer *Allensbach*-Studie aus dem Jahr 2019[91] gaben Nutzer von *WhatsApp* – also Personen, die sich bereits entschieden haben, die App trotz eventuell bestehender Bedenken zu nutzen – an, dass sie mit einigen Klauseln der *WhatsApp*-Datenschutzbestimmungen nicht einverstanden sind und diese ablehnen würden, wenn sie die Möglichkeit dazu hätten. Besonders kritisch fanden die *WhatsApp*-Nutzer dabei die folgenden Aspekte:

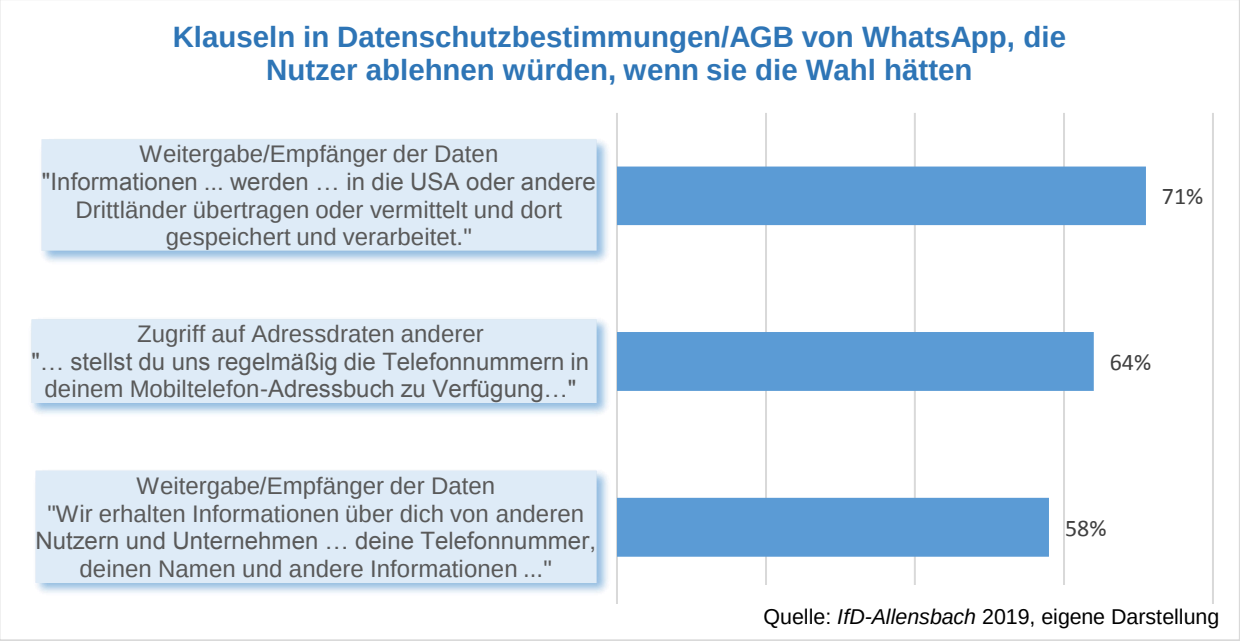


Abbildung 6: Klauseln von *WhatsApp*, die Nutzer ablehnen würden, wenn sie die Wahl hätten

Hinzu kommt, dass es dem Verbraucher unmöglich ist, die Einhaltung von Datenschutzerklärungen zu überprüfen.[92] Er kann beispielsweise nicht nachvollziehen, ob gespeicherte Daten effektiv gelöscht werden.

---

90 Vgl. *Botta/Wiedemann*, The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the *Facebook* Odyssey, The Antitrust Bulletin 2019, S. 428, 432 ff., abrufbar unter https://journals.sagepub.com/doi/pdf/10.1177/0003603X19863590.

91 *Institut für Demoskopie Allensbach*, Freiwillige und informierte Einwilligung? Die Nutzerperspektive – Untersuchung im Auftrag der *Focus Magazin Verlag GmbH*, September 2019; die Ergebnisse der Untersuchung wurden dem Bundeskartellamt freundlicherweise von der *Focus Magazin Verlag GmbH* zur Verfügung gestellt.

92 Vgl. *Arnold/Hillebrand/Waldburger*, Informed Consent in Theorie und Praxis, DuD 2015, 730, 732.

Eine amerikanische Studie kam bereits im Jahr 2008 zu dem Ergebnis, dass der durchschnittliche Nutzer allein für das einmalige Durchlesen von Datenschutzbestimmungen auf den von ihm besuchten Websites rund 40 Minuten pro Tag aufwenden müsste.[93] Es ist davon auszugehen, dass die Datenschutzbestimmungen seitdem an Umfang eher zu- als abgenommen haben – ebenso wie die online verbrachte Zeit und Anzahl genutzter Dienste und Websites. Gleichzeitig verdichten sich die Anzeichen, dass Verbraucher immer weniger bereit sind, sich mit solchen Klauselwerken eingehend auseinanderzusetzen. In einer US-amerikanischen Studie wurde festgestellt, dass 81 % der Nutzer weniger als eine Minute und 96 % der Nutzer weniger als fünf Minuten auf das Lesen der Datenschutzbestimmungen eines sozialen Netzwerks verwendeten.[94] Die Autoren der Studie hatten bei Zugrundelegung einer mittleren Lesegeschwindigkeit eine Dauer von 29 bis 32 Minuten für den Gesamttext errechnet.[95] Befragt nach dem Zeitaufwand für das Lesen von Nutzungs- und Datenschutzbestimmungen diverser populärer Internetservice-Anbieter[96], antworteten 35 - 39 % der Studienteilnehmer, sie läsen diese Texte überhaupt nicht. Die anderen gaben als Lesezeit im Durchschnitt ca. 5 Minuten an (der Median lag sogar bei nur 2 Minuten).[97]

Bei einer Studie des Forschungskonsortiums „PGuard“ im Jahr 2016 erklärten lediglich knapp 29 % der befragten Personen, sich in der Vergangenheit durch Lesen der Datenschutzbestimmungen über die Datenverarbeitung mindestens einer Webseite informiert zu haben.[98] Dieselbe Studie weist aus, dass jeweils rund 70 % der Befragten angaben, Datenschutzbestimmungen von Apps bzw. Websites seien „schwer“ oder „sehr schwer“ zu verstehen.[99]

---

93 *McDonald/Cranor*, The Cost of reading privacy policies, ISJLP 2008, 563, abrufbar unter https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1.

94 *Obar/Oeldorf-Hirsch*, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services (2018), TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016, S. 21, abrufbar unter http://dx.doi.org/10.2139/ssrn.2757465.

95 *Obar/Oeldorf-Hirsch*, a. a. O. (Fn. 94), S. 11.

96 *Facebook*, *Twitter*, *Instagram*, *Skype*, *SnapChat*, *Yik Yak*, *Xbox Live*, *iPhone Messenger*, *Gmail* und *iTunes.*

97 *Obar/Oeldorf-Hirsch*, a. a. O. (Fn. 94), S. 22.

98 *Kettner/Bolte/Heyer/Ingenrieth/Ludwig/Thorun u. a.*: Abschlussbericht PGuard, 2019, S. 26, abrufbar unter https://datenschutz-scanner.de/fileadmin/pguard/files/Abschlussbericht_PGuard_publikation.pdf.

99 *Kettner/Bolte/Heyer/Ingenrieth/Ludwig/Thorun u. a.,* a. a. O. (vorhergehende Fußnote), S. 57.

Die britische *Competition and Markets Authority* (CMA) hat 2019 in einer Studie festgestellt, dass der durchschnittliche Besuch der Datenschutzseite von *Google* 47 Sekunden dauert, wobei 85 % der Besucher weniger als 10 Sekunden und nur 0,4 % mehr als 30 Minuten dort verbringen.[100]

Die oben bereits genannte *Allensbach*-Studie[101], kommt ebenfalls zu dem Ergebnis, dass Nutzer Allgemeine Geschäftsbedingungen oder Datenschutzbestimmungen ganz überwiegend nicht lesen oder nur überfliegen:

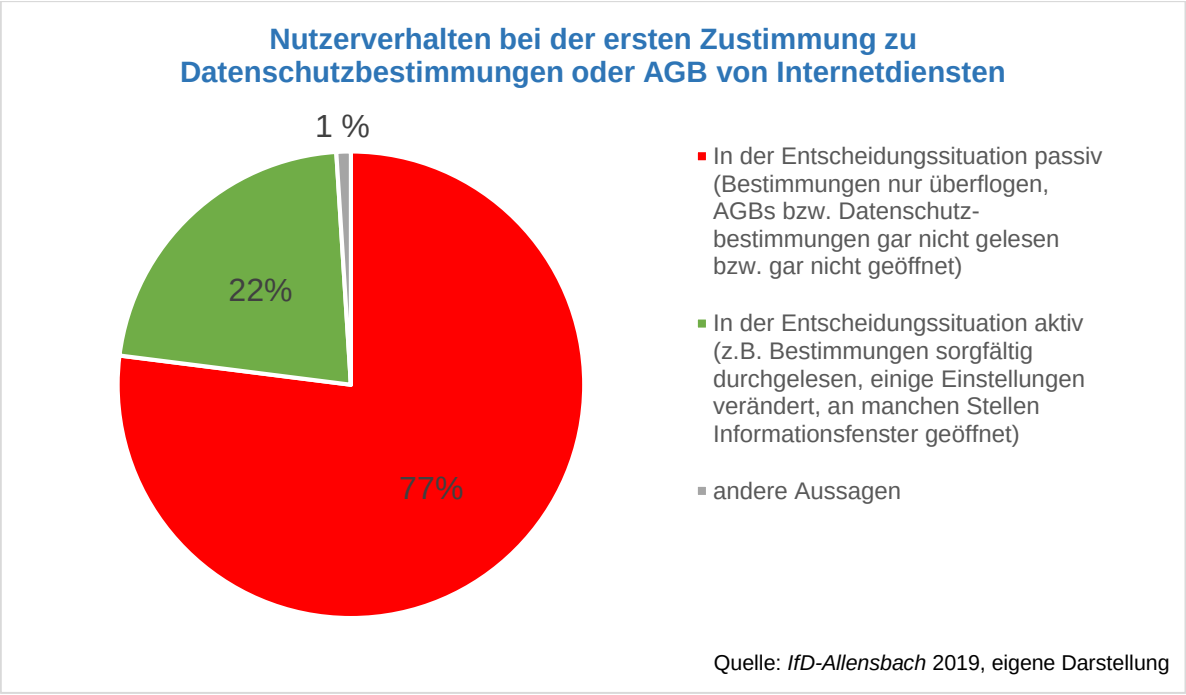


Abbildung 7: Verhalten bei der ersten Zustimmung zu Datenschutzbestimmungen/AGB

Das im Rahmen der Sektoruntersuchung vom Bundeskartellamt durchgeführte (nicht repräsentative[102]) Experiment zur Einrichtung eines Smart-TVs reiht sich in die vorgenannten Beobachtungen ein:

Die mittlere Einrichtungszeit des Smart-TVs lag bei einer Stunde und 25 Minuten[103], der Median bei einer Stunde und 16 Minuten (Minimum: 34 Minuten, Maximum: 3 Stunden und 24 Minuten).

---

100 *Competition and Markets Authority*, Online platforms and digital advertising, Market study interim report, 18.12.2019, S. 129, abzurufen unter: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#interim-report.

101 S. Fn. 91.

102 S. dazu oben, S. 26.

103 Ohne Zeiten für das Hochfahren des Geräts sowie den Sendersuchlauf und die Zeiteinstellung.

80 % der Probanden gaben an, sie hätten sich zuhause für dieselben Einrichtungsschritte weniger Zeit genommen, nämlich durchschnittlich nur rund 48 Minuten. Ihre Einrichtungszeit während des Experiments lag damit im Durchschnitt circa 75 % über der Zeit, die sie zu Hause in dieselben Einrichtungsschritte investiert hätten.

Obwohl davon auszugehen ist, dass die Beschäftigten des Bundeskartellamts berufsbedingt häufiger komplexe Texte lesen als der Bevölkerungsdurchschnitt, sich die Teilnehmer während des Experiments mehr Zeit für die Ersteinrichtung nahmen als unter gewöhnlichen Umständen[104] und sie ausdrücklich angewiesen worden waren, sämtliche Nutzungsbedingungen und Datenschutzbestimmungen zu lesen, entdeckte nur ein Viertel der Probanden alle datenschutzrelevanten Einstellungsmöglichkeiten im Verlauf der Ersteinrichtung. Zudem konnten sich die meisten Probanden (90%) nicht korrekt daran erinnern, welche Daten *Google* während der Nutzung des Smart-TVs erhebt und zu welchen Zwecken nach der Zustimmung des Probanden verarbeiten durfte. Die Zielvorgabe, das Gerät datensparsam einzurichten, setzten 35 % der Probanden nicht um.

Die Probanden hatten die Möglichkeit, im Fragebogen Anmerkungen zur Ersteinrichtung des Smart-TVs zu notieren, wovon 70% Gebrauch machten. In den Anmerkungen wurden hauptsächlich die Bedienfreundlichkeit des Smart-TVs während der Ersteinrichtung, die Verständlichkeit einzelner Datenschutzbestimmungen sowie die generelle Länge des Einrichtungsprozesses kritisiert. Mehrere Probanden merkten an, dass die Navigation, insbesondere durch die *Google*-Texte, mit der Fernbedienung „sehr mühevoll“ bzw. teilweise nicht möglich gewesen sei.

Auch über die Ausgestaltung der *Google*-Texte beschwerten sich mehrere Teilnehmer des Experiments. So sei es schwer, den Gesamtüberblick zu behalten, da wesentliche Zusatzinformationen nur über weiterführende Klicks erreichbar seien. Dem Leser sei oftmals unklar, wo im Text er sich gerade befinde. Durch diese Struktur sinke die Bereitschaft, weitere Informationen aufzunehmen. Zudem suggerierten die *Google*-Texte, dass ein Nutzer mit *Google*-Konto mehr Einfluss auf Wahrung seiner Rechte habe als Nutzer ohne Konto. Letztere seien, so der Eindruck, den Vorgaben von *Google* „schutzlos ausgeliefert“.

Ferner beanstandeten mehrere Probanden die Länge der einzelnen Datenschutzbestimmungen und Nutzungsbedingungen. Aufgrund der Länge und Komplexität der Texte sei es schwer, die Konzentration während der Ersteinrichtung aufrecht zu erhalten.

Die Ergebnisse des Experiments und der o. g. Studien zeigen, dass es Verbrauchern schwerfällt, alle Informationen aufzunehmen, die für eine informierte Entscheidung in Datenschutzsachver-

104 Das arithmetische Mittel der Vergleichszeit betrug eine Stunde und 5 Minuten.

halten benötigt werden. Die Kosten für eine adäquate Risikoanalyse (Lesen aller Datenschutzbestimmungen) können vom Verbraucher als so hoch bewertet werden, dass er die Datenschutzbestimmungen nicht oder nicht in Gänze liest. Dieses Verhalten ist auch keinesfalls irrational.[105] Zum einen gibt es Hinweise, dass die meisten Verbraucher die ihnen präsentierten Datenschutzbestimmungen schlicht nicht verstehen.[106] Zum anderen können Verbraucher in einer Vielzahl von Fällen die Übermittlung personenbezogener Daten faktisch nicht oder nur geringfügig beeinflussen oder sie haben jedenfalls nicht das Gefühl, sie könnten durch eigene Entscheidungen ihre Privatsphäre spürbar besser schützen[107]. Manche Autoren sprechen in diesem Zusammenhang von einer Resignationshaltung des Verbrauchers („privacy cynicism“).[108] Diese Sichtweise wird von den Ergebnissen der o. g. *Allensbach*-Studie bestätigt, der zufolge 77 % der Nutzer keine Alternative zur Zustimmung zu Datenschutzbestimmungen bzw. AGB sehen. Im Einzelnen äußerten die Studienteilnehmer folgende Ansichten:

---

105 *Solove* bestreitet bereits die Existenz eines *Privacy Paradox*, da das tatsächliche Verhalten des Verbrauchers keinen Rückschluss auf dessen Wertschätzung von Privatheit zulasse. Es liege somit insofern auch kein Widerspruch vor, S. *Solove*, The Myth of the Privacy Paradox, GW Legal Studies Research Paper No. 2020-10, Februar 2020, abrufbar unter https://ssrn.com/abstract=3536265.

106 S. etwa *Bailey/Parsheera/Rahman/Sane*, Disclosures in privacy policies: Does “notice and consent” work?, NIPFP Working paper series No. 246 (11.12.2018), 33 f., abrufbar unter https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf.

107 S. dazu *Bandaraa, Fernandoa u. Akter*, Explicating the privacy paradox: A qualitative inquiry of online shopping consumers, Journal of Retailing and Consumer Services 2020, 1, 6, abrufbar unter https://www.sciencedirect.com/science/article/pii/S0969698919305442.

108 *Hoffmann/Lutz/Ranzini*, Privacy cynicism: A new approach to the privacy paradox, Cyberpsychology: Journal of Psychosocial Research on Cyberspace 2016, 10(4), article 7; abrufbar unter https://cyberpsychology.eu/article/download/6280/5889; ähnlich auch *Hagittai/Marwick*, “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy, International Journal of Communication 2016, 3737, 3751 ff., abrufbar unter https://ijoc.org/index.php/ijoc/article/view/4655/1738.

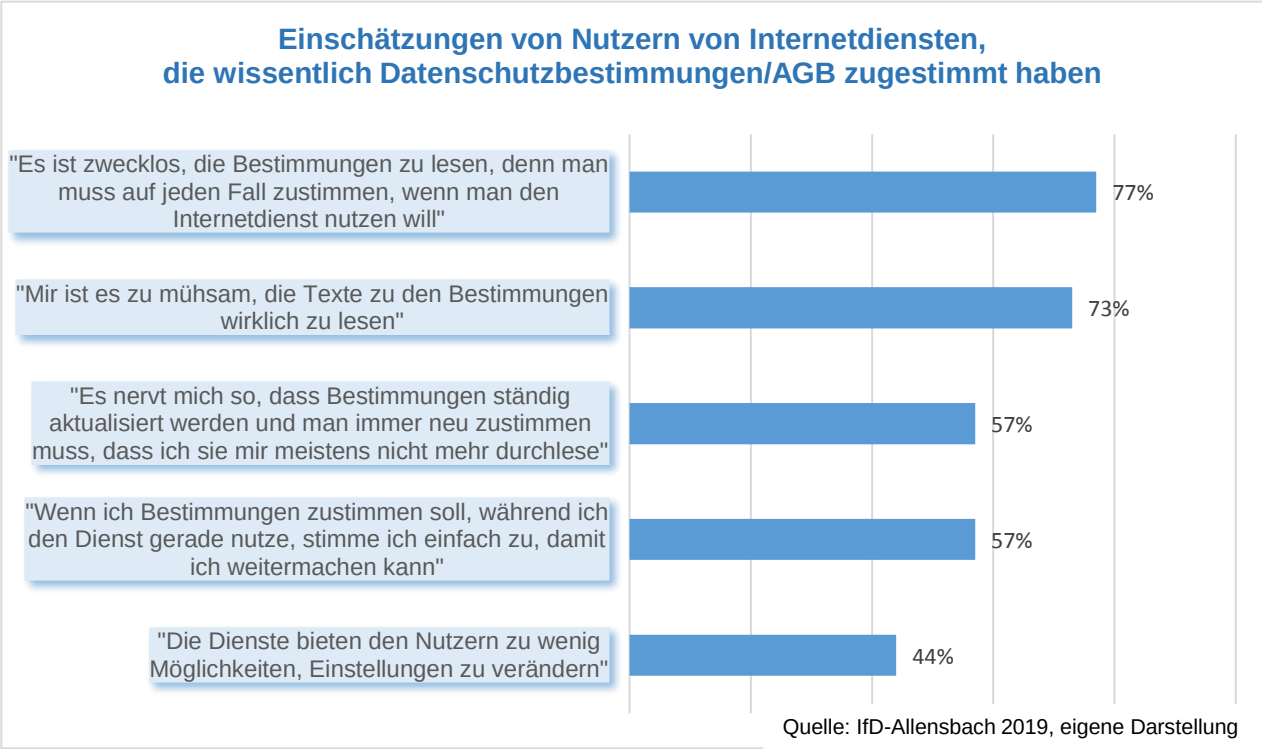


Abbildung 8: Einschätzungen von Nutzern von Internetdiensten zum Durchlesen von Datenschutzbestimmungen/AGB

Man kann somit festhalten, dass eine effektive Informationsverarbeitung durch den Verbraucher nicht einfach zu bewerkstelligen ist. Damit der Verbraucher von Datentransparenz profitiert, muss insbesondere gewährleistet sein, dass Verbraucherinformationen transparent und für den Verbraucher verständlich und schnell erfassbar sind. Dieses Leitbild zieht sich auch durch die DSGVO, deren Anforderungen nachfolgend dargestellt werden.

2. Die Transparenzanforderungen der Datenschutzgrundverordnung

Für die Sektoruntersuchung war insbesondere Art. 13 DSGVO von wesentlicher Bedeutung. Dieser sieht einerseits **Transparenz im Hinblick auf den konkreten Datenverarbeitungsvorgang** vor und fordert, dass folgende Punkte genannt werden: [109]

- der für die Datenverarbeitung datenschutzrechtlich Verantwortliche (Abs. 1 lit. a)),
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Abs. 1 lit. c)),
- die berechtigten Interessen des Verantwortlichen oder Dritter [sofern die Datenverarbeitung hierauf gestützt wird nach Art. 6 Abs. 1 UAbs. 1 lit. d) DSGVO] (Abs. 1 lit. d)),
- [bei Weitergabe von Daten] die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (Abs. 1 lit. e)),

[109] Aus Gründen der besseren Lesbarkeit erfolgt die Darstellung in geringfügig vereinfachter Form.

- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an Empfänger außerhalb der EU zu übermitteln sowie getroffener Datenschutzgarantien und der Möglichkeit, wie eine Kopie hiervon zu erhalten ist (Abs. 1 lit. f)),
- die Speicherdauer oder, falls nicht möglich, der Kriterien für die Festlegung dieser Dauer (Abs. 2 lit. a)),
- ob die Bereitstellung der personenbezogenen Daten verpflichtend ist und welche mögliche Folgen die Nichtbereitstellung hätte (Abs. 2 lit. e)).

Ferner enthält Art. 13 DSGVO eine Reihe weiterer – allgemeinerer – **Hinweispflichten** (siehe hierzu die Darstellung unter E. II. 5. ab S. 87). So muss der Verantwortliche die Kontaktdaten des Datenschutzbeauftragten nennen (Abs. 1 lit. b)) und darüber aufklären, ob eine automatisierte Entscheidungsfindung einschließlich Profiling durchgeführt wird (Abs. 2 lit. f)). Darüber hinaus muss der Verantwortliche die betroffene Person gem. Art. 13 Abs. 2 lit. b) bis d) informieren über das Bestehen der Betroffenenrechte auf

- Auskunft,
- Berichtigung,
- Löschung von Daten,
- Einschränkung der Datenverarbeitung,
- Datenübertragbarkeit,
- Widerspruch gegen die Verarbeitung,
- [falls eine Einwilligung erteilt wurde] Widerruf,
- Beschwerde bei einer Aufsichtsbehörde.

Art. 12 Abs. 1 DSGVO verlangt, dass der Verantwortliche der betroffenen Person alle nach Art. 13 DSGVO notwendigen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ übermittelt. Diese fünf Anforderungen sind nicht trennscharf voneinander abgrenzbar. Durch die kumulative Aufzählung der genannten Transparenzanforderungen stellt Art. 12 Abs. 1 DSGVO indessen sicher, dass wesentliche Transparenzvorschriften nicht nur der Form nach eingehalten, sondern effektiv umgesetzt werden.

Zwar bedeutet eine Verletzung der DSGVO-Transparenzanforderungen nicht, dass ein Datenverarbeitungsvorgang automatisch als rechtswidrig anzusehen ist.[110] Jedoch erleichtert deren Einhaltung dem Verantwortlichen beispielsweise den Nachweis, dass eine Einwilligung freiwillig

[110] S. *Albrecht/Jotzo*, Das neue Datenschutzrecht, 2017, Teil 4, Rn. 8, unter Hinweis darauf, dass Art. 6 DSGVO, der die Rechtmäßigkeit der Datenverarbeitung regelt, nicht auf Art. 13 und 14 DSGVO verweist.

erfolgt ist[111] (s. dazu E. V. 1. c) bb), S. 130). Zudem können Datenschutzbehörden entsprechende Verstöße sanktionieren und Bußgelder verhängen.[112] Zumindest theoretisch sind auch Schadensersatzforderungen Einzelner möglich.[113]

Vor diesem Hintergrund werden nachfolgend zunächst die wesentlichen Transparenzprobleme und -verstöße aufgezeigt, auf die das Bundeskartellamt im Rahmen der Sektoruntersuchung gestoßen ist.[114] Dabei wurden nicht nur die Datenschutzbestimmungen der Hersteller selbst betrachtet, sondern auch diejenigen der wesentlichen Plattformbetreiber, die ihre Dienste über die Geräte des betreffenden Herstellers anbieten.

3. Häufige Transparenzprobleme

In diesem Abschnitt werden einige zentrale Transparenzprobleme dargestellt. Die dargestellten Fälle sind im Hinblick auf die Transparenzvorgaben von Art. 12 Abs. 1 DSGVO kritisch zu sehen. Ggf. kommt auch die Verletzung anderer DSGVO-Vorschriften in Betracht.

a) Eine Datenschutzerklärung für sämtliche Dienste

Ein weit verbreitetes Phänomen ist es, dass Unternehmen für alle möglichen Anwendungen einheitliche Datenschutzbestimmungen verwenden. So schreibt etwa *Samsung* in seiner Datenschutzrichtlinie:

> „Diese Datenschutzerklärung gilt für alle Geräte und Dienste von Samsung, von Mobiltelefonen und Tablets bis hin zu TV-Geräten, Haushaltsgeräten, Onlinediensten und mehr (gemeinsam als „Dienste“ bezeichnet).“[115]

---

111 Noch weitergehend *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 26, der jedenfalls bei Einwilligungen nach Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO die Einhaltung der Transparenzpflichten als konstitutiv für die Rechtmäßigkeit der Datenerhebung erachtet.

112 Art. 83 Abs. 5 lit. d) DSGVO.

113 Art. 82 Abs. 1 DSGVO.

114 Da ein Profiling i. S. d. DSGVO jedenfalls von den Smart-TV-Herstellern offenbar ganz überwiegend nicht betrieben wird, wurde dieser Aspekt (Hinweispflicht Art. 13 Abs. 2 lit. f) DSGVO) nicht beleuchtet. Aufgrund der i. d. R. geringen Menge hinterlegter Daten spielt die Datenportabilität (Art. 13 Abs. 2 lit. b), 6. Alt. DSGVO) bei Smart-TVs keine wichtige Rolle; die Einhaltung der entsprechenden Hinweispflicht wurde daher nicht geprüft. Aufgrund geringer Relevanz wurden zudem die Klauseln zum Datenberichtigungsanspruch (Art. 13 Abs. 2 lit. b), 2. Alt. DSGVO) und zur (Nicht-)Verpflichtung zur Datenbereitstellung (Art. 13 Abs. 2 lit. e) DSGVO) nicht weiter untersucht.

115 *Samsung*, Globale Datenschutzrichtlinie.

Dieser Ansatz ist zwar verständlich, soweit Online-Dienstleistungen infrage stehen, die über mehrere Gerätearten zu erreichen sind. Für den Verbraucher wird das betreffende Regelwerk jedoch unübersichtlicher, sofern er nur ein Gerät des Anbieters nutzt und die Dienstleistungen des Anbieters für ihn nicht oder größtenteils nicht von Interesse sind. Wer *Android TV* auf seinem Fernsehgerät nutzt, muss nicht notwendigerweise auch *Google Maps, Google Mail* oder *Google Fotos* verwenden.

Bei geräte- und diensteübergreifenden Datenschutzbestimmungen kann kaum noch genau umschrieben werden, **welche Daten im Rahmen der Nutzung überhaupt verarbeitet werden**. Besonders augenfällig ist dies etwa bei *Google*:

So heißt es in den Datenschutzbestimmungen von *Google*:

> „Zu den von uns erhobenen Daten zählen eindeutige Kennungen, der Typ und die Einstellungen des Browsers, der Typ und die Einstellungen des Geräts, das Betriebssystem, Informationen zum Mobilfunknetz wie der Name des Mobilfunkanbieters und die Telefonnummer sowie die Versionsnummer der App. Wir erheben auch Daten über die Interaktion Ihrer Apps, Browser und Geräte mit unseren Diensten. Hierzu zählen u. a. die IP-Adresse, Absturzberichte, Systemaktivitäten sowie das Datum, die Uhrzeit und die Verweis-URL Ihrer Anfrage."

Aus Verbrauchersicht ist diese Formulierung unter mehreren Aspekten bedenklich. Zum einen enthält die Beispielsaufzählung Daten, die bei anderen Geräten als Smartphones nicht erhoben werden. Zum anderen ist die Aufzählung gerade bei den sensibleren Datenkategorien („Daten über die Interaktion Ihrer Apps") extrem vage. Zudem ist die Aufzählung erkennbar unvollständig formuliert („Zu den … erhobenen Daten zählen…"). Die Informationen stellen sich für den Verbraucher mithin als intransparente „Blackbox" dar.

Im Laufe der Sektoruntersuchung sind dem Bundeskartellamt auch keine Datenschutzbestimmungen bekannt geworden, bei denen der Verbraucher etwa vorab Passagen hätte hervorheben oder ein- bzw. ausblenden können, je nachdem, welche Geräte und Anwendungen er überhaupt nutzt.

b) Eine Datenschutzerklärung für alle aktuellen und künftigen Fallgestaltungen

In kaum einer der vom Bundeskartellamt untersuchten Datenschutzbestimmungen war zweifelsfrei nachvollziehbar, welches Datum auf welcher Rechtsgrundlage für welchen Zweck erhoben und wie lange gespeichert wird. Im Extremfall nannten Datenschutzbestimmungen etliche Verwendungszwecke und einen Großteil der in der DSGVO vorgesehenen Rechtsgrundlagen, ohne

diese miteinander und mit den erhobenen personenbezogenen Daten nachvollziehbar zu verknüpfen. Extrem vereinfacht lassen sich solche „one fits all"-Datenschutzbestimmungen folgendermaßen schematisch darstellen:

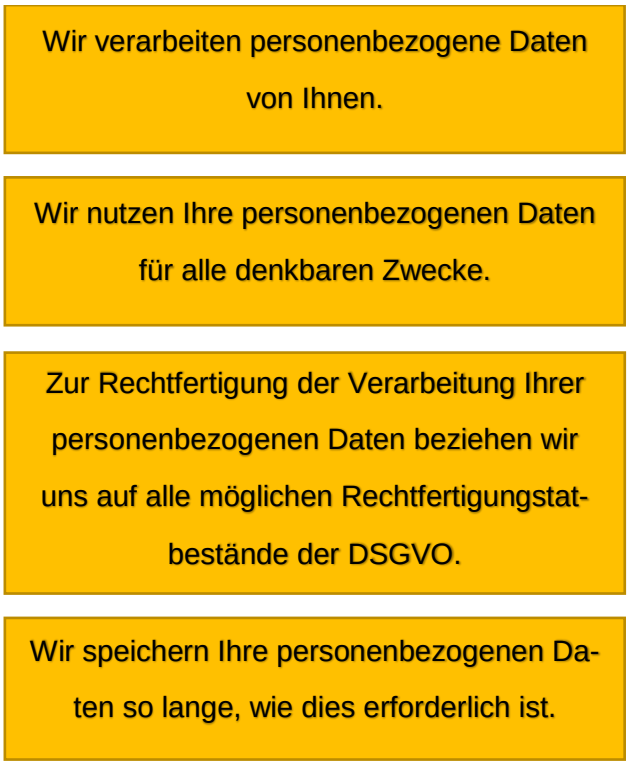


Abbildung 9: Struktur einer „one fits all"-Datenschutzerklärung

Dieses Vorgehen ist für Unternehmen sicherlich attraktiv, da es jedenfalls auf den ersten Blick sämtliche erdenklichen Fallkonstellationen der Gegenwart und Zukunft abdeckt und so scheinbar eine nachhaltige Konformität mit der DSGVO erreicht wird. Sinn und Zweck von Datenschutzbestimmungen unterscheiden sich insoweit aus Sicht von Verwender und Verbraucher fundamental.[116] Der Verbraucher kann sich keinerlei Bild davon machen, welche Daten überhaupt erhoben

116 S. hierzu *Robinson/Graux/Botterman/Valeri*, Review of the European Data Protection Directive, 2009, 29: „The evidence suggests that [the] use [of privacy policies] is predominantly targeted to meet any applicable legal transparency requirement, rather than serving a real transparency benefit towards the consumer. Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology.", abrufbar unter https://www.researchgate.net/publication/265450064_Review_of_the_European_Data_Protection_Directive – deutsche Übersetzung: „Die Indizien sprechen dafür, dass der Einsatz von Datenschutzerklärungen in erster Linie darauf abzielt, jedes einschlägige gesetzliche Transparenzkriterium zu erfüllen, anstatt dem Verbraucher einen echten Transparenzvorteil zu bieten. Datenschutzerklärungen werden von Juristen für Juristen geschrieben und nutzen der betroffenen Person aufgrund ihrer Länge, ihrer Komplexität und ihres ausufernden Gebrauchs von Rechtsbegriffen offenbar nur wenig."

werden und welche der erhobenen Daten welchem Verwendungszweck bzw. welcher Rechtsgrundlage unterfallen. Damit wird ihm jegliche Möglichkeit genommen, die Sinnhaftigkeit der Datenverarbeitung nachzuvollziehen und zu prüfen, ob eine Verwendung zu bestimmten Zwecken auf der Basis einer spezifischen Rechtsgrundlage eine rechtlich tragfähige Begründung für die Verarbeitung eines bestimmten Datums liefert. Dem Verbraucher ist möglicherweise auch nicht klar, welchen Service er eigentlich genau meiden müsste, um die Erhebung und ggf. Weiterleitung von bestimmten Daten zu verhindern oder die Datenspeicherung nur für einen für ihn akzeptablen Zweck und Zeitraum zu autorisieren. Schließlich bleibt oftmals auch im Dunklen, welche rechtlichen Möglichkeiten dem Verbraucher gegenüber dem Verantwortlichen konkret zur Verfügung stehen, etwa ein Widerruf[117] oder ein Widerspruch[118]. Macht der Verbraucher ein solches Recht geltend, kann er bei der aktuellen Ausgestaltung der meisten Datenschutzbestimmungen nicht von vornherein absehen, welche Daten von einem Widerruf oder Widerspruch überhaupt betroffen wären und welche Daten ggf. weiterhin bei dem Verantwortlichen gespeichert werden, nur eben basierend auf einer anderen Rechtsgrundlage. Die fehlende oder jedenfalls unklare Verknüpfung von verarbeitetem Datum, Zweck und Rechtsgrundlage kann daher dazu führen, den Verbraucher von einer Ausübung seiner Rechte vollständig abzuhalten.

Gegenbeispiele fanden sich in den untersuchten Datenschutzbestimmungen nur selten. TechniSat führt in seiner Datenschutzerklärung zum Punkt Geräte-Softwareupdates aus:

> „Um die Geräte-Software bereitzustellen verarbeiten wir die öffentliche IP-Adresse des Routers, DeviceID (gerätespezifische Kennung), Ländereinstellung und die interne Seriennummer (letzte einmalig pro Monat). Die interne Seriennummer und DeviceID wird ohne jegliche Verknüpfung mit anderen Daten für statistische Zwecke (wie viele Geräte eines Typs pro Monat die Geräte-Software herunterladen) gespeichert und am Monatsende, d. h. also spätestens nach fünf Wochen gelöscht. Die Rechtsgrundlage für die Speicherungen ist Art. 6 Abs. 1 Buchstabe a) (Einwilligung) der Europäischen Datenschutz-Grundverordnung."

Hier wird der Zusammenhang von Verarbeitungsprozess – betroffenen Daten – Verwendungszweck – rechtlicher Grundlage und Speicherdauer für den Nutzer nachvollziehbar erläutert.

---

117 Art. 7 Abs. 3 S. 3 DSGVO.

118 Auf das Widerspruchsrecht müsste der Verbraucher zudem gesondert hingewiesen, S. Art. 21 Abs. 4, 2. Hs. DSGVO.

c) Allgemeine Komplexität der Texte

In der bereits oben erwähnten *Allensbach*-Studie[119] beurteilten Verbraucher die ihnen vorgelegten Verbrauchertexte überwiegend als (eher) unverständlich:

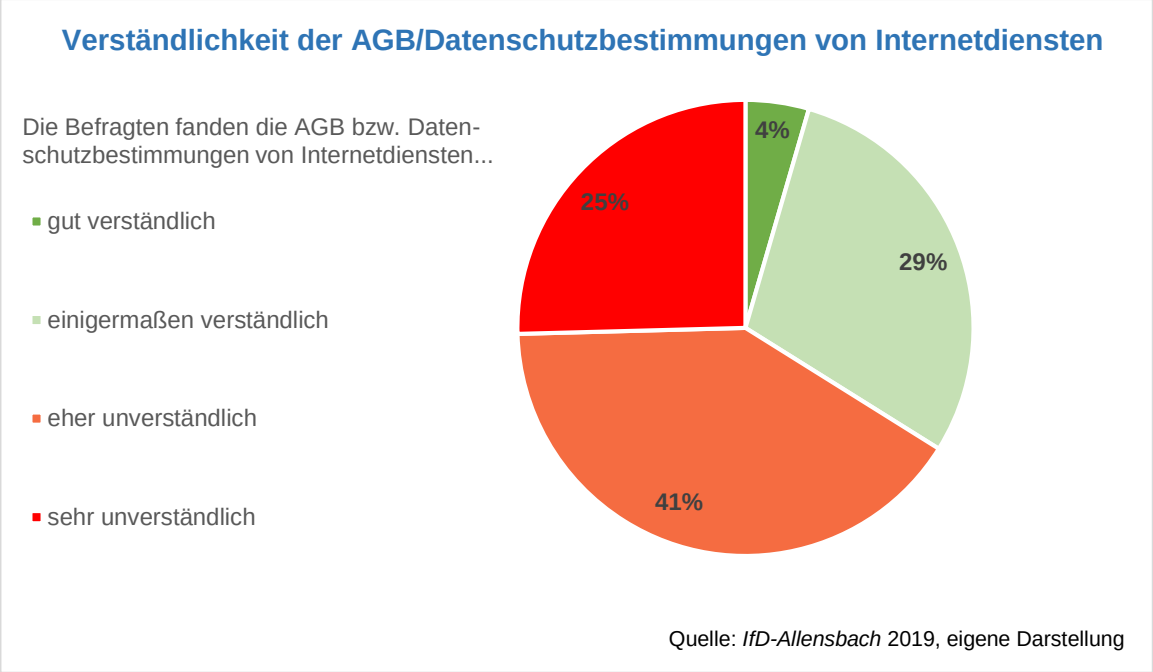


Abbildung 10:Verständlichkeit von Datenschutzbestimmungen/AGB von Internetdiensten

Die Unverständlichkeit von Datenschutzbestimmungen wird häufig angeprangert. 2019 untersuchte der Bayerische Rundfunk eine Reihe von Datenschutzbestimmungen von Onlinediensten mit einem speziellen Textanalyse-Tool. Die Analyse ergab, dass sämtliche Datenschutzbestimmungen schwerer zu lesen waren als Thomas Manns „Der Tod in Venedig“.[120] Zu einem ähnlichen Resultat gelangte eine Untersuchung der New York Times, die gleich 150 (englischsprachige) Datenschutzbestimmungen unter die Lupe nahm. Fast alle davon waren deutlich unverständlicher als englische Klassiker wie „Stolz und Vorurteil“ oder „Große Erwartungen“, einige wenige sogar schwerer zu lesen als Emmanuel Kants „Kritik der reinen Vernunft“.[121]

Es liegt auf der Hand, dass Vereinfachungen von Datenschutzbestimmungen möglich und auch geboten sind. Sicherlich ist der Satzbau häufig unnötig komplex. Auch sind Übersetzungen ins

---

119 S. Fn. 91.

120 S. *Harlan/Richt/Schnuck*, der Haken am Häkchen (web.br.de, 11.06.2019), abrufbar unter http://web.br.de/interaktiv/datenschutzerklaerungen/.

121 S. *Litman-Navarro*, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster (nytimes.com, 2019), abrufbar unter https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Deutsche nicht immer gelungen und können zu zusätzlichen Verständnisschwierigkeiten führen. Andererseits ist es in der Regel nicht möglich, Datenschutztexte durchgehend in einfacher Sprache abzufassen. Die genaue Information des Verbrauchers erfordert mitunter Fremdwörter bzw. Fachbegriffe (z. B. IP-Adresse, Server o. Ä.). Eine automatisierte Verständlichkeitsanalyse kann vor diesem Hintergrund durchaus auf Unzulänglichkeiten hinweisen, wenn Datenschutzbestimmungen einen besonders hohen Komplexitätsgrad aufweisen. Es darf aber keinesfalls der Schluss gezogen werden, dass die von einem Analysetool besser bewerteten Datenschutzbestimmungen automatisch verbraucherfreundlicher sind. Es besteht die Gefahr, dass mit einer Vereinfachung auch eine Pauschalierung einhergeht (s. dazu nachfolgend unter d)). Der Satz „Wir verarbeiten Ihre Daten“ ist zwar perfekt verständlich, aber bar jeglicher sinnvollen Information über die konkreten Datenverarbeitungsvorgänge. Auch Aussagen von Nutzern, inwieweit sie Datenschutzbestimmungen subjektiv für verständlich halten, sind nur eingeschränkt aussagekräftig. Entscheidend ist vielmehr, inwieweit Nutzer auf Basis gelesener Datenschutzbestimmungen korrekt einschätzen, welche ihrer Daten wie verarbeitet und ggf. weitergegeben werden.

Es ist daher zwar sinnvoll, auf eine Vereinfachung der Sprache von Datenschutzbestimmungen hinzuwirken, die Genauigkeit der Aussagen darf hierunter jedoch nicht leiden. Neben der sprachlichen Vereinfachung muss daher das Augenmerk auf andere Instrumente gelegt werden, um Datenschutzbestimmungen für Verbraucher leichter erfassbar zu machen (s. dazu insb. die Ausführungen in E. IV. 3., S. 104).

d) Schwammige Formulierungen

Eng verbunden mit dem Problem der „one fits all“-Datenschutzbestimmungen ist die Verwendung extrem weiter Formulierungen. So ist dem Wortlaut vieler Datenschutzbestimmungen beispielsweise nicht zu entnehmen, *welche* einzelnen personenbezogenen Daten überhaupt übertragen werden. So formuliert etwa Samsung:

> „Welche Daten erfassen wir?
>
> […]
>
> Sonstige Daten über Ihre Nutzung von Diensten, die von Ihnen verwendeten Apps, die von Ihnen besuchten Websites und die Elemente eines Dienstes, auf die Sie klicken.“[122]

[122] *Samsung*, Globale Datenschutzrichtlinie, unter *Von uns erfasste Daten – Daten über Ihre Nutzung von Diensten*.

Zum anderen finden sich sehr häufig relativierende Begriffe wie „ggf.“, „für gewöhnlich“, „teilweise oder vollständig“, „insbesondere“ oder „je nach den Umständen“. *Google* etwa schreibt in seiner Datenschutzerklärung:

> „[…] **Unter anderem könnten** folgende Aktivitätsdaten erhoben werden: […]“[123]

Dies ist nahezu eine zwingende Folge der jeweils gebündelten Darstellung verwendeter Dienste, erhobener Daten und Verwendungszwecke, ohne diese miteinander in Verbindung zu setzen. Würden für die tatsächlich infrage stehenden Dienste die erhobenen Einzeldaten, Verwendungszwecke etc. differenziert beschrieben, wären relativierende Zusätze zumeist überflüssig.

Bei der Verwendung solcher Formulierungen kann der Verbraucher sich kein zuverlässiges Bild von der erfolgenden Datenverarbeitung machen. Finden Datentransfers etwa nur statt „solange dies für den Zweck, zu dem diese gesammelt wurden, erforderlich ist“[124], kann der Nutzer nicht erkennen, ob der Verantwortliche eine konkrete Datenverarbeitung überhaupt durchführt oder nicht. Zumeist ist es ihm praktisch unmöglich herauszufinden, ob ein bestimmtes Datum bei der konkreten Nutzung des TV-Geräts verarbeitet wird und welche Zwecke bzw. welche Rechtsgrundlage hierfür einschlägig sein sollen.

Darüber hinaus kommt es auch vor, dass Betroffenenrechte verschleiert und/oder relativiert werden. Dies ist etwa der Fall, wenn in Datenschutzbestimmungen davon die Rede ist, dem Betroffenen stehe „möglicherweise“ ein bestimmtes Recht zu.

Neben einschränkenden Formulierungen finden sich in den Datenschutzbestimmungen mitunter auch unnötig komplexe Begriffe. War etwa in der *Google*-Datenschutzerklärung vom 22.01.2019 noch von der „Stimme“ des Nutzers die Rede, wurde dieser Begriff in der Datenschutzerklärung vom 31.03.2020 durch „Sprachaktivitäten“ ersetzt.

e) Überflüssige Informationen und Dopplungen

Bei vielen Datenschutzbestimmungen kommt es vor, dass dem Verbraucher völlig unnötige Informationen mitgeteilt werden. Dies kann dazu führen, dass der Informationsgehalt von Datenschutzbestimmungen stark verwässert wird.

---

123 *Google*, Datenschutzerklärung – Daten, die wir bei der Nutzung unserer Dienste erheben – Ihre Aktivitäten.

124 *LG*, Datenschutzrichtlinie, unter *4. Informations-Teilung*.

Zunächst sind überflüssige Informationen dem „one fits all"-Ansatz geschuldet (s. oben E. II. 3. a) und b), S. 58 ff.). Es kommt aber auch vor, dass Ausführungen in Datenschutzbestimmungen doppelt erscheinen. So gibt es etwa in der *Google*-Datenschutzerklärung einen Abschnitt „Daten exportieren, entfernen und löschen" sowie einen Abschnitt „Sie können Ihre Daten jederzeit exportieren oder aus Ihrem *Google*-Konto löschen". Beide enthalten z. T. identische Informationen zu Datenexport und Datenlöschung. Samsung bietet neben einer globalen Datenschutzrichtlinie ergänzende Datenschutzbestimmungen an, u. a. für die Nutzung eines *Samsung*-Smart-TVs, zu Anzeigeinformationsdiensten sowie für interessenbasierte Werbung. Die Unterscheidung nach Nutzungsprozessen ist unter Transparenzgesichtspunkten grundsätzlich zu begrüßen. Allerdings kann dies zu vielen Wiederholungen und mitunter widersprüchlichen Informationen führen.[125] Solche Dopplungen führen dazu, dass der Leser sich gezwungen sieht, die jeweiligen Regelungen auf Abweichungen hin zu überprüfen.[126] Datenschutzbestimmungen werden so zudem sehr lang. Ähnlich verhält es sich mit der Praxis einiger Unternehmen, detailliert darzulegen, wie sie mit anonymen bzw. *nicht personenbezogenen* Daten umgehen. Ein Unternehmen informierte über Widerspruchsmodalitäten, obwohl die gesamte Datenverarbeitung auf der Rechtsgrundlage der Einwilligung beruhte und das Unternehmen auch keine Direktwerbung betrieb. Ein Widerspruch war daher gar nicht möglich (sondern nur ein Widerruf der Einwilligung). Mitunter finden sich in Datenschutzbestimmungen auch Regelungen zu Datenschutzrecht in Staaten außerhalb der EU, was für den Verbraucher bestenfalls keinen Mehrwert bedeutet, schlimmstenfalls auch verwirrend wirken kann. Im strengen Sinne nicht erforderlich sind auch (teils ausschweifende) allgemeine Erklärungen von Unternehmensseite, mit den Daten der Nutzer sorgsam umzugehen.

Für den Verbraucher ist hiermit in solchen Fällen kein Informationsgewinn hinsichtlich des Schutzes seiner personenbezogenen Daten verbunden.

---

125 So enthalten beispielsweise *Samsungs* Datenschutzhinweise zu Anzeigeinformationsdiensten und die Datenschutzhinweise zu interessenbasierter Werbung jeweils Informationen zu Datentransfers in Drittstaaten und ergriffenen Sicherheitsmaßnahmen. Diese weichen von der Globalen Datenschutzrichtlinie ab, die China, Singapur, Vietnam, die Philippinen und Japan als zusätzliche Empfängerstaaten nennt. Da die Globale Datenschutzrichtlinie bei Abweichungen Vorrang genießt („Im Falle einer Abweichung von den Bestimmungen dieser Datenschutzerklärung und eines spezifischen Datenschutzhinweises haben die Bestimmungen dieser Datenschutzerklärung Vorrang.") kann der Verbraucher nicht von der Richtigkeit der in den spezifischen Datenschutzhinweisen aufgeführten Empfängerstaaten ausgehen. Positiv ist indessen *Samsungs* Ansatz, Drittländer abschließend aufzulisten; dies ist bei vielen anderen Unternehmen nicht der Fall, s. dazu unter 4. g), S. 81).

126 Vgl. hierzu – zum Fall identischer Regelungen (allerdings in unterschiedlichen Dokumenten) – LG Frankfurt, Urteil vom 10.06.2016, Az. 2-3 O 364/15, juris Rn. 303 – *VZ NRW/Samsung*.

f) Inkohärente Textgliederung

Der Verbraucher kann sich nicht darauf verlassen, dass unter einer einschlägigen Überschrift tatsächlich alle wesentlichen Informationen zu dem betreffenden Punkt aufgeführt sind. So kann es beispielsweise vorkommen, dass unter dem Abschnitt „Welche Daten wir erheben" tatsächlich *nicht* alle (Kategorien von) personenbezogenen Daten aufgeführt werden, die ein Unternehmen verarbeitet. Vielmehr können weitere verarbeitete Daten, Rechtsgrundlagen etc. in einem separaten Abschnitt zu den technischen Mitteln der Datenverarbeitung (Cookies etc.) auftauchen. Sind wesentliche in einem Sinnzusammenhang stehende Informationen innerhalb einer Erklärung an unterschiedlichen Stellen verortet, fehlt es i. d. R. an einer „leichten Zugänglichkeit", wie sie die DSGVO in Art. 12 Abs. 1 fordert.

Dass der Verbraucher Angaben nicht sinnvoll erfassen kann, kann aber auch daran liegen, dass Datenschutzinformationen unter einer unpassenden Überschrift oder in einem nicht einschlägigen Kapitel platziert werden. So informiert *Google* bei der Ersteinrichtung eines Fernsehers mit *Android TV* darüber, dass das Unternehmen Daten aus Drittquellen erheben kann, im Abschnitt „Ihre Standortdaten". Bestimmte Möglichkeiten der Einschränkung von Datenerhebungen finden sich im Abschnitt „Daten exportieren, entfernen und löschen".

Die Zugänglichkeit von Informationen kann schließlich dadurch beeinträchtigt werden, dass wesentliche Informationen nur über Verlinkungen auf externe Seiten erreichbar sind.

g) Informationen nicht auf Deutsch erhältlich

Dem Bundeskartellamt lagen zum Ende der Untersuchung Datenschutzbestimmungen der Hersteller jeweils in deutscher Sprache vor. Teilweise enthielten diese jedoch englischsprachige Passagen oder verwiesen auf englischsprachige Informationsquellen.[127]

Die DSGVO verlangt in Art. 12 Abs. 1 jedoch die Verwendung einer für den Verbraucher „verständlichen Sprache". Ob dies der Fall ist, bemisst sich am Marktortprinzip und dem intendierten Empfängerkreis.[128] Sind Datenschutzbestimmungen also auf deutsche Verbraucher ausgerichtet, so müssen sie – dem Leitbild der EuGH-Rechtsprechung folgend – für den aufmerksamen und

---

127 So verweist etwa Googles Datenschutzerklärung für Cookie-Informationen auf die Website https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?hl=en. Dort sind Informationen allerdings nur auf Englisch erhältlich. In einem ähnlichen Fall wurde ein Verweis auf einen englischsprachigen Verweis noch vor Abschluss der Sektoruntersuchung berichtigt.

128 *Paal/Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 12 DSGVO Rn. 35; *Franck* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 12 Rn. 20; *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 12 Rn. 15.

verständigen Durchschnittsverbraucher in Deutschland verständlich sein. Bei Smart-TVs handelt es sich um ein Massenprodukt für Menschen aller Bildungsniveaus. Sämtliche für den Verbraucher relevante Datenschutzbestimmungen müssen daher notwendigerweise auf Deutsch verfasst sein. Abgesehen von einer nicht unerheblichen Anzahl sprachlicher und grammatikalischer Fehler waren in diesem Zusammenhang – allerdings nur in Einzelfällen – erkennbar nachlässige Übersetzungen ins Deutsche zu beobachten, die der Verständlichkeit des Textes abträglich sein können.[129]

4. Untersuchung der Einhaltung verarbeitungsbezogener Transparenzpflichten

Das Bundeskartellamt hat untersucht, inwieweit im Hinblick auf Smart-TVs die wichtigsten Transparenzpflichten der DSGVO eingehalten werden. Zu diesem Zweck wurden die Datenschutzbestimmungen für alle Fernseherhersteller analysiert, die im Jahr 2018 einen Marktanteil (nach Stückzahlen) von mindestens 0,5 % aufwiesen. Die verwendeten Datenschutzbestimmungen decken schätzungsweise mindestens 95 % aller im Jahr 2018 verkauften Fernseher ab. Mitunter kamen die Datenschutzbestimmungen von OEM-Herstellern unverändert auch bei unter anderem Markennamen vertriebenen Geräten zum Einsatz. Des Weiteren wurden auch die Datenschutzbestimmungen von *Google* und *Foxxum* untersucht: *Google* vertreibt mit *Android TV* ein wichtiges Betriebssystem, welches z. B. auf Fernsehern der Marken *Sony*, *Philips, TCL*, *Sharp* oder *Xiaomi* Verwendung findet. *Foxxum* bietet ein webbasiertes TV-Portal an, das u. a. auf Smart-TVs von Medion und *Vestel* zum Einsatz kommt. Mit anderen Worten sind es die Betreiber der TV-Portale, die das jeweilige Gerät mit Smartfunktionen ausstatten. Es erschien daher sinnvoll, auch ihre Datenschutzerklärungen in die Analyse mit einzubeziehen. Insgesamt basieren die nachfolgend dargestellten Erkenntnisse auf der Auswertung von 14 Datenschutztexten. Dabei wurden jeweils die Datenschutzbestimmungen mit dem jüngsten Datum berücksichtigt, die dem Bundeskartellamt von den befragten Unternehmen genannt bzw. übersandt wurden. Es ist daher davon auszugehen, dass der vorliegende Bericht ein zum Publikationszeitpunkt aktuelles Lagebild liefert.

a) Umfang der Datenschutzbestimmungen

Abgesehen von der hohen Anzahl von Verbraucherinformationen verschiedener Anbieter können auch die einzelnen Regelungen sehr umfangreich ausfallen.

---

129 So handelt es sich beispielsweise bei „log information“ nicht etwa – wie in einem Fall fälschlicherweise übersetzt – um „Anmeldeinformationen“, sondern um Log-Informationen, also die Aufzeichnungsdaten unterschiedlichster Nutzungen. In einem Fall wurden die englischsprachigen Abkürzungen „EEA“ (für EWR, Europäischer Wirtschaftsraum) und „GDPR“ (für DSGVO, Datenschutz-Grundverordnung) benutzt.

aa) Ermittlungsergebnisse

Im Falle von Smart-TVs wird der Nutzer mit einer ganzen Reihe von Datenschutz- und Nutzungsbedingungen konfrontiert.[130] Das Bundeskartellamt hat getestet, wie lange Nutzer durchschnittlich für die Ersteinrichtung eines Smart-TVs brauchen, wenn sie die ihnen vorgelegten Regelungen tatsächlich durchlesen.[131] Die durchschnittliche Einrichtungszeit betrug gut eine Stunde und 25 Minuten[132], wobei 80 % der Probanden angaben, sie hätten sich zuhause für dieselben Einrichtungsschritte weniger Zeit genommen, nämlich durchschnittlich höchstens rund 48 Minuten.

Das Bundeskartellamt hat die Datenschutzbestimmungen analysiert, die die Fernsehhersteller der Nutzung ihrer jeweils drei jüngsten Modellreihen zugrunde legen. Dabei fällt bereits deren deutlich unterschiedliche Länge auf. Dies erklärt sich zum Teil dadurch, dass etwa Hersteller, deren Smart-TVs auf TV-Portale Dritter zurückgreifen, deutlich weniger Datenverarbeitungsvorgänge erläutern müssen als „integrierte“ Anbieter. Dennoch fällt insbesondere *Googles* Datenschutzerklärung mit 32 DIN-A4-Seiten[133] und über 150 anklickbaren Links zu weiterführenden Informationen aus dem Rahmen. Zu einem großen Teil handelt es sich hierbei um Begriffsdefinitionen, die für das Textverständnis durchaus hilfreich sein können. Mitunter wird jedoch auch auf andere z. T. umfangreiche *Google*-Seiten[134] verlinkt.

bb) Rechtliche Würdigung

Umfangreiche Datenschutzbestimmungen können unter zwei Gesichtspunkten problematisch sein. Zum einen können sie gegen § 305 Abs. 2 Nr. 2 BGB verstoßen, da der der Nutzer keine Möglichkeit hat, sie in zumutbarer Weise zur Kenntnis zu nehmen. Zum anderen sieht Art. 12 Abs. 1 S. 1 DSGVO vor, dass diverse Pflichtinformationen der betroffenen Person in präziser, transparenter, verständlicher und – vor allem – leicht zugänglicher Form kommuniziert werden müssen.

In dem Verfahren *Verbraucherzentrale Nordrhein-Westfalen gegen Samsung* hielt das LG Frankfurt/Main Allgemeine Geschäftsbedingungen (AGB) in Anbetracht ihres beachtlichen Umfangs

---

130 Vgl. hierzu die Ausführungen auf S. 45.

131 S. oben S. 25.

132 Ohne Zeiten für das Hochfahren des Geräts sowie den Sendersuchlauf und die Zeiteinstellung.

133 Seit 31.03.2020 in Kraft befindliche Datenschutzerklärung in pdf-Format, abrufbar unter https://www.gstatic.com/policies/privacy/pdf/20200331/acec359e/google_privacy_policy_de_eu.pdf.

134 Z. B. zur Funktionsweise und Datenverarbeitung durch *Google Analytics* (https://support.google.com/analytics/answer/6004245) oder zu Cookies (https://policies.google.com/technologies/types).

von 56 Bildschirmseiten zumindest dann für unzulässig, wenn eine Navigation im Text nicht sinnvoll möglich ist. Unter solchen Bedingungen könne nicht davon ausgegangen werden, dass der Verwender der anderen Vertragspartei die nach § 305 Abs. 2 Nr. 2 BGB erforderliche Möglichkeit verschaffe, in zumutbarer Weise vom Inhalt der AGB Kenntnis zu nehmen.[135]

Ob bzw. unter welchen Umständen Datenschutzbestimmungen als AGB anzusehen sind, ist von den Gerichten bislang nicht zweifelsfrei geklärt worden.[136] Ausgehend von § 305 Abs. 1 S. 1 BGB ist letztlich entscheidend, ob man – vom objektiven Empfängerhorizont aus betrachtet – die Datenschutzbestimmungen so auffassen muss, dass sie den Vertragsinhalt regeln sollen. Dies liegt insbesondere nahe, wenn über Datenschutzbestimmungen Einwilligungen des Verbrauchers eingeholt werden. Das KG Berlin hat es indessen auch ausreichen lassen, dass beim Verbraucher der Eindruck erweckt werde, er habe die in der Datenschutzerklärung beschriebene Praxis zu dulden, falls er die Dienstleistungen der Beklagten in Anspruch nehme. Damit gehe der Hinweis der Beklagten (*Google*) auf die in der Datenschutzerklärung beschriebene Praxis über die bloße Unterrichtung über ein tatsächliches Verhalten der Beklagten hinaus.[137] Auch wenn sich die Rechtsdogmatik mit dem Konstrukt Daten gegen (Gratis-)Dienstleistung schwertut, spricht für die Ansicht des KG Berlin, dass auch bei einer bloßen „Information“ des Verantwortlichen über Datenverarbeitungen letztlich verbindlich festgelegt wird, welchen Umfang der Datentransfer hat und welche Eingriffstiefe er für die betroffene Person bedeutet. Die Inanspruchnahme ansonsten iden-

---

135 LG Frankfurt, Urteil vom 10.06.2016, Az. 2-3 O 364/15, Rn. 214 ff. – *VZ NRW/Samsung*. In einer Entscheidung des OLG Köln wurde hingegen ein AGB-Umfang von 83 Seiten nicht *per se* als Verstoß gegen § 305 Abs. 2 BGB angesehen. Dabei hatte das Gericht betont, dass die Länge der AGB im Verhältnis zur Bedeutung des Geschäfts beurteilt werden müsse und – sinngemäß – dass die AGB flexibel am Computerbildschirm angezeigt und ohne Zeitdruck ausgiebig betrachtet werden könnten, s. OLG Köln, Urteil vom 19.02.2020, Az. 6 U 184/19, GRUR-RS 2020, 3913, Rn. 39 ff.

136 Dagegen OLG Hamburg, Beschluss vom 04.12.2014, Az. 10 U 5/11; dafür etwa KG Berlin, Urteil vom 21.03.2019, Az. 23 U 268/13, rechtskräftig nach Zurückweisung der Nichtzulassungsbeschwerde durch den BGH, Beschluss vom 23.04.2020, Az. I ZR 65/19. Die Frage, ob und inwieweit bei einer Nichteinbeziehung von als AGB eingestuften Datenschutzbestimmungen in ein Vertragsverhältnis die datenschutzrechtlichen Rechtfertigungsgründe entfallen, bedarf indessen noch der rechtsdogmatischen Klärung. Fußt die Datenverarbeitung auf einer datenschutzrechtlichen Einwilligung, so dürfte diese als Rechtsgrundlage für eine Datenverarbeitung jedenfalls ausscheiden. Für ein darüber hinausgehendes weitgehendes Entfallen der datenschutzrechtlichen Rechtsgrundlagen für die betreffenden Datenverarbeitungen *Wendehorst/Graf v. Westphalen*, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745, 3750.

137 KG Berlin, Urteil vom 21.03.2019, Az. 23 U 268/13, juris Rn. 68. Die Nutzung von Android-TV-Geräten wird gar von einer Gesamtzustimmung zu den *Google*-Nutzungsbedingungen, den *Google*-Datenschutzbestimmungen und den *Google*-Play-Nutzungsbedingungen abhängig gemacht („Akzeptieren“-Button).

tischer Leistungen kann sich für den Betroffenen somit bei einem Anbieter aufgrund der Verarbeitung von weniger personenbezogenen Daten deutlich „günstiger“ darstellen als bei dessen Wettbewerber. Datenschutzbestimmungen prägen somit regelmäßig und maßgeblich das konkrete Vertrags- und Austauschverhältnis.[138]

Ungeachtet der Frage, ob Datenschutzbestimmungen immer, unter bestimmten Voraussetzungen oder nie als AGB anzusehen sind, dürften bei der Prüfung nach AGB- bzw. Datenschutzrecht oftmals sehr ähnliche Maßstäbe heranzuziehen sein. So setzt § 305 Abs. 2 BGB voraus, dass der anderen Vertragspartei die Möglichkeit verschafft wird, die infrage stehenden Informationen „in zumutbarer Weise“ zur Kenntnis zu nehmen. Art. 13 Abs. 1 S. 1 DSGVO verlangt, dass Datenschutzangaben in „leicht zugänglicher Form“ präsentiert werden. Es ist anzunehmen, dass zur Beurteilung dieser unbestimmten Rechtsbegriffe im Wesentlichen die gleichen Kriterien herangezogen werden. Entscheidend ist demnach, dass die Mühen und Schwierigkeiten, deren es zur Kenntnisnahme der Informationen bedarf, ein gewisses dem Durchschnittskunden nach Lage des Falles zumutbares Maß nicht übersteigen dürfen.[139] Dabei ist zu berücksichtigen, dass der Aufwand der Kenntnisnahme nicht allein am Umfang eines Textes zu bemessen ist. Vielmehr sind die Gesamtumstände in den Blick zu nehmen.[140] Hier spielt etwa eine Rolle, ob sich der Text durch Hyperlinks, Suchfunktion und eine konsistente Gliederung gut erschließen lässt.[141] Die vorgenannten Aspekte ließen sich im Rahmen der Sektoruntersuchung nur in Ansätzen prüfen. Es kann jedoch festgehalten werden, dass sich die Datenschutzerklärung *Samsungs* seit dem o. g. Verfahren vor dem LG Frankfurt verändert hat und zumindest einige Kritikpunkte des Gerichts offenbar berücksichtigt wurden. Die Möglichkeit der Kenntnisnahme der Bestimmungen hat sich somit verbessert.[142]

Gewisse Zweifel bestehen indessen an einer leichten Zugänglichkeit der Datenschutzbestimmungen von *Google*. Hier fällt nicht nur deren Länge ins Gewicht, sondern auch, dass das Dokument selbst auf zahlreiche, mitunter umfangreiche ergänzende Texte verlinkt und Informationen nicht

---

138 Vgl. etwa *Wendehorst/Graf v. Westphalen*, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745, 3748, die die Einschlägigkeit des AGB-Rechts jedoch davon abhängig machen wollen, dass eine „kommerzielle Nutzung“ personenbezogener Daten über den (eng verstandenen) Vertragszweck hinaus erfolgt.

139 *Basedow* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, § 305 BGB Rn. 78.

140 LG Frankfurt, Urteil vom 10.06.2016, Az. 2-3 O 364/15 – *VZ NRW/Samsung*, Rn. 223.

141 LG Frankfurt, a. a. O. (vorhergehende Fußnote), Rn. 223.

142 Ein Urteil über den Inhalt der Datenschutzbestimmungen ist hiermit naturgemäß nicht verbunden.

ohne Weiteres auffindbar sind.[143] Hinzu kommt, dass die Navigation im Dokument mit einer TV-Fernbedienung erheblich umständlicher ist als etwa mit einer Maus, wodurch auch das Scrollen und Anklicken von Links deutlich erschwert wird.

b) Angabe der von Datenerhebung betroffenen Daten

Betroffene Personen haben nach Art. 15 Abs. 1, 2. Hs. DSGVO ein Recht auf Auskunft darüber, welche sie betreffenden personenbezogenen Daten verarbeitet werden. Die DSGVO selbst enthält indessen keine Vorschrift, die zwingend vorsieht, dass die jeweils erhobenen Daten in Datenschutzbestimmungen konkret benannt werden müssen. Es ergibt sich aber aus Sinn und Zweck etlicher DSGVO-Normen. Deren Einhaltung kann nämlich nur dann sinnvoll beurteilt werden, wenn der Verbraucher überhaupt nachvollziehen kann, welche Daten er preisgibt.

aa) Ermittlungsergebnisse

Welche personenbezogenen Daten konkret verarbeitet wurden, war den analysierten Datenschutzbestimmungen ganz überwiegend nicht zu entnehmen.

Zum einen war dies häufig auf eine Aufzählung – mitunter zahlreicher – weit gefasster Kategorien personenbezogener Daten zurückzuführen, die die konkret verarbeiteten Daten nicht oder allenfalls ansatzweise erkennen lassen, z. B. verarbeitet *Google* seiner Datenschutzerklärung zufolge

> „[…] Daten über die Interaktion Ihrer Apps, Browser und Geräte mit unseren Diensten.“[144]

Da zu den *Google*-Diensten auch das Betriebssystem *Android* gehört (welches auch in einer TV-Variante existiert), kommt es mutmaßlich zu einer erheblichen Zahl an Interaktionen; in welchem Umfang hier welche personenbezogenen Daten verarbeitet werden, bleibt völlig unklar.

---

143 S. dazu die Ausführungen der französischen Datenschutzbehörde in ihrer Entscheidung gegen *Google LLC*: CNIL , Délibération de la formation restreinte n° SAN – 2019-001, vom 21.01.2019, Rn. 96 ff. der englischen Fassung; abrufbar im Internet unter https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf. Zuletzt bestätigt durch den Conseil d’État, (Entscheidung vom 19.06.2020, Az. 430810), abrufbar unter https://www.conseil-etat.fr/site/content/download/156114/document/GOOGLE%20430810.pdf, s. hierzu *DSGVO-Verstöße: Conseil d'Etat bestätigt 50-Millionen-Strafe gegen Google* (heise.de, 20.06.2020), abrufbar unter https://www.heise.de/news/DSGVO-Verstoesse-Conseil-d-Etat-bestaetigt-50-Millionen-Strafe-gegen-Google-4790235.html.

144 *Google*-Datenschutzerklärung vom 31.03.2020 unter *Daten, die wir bei der Nutzung unserer Dienste erheben – Ihre Apps, Browser und Geräte.*

Zum anderen findet in der Regel keine Beschränkung auf die vom Verbraucher tatsächlich genutzten Dienste eines Unternehmens statt. So verwendet beispielsweise *Samsung* knapp 700 Wörter[145], um alle möglichen Datenkategorien zu beschreiben, die bei Nutzung von *Samsung*-Geräten und Inanspruchnahme verschiedenster Dienstleistungen verarbeitet werden könnten. Hinzu kommen die Ausführungen zu Datenverarbeitungen in den ergänzenden nutzungsspezifischen Datenschutzhinweisen. Dennoch bleibt die Aufzählung an einigen Stellen vage. So ist etwa davon die Rede, dass alle (nicht näher bezeichneten) Informationen, die in Cookies auf dem Nutzergerät gespeichert werden, erfasst werden können[146]. Zudem würden über bestimmte Dienste personenbezogene Daten über

> „Onlineaktivitäten [des Nutzers] auf Websites und verbundenen Geräten […] mit diversen Websites, Geräten, Apps und anderen Onlinefunktionen und -diensten von Drittanbietern“ erfasst.

Mitunter enthalten Datenschutzbestimmungen Vorbehalte, z. B.

> „Wir können die folgenden Kategorien personenbezogener Daten über Sie verarbeiten, soweit die Verarbeitung in Verbindung mit dem Zweck der Verarbeitung, die in dieser Datenschutzrichtlinie festgelegt ist, grundsätzlich notwendig ist.“[147]

oder

> „Wenn Sie das Gerät, die Software und die Dienste nutzen, erheben wir, soweit dies nach geltendem Recht zulässig ist, die folgenden personenbezogenen Daten: […]“[148]

Nur äußerst selten wurden die verarbeiteten Daten konkret und abschließend benannt; *TP Vision* etwa zählt in seiner Datenschutzerklärung unter dem Punkt „Bedienung und Wartung des Smart TV“ im Einzelnen auf, welche konkreten Daten bei diesem Nutzungsvorgang verarbeitet werden:

---

145 Ausgedruckt entspricht dies rund zwei DIN A4-Seiten.

146 *Samsung*, Globale Datenschutzrichtlinie, unter *Welche Daten erfassen wir? – Daten über ihre Nutzung von Diensten – Anmeldeinformationen*.

147 *Hisense*, Datenschutzrichtlinie, unter *3. Kategorien von durch uns verarbeitete personenbezogene Daten* (Hervorhebung hinzugefügt).

148 *Arçelik,* Smart TV Datenschutzrichtlinie unter *1. Welche personenbezogenen Daten dürfen wir erheben und zu welchem Zweck?*

> „Wir erfassen folgende persönlichen Daten: die IP-Adresse des Smart TV, Verbraucher-ID, Geräte-ID, Seriennummer, MAC-Adresse und die auf Ihrem Smart TV konfigurierten Einstellungen für Land und Sprache sowie das Datum und die Uhrzeit des Zugriffs auf den Server."

bb) Rechtliche Würdigung

Sind die erhobenen Daten nicht so konkret wie möglich umschrieben, mag dies für sich genommen noch keinen Verstoß gegen die DSGVO darstellen. Es liegt jedoch auf der Hand, dass die DSGVO-Transparenzvorschriften nicht eingehalten werden können, wenn der betroffenen Person nicht klar ist, welche ihrer personenbezogenen Daten von einem Verarbeitungsvorgang, von einer bestimmten Rechtsgrundlage oder einem bestimmten Verwendungszweck erfasst sind. Im Sinne bestmöglicher Transparenz liegt es daher sogar nahe zu fordern, dass eine Kategorisierung von Daten nur insoweit erfolgen sollte, wie eine genauere Beschreibung nicht oder nur mit offensichtlich völlig unverhältnismäßigem Aufwand darstellbar wäre.

Bei den untersuchten Datenschutzbestimmungen ist für den Verbraucher nicht zweifelsfrei nachvollziehbar, welche personenbezogenen Daten vom Verantwortlichen eigentlich verarbeitet werden und welche nicht. Dies liegt zum einen an den teils sehr weiten Definitionen. Zum anderen führen Datenschutzbestimmungen für eine Vielzahl von Diensten zu Unübersichtlichkeit. Eine nachvollziehbare Zuordnung der Datenerhebung zu einer bestimmten Nutzung findet überwiegend nicht statt. Der Nutzer kann daher nicht etwa einen Datenabfluss durch Meidung bestimmter Dienste verhindern.

Stellt ein Unternehmen die Datenverarbeitung unter den Vorbehalt der Erforderlichkeit, so schafft eine solche Aussage keine Transparenz bzgl. der tatsächlich erhobenen Daten, denn die Definition der Erforderlichkeit liegt hier faktisch im Ermessen des Unternehmens. Nicht hilfreich ist auch der Zusatz, dass eine Datenverarbeitung erfolgt, soweit dies nach geltendem Recht zulässig ist. Im Extremfall könnte dies dazu führen, dass ein Maximalkatalog an verarbeiteten Daten(kategorien) aufgestellt wird, der dann unter den Vorbehalt der rechtlichen Zulässigkeit gestellt wird. Dies führt zu Intransparenz; die Rechtslage ist vielmehr vom Unternehmen vorab zu prüfen.

Die nachfolgende Übersicht zeigt, wie viele Unternehmen in ihren Datenschutzbestimmungen die tatsächlich erhobenen Daten (nicht) klar erkennbar ausweisen:

Erkennbarkeit der erhobenen Daten	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen	1	4	1	7	1

Tabelle 2: Erkennbarkeit der tatsächlich erhobenen Daten

c) Angabe der Verwendungszwecke

Art. 13 Abs. 1 lit. c) DSGVO verlangt, dass die jeweiligen Zwecke genannt werden müssen, für die die personenbezogenen Daten erhoben werden. Werden die Zwecke zwar angegeben, aber nicht in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, so liegt ein Verstoß gegen Art. 12 Abs. 1 S. 1 DSGVO vor.

aa) Ermittlungsergebnisse

Bei nahezu keinem Unternehmen fand eine Verknüpfung von Zweck und erhobenen Daten statt. Vielmehr wurden Daten und Zwecke oftmals schlicht aufgezählt, ohne dass eine Verknüpfung stattgefunden hätte. So heißt es etwa in den Datenschutzbestimmungen von *Hisense*:

> „Wir können Ihre personenbezogenen Daten für die folgenden Zwecke verarbeiten:“[149]

Mitunter bleiben Verwendungszwecke auch lückenhaft oder offen. So heißt es etwa in der Datenschutzrichtlinie von *LG*:

> „Wir verwenden die von Ihrem LG Smart TV erlangten Informationen […] für unterschiedliche Zwecke, darunter: […]“[150]

Es kam mehrfach vor, dass die Verarbeitungszwecke nicht konkret ausgewiesen, sondern mit der Nennung der Rechtsgrundlage oder berechtigten Interessen gleichgesetzt wurden.

bb) Rechtliche Würdigung

Eine unvollständige Nennung von Zwecken verstößt gegen Art. 13 Abs. 1 lit. c) DSGVO. Werden die Zwecke hingegen vollumfänglich genannt, muss auch klar sein, auf welche Daten sich die genannten Verwendungszwecke beziehen. Ansonsten wird die Bestimmung dem Transparenzkriterium des Art. 12 Abs. 1 S. 1 DSGVO nicht gerecht und der Nutzer kann sich so kein genaues Bild des Datenverarbeitungsvorgangs machen. Er kann insbesondere kaum beurteilen, ob der Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b) DSGVO eingehalten wurde.[151]

---

149 *Hisense*, Datenschutzrichtlinie, unter *6. Wie wir die erhaltenen Informationen nutzen*.

150 *LG*, Datenschutzrichtlinie, unter *3. Wie verwendet LGE die gesammelten Daten?*

151 Vgl. *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 8; S. a. *Paal/Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 13 DSGVO Rn. 16

Die nachfolgende Übersicht zeigt, wie viele Unternehmen in ihren Datenschutzbestimmungen die Zweckbestimmungen der jeweiligen Datenverarbeitungsvorgänge (nicht) klar erkennbar und den erhobenen Daten zurechenbar ausweisen:

Erkennbarkeit der Zweckbestimmung(en) der Datenverarbeitungsvorgänge	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen	2	--	3	3	6

Tabelle 3: Erkennbarkeit der Zweckbestimmung(en) der Datenverarbeitungsvorgänge

d) Nennung von Rechtsgrundlagen

Art. 13 Abs. 1 lit. c) DSGVO zufolge müssen die jeweiligen Rechtsgrundlagen für die Erhebung der personenbezogenen Daten genannt werden. Werden die Rechtsgrundlagen zwar angegeben, aber nicht in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, so liegt ein Verstoß gegen Art. 12 Abs. 1 S. 2 DSGVO vor.

aa) Ermittlungsergebnisse

Nahezu alle Unternehmen nannten Rechtsgrundlagen nur pauschal, d. h. es wurde nicht konkret für die jeweiligen Daten(-kategorien) angegeben, auf welcher Rechtsgrundlage diese verarbeitet werden. *Hisense* gab sogar pauschal für alle Datenverarbeitungen sämtliche für nicht-öffentliche Stellen einschlägigen Rechtsgrundlagen des Art. 6 Abs. 1 UAbs. 1 DSGVO an, einschließlich „lebenswichtiger Interessen."[152]

Praktisch alle Unternehmen verzichteten zudem auf eine Nennung der jeweiligen DSGVO-Artikel, in denen die zulässigen Rechtsgrundlagen für eine Datenverarbeitung aufgeführt sind. Die Rechtsgrundlagen werden aber nahezu durchgängig wie in der DSGVO benannt; lediglich anstatt des in der DSGVO verwendeten Ausdrucks „Einwilligung" findet sich des Öfteren der Begriff „Zustimmung".

[152] *Hisense*, Datenschutzrichtlinie, unter *4. Rechtsgrundlage für die Verarbeitung personenbezogener Daten; Hisense* beabsichtigt nach eigener Aussage, diese Rechtsgrundlage aus seinen Datenschutzbestimmungen zu streichen.

bb) Rechtliche Würdigung

Soweit sich in der Literatur überhaupt Hinweise hierzu finden, gehen die Kommentatoren überwiegend davon aus, dass es nicht genügt, die Rechtsgrundlage ohne genaue Zitierung der einschlägigen DSGVO-Norm zu benennen.[153] Ohne exakte Zitierung läge demnach bereits ein Verstoß gegen Art. 13 Abs. 1 lit. c) a. E. DSGVO vor. Hiergegen ließe sich jedoch einwenden, dass die DSGVO keine expliziten Aussagen zur Zitierung der einschlägigen Normen trifft und der Mehrwert deren Nennung für den Verbraucher überschaubar ist. Hingegen wird man zumindest verlangen müssen, dass die Rechtsgrundlagen so wie in der DSGVO oder zumindest sinnwahrend bezeichnet werden[154]. Das bedeutet, dass die in einer Datenschutzerklärung genannten Rechtsgrundlagen sich zweifelsfrei und ohne größeren Aufwand einer bestimmten Rechtsgrundlage aus dem Katalog des Art. 6 DSGVO zuordnen lassen müssen. Ein pauschaler Verweis auf Art. 6 DSGVO reicht hingegen keinesfalls aus.[155]

Für den Verbraucher ist die konkrete Nennung einer Rechtsgrundlage wichtig, weil er überprüfen können muss, ob diese die betreffende Datenverarbeitung auch trägt.

Die nachfolgende Übersicht zeigt, in wie vielen Datenschutzbestimmungen die Rechtsgrundlagen der jeweiligen Datenverarbeitungsvorgänge (nicht) klar erkennbar sind:

Erkennbarkeit der Rechtsgrundlage/n der Datenverarbeitungsvorgänge	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen	1	1	2	2	8

Tabelle 4: Erkennbarkeit der Rechtsgrundlagen der Datenverarbeitungsvorgänge

e) Angabe von berechtigten Interessen

Soweit sich ein Verantwortlicher gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO auf berechtigte Interessen für die Datenverarbeitung beruft, muss er gem. Art. 13 Abs. 1 lit. d) DSGVO diese berechtigten Interessen konkret benennen. Auch hier gilt wiederum, dass dies aufgrund von Art. 12 Abs. 1

153 S. dazu *Paal/Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 13 DSGVO Rn. 16 m. w. N.

154 Aus der Sicht der betroffenen Person ist es daher nicht von entscheidender Bedeutung, ob der Begriff „Einwilligung“ (wie in der DSGVO) oder „Zustimmung“ verwendet wird.

155 *Paal/Hennemann*, a. a. O (Fn. 153); ebenso *Veil* in Gierschmann/Schlender/Stentzel/Veil [Hrsg.], Kommentar Datenschutz-Grundverordnung, Art. 13 und 14 Rn. 65.

S. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen hat.

aa) Ermittlungsergebnisse

Ganz überwiegend gaben die Unternehmen berechtigte Interessen nur pauschal für mehrere oder (jedenfalls potentiell) gar alle Datenverarbeitungsvorgänge und Daten(-kategorien) an. So heißt es etwa im Datenschutzhinweis von *Panasonic* verallgemeinernd:

> „Wir dürfen personenbezogene Daten nicht ohne gültige Rechtsgrundlage verarbeiten. Deshalb verarbeiten wir Ihre personenbezogenen Daten nur, wenn: […]
>
> oder
>
> IV. die Verarbeitung für unsere berechtigten Interessen notwendig ist […]“[156]

bb) Rechtliche Würdigung

Es ist unerlässlich, dass für jedes Einzeldatum oder ggf. jede einzelne Datenkategorie klar dargestellt wird, welches konkrete Interesse die Verarbeitung eines Datums bzw. einer Datenkategorie rechtfertigt. Für die Einhaltung des Art. 13 Abs. 1 lit. d) DSGVO ist es dabei nicht notwendig, dass es sich um ein Interesse handelt, welches offensichtlich das Interesse der betroffenen Person überwiegt. Auch die Nennung eines schwachen Interesses genügt dem Transparenzerfordernis, selbst wenn dieses Interesse Zweifel hinsichtlich der Erforderlichkeit aufwirft oder die Interessen der betroffenen Person bei einer Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO nicht aufzuwiegen vermag (s. dazu E. V.1.b) bb), S. 120).

Mitunter wird gefordert, die Abwägung[157] mit den Interessen der betroffenen Person oder das Abwägungsergebnis[158] müsse wenigstens in Grundzügen mitgeteilt werden. Eine entsprechende

---

156 *Panasonic*, Datenschutzhinweis, unter *3. Auf welcher Rechtsgrundlage verarbeiten wir personenbezogene Daten?*

157 *Bäcker* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 13 DSGVO Rn. 27; *Knyrim* in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 13 Rn. 39.

158 *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 10.

Verpflichtung lässt sich indessen nur schwerlich aus Art. 13 Abs. 1 lit. d) DSGVO herleiten.[159] Eine nachvollziehbare Darstellung des Abwägungsvorgangs wäre im Sinne besserer Transparenz einerseits wünschenswert.[160] In Anbetracht der oftmals identischen berührten Interessen würde dies aber womöglich in vielen Fällen auf eine bloße Förmelei hinauslaufen. Das eigentliche Problem bleibt die Nichterkennbarkeit der Datenverarbeitungsvorgänge selbst.

Werden die berechtigten Interessen nicht oder nur lückenhaft genannt oder bleibt offen, welches Interesse die Verarbeitung welchen Datums bzw. welcher Datenkategorie im Ergebnis rechtfertigen soll, wird es der betroffenen Person faktisch unmöglich gemacht zu prüfen, ob eine Abwägung im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO zu ihren Gunsten oder Ungunsten ausgehen würde.

Die nachfolgende Übersicht zeigt, in wie vielen Datenschutzbestimmungen die berechtigten Interessen der jeweiligen Datenverarbeitungsvorgänge (nicht) klar erkennbar sind:

Erkennbarkeit der berechtigten Interessen	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen[161]	--	--	4	1	5

Tabelle 5: Erkennbarkeit der berechtigten Interessen

f) Angaben zu Datenempfängern

Übermittelt ein Verantwortlicher Daten an andere, so muss er nach Art. 13 Abs. 1 lit. e) DSGVO diese Empfänger konkret oder nach Kategorien benennen. Die Benennung hat aufgrund von Art. 12 Abs. 1 S. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

---

159 Ablehnend auch *Paal/Hennemann* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 17. Es ließe sich allenfalls auf Art. 5 Abs. 1 lit. a) DSGVO zurückgreifen, demzufolge personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen.

160 So auch die *Artikel-29-Datenschutzgruppe*, die in ihren „Leitlinien für Transparenz gemäß der Verordnung 2016/679“ (WP 260 rev. 01 vom 11.04.2018), S. 44, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, diesbezüglich von einem „bewährten Verfahren“ spricht (bzw. auf S. 36 der englischen Fassung von „best practice“).

161 Vier Unternehmen stützten Verarbeitungen personenbezogener Daten nicht auf berechtigte Interessen gestützt; die Datenschutzbestimmungen dieser Unternehmen wurden insoweit nicht bewertet.

aa) Ermittlungsergebnisse

Überwiegend werden Datenempfänger nur pauschal angegeben (z. B. „professionelle Berater“, oder „Auftragnehmer“). Zudem bleibt zumeist unklar, welche konkreten Daten oder Datenkategorien an den betreffenden Empfänger bzw. eine Empfängerkategorie weitergegeben werden. Bei konzerninternen Datentransfers wird ganz überwiegend auf die Angabe verzichtet, um welches Konzernunternehmen es sich handelt und wo dieses seinen Sitz hat.

Die Auswertung der Unternehmensfragebögen hat indessen gezeigt, dass es sich bei den datenempfangenden Unternehmen um eine durchaus überschaubare Menge handelt und der Großteil der Datentransfers mutmaßlich konstant mit denselben Unternehmen abgewickelt wird.

bb) Rechtliche Würdigung

Es mag zunächst überraschen, dass Art. 13 Abs. 1 lit. e) DSGVO *dem Wortlaut nach* die Nennung von Empfängerkategorien auch dann zulässt, wenn eine konkrete Nennung der einzelnen Empfänger möglich wäre.[162] Allerdings hat die Artikel-29-Datenschutzgruppe argumentiert, dass der Verantwortliche – um dem Grundsatz von Treu und Glauben[163] zu genügen – die für die betroffene Person aussagekräftigste Variante zu wählen hat. In der Regel sind somit die Empfänger konkret zu benennen.[164] Dies würde auch dem Präzisions- und Transparenzerfordernis in Art. 12 Abs. 1 S. 1 DSGVO entsprechen. Wünschenswert wäre in diesem Zusammenhang eine möglichst abschließende Nennung der jeweils aktuellen Datenempfänger einschließlich der Auftragsverarbeiter[165] (z. B. auf einer regelmäßig aktualisierten Website). Eine möglichst konkrete Nennung von Datenempfängern dürfte zudem erfordern, dass auch angegeben wird, welche Ge-

---

162 Im Gegensatz hierzu verlangt etwa Art. 13 Abs. 2 lit. a) DSGVO die konkrete Nennung der Datenspeicherdauer und erlaubt die Angabe der bloßen Kriterien für die Speicherdauer nur dann, „falls dies nicht möglich ist“.

163 Treu und Glauben ist einer der Datenverarbeitungsgrundsätze in Art. 5 Abs. 1 lit. a) DSGVO.

164 S. *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679“ (WP 260 rev. 01 vom 11.04.2018), S. 47. abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227), gegen ein Wahlrecht bei bereits bekannten Empfängern etwa auch *Lorenz*, VuR 2019, 213 (216), *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 11.; *Knyrim* verlangt, dass der Verantwortliche ggf. nach Treu und Glauben nachweisen können muss, warum die Angabe bloßer Kategorien ausreichen soll, S. *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 40.

165 Diese sind ebenfalls anzugeben, S. *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 11.

sellschaft eines Konzerns die Daten an welchem Standort empfängt. Dies ist auch deshalb relevant, weil ein konzerninterner Datentransfer mitnichten stets zulässig ist, wie viele Unternehmen offenbar glauben.[166]

Verschärft wird das Problem der mangelnden Erkennbarkeit von Datenempfängern noch dadurch, dass in vielen Fällen auch nicht transparent gemacht wird, *welche Daten* diese Datenempfänger erhalten. Dies widerspricht dem Transparenzgrundsatz des Art. 5 Abs. 1 Nr. 1 DSGVO, demzufolge personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise“ verarbeitet werden müssen. Je pauschaler die Datenempfänger und die vom Datentransfer betroffenen Daten benannt werden, desto schlechter kann die betroffene Person das mit der Datenübertragung einhergehende Risiko einschätzen.

Die undifferenzierte oder pauschalierte Bezeichnung von Datenempfängern, wie sie von den meisten Unternehmen praktiziert wird, stellt aufgrund mangelnder Transparenz einen Verstoß gegen Art. 13 Abs. 1 lit. e) DSGVO i. V. m. Art. 12 Abs. 1 S. 1 DSGVO dar.

Die nachfolgende Übersicht zeigt, in wie vielen Datenschutzbestimmungen die Datenempfänger (nicht) klar erkennbar sind[167]:

Erkennbarkeit der Datenempfänger	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen[168]	2	1	2	4	4

Tabelle 6: Erkennbarkeit der Datenempfänger

166 Erwägungsgrund 48 S. 1 zufolge kann ein berechtigtes Interesse an einem Datentransfer zwischen Unternehmen innerhalb eines Konzerns bestehen, jedoch ist dieses Fallbeispiel ausdrücklich auf „interne Verwaltungszwecke“ beschränkt. Eine Weitergabe zu Werbezwecken dürfte hiervon beispielsweise nicht gedeckt sein.

167 Hiermit ist keine Wertung darüber verbunden, ob eine Datenweitergabe an diese Empfänger jeweils auch *gerechtfertigt* wäre, S. dazu E. V. 1, S. 114.

168 Ein Unternehmen übermittelte laut seinen Datenschutzbestimmungen keine personenbezogenen Daten an Dritte; die Datenschutzbestimmungen dieses Unternehmens wurden insoweit nicht bewertet.

g) Angaben zu Datentransfers in Drittländer

Art. 13 Abs. 1 lit. f) DSGVO schreibt vor, dass der Verantwortliche darüber informieren muss, dass er beabsichtigt, personenbezogene Daten an ein Drittland[169] zu übermitteln. Drittland bezeichnet jeden Staat, in dem die DSGVO nicht direkt[170] anwendbar ist, mithin Staaten außerhalb der EU und des EWR[171]. Gemeint ist selbstverständlich nicht die Datenübermittlung an einen Staat als juristische Person, sondern an jegliche Empfänger in diesem Staat[172] (auch Auftragsverarbeiter[173] und Unternehmensniederlassungen[174]). Die Benennung der Empfangsstaaten hat aufgrund von Art. 12 Abs. 1 S. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

aa) Ermittlungsergebnisse

Nahezu alle untersuchten Datenschutzbestimmungen benennen die Empfängerländer außerhalb der EU gar nicht oder nur lücken- oder beispielhaft (etwa „unter anderem…“, „Volksrepublik China oder andere Drittländer“). Welche Daten oder Datenkategorien im Einzelnen den Drittlandtransfers unterliegen, wird in keiner der Datenschutzbestimmungen ausgeführt.

bb) Rechtliche Würdigung

Die Artikel-29-Datenschutzgruppe plädierte unter Verweis auf den Grundsatz von Treu und Glauben für eine genaue Angabe der datenempfangenden Drittländer im Rahmen von Art. 13 Abs. 1 lit. e) DSGVO.[175] Dabei ist zu beachten, dass die Datenempfänger bereits aufgrund von Art. 13 Abs. 1 lit. e) DSGVO so präzise wie möglich anzugeben sind. Die obligatorische Angabe der Drittländer dient damit vorrangig dazu, die betroffene Person in die Lage zu versetzen, sich

---

169 Oder an eine internationale Organisation, was aber in der Praxis selten vorkommen dürfte und im Rahmen der vorliegenden Sektoruntersuchung ohne Relevanz war.

170 Extraterritoriale Wirkungen bleiben an dieser Stelle außer Betracht.

171 Mit Wirkung ab dem 20.07.2018 hat der gemeinsame EWR-Ausschuss am 06.07.2018 die Übernahme der DSGVO in das EWR-Abkommen beschlossen. Somit zählen Island, Lichtenstein und Norwegen nicht mehr als Drittländer.

172 S. etwa *Franck* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 19; *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 12.

173 In diesem Sinne *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 49.

174 Vgl. *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 44 DSGVO Rn. 11.

175 *Artikel-29-Datenschutzgruppe,* Leitlinien für Transparenz gemäß der Verordnung 2016/679“ (WP 260 rev. 01 vom 11.04.2018), S. 48, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

über das Datenschutzniveau in den jeweiligen Drittländern zu informieren. Nur so ist es ihr möglich, das Übermittlungsrisiko einzuschätzen[176].

Das bedeutet im Ergebnis, dass der Nutzer erkennen können muss, welche Daten an welche Empfänger (s. hierzu f)) in welchen Drittländern übermittelt werden und welche der in der DSGVO genannten Sicherheitsvorkehrungen für jedes einzelne Empfängerland eingesetzt werden (s. hierzu h)).

Die nachfolgende Übersicht zeigt, in wie vielen Datenschutzbestimmungen Datentransfers in Drittländer sowie getroffene Datenschutzvorkehrungen (nicht) klar benannt sind:

Erkennbarkeit von Datentransfers in Drittländer	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen[177]	--	--	1	--	9

Tabelle 7: Erkennbarkeit von Datentransfers in Drittländer

h) Angaben zu Datenschutzvorkehrungen und Auskunftsmöglichkeiten bei Drittland-Datentransfers

Soweit eine Datenübermittlung in Drittländer beabsichtigt ist, muss der Verantwortliche gem. Art. 13 Abs. 1 lit. f) DSGVO darlegen, ob es für ein Drittland, in das Daten übermittelt werden, einen sog. Angemessenheitsbeschluss der Kommission gibt. Wo kein Angemessenheitsbeschluss vorliegt, muss der Verantwortliche im Regelfall anderweitige geeignete Maßnahmen treffen, um ein hohes Datenschutzniveau zu gewährleisten. Der Verantwortliche muss die betroffene Person zudem über die getroffenen Datenschutzvorkehrungen informieren und ggf. darüber, wie eine Kopie der geeigneten oder angemessenen Garantien[178] zu erhalten ist bzw. wo diese verfügbar sind. Informationen über getroffene Datenschutzgarantien und entsprechende Auskunftsmöglichkeiten müssen transparent und klar dargestellt werden (Art. 12 Abs. 1 S. 2 DSGVO).

---

176 Vgl. *Bäcker* in: Kühling/Buchner/Bäcker [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 34.

177 Vier Unternehmen nahmen laut ihren Datenschutzbestimmungen keine Übermittlungen personenbezogener Daten in Drittländer vor; die Datenschutzbestimmungen dieser Unternehmen wurden insoweit nicht bewertet.

178 Je nach den Umständen Art. 46, Art. 47 oder Art. 49 Abs. 1 UAbs. 2 DSGVO.

aa) Ermittlungsergebnisse

Praktisch durchgängig wurde in den untersuchten Datenschutzbestimmungen nicht angegeben, ob ein Angemessenheitsbeschluss der Kommission für das betreffende Drittland vorliegt oder nicht. Auch wurden die Datenschutzgarantien überwiegend weder konkret bezeichnet noch wurde die jeweilige DSGVO-Norm zitiert, in der die betreffende Garantie aufgeführt wird. In Einzelfällen war zudem die Information, wie eine Kopie der einschlägigen Datenschutzgarantien bezogen werden kann oder wo diese (im Regelfall wohl im Internet) verfügbar sind, nicht vorhanden oder lückenhaft. Es kam auch vor, dass die Darstellung der Auskunftsmöglichkeiten sich (in Abwesenheit einer Nennung einer allgemein zugänglichen Quelle) nicht klar auf den Anspruch auf Erhalt einer Kopie der getroffenen Datenschutzgarantien bezog. So heißt es bei *LG* etwa „Informationen dazu, wie wir Ihre persönlichen Daten behandeln und schützen“[179].

bb) Rechtliche Würdigung

Ein Angemessenheitsbeschluss bürgt für ein Datenschutzniveau, welches demjenigen der EU im Wesentlichen gleichwertig ist.[180] Soweit es keinen Angemessenheitsbeschluss gibt, muss der Verantwortliche grundsätzlich geeignete Maßnahmen treffen, die ebenfalls ein hohes Datenschutzniveau sicherstellen. Ein Katalog solcher Maßnahmen findet sich in Art. 46 Abs. 2 und 3 DSGVO. Er enthält u. a. verbindliche interne Datenschutzvorschriften für alle Unternehmen einer Unternehmensgruppe, die von der zuständigen Aufsichtsbehörde genehmigt wurden, oder von der Europäischen Kommission verabschiedete Standarddatenschutzklauseln. Daneben können Unternehmen Art. 46 Abs. 5 S. 2 DSGVO auch auf Standardvertragsklauseln zurückgreifen, die die Kommission noch auf Basis der Datenschutzrichtlinie verabschiedet hatte. Soweit kein Angemessenheitsbeschluss existiert, muss der Verantwortliche betroffene Personen gem.

---

179 *LG*, Datenschutzrichtlinie, unter *5. Übertragung von Informationen außerhalb des Europäischen Wirtschaftsraums*.

180 Angemessenheitsbeschlüsse existieren derzeit etwa für Kanada, die Schweiz oder Japan sowie – in eingeschränktem Umfang – die USA; eine Liste der aktuell gültigen Angemessenheitsbeschlüsse ist abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. Die Kommission beabsichtigt, ihre bisher ergangenen Angemessenheitsbeschlüsse unter Berücksichtigung der für den 17.07.2020 erwarteten EuGH-Entscheidung in der Sache *Schrems II* (Az. C-311/18) zu überarbeiten, s. Communication from the Commission to the European Parliamant and the Council – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, COM(2020) 264 final, 24.06.2020, S. 11, abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:264:FIN&rid=9 (aktuell nur auf Englisch erhältlich).

Art. 13 Abs. 1 lit. f) DSGVO über die im Zusammenhang mit der Übermittlung getroffenen Datenschutzvorkehrungen informieren. Da Angemessenheitsbeschlüsse immer spezifisch für ein bestimmtes Land ergehen, bedeutet das, dass in Abwesenheit eines solchen Beschlusses für jedes Drittland klar erkennbar sein muss, welche Datenschutzvorkehrungen für Datentransfers in dieses Drittland getroffen werden. Eine Aufzählung verschiedener Datenschutzvorkehrungen ohne Erklärung, für welche Drittländer diese gelten sollen, ist somit nicht zulässig.

Fraglich ist zunächst, ob der Verantwortliche auch stets darauf hinweisen muss, wenn für ein Drittland, in das Daten übermittelt werden, *kein* Angemessenheitsbeschluss der Kommission vorliegt.[181] Bei den untersuchten Datenschutzbestimmungen war dies zumeist nicht der Fall. In Anbetracht des Wortlauts der Norm („das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß […] einen Verweis […]“[182]) wird man dies kaum als zwingend erforderlich ansehen können. Dies gilt gleichermaßen für die Zitierung der einschlägigen DSGVO-Norm, die die für einen Drittland-Datentransfer gewählte Garantie aufführt.[183] Notwendig ist es hingegen, die gewählten Datenschutzgarantien genau zu bezeichnen. Bei einem pauschalen Verweis auf Datenschutzvorkehrungen oder missverständlichen Begriffen ist dem Prinzip der transparenten Information (Art. 12 Abs. 1 S. 1 DSGVO) nicht Genüge getan.

Wo Unternehmen keine allgemein zugängliche Quelle (i. d. R. einen Internetlink) nennen und nicht darüber informieren, wie eine Kopie der getroffenen Datenschutzgarantien bezogen werden kann, liegt ein Verstoß gegen Art. 13 Abs. 1 lit. f) DSGVO vor. Ein Verstoß – und zwar gegen den in Art. 12 Abs. 1 S. 1 DSGVO niedergelegten Grundsatz der transparenten Information – kann indessen auch darin liegen, dass zwar über eine Auskunftsmöglichkeit informiert wird, aber nicht in der gebotenen konkreten Weise.

Die nachfolgende Übersicht zeigt, in wie vielen Datenschutzbestimmungen die Datenschutzgarantien für Drittland-Datentransfers bzw. die Auskunftsmöglichkeiten zu getroffenen Datenschutzgarantien (nicht) klar benannt sind:

---

181 So wohl *Ingold* in Sydow [Hrsg.], Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 13 DSGVO Rn. 19; *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 12.

182 Hervorhebung hinzugefügt.

183 Hierfür plädierte die *Artikel-29-Datenschutzgruppe* in ihren „Leitlinien für Transparenz gemäß der Verordnung 2016/679“ (WP 260 rev. 01 vom 11.04.2018), S. 47 f., abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

Darstellung der Datenschutzgarantien und Auskunftsmöglichkeiten bzgl. Datentransfers in Drittländer	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen[184]	--	1	3	3	3

Tabelle 8: Darstellung der Datenschutzgarantien und Auskunftsmöglichkeiten bzgl. Datentransfers in Drittländer

i) Angaben zur Speicherdauer

Art. 13 Abs. 2 lit. a) DSGVO verpflichtet den Verantwortlichen zur Angabe der Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, der Kriterien für die Festlegung dieser Dauer.

aa) Ermittlungsergebnisse

Bei den untersuchten Datenschutzbestimmungen war aufgrund der unklaren Nennung von Datenkategorien zumeist bereits nicht klar abgrenzbar, welche Speicherfristen bzw. -kriterien für welche der erhobenen personenbezogenen Daten gelten sollten. Zudem wurden ganz überwiegend nur pauschale Aussagen zur Speicherdauer getroffen. Es erfolgte lediglich der allgemein gehaltene Hinweis, dass die Daten gespeichert werden, solange deren Verarbeitungszweck fortbesteht. Maximale Speicherdauern nannten nur die Unternehmen *Metz, Panasonic*, *TechniSat, TP Vision* und *Arçelik. Bei Arçelik* betraf dies zwar nur Cookies, das Unternehmen gab aber zumindest an, dass personenbezogene Daten nach Aufgabe der Nutzung des TV-Geräts und der entsprechenden Dienste gelöscht würden.[185]

Mitunter gaben Unternehmen im Fragebogen oder anderweitig in der Kommunikation mit dem Bundeskartellamt maximale Speicherdauern an, die sie intern einhalten, die sie aber nicht in ihren Datenschutzbestimmungen nach außen kommunizieren.

bb) Rechtliche Würdigung

Die Angabe der Speicherdauer in Art. 13 Abs. 2 lit. a) DSGVO steht in engem Zusammenhang mit den in Art. 5 Abs. 1 lit. c) bzw. e) DSGVO betonten Prinzipien der Datensparsamkeit und der

---

184 Vier Unternehmen nahmen laut ihren Datenschutzbestimmungen keine Übermittlungen personenbezogener Daten in Drittländer vor; die Datenschutzbestimmungen dieser Unternehmen wurden insoweit nicht bewertet.

185 *Arçelik*, Smart TV Datenschutzrichtlinie, unter *3. Speicherung Ihrer personenbezogenen Daten*.

„Speicherbegrenzung“.[186] Die Artikel-29-Datenschutzgruppe vertrat hierzu die Auffassung, dass der Verantwortliche sich nicht darauf beschränken kann, lediglich festzustellen, dass eine Speicherung so lange erfolgt, wie dies für den jeweiligen Zweck erforderlich ist.[187] Diese Lesart kann sich zum einen auf das Transparenzgebot des Art. 12 Abs. 1 S. 2 DSGVO stützen. Zum anderen bringt die Norm selbst bereits zum Ausdruck, dass der Regelfall die konkrete Benennung des Speicherzeitraums sein soll. Nur dort, wo dies *unmöglich* ist, kann auf eine Benennung der Kriterien für die Speicherdauer ausgewichen werden. Dass eine möglichst präzise Angabe der Speicherdauern für konkrete Daten mit spürbarem Aufwand verbunden sein kann, erlaubt indessen kein Abweichen vom Regelfall. Eine Speicherung bis auf Weiteres lediglich mit dem Hinweis, die Speicherung erfolge, solange dies für bestimmte Zwecke erforderlich sei, ist nicht zulässig.[188]

Eine transparente Darstellung von Löschfristen für einzelne Daten(-kategorien) bedeutet indessen für die Unternehmen keinen unzumutbaren Mehraufwand. Schon aus Gründen der Datensparsamkeit sind Unternehmen angehalten, ein Löschregime zu etablieren[189], bei dem für jedes personenbezogene Einzeldatum eine Löschfrist und/oder eine Prüfung der fortbestehenden Speichernotwendigkeit hinterlegt wird.[190] Die Tatsache, dass Unternehmen im Fragebogen deutlich präzisere Angaben machten, zeigt, dass dies grundsätzlich auch in Datenschutzbestimmungen möglich wäre.

Der Speicherdauer kommt im Gesamtsystem der DSGVO eine hohe Bedeutung zu. So muss die Speicherdauer insbesondere im Rahmen der beim Rechtfertigungsgrund der „Wahrung berechtigter Interessen“ gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO vorzunehmenden „umfassenden Verhältnismäßigkeitsprüfung“[191] berücksichtigt werden. Soweit ersichtlich hat dieser Aspekt in der Rechtsliteratur bislang kaum Niederschlag gefunden. Es liegt jedoch auf der Hand, dass bei einer langfristigen oder sogar unbefristeten Speicherung personenbezogener Daten der Eingriff in die informationelle Selbstbestimmung des Datensubjekts in aller Regel erheblich schwerer wiegt als

---

186 S. hierzu *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01 vom 11.04.2018), S. 48f., abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; S. auch *Knyrim* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 52, *Lorenz*, VuR 2019, 213 (217).

187 Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (11.04.2018), S. 49, abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

188 *Dix* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 13 DSGVO Rn. 15.

189 S. etwa *Franck* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 13 Rn. 20.

190 Dies wird ausdrücklich empfohlen in DSGVO-Erwägungsgrund 39, S. 10.

191 *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 16 DSGVO Rn. 86.

bei einer nur kurzfristigen Speicherung. In diesem Zusammenhang ist auch zu beachten, dass mit längerer Speicherdauer auch die Gefahr des Eintretens von Datenpannen oder illegaler Datenzugriffe Dritter erheblich ansteigt.

Aufgrund nur pauschaler Angaben und mangelnder Erkennbarkeit der Speicherdauer für personenbezogene Daten(kategorien) verstoßen die meisten Unternehmen gegen die Vorgaben der DSGVO. Dies zeigt die folgende Übersicht:

Erkennbarkeit der Speicherdauer	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
Anzahl Unternehmen	2	2	1	1	8

Tabelle 9: Erkennbarkeit der Speicherdauer

5. Untersuchung weiterer Hinweispflichten

Abgesehen von den vorgehend untersuchten Pflichtangaben, die sich im Wesentlichen auf die Transparenz der konkreten Datenverarbeitung beziehen, enthält die DSGVO weitere Hinweispflichten. Diese dienen insbesondere dazu, der jeweiligen betroffenen Person die ihr zustehenden Rechte zu vergegenwärtigen und ggf. eine Kontaktaufnahme mit dem datenverarbeitenden Unternehmen zu erleichtern.

Im Großen und Ganzen wurden die Hinweispflichten gut eingehalten, was mutmaßlich darauf zurückzuführen ist, dass die DSGVO-Vorgaben relativ einfach mit moderaten Anpassungen und Ergänzungen in die eigenen Datenschutzbestimmungen übernommen werden können. Es gab jedoch oftmals irreführende oder einschränkende Zusätze. Diese können dazu führen, dass betroffene Personen ihre Rechte nicht wahrnehmen oder ihnen die Ausübung ihrer Rechte erschwert wird. Das Widerspruchsrecht wurde zumeist nicht vom übrigen Text getrennt dargestellt, wie Art. 21 Abs. 4, 2. Hs. DSGVO es erfordert. Mitunter waren auch unverständliche oder fehlerhafte Formulierungen sowie Formulierungen, die ohne Notwendigkeit von denjenigen in der DSGVO abweichen, zu beobachten.

Inwieweit die jeweiligen Informationspflichten eingehalten wurden, wird in der unten stehenden Tabelle dargestellt:

	Umsetzung der DSGVO-Pflichten				
Hinweise in Datenschutzbestimmungen auf…	 hervorragend	 gut	 mittelmäßig	 unzureichend	 stark mangelhaft
… Verantwortlichen	4	4	3	2	1
…Datenschutzbeauftragten[192]	4	4	--	5	1
…Recht auf Auskunftserteilung	6	1	2	4	1
…Recht auf Datenlöschung	6	1	2	4	1
…Recht auf Einschränkung der Datenverarbeitung	3	3	2	2	4
…Recht auf Widerspruch gegen die Verarbeitung [muss vom übrigen Text abgesetzt werden][193]	--	--	6	5	1
…Recht auf Widerruf erteilter Einwilligungen	4	6	1	3	--
…Beschwerdemöglichkeit bei einer Aufsichtsbehörde	4	4	1	2	3

Tabelle 10: Überblick Umsetzung von Hinweispflichten zu Kontaktpersonen/Rechten

6. Exkurs: Erschwerung der Rechteausübung

Mitunter wiesen die Unternehmen zutreffend auf die betroffenen Personen zustehenden Rechte hin, erschwerten aber die effektive Durchsetzung dieser Rechte.

192 In der Literatur werden hier z. T. sehr weitgehende Angaben gefordert, S. etwa *Lorenz*, VuR 2019, 213 (214) m. w. N.: postalische Anschrift, von der allgemeinen E-Mail-Adresse des Unternehmens abweichende E-Mail-Adresse, Telefonnummer und Telefaxnummer, sofern ein Faxgerät vorhanden ist. In der tabellarischen Übersicht wurde es für eine gute Erfüllung als ausreichend erachtet, dass der Datenschutzbeauftragte über die bereitgestellten Angaben niederschwellig und effektiv erreicht werden kann.

193 Bei zwei Unternehmen wurden Verarbeitungen personenbezogener Daten weder auf berechtigte Interessen gestützt noch betrieben diese Unternehmen Direktwerbung auf Basis der erhobenen Nutzerdaten; es gab somit keinen Bedarf für eine Widerspruchsregelung und eine Bewertung fand nicht statt.

So hatte ein Unternehmen in seinen bis Ende 2019 gültigen Datenschutzbestimmungen etwa darauf verwiesen, der Nutzer könne sich über Kontaktdaten, die auf der Garantiekarte des Geräts genannt werden, an das Unternehmen wenden, um Standardvertragsklauseln anzufordern. Es ist aber fraglich, ob die betroffene Person die Garantiekarte im Bedarfsfall überhaupt zur Hand hat. Manche Unternehmen stellen in ihren Datenschutzbestimmungen keine E-Mail-Adresse für die Kontaktaufnahme zur Verfügung, sondern verweisen für die Rechteausübung auf spezielle Kontaktformulare im Internet. Auf den betreffenden Webseiten, auf denen sich mitunter auch Tracker finden, muss der Antragsteller in unterschiedlichem Ausmaß identifizierende Angaben[194] machen.

Solche Verhaltensweisen sind nicht in erster Linie unter dem Transparenzgesichtspunkt problematisch. Sie dürften nach hier vertretener Auffassung vielmehr gegen Art. 12 Abs. 2 S. 1 DSGVO verstoßen, demzufolge der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte erleichtern muss. Die Nennung einer E-Mail-Kontaktadresse und somit eine Kontaktaufnahme per (optional verschlüsselter) E-Mail sollte den Mindeststandard darstellen. Dies ist unkompliziert möglich, der Nutzer kann den Versand seiner Nachricht besser nachvollziehen und behält im Regelfall eine Kopie seiner Nachricht in seinem Mailkonto, auf die er sich bei Bedarf zu einem späteren Zeitpunkt beziehen kann. Die ausschließliche Kontaktaufnahmemöglichkeit per Webformular ist hingegen kritisch zu sehen. Von einer Erleichterung der Ausübung von Betroffenenrechten kann jedenfalls dann nicht die Rede sein, wenn auf der entsprechenden Website unnötige identifizierende persönliche Angaben[195] gefordert werden, die Website ihrerseits Trackingtools einsetzt, keine Bestätigungsmeldung des Antragseingangs (unter Beifügung des Antragstexts)

---

194 Dies bedeutet nicht, dass entsprechende Anfragen nicht auch per E-Mail entgegen genommen würden, sofern das Unternehmen (ggf. an anderer Stelle) eine Kontakt-E-Mail-Adresse zur Verfügung stellt.

195 Die einschlägige Kommentarliteratur ist in diesem Punkt mitunter undifferenziert und hält eine weitgehende Erfassung personenbezogener Daten zu Zwecken der Identifikation der antragstellenden Person für zulässig. Der Verantwortliche muss jedoch nicht die betroffene Person selbst zweifelsfrei identifizieren. Vielmehr muss überprüft werden, ob sich ein Identifikator, zu dem personenbezogene Daten gespeichert wurden, dem Antragsteller zuordnen lässt. Identifizierende Merkmale sind nur in dem Maße erforderlich, wie sie im konkreten Fall überhaupt geeignet sind, die Legitimierung des Antragstellers als Auskunftsrechtsinhaber zu beweisen. Jedenfalls bestimmte Smart-TV-Modelle lassen sich z. B. über die Gerätenummer oder eine spezielle gerätespezifische ID zuordnen, die ggf. in der Gerätesoftware eingesehen werden kann. Werden als Voraussetzung für die Geltendmachung eines Auskunftsrechts Daten wie Geburtsdatum oder Adresse erfragt, trägt dies zum Nachweis der Legitimation des Anspruchstellers in einem solchen Fall nichts bei. Welche Daten zur Identifizierung erforderlich sind, kann je nach IoT-Gerät und -Modell variieren und auch maßgeblich vom (Nicht-)Vorhandensein eines Nutzerkontos abhängen. Letztlich geht es stets darum, Datensparsamkeit und Identifizierungsbedürfnis ins Gleichgewicht zu bringen (vgl. *Quaas* in: BeckOK Datenschutzrecht, 32. Ed., 01.02.2020, Art. 12 DSGVO Rn. 34 a. E.).

erfolgt, keine Option für Rückfragen vorgesehen, eine gesicherte Datenübermittlung nicht gewährleistet oder die Lektüre umfangreicher Datenschutzbestimmungen für die Nutzung der Website erforderlich ist.

Zusammenfassung

Diverse Studien und Marktbeobachtungen haben ergeben, dass Verbraucher einerseits großen Wert darauf legen, dass ihre personenbezogenen Daten privat bleiben. Andererseits handeln sie in Situationen des täglichen Lebens überwiegend nicht datenschutzbewusst. Dieses als *Privacy Paradox* bezeichnete Phänomen lässt sich indessen maßgeblich dadurch erklären, dass der Verbraucher in datenschutzrelevanten Entscheidungssituationen wesentliche Informationen nicht erhält, sie nicht versteht oder sich deshalb nicht informiert, weil der Aufwand hierfür hoch und der erwartete Erkenntnisgewinn gering ist. Nicht selten spielt auch eine Rolle, dass es zu einer Akzeptanz von Datenschutzbestimmungen keine realistische Alternative gibt, will man ein bestimmtes Gerät oder eine Dienstleistung nutzen. Schließlich neigen Verbraucher dazu, kurzfristigen Nutzen höher zu bewerten als ggf. langfristig eintretende Risiken.

Die Datenschutzbestimmungen der in Deutschland im Bereich der Smart-TVs wesentlichen Akteure wiesen fast durch die Bank schwerwiegende Transparenzmängel auf. Die Datenschutzbestimmungen sind vor allem deshalb für den Nutzer nicht nachvollziehbar, weil sie für eine Vielzahl von Diensten und Nutzungsprozessen gelten sollen. Die „one fits all"-Architektur der meisten Datenschutzbestimmungen führt insbesondere dazu, dass der Nutzer nicht zuverlässig erfährt

- welche konkreten personenbezogenen Daten überhaupt erhoben werden;
- welche Datenverarbeitungen durch welche Nutzungsprozesse ausgelöst werden;
- zu welchen Zwecken welche personenbezogenen Daten verarbeitet werden;
- welche Rechtfertigung für die Verarbeitung welcher konkreten personenbezogenen Daten besteht;
- wie lange welche personenbezogenen Daten gespeichert werden;
- wer außer dem Verantwortlichen noch in den Besitz der erhobenen Daten gelangt.

Für den Nutzer ist es somit kaum möglich, eine Strategie zu verfolgen, bei der er möglichst wenige oder nur weniger sensible personenbezogene Daten preisgibt oder zumindest deren Verbreitung oder Speicherdauer minimiert. Es ist erkennbar, dass Datenschutzbestimmungen primär mit dem Ziel *förmlicher* DSGVO-Konformität konzipiert wurden. So finden sich in den Datenschutzbestimmungen zumeist Ausführungen zu den einschlägigen DSGVO-Normen. Diese enthalten jedoch in vielen Fällen keine Angaben, mit denen der Verbraucher in der Praxis etwas

anfangen kann. Insbesondere Pauschalierungen führen dazu, dass Datenschutzbestimmungen erheblich an Informationsgehalt einbüßen. Wie oben gezeigt wurde, stellt dies sehr häufig einen Verstoß gegen die DSGVO dar. Nutzer, die Verbraucherinformationen wie Datenschutzbestimmungen nicht durchlesen, verhalten sich somit insoweit rational, als deren Lektüre zeitlich aufwendig ist, aber zumeist keinen echten Erkenntnisgewinn mit sich bringt. Allenfalls bei gesonderten Einwilligungsersuchen wird der Verbraucher vor eine echte Wahl gestellt.

Dieses Problem besteht keinesfalls nur bei Smart-TVs, sondern betrifft ebenso andere IoT-Geräte und die Nutzung von Dienstleistungen im Internet allgemein. Es besteht somit eine eklatante Informationsasymmetrie zulasten des Verbrauchers. Datensouveränität ist unter diesen Rahmenbedingungen eine Illusion.

III. Zeitpunkt der Verbraucherinformation

Der Verbraucher sollte sich im Idealfall bereits vor dem Kauf ein Bild davon machen können, welche Datenschutzbestimmungen für den Betrieb des Fernsehgerätes gelten, welche Geschäftsbedingungen er ggf. akzeptieren muss und in welchem Umfang der Betrieb des Smart-TVs ein Nutzerkonto o. Ä. erfordert.

1. Ermittlungsergebnisse

Im Einzelhandel werden Smart-TVs typischerweise ohne jegliche Hinweise angeboten, welche Allgemeinen Geschäftsbedingungen oder Datenschutzbestimmungen dem späteren Nutzungsverhältnis zwischen dem Käufer und dem TV-Portal-Betreiber zugrunde gelegt werden. Ob das Gerät ordnungsgemäß und in vollem Umfang betrieben werden kann, ist möglicherweise von der Erteilung von Einwilligungen abhängig. Dieses Informationsdefizit gilt für den Internethandel ebenso wie für den Kauf im Ladenlokal. Auf den Verkaufsverpackungen der Fernseher sind – außer bei Samsung[196] – keinerlei entsprechenden Hinweise aufgedruckt.

Im Gegensatz dazu stellen eine Reihe von Unternehmen andere gerätebezogene Informationen auf ihren herstellereigenen Seiten durchaus zur Verfügung, z. B. *TCL*:

196 "Bestimmte *Samsung* Smart-TV-Funktionen sind möglicherweise nicht nutzbar ohne die ausdrückliche Zustimmung zur Erhebung und Nutzung personenbezogener Informationen" (in der englischsprachigen Originalantwort: "Certain Samsung Smart TV features may not be available without express consent to the collection and use of personal information."

Abbildung 11:Herunterladbare Gerätedokumente bei *TCL*[197]

Zumeist finden sich auf den Produktseiten der Hersteller neben technischen Gerätedetails vor allem Bedienungsanleitungen und Firmware-Downloads. Nicht im unmittelbaren Kontext mit dem Gerät herunterladbar sind hingegen Datenschutzbestimmungen oder Nutzungsbedingungen für die Betriebssystemsoftware und das TV-Portal.[198] Mit diesen wird der Kunde erst konfrontiert, wenn er erstmals den Fernseher einrichtet, ggf. auch erst später.

So wird bei den Fernsehern eines Herstellers der Kunde erst nach Inbetriebnahme des Geräts darüber informiert, dass er Online-Updates der Chipsatz-Firmware nur dann erhält, wenn er im Gegenzug einwilligt, personenbezogene Daten (u. a. TV-Modell und Seriennummer des Fernsehgeräts, Häufigkeit der Nutzung von Streaming-Diensten, Nutzung von Apps u. a.) an den Chipsatz-Hersteller zu übermitteln.

Wird das TV-Portal nicht vom Hersteller selbst betrieben, sondern von einem anderen Unternehmen, so wird dies auf der Verkaufsverpackung bzw. bei Angeboten im Internet überwiegend nicht oder nicht im unmittelbaren Zusammenhang mit der Abbildung und den wesentlichen Spezifikationen des Produkts angezeigt.

Für *Android*-Smart-TVs finden sich etwa im deutschen Online-Shop von *Amazon* in der Regel keine entsprechenden Hinweise. *Media Markt* führt hingegen auf der Produktseite seines Online-Shops aus (allerdings unter „Technische Daten“):

> „Um diesen Fernseher verwenden zu können, müssen Sie den Nutzungsbedingungen und den Datenschutzrichtlinien von Google zustimmen. […]“

Sony weist auf der Verkaufsverpackung seiner *Android-TV*-Fernsehgeräte darauf hin, dass diese das Betriebssystem *Android TV* von *Google* verwenden. Auf seiner Website erläutert das Unternehmen:

---

197 Screenshot eines Teils der Webseite https://www.tcl.com/de/de/new-product-list/dp600/43-4K-UHD-HDR-TV-mit-SMART-TV-3-0.html.

198 Gelegentlich finden diese sich im – von der Produktpräsentationsseite getrennten – Download- oder Supportbereich. Allerdings werden die dort vorgehaltenen Datenschutzbestimmungen teilweise erst mit deutlicher Verzögerung aktualisiert.

> „Sie können einige Funktionen des Android TV auch ohne Anmeldung bei einem Google-Konto nutzen. Sie können TV-Sendungen ansehen und alle Anwendungen von Sony wie die Video- und TV SideView App, Heimnetzwerkfunktionen für die Album-App, die Musik-App, die Video-App und die elektronische Programmzeitschrift (Electronic Programme Guide, EPG) nutzen.
>
> Darüber hinaus sind bestimmte Funktionen wie die sprachgesteuerte Google-Suche, die Google Cast-Funktion, Surfen im Internet und die You Tube-App auch ohne Anmeldung bei einem Google-Konto verfügbar."[199]

Bei *Media Markt* finden sich (zum Zeitpunkt der Publikation dieses Berichts) keine Hinweise darauf, dass ein Fernseher mit *Fire TV* nicht ohne Weiteres betrieben werden kann, falls der Nutzer kein *Amazon*-Konto eröffnet. *Amazon* selbst führt auf den einschlägigen Produktseiten hingegen aus:

> „Um alle Funktionen der Grundig Fire TV Edition Modelle nutzen zu können, ist ein Amazon Konto (Basic oder Prime) erforderlich."

Auf Anbieter wie *Foxxum*, *Netrange* oder *Zeasn* wird beim Verkauf im Einzelhandel sowie auf den Internet-Produktseiten der Hersteller in der Regel nicht hingewiesen, selbst wenn diese die maßgeblichen[200] Portalbetreiber darstellen.

2. Rechtliche Würdigung

Gemäß § 5a Abs. 2 UWG handelt unlauter, wer unter Berücksichtigung aller Umstände dem Verbraucher eine wesentliche Information vorenthält, die dieser benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und deren Vorenthalten geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Adressat des § 5a Abs. 2 UWG können dabei sowohl der Verkäufer als auch der Hersteller sein, soweit sie einen Smart-TV bewerben und somit eine geschäftliche Handlung gegenüber Verbrauchern vornehmen[201]. Das Vorenthalten der Information muss darüber hinaus geeignet sein, die Entscheidung des Verbrauchers zu beeinflussen.

---

199 *Benötige ich ein Google-Konto/eine Google-ID, um meinen Android TV von Sony zu nutzen?*, abrufbar unter https://www.sony.de/electronics/support/articles/00115361.

200 Grundsätzlich können die Portale dieser Anbieter auch als einfache App in einem anderen „Haupt"-TV-Portal abrufbar sein.

201 Der für eine geschäftliche Handlung notwendige objektive Zusammenhang mit einer Absatz- oder Bezugsförderung liegt insoweit vor, vgl. *Keller* in Harte-Bavendamm/Henning-Bodewig [Hrsg], UWG, 4. Aufl. 2016, § 2 Rn. 7.

Ein Vorenthalten kann dabei gemäß § 5a Abs. 2 Satz 2 Nr. 3 ausdrücklich in einer nicht rechtzeitigen Bereitstellung der betreffenden Information bestehen. So ist die Situation auch beim Kauf eines Fernsehers. Fernseher ohne Smartfunktionen sind kaum noch erhältlich bzw. auf Marktnischen beschränkt (z. B. Fernseher mit kleinen Bildschirmdiagonalen). Der Fernseher bringt daher in aller Regel ein hochentwickeltes Betriebssystem einschließlich TV-Portal mit. Nimmt der Käufer den Smart-TV erstmals in Betrieb, befindet er sich in einer schwierigen Lage, da ihm bereits Kosten entstanden sind und er den Kauf abgewickelt hat. Will der Käufer den Fernseher nutzen, ist dies in vielen Fällen nur zu den Datenschutzkonditionen des TV-Portal-Betreibers und mit Zustimmung zu dessen Nutzungsbedingungen möglich. Eine Rückgabe des Geräts kommt für den Käufer aber faktisch nicht mehr in Betracht.

a) Vorlage von Rechtstexten erst bei der Erstinstallation

Dies wirft die Frage auf, ob es sich bei den einschlägigen Rechtstexten, die vorenthalten werden, um „wesentliche Informationen, die der Verbraucher für eine informierte geschäftliche Entscheidung benötigt“ im Sinne von § 5a Abs. 2 Satz 1 Nr. 1 UWG handelt. Bei Angeboten zu einem Geschäftsabschluss gelten die Leistungsbedingungen jedenfalls dann als wesentliche Informationen, wenn ihre Inhalte von den Erfordernissen der unternehmerischen Sorgfalt abweichen (§ 5a Abs. 3 Nr. 4 UWG). Dies bedeutet, dass eine Aufklärungspflicht besteht, wenn die Bedingungen ungewöhnlich und unüblich sind.[202] Bedingungen, die in diesem Sinne von den billigerweise zu erwartenden Standards abweichen, können etwa vorliegen, wenn die Nutzung wesentlicher Funktionen des Smart-TVs von dem Anlegen eines Nutzerkontos beim TV-Portal-Betreiber abhängig gemacht wird (hierzu nachfolgend unter c)).

Nach der Rechtsprechung des Bundesgerichtshofs ist eine Information ansonsten nicht schon deshalb wesentlich, weil sie für eine geschäftliche Entscheidung des Verbrauchers von Bedeutung sein kann. Vielmehr muss ihre Angabe unter Berücksichtigung der beiderseitigen Interessen vom Unternehmer erwartet werden können und ihr für die vom Verbraucher zu treffende geschäftliche Entscheidung ein erhebliches Gewicht zukommen.[203] Dies bemisst sich u. a. nach der Bedeutung der Information innerhalb des Entscheidungsprozesses.[204] Erforderlich ist mithin eine Interessenabwägung, bei der die Bedeutung für den Verbraucher und die Zumutbarkeit (der Belastung) für das Unternehmen ins Verhältnis zu setzen und alle Umstände des Einzelfalls zu berücksichtigen sind.

---

202 S. *Alexander* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 5a UWG Rn. 398.

203 BGH, Urteil vom 27.04.2017, Az. I ZR 55/16, BGHZ 215, 12, Rn. 19 – *Preisportal*; BGH, Urteil vom 16.05.2012, Az. I ZR 74/11, juris Rn. 36. Zur dogmatisch fragwürdigen Einbeziehung der Unternehmerinteressen in den Wesentlichkeitsbegriff s. Fn. 527.

204 S. *Alexander* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 5a UWG Rn. 226.

Einerseits können Nutzungsbedingungen und Datenschutzbestimmungen ganz erhebliche Auswirkungen auf die Rechtsposition des Käufers, insbesondere die Preisgabe seiner personenbezogenen Daten und die Akzeptanz von Werbung haben. Der durchschnittliche Verbraucher wäre daher gut beraten, die betreffenden Texte frühzeitig zu lesen und seine Kaufentscheidung hiernach auszurichten. In der Realität stellt solches Verbraucherverhalten jedoch die absolute Ausnahme dar.[205] Auch vor dem Kauf eines Smart-TVs dürfte sich der „Durchschnittsverbraucher, der angemessen gut unterrichtet und angemessen aufmerksam und kritisch ist“,[206] kaum eingehend über Nutzungsbedingungen und Datenschutzbestimmungen der verschiedenen Anbieter informieren.[207] An dieser Einschätzung ändert auch die Tatsache nichts, dass womöglich die mitunter schwer zugängliche Ausgestaltung und Präsentation dieser Rechtstexte selbst maßgeblich zur Apathie der Verbraucher beigetragen hat.

Für den Erwartungs- und Verständnishorizont des Durchschnittsverbrauchers ist die Vorabkenntnis der für die Nutzung des Smart-TVs maßgeblichen Rechtstexte somit kein hinreichend gewichtiger Entscheidungsparameter. Der bloße zeitliche Versatz, mit dem der Verbraucher die relevanten Rechtstexte vom Smart-TV-Anbieter zur Kenntnis erhält, löst damit noch keinen UWG-Verstoß aus.

b) Keine Vorabinformation über TV-Portal-Betreiber

Die Tatsache, dass der Verbraucher i. d. R. vor dem Kauf keine Information darüber erhält, ob ggf. ein anderes Unternehmen als der Hersteller das TV-Portal eines Smart-TVs betreibt, wird man isoliert betrachtet auch nicht als Vorenthalten einer wesentlichen Verbraucherinformation i. S. d. Lauterkeitsrechts werten können. Soweit er sich hierüber überhaupt Gedanken macht, dürfte der Durchschnittsverbraucher zwar normalerweise annehmen, dass der Hersteller des Fernsehers auch das TV-Portal des Fernsehers betreibt. Es handelt sich hierbei aber nicht um eine maßgebliche Erwartung, die einen mit ausschlaggebenden Faktor im Kaufentscheidungsprozess darstellen würde. Der Verbraucher muss ohnehin davon ausgehen, neben dem Kaufvertrag mit dem Einzelhändler (mindestens) einen zusätzlichen Nutzungsvertrag für den Gebrauch des Smart-TVs abschließen zu müssen. Die Person des späteren Vertragspartners als solche dürfte für ihn keine entscheidende Bedeutung haben.

---

205 S. hierzu oben ausführlich unter E. II. 1., S. 48 ff.

206 S. Erwägungsgrund 18 der UGP-Richtlinie; EuGH, Urteil vom 08.02.2017, Az. C-562/15, EU:C:2017:95 – *Carrefour Hypermarchés SAS*, Rn. 31.

207 *Raue* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 4a UWG Rn. 71, weist in diesem Zusammenhang darauf hin, dass Verbraucher in relevantem Umfang zu wenig verständigem, irrationalem Verhalten neigen können.

c) Information über Nutzungseinschränkungen erst bei der Erstinstallation

Will der Verbraucher den vollen Funktionsumfang eines Smart-TVs ausschöpfen, so setzt dies mitunter ein Nutzerkonto beim TV-Portal-Betreiber voraus. Dies ist etwa bei dem Betriebssystem *Android TV* sowie dem erst seit Herbst 2019 in Deutschland vertriebenen *Fire TV* von *Amazon* der Fall. Es stellt sich die Frage, ob hierin eine im Sinne von § 5a Abs. 2 Satz 1 Nr. 1 UWG „wesentliche Information, die der Verbraucher für eine informierte geschäftliche Entscheidung benötigt", zu sehen ist. Man mag einerseits zweifeln, ob es sich hierbei um eine Information handelt, welcher der Durchschnittsverbraucher Bedeutung für seine Kaufentscheidung beimisst. Andererseits ist bei den meisten Smart-TVs – anders als bei Smartphones – eine Nutzung von Smartfunktionalitäten und Apps ohne Nutzerkonto möglich. Man kann daher nicht davon ausgehen, dass der durchschnittlich aufmerksame Verbraucher ohnehin damit rechnet, ein Nutzerkonto eröffnen zu müssen, selbst wenn ihm eventuell bewusst ist, dass ein *Fire TV* in Zusammenarbeit mit *Amazon* angeboten wird. In einem entsprechenden Erfordernis kann daher eine Leistungsbedingung gesehen werden, die ungewöhnlich und unüblich ist und somit im Sinne des § 5a Abs. 3 Nr. 4 UWG von den Erfordernissen der unternehmerischen Sorgfalt abweicht. Die Information über die Notwendigkeit eines Nutzerkontos ist für den Verbraucher auch durchaus gewichtig, insbesondere weil ein solches Konto abgesehen vom Aufwand des Einrichtens praktisch immer eine erhöhte Identifizierbarkeit und ein Mehr an Verarbeitung personenbezogener Daten bedeutet.

M. a. W. ist eine Vorabinformation des Verbrauchers immer dann vonnöten, wenn der vom Verbraucher erwartbare Funktionsumfang von einer Überlassung personenbezogener Daten in wesentlichem Umfang abhängig gemacht wird. Denn der Verbraucher kann davon ausgehen, dass ihm die wesentlichen Funktionalitäten ohne weitere Leistung seinerseits zur Verfügung stehen.[208] Der erwartbare Funktionsumfang schließt insbesondere folgende Aspekte ein:

- lineares „traditionelles" Fernsehen,
- die Nutzung wesentlicher[209] Apps,
- Aktualisierungen der Firmware aus Sicherheitsgründen und
- den Anschluss von Zuspielgeräten (z. B. DVD-Player, Magenta-TV-Stick o. Ä.)

---

208 Vgl. zu Funktionseinschränkungen bei sog. Shareware BGH, Urteil vom 24.06.1999, Az. I ZR 51/97, juris Rn. 17 f. – *Shareware-Version*.

209 S. hierzu die Ausführungen auf S. 138, die hier entsprechend gelten können.

Eine Überlassung personenbezogener Daten in wesentlichem Umfang wäre beispielsweise anzunehmen beim obligatorischen Anlegen eines Nutzerkontos beim TV-Portal-Betreiber[210], welches personenbezogene Daten erfordert. Werden unklare Formulierungen verwendet (z. B. Überlassung nicht näher bezeichneter „Nutzerdaten"), so ist ebenfalls von der Verarbeitung personenbezogener Daten in wesentlichem Umfang und einer entsprechenden Vorab-Informationspflicht auszugehen.

Soweit ersichtlich, sind Fernseher mit *Android TV* unterschiedlich ausgestaltet und können durchaus die Verwendung wesentlicher Apps und auch Sicherheits-Firmware-Updates zulassen, ohne dass ein *Google*-Konto unbedingt erforderlich wäre. Insofern muss im konkreten Einzelfall beurteilt werden, ob über die Notwendigkeit eines *Google*-Kontos vorab informiert werden müsste. Bei den Fernsehern mit *Fire TV*, die bislang nur einen geringen Marktanteil auf sich vereinigen, ist hingegen jegliche App-Nutzung nur mit *Amazon*-Konto möglich, worauf bereits vor dem Kauf hingewiesen werden müsste. Ein Verstoß gegen § 5a Abs. 2 UWG liegt auch in dem Fall vor, in dem die Aktualisierungen der Chipsatz-Software von der Einwilligung in die oben auf S. 92 beschriebene Übermittlung personenbezogener Daten abhängig gemacht werden.

Zusammenfassung

Unter Transparenz- und Verbraucherschutzgesichtspunkten ist es wünschenswert, dass alle für den Verbraucher wichtigen Informationen bereits vor dem Kauf verfügbar sind. Andernfalls kann sich der Verbraucher kein umfassendes Bild von dem zu kaufenden Produkt machen.

Das Lauterkeitsrecht stellt in § 5a Abs. 2 UWG jedoch nicht auf die Vollständigkeit von Verbraucherinformationen ab. Die Vorschrift greift vielmehr nur dann ein, wenn der – ohnehin schwer zu bestimmende – Durchschnittsverbraucher eine Information benötigt, um eine sachkundige Kaufentscheidung treffen zu können. Werden bestimmte Informationen trotz objektiver Wichtigkeit vom angemessen gut unterrichteten und angemessen aufmerksamen und kritischen Verbraucher i. d. R. nicht in ihren Entscheidungsprozess einbezogen, so kann § 5a Abs. 2 UWG bei solchen Marktgegebenheiten keine Abhilfe schaffen. Es besteht daher insoweit keine lauterkeitsrechtliche Pflicht, Datenschutzbestimmungen oder Allgemeine Geschäftsbedingungen schon vor dem Kauf zur Verfügung zu stellen, die erst bei der späteren Nutzung eines Smart-TVs relevant werden.

Anders fällt hingegen die rechtliche Beurteilung aus, soweit der Verbraucher den gekauften Smart-TV nicht „out of the box" für alle wesentlichen Verwendungen nutzen kann, ohne dass er – beim Ersteinrichtungsprozess oder ggf. auch zu einem späteren Zeitpunkt – in wesentlichem

[210] Unschädlich ist es in diesem Zusammenhang natürlich, wenn die App-Nutzung die Eröffnung eines Nutzerkontos *beim App-Anbieter* erfordert, wie dies etwa bei *Netflix* oder *Spotify* der Fall ist.

Umfang personenbezogene Daten preisgeben muss (etwa durch das Erfordernis eines Nutzerkontos). Wird hierüber nicht bereits vor dem Kauf informiert, liegt ein Verstoß gegen § 5a Abs. 2 UWG vor.

IV. Verbraucherinformation – Informationsasymmetrien überwinden

Neben intransparenten Datenschutzerklärungen und Informationen, die viel zu spät übermittelt werden, als dass sie noch Grundlage informierter Entscheidungen werden könnten, sehen sich Verbraucher einer Reihe weiterer Informationsnachteile gegenüber. Diese können jegliche Bemühungen der Verbraucher konterkarieren, informierte Entscheidungen zu treffen und bei ihren Kaufentscheidungen Datenschutz als qualitätsbildenden Faktor von IoT-Produkten wahrzunehmen und zu berücksichtigen.

1. Aktiver Beitrag des Verbrauchers

Schon jetzt ist der Absatz von Smart-TVs stark marketinggetrieben. Die Eigenschaft eines Gerätes als besonders datensparsam, datenschützend und datensicher kann insofern vom Anbieter als zusätzliches verkaufsförderndes Element eingesetzt werden. In der Praxis ist dies allerdings nicht ohne Weiteres zu erwarten.

Die Verbraucherpräferenzen sind – was den Datenschutz angeht – kontextspezifisch, uneinheitlich und nicht immer wohlüberlegt (zum sog. ***Privacy Paradox*** s. E. II. 1, S. 48).[211] Wenn Verbraucher einen Smart-TV oder ein anderes Gerät des Internets der Dinge erwerben, tätigen sie eine zusammengesetzte Transaktion.[212] Ihr Hauptaugenmerk liegt auf dem Erwerb des Produktes. Die Datenverarbeitungstransaktion fällt zusätzlich an; als zeitlich nachgelagerter Nebeneffekt findet sie weniger Beachtung.

Hersteller werden erst dann in Datenschutz investieren und dies verständlich kommunizieren oder sogar bewerben, wenn der Verbraucher **Datensparsamkeit, Datenschutzkonformität und Datensicherheit als Qualitätsmerkmal** seines Produktes ansieht. Datenschutz könnte dann zum **Wettbewerbsvorteil** von Herstellern werden. Dafür ist der Verbraucher nicht nur zu informieren, sondern auch zu motivieren, die notwendigen Informationen von den Anbietern einzufordern, indem nur dort gekauft wird, wo **informierte Entscheidungen** möglich sind. Notwendig dazu ist aber nicht nur, die Verbraucher zu aktivieren und in ihnen das Bedürfnis zu wecken,

---

211 Vgl. *Kerber*, Digital markets, data and privacy: Competition Law, Consumer Law and Data Protection, Joint Discussion Paper Series in Economics No. 14, 2016, S. 7, abrufbar unter https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/14-2016_kerber.pdf.

212 Vgl. *Jentzsch*, State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO – Innovation Framework for ICT Security Deliverable, 2016, S. 35, abrufbar unter https://www.econstor.eu/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

datenschützende IoT-Geräte zu erwerben. Sie müssen sich auch mit vertretbarem Aufwand über die Datenschutzqualität des gewünschten Produktes informieren und vergleichen können. Derzeit ist das nicht möglich. Selbst wenn sich die Verbraucher um mehr Informationen zum Datenschutz bei Nutzung des gewünschten Produktes bemühen, wird es ihnen schwer gemacht, diese ausfindig zu machen.

2. Informationsasymmetrien vor und nach Vertragsabschluss

Wie Verbraucher die Qualitätseigenschaften eines Produktes bewerten, kann mit dem sog. **Qualitätsunsicherheitsansatz**[213] veranschaulicht werden. Dabei werden drei Güterkategorien gebildet, die sich danach unterscheiden, ob die Verbraucher die Qualität eines Produktes vor und/oder nach dem Kauf beobachten können. Bei den sog. **Suchgütern** kennen die Verbraucher die Qualität des Produktes vor und nach dem Kauf. Bei den sog. **Erfahrungsgütern** können die Verbraucher die Qualität des Produktes erst nach dem Kauf beurteilen. Sog. **Vertrauensgüter** kennzeichnet, dass die Qualität des Produktes den Verbrauchern auch nach dem Kauf noch verborgen bleibt. Wenn es um die Datenschutzqualität geht, dürften Verbraucher viele Produkte derzeit als Erfahrungsgüter, wenn nicht gar Vertrauensgüter beschreiben. Wie die Sektoruntersuchung gezeigt hat, können sich Verbraucher vor dem Kauf kaum einen Überblick über alle datenschutzrelevanten Eigenschaften des favorisierten Produktes machen. Die Datenschutzpraktiken der Hersteller sind uneinheitlich und intransparent. Die Verbraucher stellen z.B. möglicherweise erst bei Inbetriebnahme eines gekauften Smart-TV fest, dass sie personenbezogene Daten preisgeben müssen, um bestimmte über die Grundfunktionen hinaus gehenden Eigenschaften des Geräts nutzen zu können. Einige Verbraucher würden wahrscheinlich – wenn es um die Datenschutzqualität von IoT-Geräten geht – auch von Vertrauensgütern sprechen. Bestimmte Verbrauchergruppen blenden bisher jegliche datenschutzrechtlichen Aspekte bei ihren Kaufentscheidungen aus, sei es aus Unkenntnis, Desinteresse, aus Zeitmangel oder einfach, weil sie angesichts der Komplexität der Informationsbeschaffung aufgegeben haben. Außerdem ist auch den interessierten und informierten Verbrauchern meistens nicht bewusst, in welchem Ausmaß ihre Daten erhoben sowie von wem und wofür sie verwendet werden. Schließlich ist der tatsächliche Datenfluss nur mit erheblichem technischem Aufwand und im Hinblick auf die konkret übermittel-

213 Vgl. *Nelson*, Advertising as Information, in: Journal of Political Economy 1974, 729, abrufbar unter https://www.jstor.org/stable/1837143?seq=1, sowie *Darby/Karni*, Free Competition and the Optimal Amount of Fraud, in: Journal of Law and Economics 1973, 67, abrufbar unter https://www.journals.uchicago.edu/doi/10.1086/466756.

ten Inhalte häufig überhaupt nicht überprüfbar. Unter solchen Bedingungen können keine informierten Entscheidungen getroffen werden. Die Suchkosten[214] der Verbraucher sind zu hoch und müssen gesenkt werden. Dies dürfte in den Augen der Verbraucher hauptsächlich die Zeit betreffen, die sie aufwenden müssen, um ihren Informationsstand zu verbessern.

Die Maßnahmen, die den Informationsstand der Verbraucher verbessern, müssen die individuellen Eigenschaften und Wahrnehmungen der Verbraucher – wie sie das *Privacy Paradox* beschreibt – einfangen können. Als theoretischer Hintergrund können neuere verhaltensökonomische Erklärungsansätze[215] dienen, aber auch die Neue Institutionenökonomik[216], welche seitdem in verschiedensten Forschungsbereichen verwendet wurde, um Austauschbeziehungen und ihre Risiken zu analysieren und sie risikominimierend und kosteneffizient zu gestalten. Der Verhaltensökonomik sind u. a. Überlegungen zu verdanken, dass Informationen nicht in beliebiger Menge und in beliebig kurzer Zeit wahrgenommen und verarbeitet werden können. Ein zu großes, unübersichtliches Angebot an Entscheidungsalternativen wird eher dazu führen, dass Entscheidungen verweigert oder aufgeschoben werden.[217]

Mehr als verhaltensökonomische Ansätze bieten neoinstitutionenökonomische Erklärungstheorien verallgemeinerbare, einfach verständliche und klar strukturierte Empfehlungen, wie Informationsasymmetrien überwunden werden können. Sie eignen sich auch für die Analyse der Aus-

---

214 Suchkosten sollen hier weit interpretiert werden und umfassen die Kosten jeglicher alternativer bewerteter Verwendung von Ressourcen, die aufgewendet werden müssen, um Informationssuche zu betreiben.

215 Wesentlich ist das Konzept der sog. Beschränkten Rationalität (bounded rationality). Vgl. *Simon,* Rational Choice and the Structure of Environments, in: Psychological Review 1956, 123, abrufbar unter https://pdfs.semanticscholar.org/23a9/4ce42fe0d50f5c993f34d4c9602f8aeac507.pdf. Grundlage verhaltensökonomischer Erklärungsansätze sind empirische und experimentelle Beobachtungen sowie spieltheoretische Experimente.

216 Vgl. für einen Überblick z. B. *Terberger*, Neo-institutionalistische Ansätze, 1994, und *Richter/Furubotn*, Neue Institutionenökonomik, 1996. Die Neue Institutionenökonomik umfasst verschiedene theoretische Erklärungsansätze, die im Wesentlichen in vier Schulen unterteilt werden: Der Property-Rights-Ansatz oder Theorie der Verfügungsrechte, der Transaktionskostenansatz, der Prinzipal-Agent-Ansatz und informationsökonomische Ansätze, vgl. *Picot*, Ökonomische Theorien der Organisation – ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [Hrsg.]: Betriebswirtschaftslehre und Ökonomische Theorie, 1991, S. 143, sowie *Kaas*, Marketing und Neue Institutionenökonomik, in: *Kaas* [Hrsg.]: Kontrakte, Geschäftsbeziehungen, Netzwerke – Marketing und Neue Institutionenökonomik, 1995, S. 1. Auch wenn die verschiedenen Ansätze unterschiedliche Aspekte einer Transaktionsbeziehung in den Blick nehmen, basieren sie auf gemeinsamen Grundannahmen über die Motivation der Wirtschaftssubjekte.

217 Gerne zusammengefasst als Politikwechsel von „Viel hilft viel!“ zu „Keep it simple!“.

tauschbeziehung zwischen Unternehmen und Verbrauchern in Fragen von Datenschutz als Produkteigenschaft. Die **Annahmen zum menschlichen Verhalten**[218] erinnern dabei an aktuelle Tendenzen in der Forschung zum **Verbraucherleitbild**. Zuletzt ist ein eher differenziertes Verbraucherleitbild mit verantwortungsvollen, verletzlichen oder vertrauenden Verbrauchern[219] diskutiert worden.[220] Es erscheint insofern inzwischen weitgehend Einigkeit zu bestehen, dass Unterschiede zwischen den Verbrauchern, was ihre Wahrnehmung, Emotion und Motivation angeht, zu berücksichtigen sind.[221] Ausgangspunkt der neoinstitutionenökonomischen Analyse sind gerade individuelle Verhaltensweisen der Wirtschaftssubjekte bei Unsicherheit.[222] Auch die weiteren Annahmen entsprechen in ihren Grundzügen typischen beobachtbaren Verhaltensweisen der Verbraucher im Umgang mit IoT-Produkten: Es wird Nutzenmaximierung angestrebt, aber nur eingeschränkt rational gehandelt. Die Kapazitäten der Verbraucher für die Informationsaufnahme sind beschränkt und (Datenschutz-) Risiken werden nicht einheitlich bewertet. Schließlich wird

---

218 Im neoinstitutionenökonomischen Modell wird vom Menschenbild des rational gesteuerten Homo Oeconomicus Abstand genommen, welches Grundlage klassischer mikroökonomischer Erklärungsansätze ist. Stattdessen werden verhaltensrelevante Determinanten u. a. psychologischer und soziologischer Art sowie kulturelle und persönlichkeitsbedingte Einflüssen einbezogen, vgl. z. B. *Richter/Furubotn*, Neue Institutionenökonomik, 1996, oder *Aufderheide/Backhaus*, Institutionenökonomische Fundierung des Marketing: Der Geschäftstypenansatz, in *Kaas* [Hrsg.]: Kontrakte, Geschäftsbeziehungen, Netzwerke, 1995, S. 43.

219 Die europäische Rechtsprechung stellt bislang auf den mündigen oder durchschnittlich informierten, aufmerksamen und verständigen Durchschnittsverbraucher ab, vgl. EuGH, Urteil vom 16.07.1998, C-210/96, Slg. 1998, I-4657, Rn. 31 – *Gut Springenheide*. Die deutsche Rechtsprechung hat dies übernommen und zuletzt mit der „situationsadäquaten Aufmerksamkeit“ weiter präzisiert, vgl. etwa BGH, Urteil vom 20.10.1999, Az. I ZR 167/97, juris Rn. 20 – *Orient-Teppichmuster*.

220 Vgl. *Micklitz*, Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik, Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim BMELV, 2010, abrufbar unter https://www.vzbv.de/sites/default/files/downloads/Strategie_verbraucherpolitik_Wiss_BeiratBMELV_2010.pdf sowie *Pagel***,** Das Verbraucherleitbild in der digitalen Welt, Impulsvortrag, o. Jg., Hochschule Mainz**,** abrufbar unter https://mffjiv.rlp.de/fileadmin/MFFJIV/Verbraucherschutz/Digital-Dialog_Impulsvortrag_210317_SP.pdf und *Ernste*, Verbraucherschutz und Verhaltensökonomik. Zur Psychologie von Verhalten und Kontrolle, IW Analysen 106, 2016, abrufbar unter https://www.iwkoeln.de/studien/iw-analysen/beitrag/dominik-enste-mara-ewers-christina-heldman-regina-schneider-verbraucherschutz-und-verhaltensoekonomik-291323.html.

221 Vgl. *Becker*, Bundeskartellamt und Verbraucherschutz, ZWeR, 2018, 229, 244; so auch BDI, Studie Verbraucherleitbild und Positionsbestimmung zum mündigen Verbraucher, 2014, abrufbar unter https://bdi.eu/media/publikationen/?publicationtype=Studien#.

222 Es wird vom methodologischen Individualismus ausgegangen. Vgl. *Richter*, Sichtweise und Fragestellungen der Neuen Institutionenökonomik, in: Zeitschrift für Wirtschafts- und Sozialwissenschaften, 1990, 571, 573.

vorausgesetzt, dass Wirtschaftssubjekte – d. h. alle Marktteilnehmer, einschließlich Verbrauchern und Herstellern – immer ihrem Eigeninteresse folgen, auch wenn dies zu Lasten ihrer Vertragspartner geht.[223] Vor diesem Hintergrund werden verschiedene Ausprägungen von **Informationsasymmetrien** analysiert, mit denen Verbraucher beim Erwerb von IoT-Geräten wie Smart-TVs umgehen müssen. In informationsökonomischen Ansätzen werden grundlegende Mechanismen vorgeschlagen, um Informationsnachteile zu mildern und Risiken zu reduzieren.

In informationsökonomischen Ansätzen[224] geht es – über den o. g. Qualitätsunsicherheitsansatz hinaus – zunächst darum, **Qualitätsunsicherheit** zu verringern. Verbraucher können vor und nach Vertragsabschluss, was die **(Datenschutz-) Qualität** des gewählten Produktes angeht, unsicher sein. Zwei Varianten an Aktivitäten sind geeignet, Informationsnachteile abzubauen. Sog. Screening-Aktivitäten zur Informationsbeschaffung können sowohl außerhalb als auch innerhalb einer vertraglichen Beziehung unternommen werden. Screening kann alle denkbaren Suchaktivitäten umfassen. Es gehören sowohl alltägliche Sucharbeiten im Internet oder Recherche in anderen Medien dazu als auch komplexere Regelungssysteme, wie z.B. Selbstwahlschemata. Hier führt eine bestimmte vertragliche Bedingung dazu, dass nur derjenige den Vertrag schließt, der diese Bedingung erfüllt (vgl. Selbstbeteiligungsklausel bei Versicherungen).[225] Auch Aktivitäten zur **Informationsübertragung („Signaling“)** können geeignet sein, Informationsnachteile abzubauen. Signaling kommt sowohl bei feststehenden, nicht veränderbaren Eigenschaften (sog. *Indices*) in Frage als auch bei Eigenschaften, die zwar beobachtbar sind, aber noch vom Informanten verändert werden können (Signale i. e. S.).[226] In letztere Kategorie dürfte die Datenschutzqualität einzuordnen sein, welche von Anbietern an die Verbraucher über verschiedenste Maßnahmen signalisiert werden könnte.

---

223 Vgl. *Williamson*, Die ökonomischen Institutionen des Kapitalismus, 1990, S. 54.

224 Vgl. die grundlegenden Arbeiten von *Stigler*, The Economics of Information, in: The Journal of Political Economy 1961, 213, abrufbar unter https://home.uchicago.edu/~vlima/courses/econ200/spring01/stigler.pdf und *McCall*, The Economics of Information and Job Search, in: Quarterly Journal of Economics, 1970, S. 113 – 126. Informationsökonomische Ansätze sind Teil der Neuen Institutionenökonomik. Diese umfasst verschiedene theoretische Erklärungsansätze, die im Wesentlichen in vier Schulen unterteilt werden: Der Property-Rights-Ansatz oder Theorie der Verfügungsrechte, der Transaktionskostenansatz, der Prinzipal-Agent-Ansatz und informationsökonomische Ansätze, vgl. z. B. *Picot*, Ökonomische Theorien der Organisation – ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [Hrsg.]: Betriebswirtschaftslehre und Ökonomische Theorie, 1991, S. 143.

225 Vgl. *Woratschek*, Betriebsform, Markt und Strategie, 1992, S. 96.

226 Vgl. *Spence*, Informational Aspects of Market Structure: An Introduction, in Quarterly Journal of Economics 1976, 591, 593. Die Effizienz der Informationsmaßnahmen kann anhand der Kosten für Signaling- und Screening-Aktivitäten beurteilt werden.

Neben der Qualitätsunsicherheit sind für die Verbraucher **zwei weitere Ausprägungen von Informationsasymmetrien** in Datenschutzfragen relevant, wenn sie Verträge mit Anbietern schließen. Eine asymmetrische Informationsverteilung kann Ursprung von Konflikten sein, wenn der besser informierte Vertragspartner nach Vertragsschluss seinen Informationsvorsprung zu seinen eigenen Gunsten ausnutzt.[227] So können die Verbraucher die **Fairness des Anbieters nach eingegangener Vertragsbeziehung** vor und nach Vertragsabschluss nicht beurteilen oder abschätzen.

Für die Analyse wird zwischen der Vertragspartei, die als Auftraggeber bessere Informationen über das Kooperationsziel hat und nicht geschädigt werden will, und dem Auftragnehmer, der bessere Informationen über Gegenstand und Aufgabe besitzt, unterschieden.[228] Übertragen auf einen Kaufvorgang mit **Vertragsabschluss** zwischen Anbietern und Verbrauchern käme den Verbrauchern die Rolle des Auftraggebers zu, während die Anbieter von IoT-Geräten als Auftragnehmer agieren. Verletzt beispielsweise ein Hersteller die Datenschutzrechte des Verbrauchers nach Vertragsschluss, was diesem nachträglich bekannt wird, so hatte er **verborgenen Absichten** (sog. *Hidden Intention* oder *Hold-up*). Dem Verbraucher entgeht Nutzen, wenn seine Investition in den Kauf des Produktes durch die Rechtsverletzung wertlos wird oder an Wert verliert.

Im Fall von **verborgenen Handlungen** (sog. *Hidden Action* mit *Moral Hazard*) bleibt dem Verbraucher (Auftraggeber) die Verletzung von Datenschutzrechten durch den Anbieter (Auftragnehmer) vollständig unbekannt oder wird erst nach einiger Zeit deutlich. Von *Moral Hazard* könnte auch dann gesprochen werden, wenn Hersteller von IoT-Geräten beispielsweise mehr Daten der Verbraucher erfassen und verwerten würden als in den Datenschutzbestimmungen des gekauften Produktes angegeben wird und der Verbraucher dies gar nicht oder viel zu spät entdeckt.

Verbraucher können aufgrund dieser Risiken vor Vertragsabschlüssen zurückschrecken. Auftragnehmer (hier: Smart-TV-Anbieter) können dem durch eine zielgerichtete **Risikokommunikation** begegnen. Kommuniziert werden können grundsätzlich alle Maßnahmen, die die Autorität des

---

227 Opportunistisches Verhalten wird auch in einer einschlägigen BDI-Studie thematisiert, vgl. *BDI*, Verbraucherleitbild und Positionsbestimmung zum "Mündigen Verbraucher", 2014, S. 14, abrufbar unter https://bdi.eu/media/presse/publikationen/gesellschaft-verantwortung-und-verbraucher/BDI_Studie_zum_muendigem_Verbraucher.pdf.

228 Diese Überlegungen sind Grundlage des sog. Prinzipal-Agent-Ansatzes, der sich ursprünglich auf Vertragsverhältnisse auf der gleichen Marktseite bezieht, aber auch für die Analyse anderer Vertragsverhältnisse genutzt werden kann. Vgl. für einen Überblick über den Prinzipal-Agent-Ansatz z.B. *Richter/Furubotn*, Neue Institutionenökonomik, 1996. *Matten* hat den Prinzipal-Agent-Ansatz genutzt, um das Verhältnis zwischen Unternehmen und Stakeholdern zu untersuchen, vgl. *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 198.

Verbrauchers als Auftraggeber erhöhen und die Sorge vor opportunistischem Verhalten mildern.[229]

Neben einer Schärfung des Verbraucherbewusstseins sind somit Maßnahmen zur Überwindung dieser Informationsasymmetrien unerlässlich. Soweit dies gelingt, werden Verbraucher zu mehr Eigeninitiative ermutigt und die Nachfrage nach datenschutzfreundlichen Produkten langfristig gefördert.

3. Ansätze für mehr wettbewerblichen Datenschutz

Vieles spricht dafür, dass die Menge und vor allem Ungenauigkeit und Unübersichtlichkeit der von Smart-TV-Herstellern zur Verfügung gestellten Informationen den Verbraucher schon jetzt überfordert.[230] In der Literatur finden sich verschiedene Ansätze, wie der Verbraucher besser über Datenschutzbestimmungen informiert werden kann. Einige dieser Ansätze werden nachfolgend kurz dargestellt.

a) Digitale Helfer

Der Einsatz digitaler Instrumente kann informierte Entscheidungen und aktives Mitwirken von Verbrauchern fördern. Zu denken ist hier beispielsweise an Datenschutz-Cockpits[231], mit denen sich die Intensität der Datenverarbeitung durch den Verbraucher regulieren ließe. Mithilfe eines solchen Datenschutz-Cockpits sollte sich einerseits sämtliche nicht systemrelevante Software einschließlich Apps deinstallieren lassen. Zum anderen sollte der Nutzer hierdurch in die Lage versetzt werden, sämtliche Datenschutzoptionen zu überprüfen und zu ändern. Der Nutzer muss insbesondere sämtliche erteilte Einwilligungen einsehen[232] und ggf. widerrufen sowie Datenverarbeitungsberechtigungen für Software, insbesondere Apps, granular gewähren und entziehen können.

---

229 Vgl. für eine praktische Anwendung der Erklärungsansätze zur Risikokommunikation *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 203. Bei moralischen Risiken in einzelwirtschaftlichen individuellen Vertragsbeziehungen auf der gleichen Marktseite können auch Anreiz- und Belohnungssysteme risikomindernd eingesetzt werden.

230 Vgl. zum „information overload“ bzw. „Informationsverdruss“ bei Finanzprodukten *Buck-Heeb/Lang* in: BeckOGK, Stand: 01.03.2020, § 675 BGB Rn. 237 - 239 m. w. N. aus Rechtsprechung und Literatur.

231 Im englischsprachigen Raum wird anstelle von „Cockpit“ der treffendere Begriff „dashboard“, also „Armaturenbrett“, verwendet. Nach allgemeinem Sprachverständnis ist ein Armaturenbrett deutlich weniger komplex ausgestaltet als ein (Flugzeug-)Cockpit. Der „Begriff Datenschutz-Armaturenbrett“ wäre aber wohl schlicht nicht griffig genug. Auch beim Datenschutz-Cockpit kommt es aber entscheidend auf Übersichtlichkeit und schnelle Erfassbarkeit der wesentlichen Einstellungen an.

232 Dies ist aktuell nicht immer der Fall. Um Änderungen vornehmen zu können, blieb mitunter als einzige Möglichkeit das Zurücksetzen des Geräts auf den Werkszustand.

Mittel- bis langfristig könnten Apps aus dem Bereich *Legal Tech* zum Einsatz kommen, mit denen der Verbraucher Datenschutzbestimmungen von Softwareanwendungen auf Konformität mit dem Datenschutzrecht überprüfen kann. Auch hier gibt es bereits erste Pilotprojekte, insbesondere zu *Privacy Bots*[233]. So hatte das Forschungskonsortium „PGuard“ u. a. einen Prototyp für eine Datenschutzscanner-App entwickelt, mit deren Hilfe Datenschutzbestimmungen auf kritische Passagen hin untersucht werden können.[234]

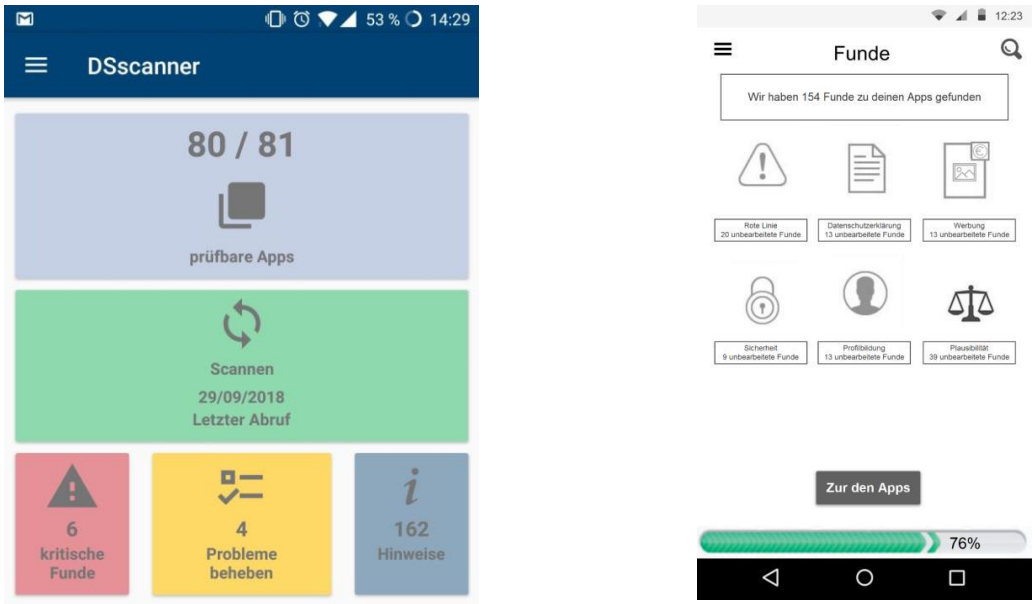


Abbildung 12:Datenschutz-Scanner – Screenshots [235]

Das Europäische Hochschulinstitut stellt mit *CLAUDETTE*[236] ein auf maschinellem Lernen basierendes Tool zur Verfügung, mit dem Texte von englischsprachigen Allgemeinen Geschäftsbedingungen auf ihre Rechtmäßigkeit hin überprüft werden können. Seit 2019 werden zudem die englischsprachigen Datenschutzbestimmungen einiger großer Internetdienstleister auf ihre Vereinbarkeit mit der DSGVO hin analysiert.

---

233 Vgl. dazu *Nüske/Olenberger/Rau/Schmied*, Privacy Bots, DuD 2019, 1; *Specht-Riemenschneider/Bienemann*, Informationsvermittlung durch standardisierte Bildsymbole, in: Specht-Riemenschneider/Werry/Werry [Hrsg.], Datenrecht in der Digitalisierung, 2019, S. 324, 332.

234 S. zum Projekt *Kettner/Bolte/Heyer/Ingenrieth/Ludwig/Thorun u.a.*: Abschlussbericht PGuard (Fn. 98).

235 Teil-Screenshot von http://www.claudette.eu/gdpr/answers/Facebook.html.

236 Entnommen aus *Kettner/Bolte/Heyer/Ingenrieth/Ludwig/Thorun u. a.*: Abschlussbericht PGuard (Fn. 98, 2019, S. 105 (linkes Bild), S. 114 (rechtes Bild).

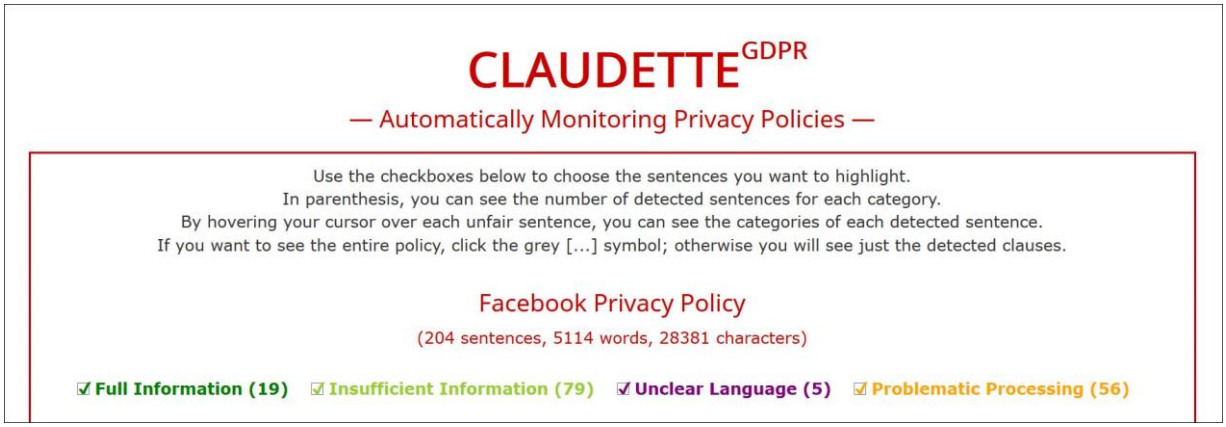


Abbildung 13:CLAUDETTE-Analyse der Facebook-Datenschutzbestimmungen[237]

Der Ansatz, Verbrauchertexte mit lernenden Algorithmen zu analysieren, ist durchaus vielversprechend und könnte für Verbraucher in Zukunft eine wertvolle Hilfestellung darstellen. Auch Behörden und Verbände könnten entsprechende Online-Tools oder Apps einsetzen und ggf. zu deren Weiterentwicklung beitragen. Solche Anwendungen würden eine konsequente Durchsetzung von Verbraucherrechten durch Behörden und Private (Verbände) indessen keinesfalls überflüssig machen. Zum einen besteht die Gefahr, dass Unternehmen versuchen, ein „Anschlagen" der Algorithmen durch laufende Textanpassungen gezielt zu verhindern. Zum anderen würden die eingesetzten Algorithmen in erster Linie auf bereits gefestigter Rechtsprechung bzw. Entscheidungspraxis aufbauen und daher neuartige Rechtsverletzungen schwerer erkennen können. Eine beständige Rechtsdurchsetzung würde somit wiederum zur Verbesserung der Algorithmen beitragen.

Algorithmenbasierte Analysewerkzeuge sind mithin zum einen langfristig eine interessante Option, zum anderen wäre vorstellbar, dass Unternehmen auf – jedenfalls zunächst – freiwilliger Basis Informationen in einer für die Prüfalgorithmen auslesbaren Form zur Verfügung stellen. So könnten diese zentrale Informationen schnell, fehlerfrei und idealerweise in mehreren Sprachversionen erfassen und für den Verbraucher oder – zur einfacheren Verarbeitung – auch dessen Einwilligungsassistenten aufbereiten.

b) Zertifizierungen/Prüfsiegel

Bei Datenschutz-Zertifizierungen bestätigt ein Dritter (Behörde, Unternehmen oder Organisation), dass ein Produkt oder eine Dienstleistung konkret festgelegte Datenschutz-Kriterien erfüllt oder dass bei bestimmten Datenverarbeitungsvorgängen solche Datenschutz-Kriterien einhalten werden. Der Mehrwert einer Zertifizierung für Verwender und Verbraucher hängt maßgeblich davon

237 Teil-Screenshot von http://www.claudette.eu/gdpr/answers/Facebook.html.

ab, dass das mit der Zertifizierung bestätigte Datenschutzniveau als anspruchsvoll angesehen wird und die zertifizierende Institution selbst Vertrauen beim Verbraucher genießt.[238]

c) Datenschutz-Labels

Labels haben den Vorteil, dass sie bereits prominent an der Verkaufsverpackung angebracht oder in unmittelbarer Nähe einer Produktabbildung dargestellt werden können. Beispiele sind etwa das europäische Energie-Label oder der Nutri-Score. Es läge daher nahe, auch für IoT-Geräte eine entsprechende Kennzeichnung zu fordern, die es dem Verbraucher zudem erlauben würde, die Datenschutzqualität verschiedener Produkte zu vergleichen.

Ein einfach zu erfassendes Datenschutz-Label könnte etwa wie folgt aussehen:

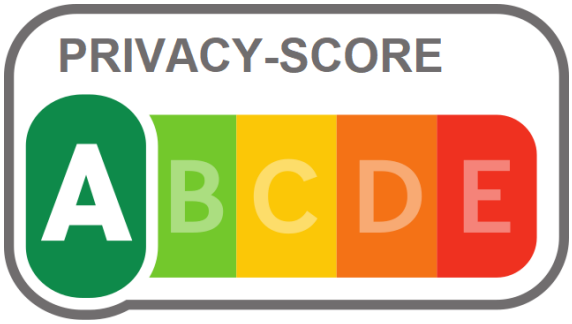


Abbildung 14:Nutri-Score für Datenschutzbestimmungen[239]

Man darf allerdings nicht vergessen, dass – anders als bei der Beurteilung von Inhaltsstoffen in Lebensmitteln – der hohen Komplexität von Datenschutzbestimmungen Rechnung getragen werden muss. Insbesondere müsste vor Einführung eines Labels ein Konsens etwa darüber bestehen, welche Verarbeitungen besonders gefährlich sind, welche Datentransfers risikoerhöhend wirken, welche Standard-Löschungsautomatismen eingreifen sollten etc. Zudem müssten Wechselwirkungen bedacht werden. So wirkt der Eingriff in die informationelle Selbstbestimmung bei langen Speicherdauern deutlich stärker als bei kurzen Speicherdauern. Schließlich wäre zu überlegen, inwieweit Sicherheitsstandards in das Datenschutz-Label einfließen müssten, da ein hohes Datenschutzniveau bei bestehenden Sicherheitslücken nicht gewährleistet werden könnte. Ein wirklich „einfaches“ Datenschutz-Label könnte daher allenfalls am Ende eines längeren Diskussionsprozesses stehen. Jedenfalls kurzfristig ist es kein geeignetes Instrument, um das Informationsdefizit auf Verbraucherseite effektiv zu verringern.

---

238 S. *Siegel treiben den Umsatz* (handelsjournal.de, 29.10.2019), abrufbar unter https://handelsjournal.de/unternehmen/marketing/siegel-treiben-den-umsatz.html (unter Beugnahme auf eine Gütesiegel-Studie von Splendid Reseach).

239 Eigene Darstellung auf Basis einer gemeinfreien Nutri-Score-Abbildung.

Ein Datenschutz-Label mit Benotung wäre vor dem Hintergrund einer notwendigen Gesamtbeurteilung eines Produkts schwierig umzusetzen. Es gibt jedoch Ansätze, die darauf abzielen, dem Nutzer in Form eines Labels eine überschaubare Anzahl wesentlicher Informationen zu präsentieren. So haben Wissenschaftler auf Basis von Interviews mit Datenschutz-Experten und Verbrauchern[240] folgendes Label entwickelt:

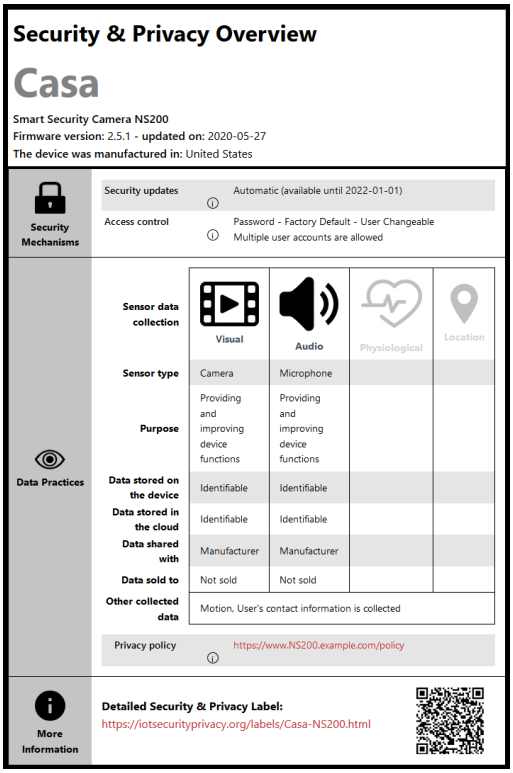


Abbildung 15:IoT-Label für Datenschutz- und Datensicherheit[241]

Man mag darüber streiten, ob dieser Prototyp tatsächlich die wesentlichen Eigenschaften des Produkts wiedergibt.[242] Es enthält jedoch (z. T. auf Seite 2) – differenziert nach Nutzungsprozess – wichtige Verbraucherinformationen wie Update-Zeitraum, Datenempfänger, Speicherdauern

240 S. dazu *Emami-Naeini/Agarwal/Cranor,* Specification for an IoTPrivacy and Security Label, abrufbar unter https://www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf.

241 Grafik entnommen aus der Website https://www.iotsecurityprivacy.org/labels.

242 Es ist fraglich, ob die für den Großteil der Verbraucher ohnehin nicht verständlichen Sicherungsmechanismen (insb. auf Seite 2) nicht zu viel Raum einnehmen; hier wäre ggf. eine Verlinkung sinnvoller. Umgekehrt ist dem Label (auch nicht dessen Seite 2) beispielsweise nicht genau zu entnehmen, welche Daten(kategorien) konkret bei welcher Nutzung erhoben werden. Zudem lässt das Label Raum für pauschalierende Angaben.

und einen Link zu den Datenschutzbestimmungen. Ungeachtet des sicherlich vorhandenen Verbesserungspotentials wäre eine branchenweite Verwendung eines solchen Labels ein Informationsgewinn für den Verbraucher.

Von wissenschaftlicher Seite wurden darüber hinaus Vorschläge für Datenschutz-Label unterbreitet, die jedoch viel Raum einnehmen und daher weniger als Label im Sinne eines Etiketts (jedoch ggf. als *One-Pager*, s. dazu unten e)) geeignet sind:

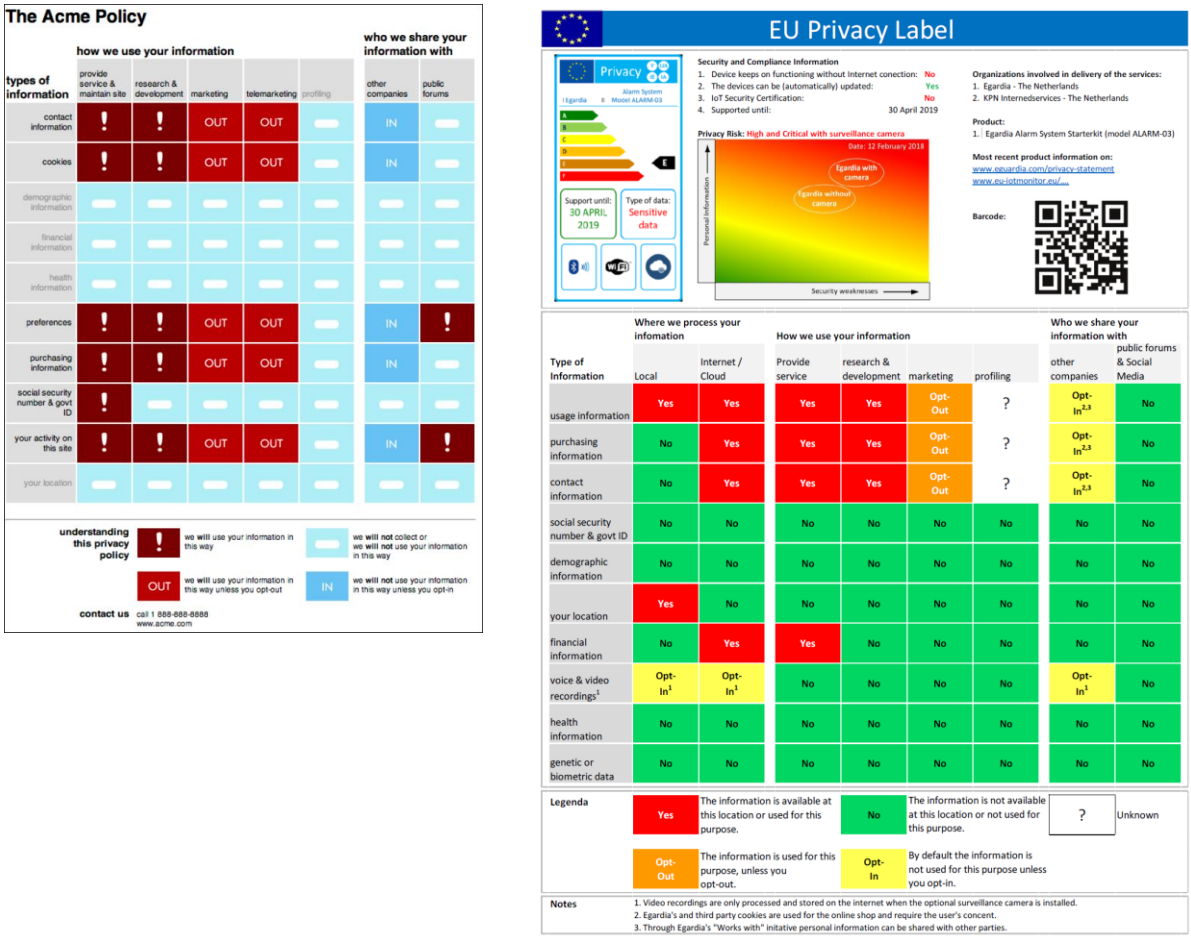


Abbildung 16:Beispiele für Entwürfe sehr ausführlicher Datenschutz-Labels[243]

d) Bildsymbole

Bildsymbole eignen sich für eine schnelle Verbraucherinformation, da im Idealfall auf einen Blick erfasst werden kann, welche Eigenschaft(en) ein Produkt oder eine Dienstleistung aufweist. Auch

243 Linkes Beispiel: *Kelley/Bresee/Cranor/Reeder*, A "Nutrition Label" for Privacy, SOUPS 2009, 1, 6., abrufbar unter https://dl.acm.org/doi/pdf/10.1145/1572532.1572538; rechtes Beispiel: van Diermen, The Internet of Things: a privacy label for IoT products in a consumer market

die Bundesregierung hält Piktogramme, Icons oder Bildsymbole für ein probates Mittel, um bei den Nutzern für eine bessere Verständlichkeit von Datenschutzbestimmungen zu sorgen.[244]

Voraussetzung für einen effektiven Einsatz von Bildsymbolen ist insbesondere, dass es sich um nicht bereits anderweitig etablierte Zeichen handelt. Zudem sollten sie aus sich heraus hinreichend aussagekräftig sein. Zumeist kann eine Kombination von Bildsymbol und kurzem Beschreibungstext für die bestmögliche Verständlichkeit sorgen.[245] Schließlich sollte ein einheitlicher Symbolkanon verwendet werden, der sich dem Verbraucher nachhaltig einprägt.[246]

Für eine Verbraucherinformation mittels smarter Bildsymbolik eignen sich zunächst Hinweise, die bereits vor dem Kauf eines Produkts auf der Verkaufsverpackung oder im Fernabsatz in der Nähe der Preisauszeichnung platziert werden könnten. Wie oben im Bericht erwähnt, sind beispielsweise der Speicherort für persönliche Daten[247] und der Mindestversorgungszeitraum mit Software-Sicherheitsupdates[248] für Verbraucher von großer Bedeutung. Beide Aspekte ließen sich gut als Bildsymbole darstellen, etwa folgendermaßen[249]:

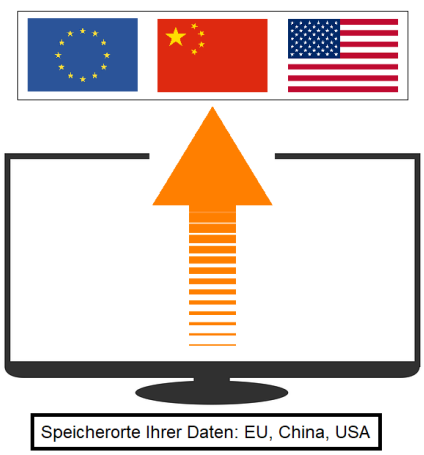


Abbildung 17:Beispiele für Bildsymbole[250]

244 S. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Müller-Böhm, Thomae, Aggelidis u. a. der Fraktion der FDP* (Fn. 574), S. 6.

245 S. *Harley*, Icon Usability (nngroup.com, 27.07.2014), abrufbar unter https://www.nngroup.com/articles/icon-usability/.

246 S. *Heckmann/Paschke* in in Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 12 Rn. 54.

247 S. dazu Abbildung 6, S. 51.

248 S. S. 226.

249 Bei anderen IoT-Geräten ließe sich das Fernsehersymbol austauschen, etwa gegen ein Smartphone- oder Tablet-Symbol.

250 Eigene Darstellungen unter Verwendung gemeinfreier Bilder.

Ergänzt werden könnten sie durch einen QR-Code, über den der Nutzer bereits vor dem Kauf sämtliche Nutzungs- und Datenschutzbestimmungen und andere wichtige Informationen wie z. B. datenempfangende Unternehmen *en détail* bereits vor dem Kauf auf einer hierfür vorgesehenen Website abrufen kann. Dies könnte einerseits durch Einscannen des Codes mittels einer Barcode-App oder durch Anklicken des Hinweistextes geschehen:

Abbildung 18:Beispiel für Datenschutz-QR-Code[251]

Des Weiteren ließen sich Bildsymbole in dem Moment einsetzen, in dem eine Einwilligung eingeholt wird. Falls die Einwilligung etwa dazu führt, dass das Fernsehverhalten des Nutzers oder seine biometrischen Daten erfasst werden, so könnten in der Nähe der Einwilligungs-Schaltfläche folgende Hinweissymbole angezeigt werden:

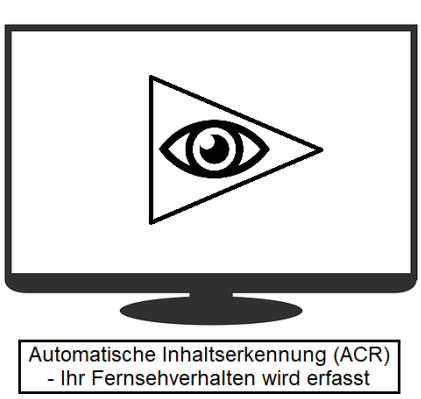


Abbildung 19:Beispiele für Bildsymbole[252]

251 Eigene Darstellung unter Verwendung gemeinfreier Bilder.

252 Eigene Darstellungen unter Verwendung gemeinfreier Bilder.

e) *One-Pager*

Beim sog. *One-Pager* handelt es sich um eine Kurzfassung der Datenschutzbestimmungen, welche deren wesentlichen Inhalt wiedergibt. Mit diesem Instrument soll die Abschreckungswirkung abgebaut werden, die von oftmals langen Datenschutzbestimmungen ausgeht. Ein *One-Pager* erscheint in diesem Zusammenhang erfolgversprechender als etwa Zwischenzusammenfassungen, wie sie von manchen Unternehmen in ihren Datenschutzbestimmungen verwendet werden.

Entscheidend für die Verständlichkeit eines *One-Pagers* ist indessen nicht die Tatsache, dass dieser die Länge von einer Seite nicht überschreitet, sondern dass er die wirklich relevanten Informationen kompakt auf den Punkt bringt. Dies zu bewerkstelligen, ist keine einfache Aufgabe, wie etliche Datenschutz-*One-Pager* beweisen, die im Internet auffindbar sind. Aus schlechten Datenschutzbestimmungen wird durch bloße Zusammenfassung oder Kürzung kein guter *One-Pager*. Und selbst bei guten Datenschutzbestimmungen muss sorgsam darauf geachtet werden, dass bei einer kompakten Darstellung tatsächlich die wichtigsten Informationen wiedergegeben werden.[253] Soweit ein *One-Pager* nichtssagende Angaben erlaubt, ist hiermit für den Verbraucher kein Mehrwert verbunden. Diese Schwierigkeiten mögen auch die Ergebnisse einer Studie des Instituts *ConPolicy* aus dem Jahr 2018 erklären. Diese hatte ergeben dass *One-Pager* – jedenfalls bei isolierter Verwendung – zwar die Lesewahrscheinlichkeit erhöhen, jedoch allenfalls unwesentlich zu einer besseren Informiertheit der Verbraucher beitragen.[254] Ein alternativer Ansatz könnte es sein, die oben in Abbildung 17, S. 110 dargestellten Labels oder Elemente hieraus im Rahmen eines *One-Pagers* zu verwenden.

f) Tabellarische Darstellung

Auch eine tabellarische Übersicht über Datenverarbeitungsvorgänge – anstelle des *One-Pagers* oder zu dessen Ergänzung als separate Übersicht oder Teil der ausführlichen Datenschutzbestimmungen – sollte daher erwogen und erprobt werden.

Dies könnte in etwa so aussehen:

---

253 Da beispielsweise die Auskunftsrechte betroffener Personen in der DSGVO eingehend geregelt sind, müssen diese nicht einzeln aufgeführt werden; ein Verweis auf eine Website mit ausführlicheren Informationen wäre insoweit ausreichend. Ebenso würde es genügen, Details zu Trackingtools per Link abzurufen. Umgekehrt ist es z. B. von essentieller Bedeutung für die betroffenen Personen, welche Dritten ihre Daten zu welchen Zwecken erhalten.

254 *ConPolicy*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des *One-Pager*-Ansatzes und weiterer Lösungsansätze im Datenschutz, 28.02.2018, abrufbar unter https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf.

Nutzung	erhobene Daten	Zweck	Rechtsgrundlage	Datenweiterleitung? Falls ja, mit Empfänger und Sitz	Speicherort und maximale Speicherdauer
Firmware-Update	IP-Adresse, Gerätestandort, aktuell installierte Firmwareversion	Aktualisierung der Firmware Ihres Geräts zu Sicherheitszwecken und/oder zur Verbesserung der Gerätesoftware	Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO)	nein	Deutschland, 1 Tag

Tabelle 11: Beispiel für übersichtliche und konkrete Datenverarbeitungsdarstellung

Eine solche Darstellung bietet sich insbesondere dann an, wenn unterschiedliche Handlungen der betroffenen Person verschiedenartige Datenverarbeitungen auslösen.

g) Umsetzung als Schichtenmodell

Um eine bessere Zugänglichkeit der wesentlichen Informationen zu erreichen, sollte auf eine vereinfachte Darstellung von Datenschutzbestimmungen hingewirkt werden. Dies lässt sich insbesondere durch ein gestuftes Zugänglichmachen erreichen. Ein entsprechendes Modell könnte etwa wie folgt aussehen:

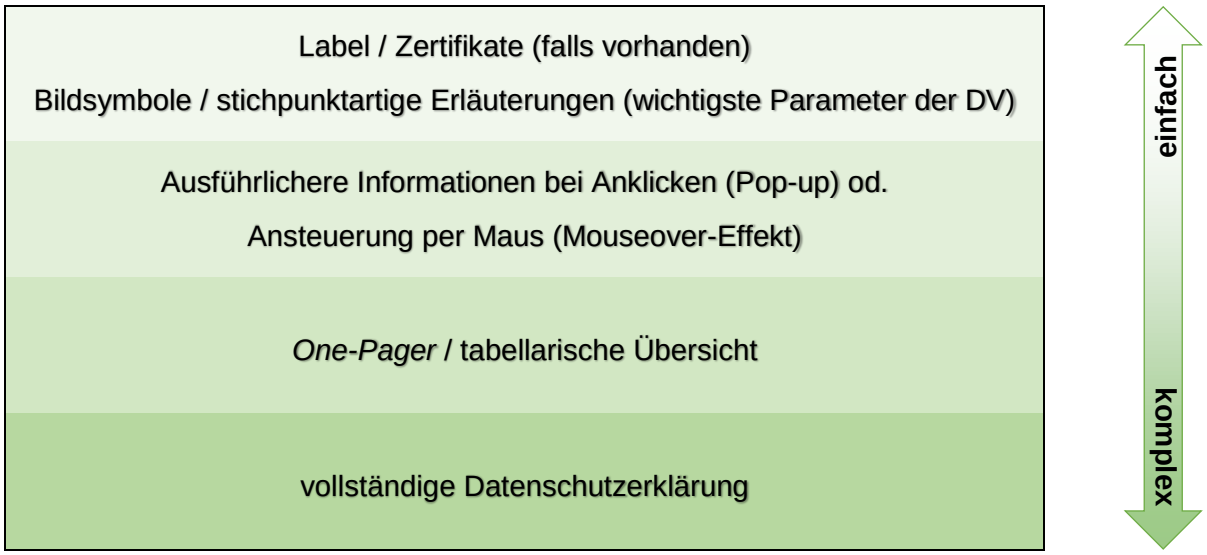


Abbildung 20:Datenschutzinformationen im Schichtenmodell

Es steht zu hoffen, dass sich mit einer weiteren Verbreitung von Schichtenmodellen auch Darstellungs- und Qualitätsstandards herausbilden, ggf. auch unterstützt durch die Datenschutz-Aufsichtsbehörden. Je aussagekräftiger und zugänglicher gerade die obersten Informationsschichten werden, desto größer sind die Chancen, dass Nutzer sie auch tatsächlich lesen. Die oben dargestellten Schichten sind dabei keineswegs in Stein gemeißelt. Sie können auch vollständig oder in Teilen kombiniert oder weiter aufgeteilt werden, je nach Komplexität der Datenverarbeitungen, die darzustellen sind und stets unter dem Leitmotiv bestmöglicher Verständlichkeit und Informationsvermittlung.

In Summe werden dem Verbraucher mit dem Schichtenmodell natürlich mehr Informationen präsentiert als zuvor. Aber angesichts der Tatsache, dass ohnehin kaum jemand ausführliche Verbrauchertexte mit der gebotenen Gründlichkeit liest (s. dazu S. 52 ff.), kann durch die deutlich besser erfassbaren oberen Informationsschichten letztlich eine viel effektivere Verbraucherinformation bei deutlich verringertem Zeitaufwand erreicht werden.

V. Praxis der Datenverarbeitung

Eine intransparente oder nicht rechtzeitige Information des Verbrauchers kann auch für die Frage von Bedeutung sein, ob eine hinreichende Rechtsgrundlage für die Datenverarbeitung durch den Smart-TV-Hersteller besteht. Mit der Rechtmäßigkeit der Datenverarbeitung (dazu unter 1.) dem Problem des *Digital Nudging* (dazu unter 2.) und der Verantwortung für die Datenverarbeitung (dazu unter 3.) befasst sich der folgende Abschnitt.

1. Rechtmäßigkeit der Datenverarbeitung

Eine Verarbeitung personenbezogener Daten ist nach Art. 8 Abs. 2 S. 1 der Europäischen Grundrechtecharta verboten, es sei denn es besteht hierfür eine Einwilligung der betroffenen Person oder eine sonstige „gesetzlich geregelte legitime Grundlage“. Dieses Verbot mit Erlaubnisvorbehalt nimmt Art. 6 DSGVO auf und liefert die notwendigen Rechtsgrundlagen für eine legitime Datenverarbeitung. Im Hinblick auf IoT-Geräte bietet die DSGVO insbesondere drei Rechtsgrundlagen, die für die Verarbeitung personenbezogener Daten herangezogen werden können: die Notwendigkeit für die Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO), die Wahrung berechtigter Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO) oder die Einwilligung der betroffenen Person (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO).[255] Diese drei wichtigsten Rechtsgrundlagen werden nachfolgend eingehender untersucht.

a) Notwendigkeit für die Vertragserfüllung

Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO zufolge ist die Verarbeitung personenbezogener Daten erlaubt, soweit sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist,

---

255 Nach wohl überwiegender Meinung dürfte es auch zulässig sein, eine Datenverarbeitung auf mehrere Rechtsgrundlagen zu stützen, solange dies nach Treu und Glauben in der erforderlichen transparenten Form geschieht und der betroffenen Person insbesondere keine in Wirklichkeit nicht vorhandene Entscheidungsgewalt suggeriert wird, S. etwa *Schulz* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 11 f.; *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 12. Für diese Auffassung spricht auch Art. 17 Abs. lit. b) DSGVO, der den Fall vorsieht, dass nach Widerruf der Einwilligung eine andere Rechtsgrundlage eingreift.

oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

aa) Ermittlungsergebnisse

Die befragten Unternehmen machen in unterschiedlichem Umfang Gebrauch vom Rechtfertigungsgrund der Notwendigkeit für die Vertragserfüllung. Häufiger werden (z. T. auch ergänzend) die Einwilligung des Nutzers oder die Wahrung berechtigter Interessen des Verantwortlichen zur Rechtfertigung herangezogen. Soweit auf die Notwendigkeit für die Vertragserfüllung verwiesen wird, werden z. T. daneben noch andere Rechtfertigungsgründe angeführt.

Unterschiedlich deutlich wird in den Datenschutzbestimmungen, welche Daten für welchen Zweck auf Grundlage der Vertragserfüllungsnotwendigkeit verarbeitet werden. Anschaulich wurde dies etwa in der „Datenschutzerklärung Smart TV Services“ von *TCL* für den Zweck der Ferndiagnostik formuliert:

> „ […] Ferndiagnostik: Als Teil der Services stellen wir Ihnen Ferndiagnostikleistungen zur Verfügung. Hierfür verarbeiten wir die Device-ID, Gerätenummer, Seriennummer, MAC-Adresse sowie Fehlerprotokolle, Fehlercodes und Fehlerbeschreibungen, die uns von dem fehlerhaften Modul (Anwendung, Middleware-System) zur Verfügung gestellt werden.
>
> Rechtsgrundlage für die entsprechende Verarbeitung Ihrer personenbezogenen Daten sind vertragliche Zwecke gemäß Art. 6 (1) b) der DSGVO.“[256]

An konkreten Sachverhalten wurden darüber hinaus in Datenschutzbestimmungen beispielsweise genannt:

- die Übermittlung von Gerätedaten wie Firmware-Version zur Durchführung eines Firmware-Updates;
- die Übermittlung von Spracheinstellungen zur Anzeige des TV-Portals in der betreffenden Sprache oder
- die Übermittlung von Kundendaten zur Erbringung von Kundendienstleistungen.

256 *TCL*, Datenschutzerklärung – Smart TV Services, unter *4. Zwecke für die wir Ihre personenbezogenen Daten verarbeiten und/oder nutzen und Rechtsgrundlagen*. Diese Datenschutzerklärung wurde mit Wirkung vom 20.12.2019 abgelöste von den TCL-Datenschutzbestimmungen mit dem Titel „TCL Globaler Datenschutzhinweis“, in dem die zitierte Textpassage nicht mehr vorkommt.

Überwiegend wurde die Rechtsgrundlage der Vertragserfüllungsnotwendigkeit lediglich angegeben, ohne einen direkten Bezug zu den konkret verarbeiteten Daten herzustellen. So heißt es etwa im Datenschutzhinweis von *Panasonic*:

> „[…] Wir dürfen personenbezogene Daten nicht ohne gültige Rechtsgrundlage verarbeiten. Deshalb verarbeiten wir Ihre personenbezogenen Daten nur, wenn:
>
> […] II. die Verarbeitung notwendig ist, damit wir unseren vertraglichen Verpflichtungen Ihnen gegenüber nachkommen können oder auf Ihre Anfrage hin vorvertragliche Schritte unternehmen können, […]“[257]

bb) Rechtliche Würdigung

Gem. Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO ist zum einen eine Datenverarbeitung zulässig, die für die Erfüllung eines rechtsgeschäftlichen Schuldverhältnisses[258], dessen Partei die betroffene Person ist, erforderlich ist. Zum anderen dürfen personenbezogene Daten verarbeitet werden, soweit dies zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Wie eng oder weit das Kriterium der Erforderlichkeit auszulegen ist, ist bislang nicht geklärt. Unstreitig ist, dass jedenfalls die Datenverarbeitungsvorgänge rechtmäßig sind, ohne die ein Vertrag überhaupt nicht durchgeführt werden kann bzw. die eine unentbehrliche Grundlage für das Zustandekommen des Vertrags bilden. Denkt man in diesen Fällen die Datenverarbeitung hinweg, kann der Vertrag unter keinen Umständen durchgeführt werden bzw. zustande kommen. So kann etwa ein Zeitungsabonnement nicht ohne eine Adressangabe funktionieren. Ist in diesem Sinne eine *objektive Erforderlichkeit*[259] der Datenverarbeitung gegeben, ist diese auch zulässig.

Darüber hinaus wird vertreten, Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO erlaube auch solche Datenverarbeitungen, die zwar nicht unabdingbar für die Vertragserfüllung, aber ohne zumutbare Alternative[260] oder zumindest förderlich für die Erreichung des Geschäftszwecks[261] seien. Bislang nur

---

257 *Panasonic*, Datenschutzhinweis, unter *3. Auf welcher Rechtsgrundlage verarbeiten wir personenbezogene Daten?*

258 Gesetzliche Schuldverhältnisse scheiden aus, da sie nicht auf autonomem Parteiwillen beruhen, S. dazu *Wolff* in Schantz/Wolff [Hrsg.], Das neue Datenschutzrecht, 2017, Rn. 546.

259 *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO, Rn. 16.

260 *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO, Rn. 20, unter Verweis auf DSGVO-Erwägungsgrund 39; *Buchner/Petri* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 45.

261 *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO, Rn. 21.

vereinzelt diskutiert wird in der Literatur die Frage, ob ein echter Tausch personenbezogener Daten gegen Gratisleistungen als (zusätzlicher) Vertragszweck im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO definiert werden könnte.[262] Wäre dies möglich, wäre grundsätzlich jede rechtlich zulässige Datenverarbeitung als für die Vertragserfüllung erforderlich anzusehen, sofern diese explizit zum Vertragsgegenstand gemacht würde.

Der Europäische Datenschutzausschuss (EDSA) vertritt die Auffassung, dass eine Datenverarbeitung zur Vertragserfüllung dann nicht erforderlich ist, wenn es zu dieser realistische, weniger einschneidende Alternativen gibt.[263] Der EDSA verweist in diesem Zusammenhang mehrfach darauf, was die betroffene Person vernünftigerweise erwarten bzw. vorhersehen kann.[264] Auch der EDSA geht somit nicht von einem absoluten Ansatz der unbedingten Erforderlichkeit aus. Er stellt jedoch unmissverständlich klar, dass Datenverarbeitungen nicht von Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO gedeckt sind, die lediglich nützlich für die Vertragserfüllung sind. Es müsse untersucht werden, ob die Datenverarbeitungsvorgänge wirklich erforderlich seien für die Erfüllung des Vertrags oder doch eher für das Geschäftsmodell des Verantwortlichen.[265]

Der Auffassung des EDSA ist zuzustimmen. Dies gilt zum einen für die Beurteilung der Erforderlichkeit aus der Perspektive der betroffenen Person und nicht dessen Vertragspartners.[266] Entscheidend für die Erforderlichkeit einer Datenverarbeitung ist daher nicht die Zumutbarkeit von Ausweichalternativen für den Verantwortlichen. Diese wäre im Einzelfall auch nicht immer einfach zu bestimmen. Es trifft zwar zu, dass gem. DSGVO-Erwägungsgrund 32 S. 9 eine Datenverar-

---

262 Dies andeutend etwa *Assion/Nolte/Veil* in Gierschmann/Schlender/Stentzel/Veil [Hrsg.], Kommentar Datenschutz-Grundverordnung, Art. 6 Rn. 90. Ablehnend *Specht-Riemenschneider/Dehmel/Kenning/Liedtke/Micklitz/Scharioth*, Grundlegung einer verbrauchergerechten Regulierung interaktionsmittelnder Plattformfunktionalitäten - Stellungnahme des Sachverständigenrats für Verbraucherfragen bei dem Bundesministerium der Justiz und für Verbraucherschutz, 2020, S. 26 f., abrufbar unter https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Stellungnahme_Regulierung_Plattformfunktionalit%C3%A4ten.pdf.

263 *Europäischer Datenschutzausschuss*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 vom 08.10.2019, Rn. 25 (auf Deutsch bislang nicht veröffentlicht), abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

264 *Europäischer Datenschutzausschuss*, a. a. O. (Fn. 263), Rn. 32 f., 38.

265 *Europäischer Datenschutzausschuss*, a. a. O. (Fn. 263), Rn. 37.

266 So zutreffend *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 32; vgl. auch Bundeskartellamt, Beschluss vom 6.02.2019, Az. B6-22/16, Rn. 672, 688 ff. – *Facebook*.

beitung dann als erforderlich anzusehen ist, wenn der „Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann“. Zumutbarkeit kann sich in diesem Kontext nur auf die Sicht des Verantwortlichen beziehen, der zwischen mehreren Alternativen wählen kann. Allerdings dürfte es sich insofern um eine mangelhafte Übersetzung in der deutschen DSGVO-Fassung handeln. So spricht die englische Sprachfassung von einem Verarbeitungszweck, der „reasonably“ (französisch: „raisonnablement“, niederländisch: „redelijkerwijs“), also vernünftigerweise, nicht mit anderen Mitteln erreicht werden kann. In DSGVO-Erwägungsgrund 47 S. 4, wo es darum geht, welche Verarbeitungszwecke die betroffene Person vorhersehen kann, werden die vorgenannten fremdsprachigen Begriffe in der deutschen Fassung auch mit „vernünftigerweise“ übersetzt. Dies spricht für eine (objektivierte) Betrachtung aus Perspektive der betroffenen Person. Abzustellen ist somit darauf, ob eine Datenverarbeitung aus Sicht der betroffenen Person vernünftigerweise nicht anders erwartet werden kann. Zu bejahen wäre dies etwa bei der im Bedarfsfall erfolgenden Verarbeitung von Adressdaten für Zwecke des Kundendienstes (Vor-Ort-Reparatur oder Austausch des Fernsehgeräts). [267]

Während – in beschränktem Umfang – eine wertende Betrachtung im Rahmen der Erforderlichkeit geboten ist, lässt Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO für eine echte Interessenabwägung keinen Raum. Entsprechende Überlegungen zugunsten des Verantwortlichen können vielmehr im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO angestellt werden.[268] Zudem besteht die Möglichkeit, eine Datenverarbeitung durch eine Einwilligung der betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO zu legitimieren (dazu unter c), S. 125).

Ein Vorteil der engen Auslegung des Erforderlichkeitsbegriffs in Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO ist zudem, dass schwierige Abgrenzungsfragen vermieden werden. Bei einer weiten Interpretation im Sinne einer „wirtschaftlichen Erforderlichkeit“ müsste man analysieren, ob die betreffenden Datenverarbeitungen für den Verantwortlichen tatsächlich wirtschaftlich erforderlich oder nur lediglich wirtschaftlich vorteilhaft sind. Infolgedessen müsste man im Rahmen der Erforderlichkeitsprüfung stets die Frage nach möglichen milderen Mitteln stellen. So dürfte man insbesondere nicht außer Acht lassen, dass Werbeeinnahmen grundsätzlich auch ohne Profilbildung erzielt werden können. Je nachdem könnten manche personenbezogenen Daten für die Erbringung einer Gratisdienstleistung tatsächlich erforderlich sein, andere hingegen nicht. Die

---

267 Ähnliches Beispiel (Weitergabe von Adressdaten an Speditionsunternehmen zur Kaufabwicklung) bei *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO Rn. 20. Naturgemäß dürften sich die anzustellenden Erwägungen im Rahmen der „Erwartbarkeit“ aus Sicht der betroffenen Person und der „Zumutbarkeit“ von Alternativen beim Verantwortlichen zu einem großen Teil überschneiden.

268 *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 32.

besseren Argumente sprechen dafür, diese Diskussion im Rahmen einer echten Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO oder der Beurteilung der Freiwilligkeit einer Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO vorzunehmen.

Soweit die im Rahmen der Sektoruntersuchung analysierten Datenschutzbestimmungen konkret die verarbeiteten Daten und Verarbeitungszwecke benannten, die auf die Rechtfertigung wegen Vertragserfüllungsnotwendigkeit gestützt wurden, war dies weitgehend nachvollziehbar. Es ließ sich in diesen Fällen in der Regel ein konkreter enger Bezug der verarbeiteten Daten zur Erbringung der vertraglich geschuldeten Dienstleistung herstellen, etwa die Übermittlung der individuellen Spracheinstellungen für die Anzeige des TV-Portals in der betreffenden Sprache.

Häufig wurde jedoch die Vertragserfüllungsnotwendigkeit in den Raum gestellt, ohne die auf Basis dieses Rechtfertigungsgrundes verarbeiteten Daten konkret zu benennen. In diesen Fällen muss eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO verneint werden, da eine generelle Erforderlichkeit der Verarbeitung sämtlicher verarbeiteter Daten (zu meistens unbestimmten Zwecken) nicht gegeben ist.[269]

b) Wahrung berechtigter Interessen

Der Wahrung berechtigter Interessen kommt als Rechtsgrundlage für Datenverarbeitungen erhebliche praktische Bedeutung zu. Für eine Vielzahl von Sachverhalten sind die anderen Rechtsgrundlagen der DSGVO schlicht nicht passend.[270]

aa) Ermittlungsergebnisse

Die meisten Datenschutzbestimmungen der befragten Unternehmen verweisen zumindest im Hinblick auf einen Teil der verarbeiteten personenbezogenen Daten auf den Rechtfertigungsgrund der Wahrung berechtigter Interessen. In den von den Unternehmen vorgelegten Datenschutzbestimmungen wurden oftmals berechtigte Interessen – z. T. extrem – weit formuliert und nicht näher konkretisiert. Teilweise fand auch eine Vermengung von Verarbeitungszwecken und berechtigten Interessen statt.

Zwar sind die berechtigten Interessen im Lichte der Verarbeitungszwecke zu interpretieren. Allerdings fallen auch die Beschreibungen der Zwecke mitunter vage aus (z. B. „zur Durchsetzung

---

269 Zu diesem Ergebnis käme man sogar, wenn man die Erforderlichkeit im weiten Sinne einer Notwendigkeit der Erbringung der vertraglichen Leistung der betroffenen Person ansähe. Denn selbst in diesem Fall müsste vertraglich klar definiert werden, worum es sich bei der geschuldeten Leistung überhaupt handelt, d. h. welche Daten konkret zu übermitteln wären.

270 S. dazu *Frenzel* in: Paal/Pauly [Hrsg], DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 26 m. w. N.

oder Anwendung unserer Nutzungsbedingungen und anderer Vereinbarungen“ [271], „Gesundheits- und Sicherheitsbewertungen“[272]) oder sie sind als unternehmensinterne Zwecke für betroffene Personen schwer einzuordnen, (etwa „Verwaltung unserer Kommunikationssysteme“[273] oder schlicht „für interne Aufzeichnungen“[274]). In den meisten Datenschutzbestimmungen findet sich das berechtigte Interesse an der Weiterentwicklung oder Verbesserung von Produkten bzw. Dienstleistungen, z. T. auch in Form der „Verbesserung der Nutzererfahrungen“.

Den Datenschutzbestimmungen lässt sich zumeist nicht entnehmen, für welche konkreten Datenverarbeitungen das berechtigte Interesse die Rechtsgrundlage bildet. Verarbeitete Daten, Verarbeitungszwecke und berechtigte Interessen stehen zumeist als Aufzählungen unverknüpft nebeneinander (s. dazu auch E. II. 4. e), S. 76). Eine Auseinandersetzung mit den Interessen der betroffenen Personen ist den Datenschutzbestimmungen nicht zu entnehmen.

bb) Rechtliche Würdigung

Es wird oft übersehen, dass der Rechtfertigungsgrund der berechtigten Interessen nur **unter bestimmten Voraussetzungen** geltend gemacht werden kann: So muss zunächst erläutert werden, welche berechtigten Interessen des Verantwortlichen oder eines Dritten konkret betroffen sind. Dies ergibt sich bereits zweifelsfrei aus Art. 13 Abs. 1 lit. d) DSGVO. Nach allgemeiner Auffassung ist der Begriff der berechtigten Interessen sehr weit auszulegen.[275] Es kann sich dabei auch um wirtschaftliche oder ideelle Interessen handeln.[276] Mit diesem „groben Filter“ werden somit letztlich nur von der Rechtsordnung missbilligte Interessen ausgeschlossen.[277]

Die Datenverarbeitung muss **erforderlich** sein, um die im Rahmen der berechtigten Interessen verfolgten Zwecke zu erreichen. Die berechtigten Interessen müssen dabei letztlich immer im

---

271 S. *Panasonic*, Datenschutzhinweis, unter *5. Warum verwenden wir Ihre personenbezogenen Daten? IX.*

272 *Hisense*, Datenschutzrichtlinie, unter *6. Wie wir die erhaltenen Informationen nutzen*.

273 *Hisense*, a. a. O. (vorhergehende Fußnote).

274 *LG*, Datenschutzrichtlinie, unter *3. Wie verwendet LGE die gesammelten Daten?*

275 S. *Albers/Veit* in: BeckOK Datenschutzrecht, 32. Ed., 01.05.2020, Art. 6 DSGVO Rn. 49. Bestehen Zweifel, inwieweit ein Interesse als „berechtigt“ anzusehen ist, kann dies auch im Rahmen der vorzunehmenden Interessenabwägung noch angemessen berücksichtigt werden.

276 *Schulz* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 57.

277 Vgl. *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs.1 DSGVO Rn. 98.

Zusammenhang mit den Zwecken der Datenverarbeitung gesehen werden.[278] Die Erforderlichkeit ist zu bejahen, soweit die verfolgten Zwecke ohne die konkrete Verarbeitung nicht anderweitig ebenso effektiv erreicht werden können[279]. Beispielsweise ist schwer vorstellbar, wie Direktmarketingmaßnahmen ohne die Verarbeitung von Adressdaten funktionieren sollten. Es ist aber auch denkbar, dass für bestimmte Zwecke gar keine personenbezogenen Daten benötigt werden, da anonymisierte Daten ebenfalls ausreichen würden. Dann liegt keine Erforderlichkeit vor. So ist etwa nicht nachvollziehbar, weshalb für die Sprachdarstellung im Browser eine eindeutige personenbezogene ID gespeichert werden müsste.[280]

Ferner muss zwingend eine **Abwägung** mit den Interessen der betroffenen Person erfolgen[281]. Kennt der Verantwortliche die betroffene Person nicht, wie dies bei der Massendatenverarbeitung der Fall ist, genügt eine typisierte Abwägung.[282] Wiegen die Interessen des Verantwortlichen (oder eines Dritten) zumindest gleich schwer, ist die Datenverarbeitung als rechtmäßig anzusehen.

Die DSGVO selbst gibt nur wenig Hinweise darauf, wie die die jeweiligen Interessen gegeneinander abzuwägen sind[283]. Es dürfte aber klar sein, dass der Verantwortliche bei der Abwägung nicht lediglich widerstreitende abstrakt formulierte Interessen einander gegenüberstellen kann. Wie

---

278 Vgl. *Buchner/Petri* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 152.

279 S. DSGVO-Erwägungsgrund 39, S. 9.

280 So aber die beispielhafte Begründung in der *Google*-Datenschutzerklärung vom 31.03.2020 unter dem Punkt *Im Folgenden erklären wir Ihnen, welche Arten von Daten wir erheben, während Sie unsere Dienste nutzen*.

281 *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO Rn. 51.

282 So auch *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO Rn. 57, unter Verweis auf DSGVO-Erwägungsgrund 47. *Schulz* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 59, spricht insoweit von einer „summarische[n] Prüfung der Belange der betroffenen Personen unter Zugrundelegung von Erfahrungswerten".

283 Es lässt sich lediglich DSGVO-Erwägungsgründen 47 bzw. 48 entnehmen, dass eine Datenverarbeitung zur Betrugsbekämpfung als berechtigtes Interesse gilt und dass Direktmarketing sowie die Datenweitergabe im Konzern zu Verwaltungszwecken als berechtigte Interessen jedenfalls infrage kommen. Für Anbieter der Telemedien haben die Datenschutz-Aufsichtsbehörden eine Orientierungshilfe herausgegeben, die auch Hinweise zur Vornahme der Interessenabwägung enthält, s. Datenschutzkonferenz (DSK), Orientierungshilfe für Anbieter von Telemedien, März 2019, S. 12 ff.; abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf. Zur alten Rechtslage finden sich Abwägungshinweise in einem Arbeitspapier der Artikel-29-Datenschutzgruppe. S. *Artikel-29-Datenschutzgruppe,* Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (WP 217 vom 09.04.2014), insb. S. 43 ff.; abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.

oben bereits dargestellt, sind insbesondere die Zwecke der Verarbeitung relevant. Darüber hinaus muss der Verantwortliche aber stets alle Umstände des Einzelfalls – soweit ihm diese bekannt sind oder sein können – einbeziehen.[284]

Im Rahmen einer Interessenabwägung ist zunächst die Schwere des Eingriffs in die Rechte und Interessen der betroffenen Person umfassend zu analysieren. Im Vordergrund steht hierbei regelmäßig das Recht auf informationelle Selbstbestimmung.[285] Dementsprechend sind etwa Art und Umfang der verarbeiteten personenbezogenen Daten[286] einschließlich des Grads der Privatheit, die Speicherdauer, Maßnahmen zur Gewährleistung von Datensicherheit oder die Tatsache zu berücksichtigen, ob und an ggf. wie viele konzerninterne und externe Empfänger die Daten weitergegeben werden. Die Eingriffsintensität der Datenverarbeitung wird zudem maßgeblich dadurch beeinflusst, ob der Nutzer eine Datenverarbeitung zumindest abwählen oder ob er auf diese gar keinen Einfluss nehmen kann, ihr also letztlich ausgeliefert ist. Von Bedeutung ist auch, ob die betroffene Person in der konkreten Situation mit der Datenverarbeitung vernünftigerweise rechnen kann.[287] Schließlich sind die Grundsätze des Art. 5 Abs. 1 DSGVO, insbesondere die Grundsätze der Datensparsamkeit und der Zweckbindung, zu beachten.

Sodann ist zu untersuchen, ob die vom Verantwortlichen angeführten berechtigten Interessen (z. B. die Verbesserung konkret genannter Software-Funktionalitäten) unter Berücksichtigung der angegebenen Datenverwendungszwecke den zuvor festgestellten Eingriff zumindest aufwiegen. Soweit berechtigte Interessen weit formuliert und nicht hinreichend konkretisiert werden (auch nicht durch die Verarbeitungszwecke), ist die Darstellung nicht hinreichend präzise und transparent.[288] In solchen Fällen ist i. d. R. bereits von einem Verstoß gegen Art. 13 Abs. 1 lit. d) i. V. m. Art. 12 Abs. 1 S. 1 DSGVO auszugehen (s. dazu E. II. 4. e), S. 76). Bei einer Abwägung mit den

---

284 Bundeskartellamt, Beschluss vom 06.02.2019, Az. B6-22/16, Rn. 727 ff. – *Facebook*.

285 Zu anderen möglicherweise beeinträchtigten Rechten der betroffenen Person S. *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs.1 DSGVO Rn. 101.

286 *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs.1 DSGVO Rn. 105.

287 S. DSGVO-Erwägungsgrund 47, S. 3 und 4. Man wird hier zugunsten der betroffenen Person allerdings unterstellen müssen, dass diese „vernünftigerweise“ nicht mit unangekündigten Datentransfers oder rechtswidrigen Verarbeitungsmaßnahmen rechnen muss, selbst wenn diese faktisch weit verbreitet sein sollten.

288 Die Artikel-29-Datenschutzgruppe hat berechtigte Interessen wie “Verbesserung der Nutzererfahrung“, „Marketingzwecke“, „IT-Sicherheitszwecke“ oder „zukünftige Forschung“ – soweit keine weiteren Details genannt werden – als nicht hinreichend präzise (i. S. von Art. 6 Abs. 1 lit. b) der Datenschutzrichtlinie) eingestuft, s. *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation (WP 203, 02.04.2013), abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Interessen des Nutzers wird man solch unkonturierten Interessen nur ein geringes Gewicht beimessen können.[289] Dasselbe gilt für Interessen, bei denen nicht erkennbar ist, welche konkreten Datenverarbeitungen zu welchen Zwecken sie überhaupt rechtfertigen sollen.

Im Kontext von Smart-TVs ist zu beachten, dass es sich bei den betroffenen Personen im Regelfall um Verbraucher handelt, die das Fernsehgerät zuvor zu einem nicht unerheblichen Preis gekauft haben. Der Verbraucher hat mithin für die von einem Smart-TV vernünftigerweise erwartbaren Leistungen bereits ein Entgelt bezahlt. In dieser Situation kann der Verantwortliche sich nur schwer darauf berufen, die Verarbeitung personenbezogener Daten über das vertraglich erforderliche Maß hinaus sei notwendig, um eine Gratisleistung zur Verfügung zu stellen.

Auch wenn den Datenschutzbestimmungen kaum jemals Ausführungen zu konkreten Abwägungsvorgängen zu entnehmen sind[290], spielen diese für den Einzelnen eine wesentliche Rolle. Die betroffenen Personen können die rechtliche Situation nur schwer einschätzen, wenn in Datenschutzbestimmungen keine nachvollziehbare Auseinandersetzung mit ihren Interessen erfolgt oder schlicht behauptet wird, die Interessen der betroffenen Person seien nicht als überwiegend zu betrachten. Dieses Problem wird noch dadurch verschärft, dass Datenschutzbestimmungen oftmals keine nachvollziehbaren Angaben etwa zu den konkret erhobenen Daten oder Speicherdauern machen (s. dazu E. II. 4. b) und i), S. 71 bzw. S. 85). Die betroffenen Personen können so nicht erkennen, ob der Verantwortliche überhaupt eine ernsthafte und umfassende Interessenabwägung vorgenommen hat. Dieses Szenario ist keineswegs unrealistisch, zumal eine gewisse Voreingenommenheit des Verantwortlichen zugunsten der Datenverarbeitung[291] unterstellt werden kann.

Während eine Nachprüfung der Interessenabwägung durch Behörden grundsätzlich denkbar ist, ist dies für Privatpersonen kaum möglich. Es gibt in der DSGVO kein explizites Auskunftsrecht zur Vornahme der Interessenabwägung. Das Widerspruchsrecht gegen die Datenverarbeitung nach Art. 21 Abs. 1 S. 1 DSGVO ist ein stumpfes Schwert, denn die betroffene Person müsste spezifische Gründe vorbringen, die sich aus ihrer besonderen Situation ergeben, sie mithin aus der Masse der Nutzer herausheben. Dies stellt eine hohe Hürde dar. Das Argument, dass – bezogen auf alle Nutzer – eine Interessenabwägung nicht ordnungsgemäß durchgeführt wurde oder die Interessen jeder einzelnen betroffenen Person überwiegen, ist in diesem Zusammenhang irrelevant. Dem Einzelnen bleibt neben einer Beschwerde bei einer Aufsichtsbehörde

289 Vgl. Bundeskartellamt, Beschluss vom 06.02.2019, Az. B6-22/16, Rn. 736 ff. – *Facebook*.

290 Zu einer entsprechenden Darstellung besteht nach hier vertretener Auffassung keine Verpflichtung, s. S. 77.

291 S. dazu *Frenzel* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 27; *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 87.

(Art. 77 Abs. 1 DSGVO) allenfalls die Möglichkeit einer gerichtlichen Klärung. Voraussetzung hierfür ist gem. Art. 79 Abs. 1 DSGVO jedoch, dass die betroffene Person vorträgt[292], durch eine DSGVO-widrige Datenverarbeitung in ihren ihr nach der DSGVO zustehenden Rechten verletzt worden zu sein. Im Sinne einer effektiven Rechtsdurchsetzung von Grundrechten und EU-Recht wird man ein solches Recht spiegelbildlich auch in der Verpflichtung des Verantwortlichen zur Vornahme einer Interessenabwägung in Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO erkennen können.[293]

Das Bundeskartellamt hat in den ihm vorgelegten Datenschutzbestimmungen etliche Datenverarbeitungsvorgänge gefunden, bei denen zweifelhaft ist, ob diese von der Rechtsgrundlage der – zumindest gleich schwer wiegenden – berechtigten Interessen des Verantwortlichen gedeckt sind. Man kann hier insbesondere vier Konstellationen unterscheiden (die sich auch überschneiden können):

(1) Vielen Datenschutzbestimmungen lässt sich bereits nicht mit hinreichender Bestimmtheit entnehmen, welche personenbezogenen Daten überhaupt verarbeitet werden. Dies macht es unmöglich, die Eingriffsintensität zu bewerten und die Erforderlichkeit der Datenverarbeitung zu beurteilen oder eine Interessenabwägung vorzunehmen.

(2) Es ist nicht erkennbar, welche Daten zu welchem Zweck und aufgrund welchen berechtigten Interesses verarbeitet werden. Dies ist in Datenschutzbestimmungen der Fall, in denen verarbeitete Daten, Verarbeitungszwecke und Rechtfertigungsgründe nacheinander aufgelistet werden, ohne aufeinander Bezug zu nehmen. Auch hier ist es nicht möglich zu bestimmen, welche Eingriffsschwere aufgewogen werden muss, da die für das konkret geltend gemachte berechtigte Interesse erforderlichen Daten und Zwecke nicht bestimmbar sind. Eine Erforderlichkeitsprüfung oder Interessenabwägung ist unter diesen Voraussetzungen unmöglich.

(3) Berechtigte Interessen und Verarbeitungszwecke sind begrifflich so unbestimmt, dass deren Gewicht nicht beurteilt werden kann und eine Erforderlichkeitsprüfung oder Interessenabwägung nicht vorgenommen werden kann.

---

292 *Bergt* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 79 DSGVO Rn. 7.

293 Nicht unstrittig; *Martini* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 79 DSGVO Rn. 19 sieht hiervon ausdrücklich den Fall der Überschreitung einer Rechtsgrundlage als erfasst an; für ein weites Verständnis der nach der DSGVO bestehenden eigenen Rechte auch *Boehm* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 79 DSGVO Rn. 10; für eine Beschränkung auf Kapitel III der DSGVO hingegen *Kreße* in Sydow [Hrsg.], Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 79 Rn. 7 ff.

(4) Die Interessen des Unternehmens (soweit konkret erkennbar) werden ohne Weiteres und ohne erkennbare Abwägung als schwerwiegender erachtet als diejenigen des Nutzers, selbst wenn die Unternehmensinteressen offensichtlich schwach sind.[294]

Auf Basis der vorgelegten Datenschutzbestimmungen erweist sich der Rechtfertigungsgrund der Wahrung berechtigter Interessen somit ganz überwiegend als nicht tragfähig. Im Ergebnis bedeutet dies, dass die Datenverarbeitungen, die seitens der Smart-TV-Anbieter auf berechtigte Interessen gestützt werden, in ihrer großen Mehrheit als nicht DSGVO-konform einzustufen sind.[295]

c) Einwilligungen

Eine Verarbeitung personenbezogener Daten ist in aller Regel stets möglich, wenn die hiervon betroffene Person freiwillig in die Datenverarbeitung einwilligt.

aa) Ermittlungsergebnisse

Bei Smart-TVs stellt sich – wie bei anderen IoT-Geräten auch – das Problem, dass das Produkt zunächst beim Einzelhändler erworben wird, der Käufer aber erst bei Inbetriebnahme Einblick in diverse Datenschutz- und Nutzungsbestimmungen erhält (siehe dazu E. III. 1., S. 91). Als einziger Hersteller weist *Samsung* Verbraucher auf der Einzelhandel-Verkaufsverpackung darauf hin, dass bei der Nutzung bestimmter Funktionen des Smart-TVs personenbezogene Daten übermittelt werden. Dieser Hinweis ist allerdings äußerst unbestimmt und kann zudem beim Online-Kauf nicht zur Kenntnis genommen werden.

Bei der Ersteinrichtung von Smart-TVs wird der Nutzer oftmals mit sog. „Take-it-or-leave-it choices“ konfrontiert, also Auswahlsituationen, bei denen eine Ablehnung keine wirkliche Option ist. Dies zeigt das nachfolgende Beispiel:

---

294 Beispielsweise ist, da der Nutzer sein Gerät käuflich erworben hat, grundsätzlich kein unternehmerisches Refinanzierungsinteresse anzuerkennen.

295 Die Datenflüsse, die die Unternehmen im Rahmen der Sektoruntersuchung angaben, ließen sich mutmaßlich zum größten Teil auf der Rechtsgrundlage „berechtigte Interessen“ rechtfertigen, wenn insbesondere nachvollziehbar wäre – und damit in eine Abwägung eingestellt werden könnte –, welche Daten konkret betroffen sind und wie mit diesen Daten weiter verfahren wird (insb. Verwendungszweck, Speicherdauer, Speicherort, Weitergabe).

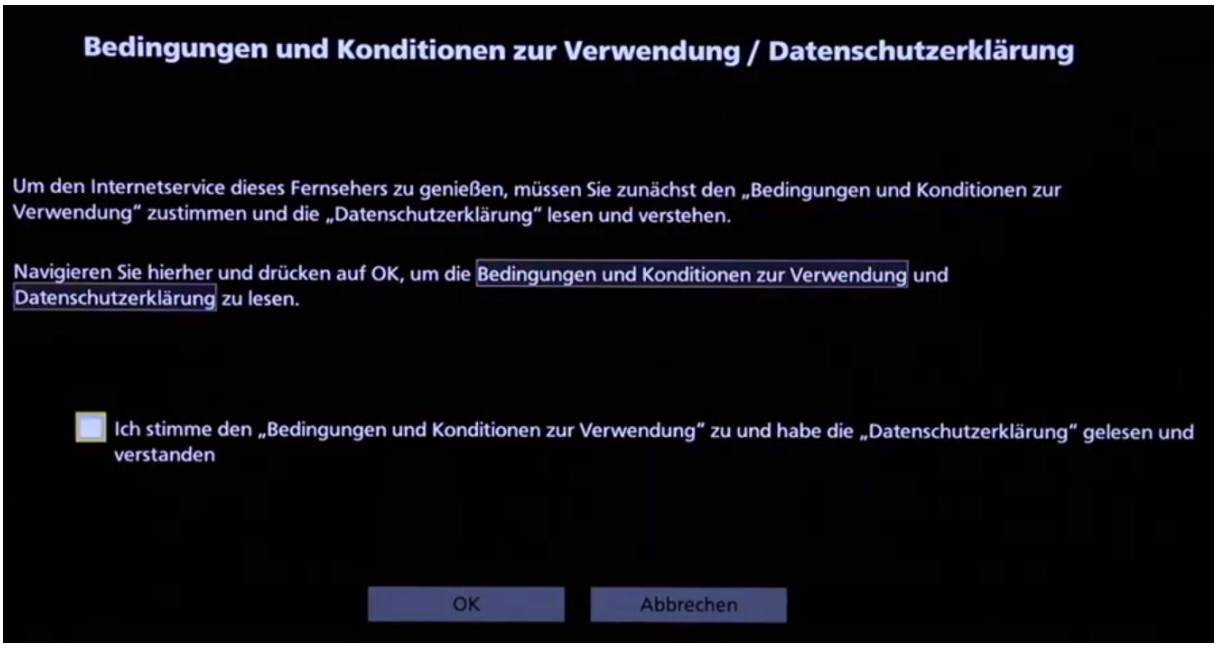


Abbildung 21:Screenshot Ersteinrichtung eines Smart-TVs von *Panasonic*[296]

Demgegenüber werden dem Nutzer im Rahmen der Ersteinrichtung auch häufig „echte" Einwilligungsersuchen präsentiert.

Nachfolgend sind exemplarisch zwei Einwilligungssituationen bei der Erstinbetriebnahme eines Smart-TVs größerer Hersteller abgebildet:

296 Entnommen aus dem Video *Ersteinrichtung + Sendersortierung Panasonic OLED oder LED 2020 Onlineshop Thomas Electronic* https://www.youtube.com/watch?v=rYhWuAmCevM (Minute 3:56).

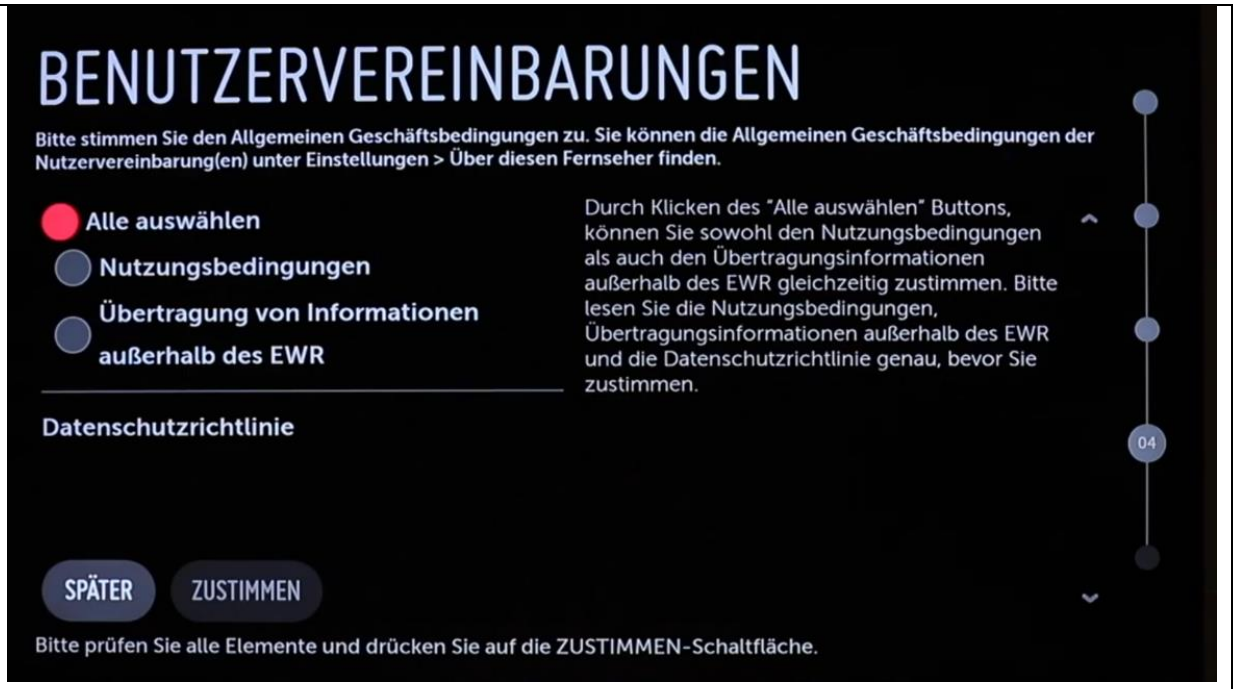


Abbildung 22:Screenshot Ersteinrichtung eines Smart-TVs von *LG*[297]

Bei Betätigung der Schaltfläche „Übertragung von Informationen außerhalb des EWR“ erscheint folgende Information:

Zusammen mit der Datenschutzrichtlinie, beschreibt diese Einverständniserklärung, wie Ihre Daten auf Übersee oder außerhalb des Europäischen Wirtschaftsraums oder die Schweiz übertragen werden. Solange Sie der vorliegenden Vereinbarung nicht zustimmen, werden Sie nicht imstande sein, viele Ihrer Smart TV Funktionen zu nutzen. […]

[…] Ich nehme zur Kenntnis und erkläre mich einverstanden damit, dass LGE als globale Organisation, ihre Tochtergesellschaften, Niederlassungen und Zulieferer meine Informationen (einschließlich meiner persönlichen Informationen) außerhalb des Landes übertragen können, in dem Ihr LG Smart TV sich befindet, wie die Republik Korea, um Ihnen unsere Smart TV Services und zu sonstigen, in unserer Datenschutzrichtlinie genannten Zwecken zu liefern. Dies umfasst die Übertragung meiner Informationen außerhalb des Europäischen Wirtschaftsraumes oder der Schweiz, falls mein Smart TV dort gelegen ist.

[…] Ich nehme zur Kenntnis, dass ich mein Einverständnis zur Übertragung von Informationen außerhalb des Europäischen Wirtschaftsraums durch LGE jederzeit durch Anpassung der Einstellungen im Einstellungsmenü zurückziehen kann. […]

297 Entnommen aus dem Video *LG TV 2019 Ersteinrichtung Thomas Electronic Online Shop Erstinstallation LG LineUp 2019* vom 21.11.2019, abrufbar unter https://www.youtube.com/watch?v=Vqsa-wIPlaKs (Minute 1:30).

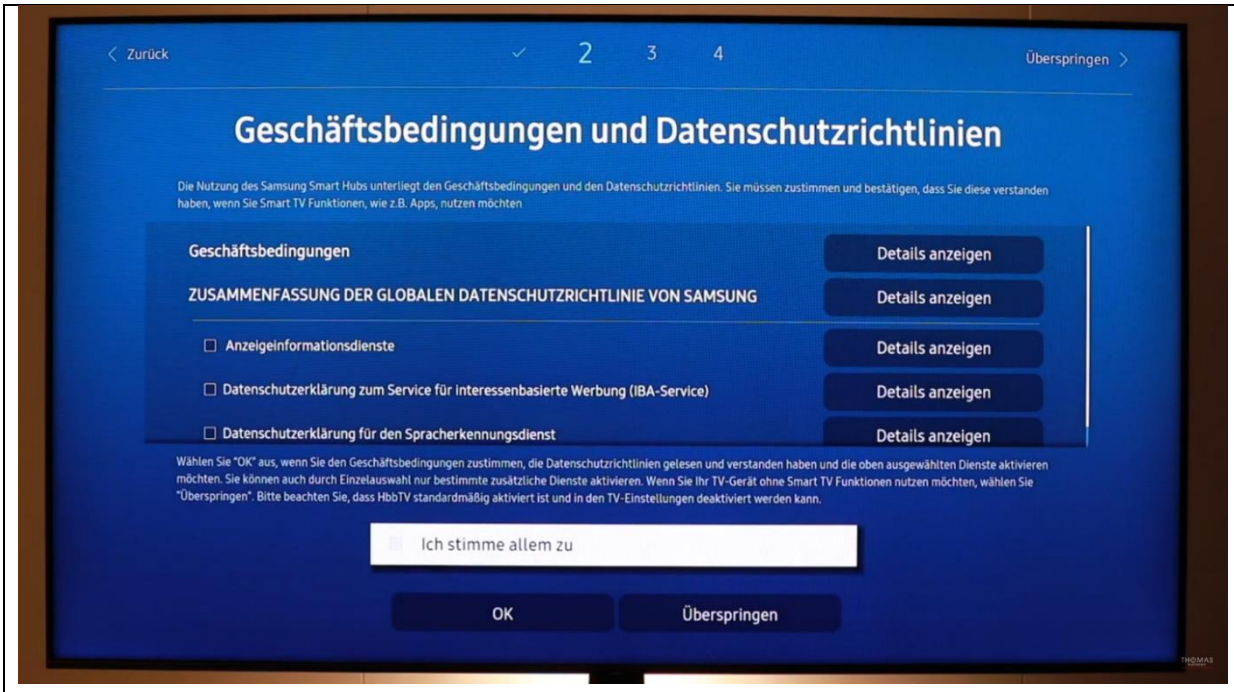


Abbildung 23:Screenshot Ersteinrichtung eines Smart-TVs von *Samsung*[298]

Bei Betätigung der Schaltfläche „Details anzeigen“ zu *Datenschutzerklärung zum Service interessenbasierte Werbung (IBA-Service)* erscheint folgende Information:

[…] Folgende Informationstypen werden erfasst:

- Geräteinformationen. Wir erfassen Informationen wie Gerätemodell, Betriebssystemversionen, Konfigurationen und Einstellungen des Geräts, IP-Adresse, Gerätekennungen und weitere Kennungen.
- Gerätenutzung und Protokollinformationen. Wir erfassen Informationen dazu, wie, wann und wie lange Sie Ihre Geräte nutzen, darunter auch Ihre Interaktionen mit dem IBA-Service und Geräte-Apps und -Services von Samsung und Dritten (z. B. App-Listen auf Ihren Geräten).
- Anzeigeinformationen. Wir erfassen Ihren TV-Anzeigeverlauf. Ihr TV-Anzeigeverlauf enthält Informationen über Netze, Sender, besuchte Websites und auf dem Samsung Smart TV gesehene Sendungen sowie die für deren Betrachtung aufgewendete Zeit. Wir verwenden zur Erhebung dieses TV-Anzeigeverlaufs die automatische Inhaltserkennung (ACR) und andere Technologien.
- Statistische Informationen. Wir nutzen statistische Informationen zu Ihnen und Ihren Geräten wie den generalisierten Standort und die geschätzte Altersgruppe. Diese statistischen Informationen rufen wir aus handelsüblichen

298 Entnommen aus dem Video *Ersteinrichtung Samsung QLED 2020 Onlineshop Thomas Electronic* vom 25.03.2020, abrufbar unter https://www.youtube.com/watch?v=dDd9_JL9HQk&list=PLO6t7DBoZlu0s4TwuZXxBCqCaodCht1LC (Minute 2:37).

> Quellen (im gesetzlich zulässigen Umfang) wie unseren Drittanbietern ab. Wir arbeiten ausschliesslich mit Drittanbietern zusammen, die sicherstellen, dass diese Informationen gemäss den anwendbaren Gesetzen erfasst wurden und zur Nutzung und Weitergabe bereitgestellt werden dürfen.
>
> […]
>
> Wir nutzen die über den IBA-Service erfassten Daten für folgende Zwecke: […]
>
> Die rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch Samsung bildet eine Verarbeitung: die für die Erfüllung des Vertrags zwischen Ihnen und Samsung notwendig ist […], die zur Einhaltung rechtlicher Anforderungen erforderlich ist […]; oder die für die legitimen Interessen von Samsung nötig ist […] Darüber hinaus kann eine Verarbeitung auf Grundlage der gesonderten Zustimmung unserer Kunden erfolgen […]
>
> […] Sie können den IBA-Service ausserdem jederzeit im Einstellungsmenü Ihres Samsung Smart TV deaktivieren. […]

Einwilligungen kommen in allen untersuchten Datenschutzbestimmungen in unterschiedlichem Umfang vor. Zumeist werden sie eingesetzt, wenn Nutzungsdaten der betroffenen Person erhoben werden sollen.[299] Soweit ersichtlich, werden Daten aus einer automatisierten Inhaltserkennung (ACR) stets auf Grundlage einer gesonderten Einwilligungserklärung erhoben.

Einwilligungen können auf bestimmte Arten der Gerätenutzung beschränkt sein, die nicht für jeden Nutzer relevant sind. So wird etwa häufig darauf verwiesen, dass bei einer bestimmten Nutzung – etwa beim Einsatz eines Sprachassistenten – eine Einwilligung vonnöten ist. Diese kann ggf. auch erst zu einem späteren Zeitpunkt eingeholt werden wie dem erstmaligen Aufrufen der betreffenden Funktion.[300] Der Nutzer kann so entscheiden, ob er die betreffende Software überhaupt aktivieren will.

Aus den Ermittlungen ergibt sich, dass zumindest in zwei Fällen eine Zustimmung zur Datenschutzvereinbarung in Gänze als Einwilligung in die Verarbeitung von (insb. Nutzungs-)Daten angesehen wird. Bei den Geräten eines Herstellers wird der Kunde erst nach Inbetriebnahme des Geräts darüber informiert, dass er Online-Updates der Chipsatz-Firmware nur dann erhält, wenn er im Gegenzug in die Preisgabe personenbezogener Daten (u. a. TV-Modell und Seriennummer des Fernsehgeräts, Häufigkeit der Nutzung von Streaming-Diensten, Nutzung von Apps u. a.) an den Chipsatz-Hersteller einwilligt.

---

299 Ein Unternehmen stützte die Verarbeitung von Nutzungsdaten auf den Rechtfertigungsgrund der berechtigten Interessen (Produktverbesserung). Bei einigen Datenschutzbestimmungen war nicht klar erkennbar, ob die Verarbeitung von Nutzungsdaten auf Basis einer Einwilligung oder berechtigter Interessen erfolgt, da diese als Rechtfertigungsgründe nebeneinander angegeben wurden.

300 Dies ist etwa bei der *Google*-Datenschutzerklärung der Fall. Auch *Samsung* stellt gleich zu Anfang seiner Globalen Datenschutzrichtlinie klar: „Diese Datenschutzrichtlinie dient nicht dazu, eine Einwilligung von Ihnen einzuholen."

Eine Widerrufsmöglichkeit bzgl. erteilter Einwilligungen ist zumeist, jedoch nicht in allen Datenschutzbestimmungen vorgesehen. Während bei einigen Geräten der Wiederruf einer Einwilligung durch Vornahme entsprechender Einstellungen im Fernseher-Menü vorgenommen werden kann, ist der Widerruf bei anderen nicht konkret geregelt und bedarf der Kontaktaufnahme mit dem datenverarbeitenden Unternehmen.

Mitunter wird für die Nutzung bestimmter Apps bzw. Smartfunktionalitäten ein Nutzerkonto beim TV-Portal-Betreiber benötigt (*Google*, *Amazon*, S. oben S. 92). Das Anlegen von Nutzerkonten selbst wird von den TV-Portal-Betreibern jedoch nicht mit einer formellen Einwilligung in Datenverarbeitungen verbunden und wird daher an dieser Stelle nicht weiter untersucht.

bb) Rechtliche Würdigung

Art. 6 Abs. 1 DSGVO nennt unter Buchstabe a) an erster Stelle die Einwilligung der betroffenen Person als Rechtsgrundlage für eine Datenverarbeitung. Art. 4 Nr. 11 DSGVO bestimmt den Begriff der Einwilligung wie folgt:

> „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

Die Freiwilligkeit ist somit bereits *conditio sine qua non* für das Vorliegen einer Einwilligung. Dass die DSGVO an anderer Stelle sozusagen tautologisch von der stets freiwillig zu erteilenden Einwilligung spricht, bringt zum Ausdruck, dass der EU-Gesetzgeber diesem Merkmal eine herausragende Bedeutung zugedacht hat.[301]

DSGVO-Erwägungsgrund 43 weist darauf hin, dass insbesondere in drei Fällen nicht von Freiwilligkeit – und damit auch nicht vom Vorliegen einer wirksamen Einwilligung – ausgegangen werden kann, nämlich

- bei einem klaren Ungleichgewicht zwischen Verantwortlichem und betroffener Person;
- wenn in verschiedene abgrenzbare Datenverarbeitungsvorgänge nur einheitlich eingewilligt werden kann, obwohl dies im Einzelfall nicht angebracht ist, oder
- wenn die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird, obwohl die Einwilligung hierfür nicht erforderlich ist.

Letzterer Punkt findet sich auch in Art. 7 Abs. 4 DSGVO.

---

301 Vgl. Bundeskartellamt, Beschluss vom 06.02.2019, Az. B6-22/16, Rn. 644 – *Facebook*.

DSGVO-Erwägungsgrund 42 zufolge „sollte nur dann davon ausgegangen werden, dass [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“.

Zusammenfassend lässt sich festhalten, dass eine wirksame Einwilligung in inhaltlicher Hinsicht zumindest Folgendes erfordert: Die Einwilligung ist notwendigerweise auf bestimmte konkrete Zwecke und auf den konkreten Fall zu beschränken. Die betroffene Person muss eine bewusste Entscheidung auf Grundlage aller wesentlichen Informationen treffen. Dem dient auch die Vorgabe in Art. 7 Abs. 2 DSGVO, demzufolge Einwilligungsersuchen nicht in weitergehenden Informationen versteckt werden dürfen, sondern sachverhaltsbezogen und in verständlicher und leicht zugänglicher Form jeweils getrennt dargestellt werden müssen. Es darf ferner keine Drucksituation vorliegen, die sich aufgrund der Umstände und/oder des Verhaltens des Verantwortlichen ergeben kann. Vor Abgabe der Einwilligungserklärung muss die betroffene Person auf ihr jederzeitiges Widerrufsrecht hingewiesen werden (Art. 7 Abs. 3 S. 4, Art. 13 Abs. 2 lit. c) DSGVO). Sie muss schließlich ihre Einwilligung unmissverständlich kundtun (Art. 7 Abs. 4 DSGVO).

Dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat, muss der Verantwortliche nachweisen können (Art. 7 Abs. 1 DSGVO). Das bedeutet, dass er ein Einwilligungsmanagement unterhalten muss.

Das Einholen einer wirksamen Einwilligung stellt damit für den Verantwortlichen eine echte Herausforderung dar. Die einzelnen Voraussetzungen, die nicht klar voneinander trennbar sind und sich daher häufig überschneiden können, werden nachfolgend beleuchtet.

(1) Bestimmtheit der Einwilligung

Im Zeitpunkt der Einholung der Einwilligung muss der Zweck der Datenverarbeitung festgelegt und bestimmt sein. Eine pauschale Einwilligung, die nicht auf die konkreten Zwecke abstellt, ist deshalb unwirksam.[302] Nur eng gefasste Zwecke bannen die Gefahr einer schleichenden Zweckerweiterung („function creep“) und erlauben granulare Einwilligungsmöglichkeiten.[303] Für eine enge, konkrete Zwecksetzung spricht auch der Umkehrschluss aus DSGVO-Erwägungsgrund

---

302 *Heberlein* in Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 9; S. auch *Schulz* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 24.

303 S. *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679 - Version 1.1 vom 13.05.2020, Rn. 55, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (bislang nur auf Englisch erhältlich).

33. Da die Zwecke von Forschungsprojekten nicht immer von Anfang an zuverlässig umschrieben werden können, ist insoweit ausnahmsweise eine unspezifische Zwecksetzung möglich.[304]

Das in Art. 4 Nr. 11 DSGVO enthaltene Tatbestandsmerkmal „für den bestimmten Fall“ (im Englischen „specific consent“) erschöpft sich indessen nicht in dem Erfordernis enger Zweckbestimmungen.[305] Damit eine Einwilligung bestimmt sein kann, muss die zu legitimierende Datenverarbeitung selbst im Einwilligungsersuchen hinreichend bestimmt sein. Dies erfordert eine klare und konkrete Beschreibung der betroffenen personenbezogenen Daten, der Verarbeitungsform(en), des Verantwortlichen und ggf. weiterer Datenempfänger.[306] Man wird darüber hinaus auch verlangen müssen, dass eine „spezifische“ Einwilligung nur insoweit erteilt werden kann, wie deren Tragweite für die betroffene Person überschaubar ist.[307] Zu bejahen wäre dies jedenfalls für die in der Einwilligungssituation aus Sicht der betroffenen Person unmittelbar bevorstehenden (und sich ggf. fortsetzenden oder zukünftig wiederholenden gleichartigen) Datenverarbeitungsvorgänge. Ein Ersuchen, mit dem eine „spezifische“ Einwilligung eingeholt werden soll, kann jedoch nicht andere als die unmittelbar erwartbaren Datenverarbeitungsvorgänge umfassen.[308] Eine Einwilligung wäre z. B. zweifelhaft, soweit bereits Datenverarbeitungsvorgängen zugestimmt werden soll, die erst bei Nutzung anderer Dienstleistungen eines Verantwortlichen oder eines Dritten initiiert werden.

Die Praxis, dem Nutzer zu Einwilligungszwecken eine Gesamtdatenschutzerklärung „en bloc“ vorzulegen, ist im Hinblick auf das Bestimmtheitserfordernis kritisch zu sehen. Dies gilt jedenfalls, wenn die vorgelegten Datenschutzbestimmungen mehr als ein klar erkennbares, und im Kontext der Zustimmungserteilung nicht übersehbares konkretes Einwilligungsersuchen enthalten. Eine abgegrenzte spezifische Einwilligung „für den bestimmten Fall“, wie es Art. 4 Nr. 11 DSGVO verlangt, begegnet insofern auch Schwierigkeiten, weil der „Fall“ nicht nur durch den angegebenen Zweck, sondern auch dadurch determiniert wird, welche personenbezogenen Daten von der Verarbeitung betroffen werden. So werden die erhobenen Daten bei dem in Abbildung 22 gezeigten Einwilligungsersuchen nicht einmal ansatzweise beschrieben (nur pauschal als „meine Informationen“). Bei dem Ersuchen von Samsung (Abbildung 23) sind die verarbeiteten Daten hingegen

---

304 S. *Schantz* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 9.

305 In der Literatur wird hier oftmals verkürzend nur auf die Verwendungszwecke abgestellt.

306 Vgl. *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 68.

307 Ähnlich *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 69.

308 Auch wäre oftmals fraglich, ob die betroffene Person überhaupt eine „informierte Entscheidung“ (dazu nachfolgend unter (2).) treffen könnte, soweit sie um Einwilligung in weitere, ggf. noch nicht einmal in Umrissen absehbare Datenverarbeitungen ersucht würde.

weitestgehend erkennbar; es ist jedoch verwirrend, dass im Rahmen eines Einwilligungsersuchens andere ggf. für die Datenverarbeitung einschlägige Rechtsgrundlagen genannt werden, so dass für den Nutzer wiederum nicht klar ist, welche Daten nun genau der Einwilligung (und konsequenterweise auch einem späteren Widerruf der Einwilligung) unterfallen.

(2) Informierte Entscheidung

Die Bedingung einer *informierten Einwilligung* erfordert, dass die betroffene Person vorab unbeschadet der weiteren Anforderungen der Artikel 13 und 14 DSGVO jedenfalls darüber informiert worden ist, welche Daten zu welchem Zweck und von wem verarbeitet werden.[309] Für eine umfassende Information muss der betroffenen Person auch mitgeteilt werden, ob und an wen eine Übermittlung geplant ist.[310] Hier kommt es naturgemäß zu weitgehenden Überschneidungen mit dem Erfordernis der Bestimmtheit der Einwilligung (s. oben unter (1))[311]. De, Europäischen Datenschutzausschuss zufolge sind der betroffenen Person zumindest mitzuteilen:[312]

- die Identität des Verantwortlichen,
- der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird,
- die (Art) Daten, die erhoben und verwendet werden,
- das Vorliegen des Rechts, die Einwilligung zu widerrufen,
- gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Art. 22 Absatz 2 Buchstabe c DSGVO, und
- Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien gemäß Art. 46 DSGVO.

309 *Heberlein* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 6 Rn. 8; S. a. DSGVO-Erwägungsgrund 42, S. 4.

310 *Schild* in: BeckOK Datenschutzrecht, 32. Ed., 01.05.2020, Art. 4 DSGVO Rn. 129.

311 *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 72, spricht in diesem Zusammenhang von der Informiertheit als subjektivem Gegenstück zur Bestimmtheit.

312 *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679 (Fn. 303), Rn. 64.

Falls sich dies nicht aus dem Zusammenhang ergibt, erfordert eine informierte Entscheidung ferner, dass die Konsequenzen der Nichteinwilligung klar kommuniziert werden, d. h. welche Leistungseinschränkungen mit der Einwilligungsverweigerung verbunden sind.[313] Als wichtige Parameter für die Eingriffstiefe einer Datenverarbeitung wäre zudem anzugeben, ob und welche Dritte die Daten erhalten und wie lange die personenbezogenen Daten gespeichert werden sollen.[314]

Soweit Einwilligungssituationen nachvollzogen werden konnten, war jeweils weitgehend unklar, welche Daten für welche Zwecke und für welchen Zeitraum erhoben werden sollten. Die Einwilligungsersuchen sind zudem – auch wenn man sie im Zusammenhang mit den jeweiligen (Gesamt-)Datenschutzbestimmungen liest (dazu unter E. II. 4. f), S. 78) – bei der Darstellung der Datenübermittlung an Dritte und hinsichtlich der Angabe der Speicherdauer lückenhaft oder unkonkret und daher mangelhaft. Dies illustrieren auch die bereits oben abgebildeten Beispiele:

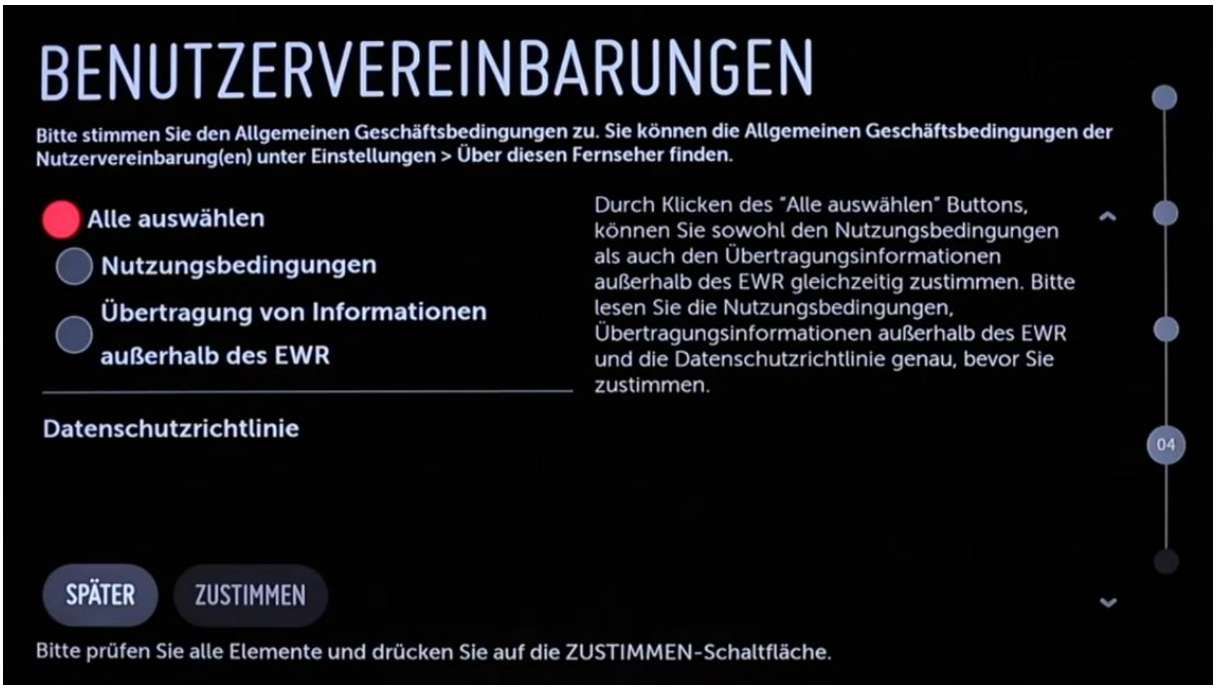


Abbildung 24:Screenshot Ersteinrichtung eines Smart-TVs von *LG*[315]

Dem Nutzer fehlen hier – auch nach Lektüre der aufrufbaren Texte – einige Angaben, die er bräuchte, um eine informierte Entscheidung zur Übertragung von Informationen außerhalb des EWR zu treffen, insb.:

313 In diesem Sinne *Schulz* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 7 Rn. 39.

314 Diese Kriterien nennt auch *Ernst* in: Paal/Pauly [Hrsg.], 2. Aufl. 2018, DSGVO Art. 4 DSGVO Rn. 83.

315 Entnommen aus dem Video *LG TV 2019 Ersteinrichtung Thomas Electronic Online Shop Erstinstallation LG LineUp 2019* vom 21.11.2019, abrufbar unter https://www.youtube.com/watch?v=Vqsa-wIPlaKs (Minute 1:39).

- Welche Daten sind konkret von der Übermittlung betroffen und welchen Zwecken dient die Verarbeitung?
- Welche konkreten TV-Funktionen können im Verweigerungsfall nicht genutzt werden?
- An welche Dritte werden die Daten übermittelt?
- In welche Länder werden die Daten übermittelt?
- Wie lange werden die Daten gespeichert?

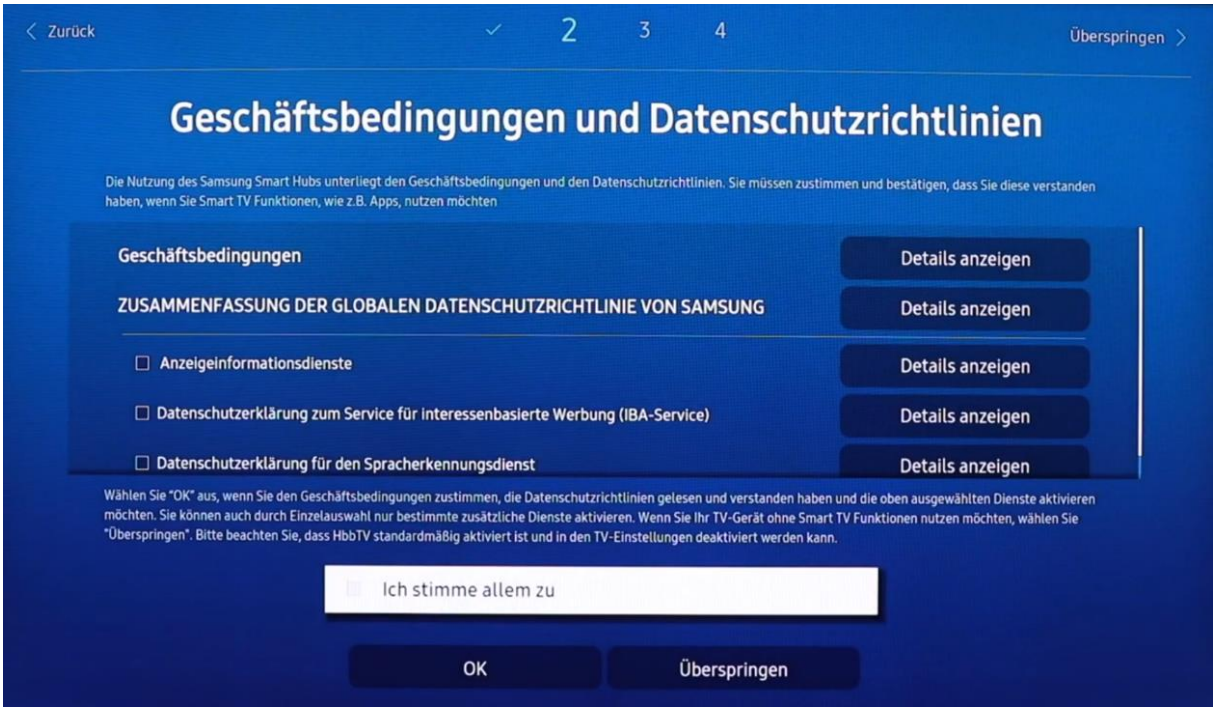


Abbildung 25:Screenshot Ersteinrichtung eines Smart-TVs von *Samsung*[316]

In diesem Fall wären – auch nach Lektüre der aufrufbaren Texte – für eine informierte Entscheidung bei der Einwilligung in den Erhalt interessenbasierter Werbung beispielsweise folgende Angaben vonnöten:

- Werden Daten auch auf anderer Rechtsgrundlage als der (widerruflichen) Einwilligung verarbeitet?
- An welche Dritten werden die Daten übermittelt?
- In welche Länder werden die Daten übermittelt?

316 Entnommen aus dem Video *Ersteinrichtung Samsung QLED 2020 Onlineshop Thomas Electronic* vom 25.03.2020, abrufbar unter https://www.youtube.com/watch?v=dDd9_JL9HQk&list=PLO6t7DBoZlu0s4TwuZXxBCqCaodCht1LC (Minute 2:37).

- Wie lange werden die Daten gespeichert?

Diese Beispiele veranschaulichen exemplarisch die Lückenhaftigkeit der meisten Einwilligungsersuchen. Unter diesen Bedingungen ist eine informierte Verbraucherentscheidung nicht möglich, die Einwilligung mithin jeweils nicht wirksam erteilt.

(3) Keine Drucksituation

Nach DSGVO-Erwägungsgrund 43 kann sich eine die Freiwilligkeit ausschließende Drucksituation insbesondere unter zwei Aspekten ergeben. Zum einen aus einem offensichtlichen Ungleichgewicht zwischen Verantwortlichem und betroffener Person, zum anderen aus dem Verlangen einer Einwilligung, die über das eigentlich Erforderliche hinausgeht. Das Vorliegen eines offensichtlichen Ungleichgewichts wird in Rechtsprechung und Literatur bei diversen Fallgestaltungen bejaht. So wird allgemein nicht von einer freiwilligen Einwilligung ausgegangen, wenn die betroffene Person einem Hoheitsträger in einem öffentlich-rechtlichen Subordinationsverhältnis gegenübersteht.[317] Im privatrechtlichen Bereich wird eine freiwilligkeitsausschließende Asymmetrie der Verhandlungspositionen in sozialen Abhängigkeitsverhältnissen i. d. R. bejaht,[318] ebenso bei marktmächtigen Anbietern essentieller Güter oder Dienstleistungen.[319] Gem. Art. 7 Abs. 4 DSGVO ist zur Beurteilung der Freiwilligkeit dem Umstand „in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind“. Aus dieser Formulierung wird deutlich, dass kein absolutes „Kopplungsverbot“ besteht, jedoch sorgfältig zu prüfen ist, ob eine Kopplung die Entscheidungsfreiheit der betroffenen Person unangemessen einschränkt. Die Formulierung von Art. 7 Abs. 4 DSGVO ist insofern etwas unglücklich, als Datenverarbeitungen, die zur Erfüllung des Vertrags erforderlich sind, ohnehin bereits von Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO abgedeckt sind (siehe dazu E. V. 1. a), S. 114 ff.). Die „überschießenden“ Datenverarbeitungen können durch die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO gerechtfertigt werden. Erwägungsgrund 43 S. 2 DSGVO stellt für solche Fälle jedoch eine widerlegliche Vermutung der Unfreiwilligkeit auf.[320]

---

317 S. DSGVO-Erwägungsgrund 43 S. 1; *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 51.

318 *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 64.

319 *Klement* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 62; Bundeskartellamt, Beschluss vom 6.02.2019, Az. B6-22/16, Rn. 644 ff. – *Facebook*.

320 *Schantz*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841 (1845), hält dies für zu weitgehend.

Unbeschadet der obigen Ausführungen erfordert eine Beurteilung der Freiwilligkeit einer Willensbekundung stets eine Einzelfallbetrachtung.[321] Ausweislich DSGVO-Erwägungsgrund 42 S. 5 muss die betroffene Person in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Ob dies der Fall ist lässt sich insbesondere an zwei Kriterien festmachen.

Zum einen ist nach der Tragweite des Nachteils für die betroffene Person zu fragen. Nach allgemeiner Auffassung kann nicht jedweder Nachteil eine Unfreiwilligkeit begründen. Es muss mit der Verweigerung der Einwilligung vielmehr ein Nachteil von einer gewissen Erheblichkeit einhergehen.[322] Um die Drucksituation für die betroffene Person zutreffend zu erfassen, wird man insoweit auf eine durchschnittliche Person abstellen müssen, die Teil der Zielgruppe des Produkts oder der Dienstleistung ist. Handelt es sich bei dem durch eine Einwilligungsverweigerung erlittenen Nachteil für die betroffene Person um eine bloße Bagatelle, so wird die Freiwilligkeit der Willensbekundung hierdurch nicht infrage gestellt. Dies wird man etwa bei der Nichtteilnahme an einem Gewinnspiel grundsätzlich annehmen können.[323]

Zum anderen stellt sich die Frage, ob – selbst wenn der Nachteil mehr als nur Bagatellcharakter hat – die betroffene Person das „Erleiden“ dieses Nachteils mit vertretbarem Aufwand abwenden kann. Ist dies nämlich der Fall, so kann die betroffene Person ihre Einwilligung ohne Weiteres verweigern oder zurückziehen. In der Einzelfallbeurteilung ist daher als wesentliches Kriterium die – verbleibende – Wahlfreiheit der betroffenen Person zu berücksichtigen, d. h. die Möglichkeit und Zumutbarkeit des Ausweichens auf andere Alternativen (soweit dies nicht schon zur Bejahung eines freiwilligkeitsausschließenden offensichtlichen Ungleichgewichts berücksichtigt wurde). Der EDSA lehnt es in diesem Zusammenhang ab, Alternativangebote anderer Anbieter in die Freiwilligkeitsbetrachtung einzubeziehen.[324] Er verweist insbesondere darauf, dass die Rechtmäßigkeit der Einwilligung dann letztlich immer nach den jeweils aktuellen Marktentwick-

---

321 *Buchner/Kühling* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 7 DSGVO Rn. 44, unter Verweis auf DSGVO-Erwägungsgrund 43.

322 *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil [Hrsg.], Kommentar Datenschutz-Grundverordnung, Art. 7 Rn. 50.

323 S. dazu OLG Frankfurt, Urteil vom 27.06.2019 – 6 U 6/19, juris Rn. 13. Ungeachtet dessen kann die Einwilligung natürlich an anderen Kriterien scheitern, vgl. dazu BGH, Urteil vom 28. Mai 2020 - I ZR 7/16 (zum Zeitpunkt der Publikation dieses Berichts noch nicht veröffentlicht), Pressemitteilung des BGH Nr. 67/2020 vom 28.05.2020 – *Cookie-Einwilligung II*.

324 Vgl. *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679 (Fn. 303), Rn. 38.

lungen beurteilt werden müsse. In der Literatur werden hierzu gegenteilige Auffassungen vertreten.[325] In Anbetracht der Unfreiwilligkeitsvermutung bei Einwilligung in nicht zur Vertragserfüllung erforderliche Datenverarbeitungen[326] wird man jedenfalls fordern müssen, dass aus Perspektive der betroffenen Person eine sehr niederschwellige Möglichkeit zur Inanspruchnahme eines Alternativangebots bestehen muss.[327]

Bei der Erstinbetriebnahme von Smart-TVs kann im Falle einer Einwilligungsverweigerung zwischen drei verschiedenen Konsequenzen unterscheiden werden:

1. einzelne Funktionen, Apps oder zusätzliche Serviceleistungen[328] können nicht oder nicht sinnvoll genutzt werden;
2. wesentliche (Smart-)Funktionen des Fernsehers können nicht oder nicht sinnvoll genutzt werden;
3. nicht einmal die Grundfunktionen des Fernsehers können genutzt werden.

Unbeschadet anderer Prüfungspunkte ist bei der Frage der Freiwilligkeit einer Einwilligung zu untersuchen, ob bei der betroffenen Person aufgrund der konkreten Umstände des (typisierten) Einzelfalls eine Drucksituation vorliegt. Diese kann sich – wie oben beschrieben – bereits aus einem offensichtlichen Machtungleichgewicht der Vertragsparteien oder mangelnder Granularität der Einwilligungsmöglichkeiten (dazu unter (1)) ergeben. Wo dies nicht der Fall ist, wird man bei der Beurteilung einer Drucksituation für die betroffene Person insbesondere auf die Schwere des Nachteils bei Einwilligungsverweigerung und bestehende Ausweichmöglichkeiten abstellen müssen.

Dass der Käufer eines Smart-TVs einzelne Funktionen oder Apps im Falle einer Einwilligungsverweigerung ggf. nicht verwenden kann, stellt für ihn nicht notwendigerweise einen beachtlichen Nachteil dar. Würde sich der Nutzer etwa gegen die Verwendung eines elektronischen Programmführers des Smart-TV-Herstellers entscheiden, weil dieser exzessive Datenzugriffsberech-

---

325 S. etwa *Buchner/Kühling* in: Kühling/Buchner [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 7 DSGVO Rn. 52 f.; *Wolff* in Schantz/Wolff [Hrsg.], Das neue Datenschutzrecht, 2017, Rn. 503 ff.

326 DSGVO-Erwägungsgrund 43 S. 2 und Art. 7 Abs. 4 DSGVO, S. dazu auch E. V. 1. a), S. 114 ff.).

327 Die Freiwilligkeit der Einwilligung könnte so etwa im Einzelfall auch dann gegeben sein, wenn aus Sicht der betroffenen Person das begehrte Produkt bzw. die begehrte Dienstleistung ohne nennenswerten Aufwand anderweitig bezogen werden kann. Voraussetzung dafür ist wiederum, dass es eine offensichtliche Ausweichalternative gibt, die aus Sicht der betroffenen Person funktional gleichwertig ist und die nicht ebenfalls die unerwünschte Preisgabe nicht für die Vertragsdurchführung erforderlicher personenbezogener Daten erfordert.

328 Beispielsweise eine Garantieverlängerung um ein Jahr.

tigungen einfordert, wäre die Nutzung des Smart-TVs nur in geringfügigem Umfang eingeschränkt. Es handelte sich somit um einen Nachteil mit Bagatellcharakter, der für den Nutzer keine freiwilligkeitsausschließende Drucksituation entstehen lässt. Anders kann sich die Situation etwa bei Apps darstellen, die für die Nutzung des Smart-TVs als wesentlich anzusehen sind, etwa besonders populäre Video-Streaming-Dienste wie *Youtube* oder *Netflix*. Der Maßstab wäre demnach, ob der durchschnittliche Nutzer eine bestimmte Funktionalität oder eine bestimmte App (bzw. zumindest deren Installierbarkeit) erwartet oder nicht. Dabei kann auch eine Rolle spielen, dass bestimmte Eigenschaften oder Funktionalitäten des Gerätes explizit beworben werden[329]. Kann der Nutzer diese Eigenschaften oder Funktionalitäten nur nutzen, sofern er im Verhältnis zum TV-Portal-Betreiber[330] über die vertragserforderlichen Datenverarbeitungen (s. dazu E. V. 1. a), S. 114 ff.) hinaus personenbezogene Daten preisgibt, liegt *prima facie* eine unfreiwillig erteilte Einwilligungserklärung vor. Dies gilt ebenso, wenn ohne die Einwilligung Kernfunktionen des Fernsehgeräts nicht genutzt werden können, also etwa der Empfang von Fernsehprogrammen oder das Zuspielen von Videosignalen durch externe Geräte unmöglich ist.

Bei der Beurteilung des Vorliegens einer Drucksituation ist insbesondere zu berücksichtigen, dass der Erwerber den Smart-TV bereits bezahlt und in Betrieb genommen hat sowie ggf. vor dem Kauf nicht auf die Notwendigkeit einer Einwilligung hingewiesen wurde. Eine Rückgabe ist nicht in allen Fällen möglich und würde zudem hohen Aufwand verursachen. Der Kauf eines Alternativgeräts wäre mit zusätzlichen Kosten verbunden. Zudem wäre i. d. R. für den Verbraucher nicht ohne Weiteres ersichtlich, welche datenschutzrechtlichen Einwilligungen ein anderes Gerät erfordern würde. Eine realistische niederschwellige Ausweichalternative liegt damit bei Smart-TVs nicht vor.

Basierend auf der nur eingeschränkt möglichen Prüfung von Einwilligungsszenarien lässt sich eine Drucksituation, welche typischerweise im Rahmen der Erstinbetriebnahme des Fernsehgeräts auftritt, überwiegend ausschließen. In der Regel werden dem Verbraucher bei der Erstinbetriebnahme des Smart-TVs nur selektiv Ersuchen um Einwilligung i. S. v. Art. 4 Nr. 11 DSGVO vorgelegt. Wo dies der Fall ist, kann das Vorliegen einer Drucksituation nicht ohne Weiteres beurteilt werden. Eine Schaltfläche, die den Eindruck erweckt, eine Einrichtung sei ohne Einwilligung in den Gesamttext der Datenschutzerklärung (mit echten Einwilligungstatbeständen) nicht möglich – z. B. mit den Alternativen „Zustimmen“ oder „Abbrechen“ – ruft jedenfalls eine Drucksituation hervor. Ein Ausschluss von Sicherheitsupdates der Chipsatz-Software bei Verweigerung der Preisgabe personenbezogener Daten ist als Druckausübung zu werten, die die Freiwilligkeit

329 Dies kann auch durch Abbildungen geschehen, auf denen bestimmte populäre Apps klar erkennbar sind.

330 Das Vertragsverhältnis zum App-Anbieter ist hiervon zunächst unabhängig zu sehen und kann durchaus die Eröffnung eines Kundenkontos o. Ä. erfordern.

der Nutzereinwilligung ausschließt. Auch eine Aussage wie die von *LG*, eine Vielzahl von Smart-TV-Funktionen könne ohne Einwilligung nicht genutzt werden (ohne dass diese genannt würden), kann im Sinne einer Druckausübung verstanden werden.

(4) Hinweis auf Widerruflichkeit der Einwilligung

Die Einwilligung in die Verarbeitung personenbezogener Daten ist grundsätzlich widerruflich ausgestaltet. Auf die Möglichkeit des Widerrufs muss der Verantwortliche ausdrücklich hinweisen, S. Art. 13 Abs. 2 lit. c) DSGVO (siehe dazu E. II. 5., S. 87).

Ein Widerruf führt ausweislich Art. 7 Abs. 3 S. 2 DSGVO nicht zum Entfallen der Einwilligung für die Vergangenheit, so dass von der Einwilligung gedeckte bis zum Widerruf erfolgte Datenverarbeitungsvorgänge grundsätzlich rechtmäßig sind. Der Widerruf der Einwilligung muss dabei stets so einfach wie die Erteilung der Einwilligung sein (Art. 7 Abs. 3 S. 4 DSGVO).

Hier bietet sich ein unterschiedliches Bild. Eine Einwilligung erfolgt in der Regel durch das Anklicken einer Schaltfläche. Einige Unternehmen bieten die Rücknahme von Einwilligungen über das Fernsehermenü an. Soweit dies ohne wesentlichen Suchaufwand[331] möglich ist, ist die Rücknahme der Einwilligung annähernd so einfach möglich wie die Vornahme der Einwilligung und somit DSGVO-konform. Erfordert eine Geltendmachung eines Widerrufs hingegen zwingend eine Kontaktaufnahme per E-Mail oder gar Web-Formular (s. dazu die Ausführungen unter E. II. 6., S. 88), so geht der hiermit einhergehende Aufwand sehr deutlich über das bloße Anklicken einer Einwilligungsfläche hinaus. In diesen Fällen ist die Widerrufsmöglichkeit nicht ebenso einfach ausgestaltet[332] wie die Erteilung der Einwilligung selbst und steht damit grundsätzlich nicht im Einklang mit der DSGVO.[333]

---

331 Nicht ausreichend wäre etwa ein pauschaler Verweis auf die Einstellungen des Fernsehers, wenn dort nicht unmittelbar in der ersten Menüebene ein entsprechender Punkt existiert (z. B. „Datenschutz“ oder „Privatsphäre“).

332 In diesem Sinne auch der EDSA, s. EDSA, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (13.05.2020), abrufbar (bislang nur auf Englisch) unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

333 In der Literatur ist mitunter die Rede davon, dass der Widerrufende zuverlässig identifiziert werden können muss (s. etwa *Stemmer* in: BeckOK Datenschutzrecht, 32. Ed., 01.02.2020, Art. 7 DSGVO Rn. 90b). Bei Smart-TVs setzt dies in der Regel nicht voraus, dass eine Angabe von Name, Adresse o. Ä. erfolgen muss. Bei den meisten Einwilligungsszenarien wird das Fernsehgerät anhand einer ID identifiziert, so dass auch ein Widerruf direkt auf das betreffende Fernsehgerät zurückgeführt werden könnte.

(5) Unmissverständliche Einwilligungserklärung/-handlung

Für die Wirksamkeit einer Einwilligung fordert Art. 4 Nr. 11 DSGVO eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung". Dies bedeutet zunächst, dass eine Einwilligungserklärung nicht schriftlich abgegeben werden muss, was auch aus DSGVO-Erwägungsgrund 32 S. 1 eindeutig hervorgeht. Gem. Art. 7 Abs. 1 DSGVO hat der Verantwortliche aber den Nachweis für jede Einwilligung zu erbringen, die die Basis für eine Datenverarbeitung bildet. Im Ergebnis bedeutet dies eine Dokumentationspflicht des Verantwortlichen.[334]

Im Kontext von Smart-TVs stellt die Unmissverständlichkeit der Abgabe einer Erklärung im Regelfall kein Problem dar. Wie DSGVO-Erwägungsgrund 32 S. 2 ausführt, ist das Anklicken eines Kästchens o. Ä. hierfür ausreichend.[335] Es genügt allerdings nicht, dass der Nutzer bestätigt, Datenschutzbestimmungen lediglich gelesen zu haben.[336]

Im Rahmen der Sektoruntersuchung konnte dieser Punkt nicht umfassend geprüft werden, da zwar die Datenschutzbestimmungen vorgelegt wurden, aber nur teilweise mit der Ausgestaltung der Einwilligungsschaltfläche. Es ist jedoch davon auszugehen, dass im Regelfall Einwilligungsersuchen nicht nur mit einem Lesebestätigungsbutton angezeigt werden. Zu Problemen führen jedoch „Gesamteinwilligungen", die einen längeren Text mit Datenschutzbestimmungen umfassen sollen. Selbst wenn hier eine Schaltfläche mit „Akzeptieren" oder „Zustimmen" oder dergleichen (ohne präzisierende Zusätze) eingeblendet wird, bedeutet dies nicht, dass das Anklicken der Schaltfläche als Einwilligung verstanden werden kann. Dem „Einwilligenden" fehlt es in diesen Fällen an einem entsprechenden Erklärungsbewusstsein, was für den Verantwortlichen – auch bei einer typisierten Gesamtbetrachtung aller Einwilligungssituationen – auch ersichtlich ist.

Es ist daher davon auszugehen, dass auch unter dem Aspekt der Unmissverständlichkeit der Einwilligungshandlung in einigen wenigen Fällen keine wirksame Einwilligung in die Datenverarbeitung durch Hersteller bzw. TV-Portal-Betreiber erfolgt.

---

334 Vgl. *Plath* in Plath [Hrsg.], DSGVO/BDSG, 3. Aufl. 2018, Art. 7 DSGVO Rn. 8.

335 Dessen ungeachtet kann die unmissverständlich erteilte Einwilligung ggf. nicht die hinreichende Bestimmtheit aufweisen, S. dazu oben S. 131.

336 So zutreffend das KG Berlin, Urteil vom 21.03.2019, Az. 23 U 268/13, juris Rn. 67. Im Regelfall dürfte eine solche Pauschalerklärung auch gegen den Grundsatz der Bestimmtheit der Einwilligung verstoßen.

2. *Digital Nudging*

Der Begriff des *Nudging* entstammt der Verhaltensökonomik und wurde ursprünglich nahezu ausschließlich im Kontext staatlichen oder durch den Staat angestoßenen Handeln erörtert („libertärer Paternalismus“[337]). Im Kern geht es darum, durch einen *Nudge* (engl. für Stups, Schubs oder Anstoß) das Verhalten von Menschen zu beeinflussen.[338]

Unabhängig von der Person des sog. Entscheidungsarchitekten stellt der Begriff des sog. *Digital Nudging*[339] auf digitale Entscheidungssachverhalte ab. Er bezieht so den privatwirtschaftlichen Bereich jedenfalls implizit mit ein.

Angesichts der dem *Nudging* innewohnenden Manipulationsgefahr wird immer wieder die Wichtigkeit ethisch-moralischer Standards bei dessen Einsatz angemahnt[340]. In diesem Zusammenhang wird betont, dass *Nudges* jedenfalls im Grundsatz transparent sein und die Wahlfreiheit der

---

337 *Thaler/Sunstein*, Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008, S. 4 - 6 (deutscher Titel Nudge: Wie man kluge Entscheidungen anstößt).

338 S. *Wikipedia.de*, Nudge, unter Verweis auf *Thaler/Sunstein*, a. a. O. (vorhergehende Fußnote), S. 6.

339 S. etwa *Schneider/Weinmann/vom Brocke*, Digital Nudging – Guiding Online User Choices through Interface Design, Bus Inf Syst 2016, 433, abrufbar unter https://link.springer.com/content/pdf/10.1007/s12599-016-0453-1.pdf; *Mirsch/Lehrer/Jung*, Digital Nudging: Altering User Behavior in Digital Environments, in Leimeister/Brenner [Hrsg.]: Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 634, abrufbar unter https://wi2017.ch/images/wi2017-0370.pdf; *Mirsch/Jung/Rieder/Lehrer*, Mit Digital Nudging Nutzererlebnisse verbessern und den Unternehmenserfolg steigern, Controlling 2018, 12; abrufbar unter https://rsw.beck.de/docs/librariesprovider37/default-document-library/controlling-05-2018-beitrag-mirsch-jung-rieder-lehrer.pdf?sfvrsn=4a6b9143_0; *Reisch*, Nudging hell und dunkel: Regeln für digitales Nudging, Wirtschaftsdienst 2020, 87, abrufbar unter https://www.springerprofessional.de/nudging-hell-und-dunkel-regeln-fuer-digitales-nudging/17729756; Beispiele bei *de Weerd*, Nudge Marketing Examples: How to drive online purchase behavior (crobox.com, 16.04.2019), abrufbar unter https://blog.crobox.com/article/nudge-marketing.

340 *Sunstein*, The Ethics of Nudging, Yale Journal on Regulation 2015, 413, abrufbar unter https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1415&context=yjreg.

entscheidenden Person („choice maker“) gewährleisten sollten.[341] Beim digitalen *Nudging*, welches ja auch von Unternehmen betrieben wird, haben sich indessen bislang keine konkreten ethischen Maßstäbe herausgebildet[342], geschweige denn etabliert[343].

Im juristischen Bereich findet eine Auseinandersetzung mit dem Phänomen des digitalen *Nudgings* nur vereinzelt ihren Niederschlag in spezifischen Rechtsnormen. So greift etwa die Verbraucherrechte-Richtlinie[344] auch einzelne *Nudging*-anfällige Situationen auf, wie Kostenfallen durch intransparente Formulierungen auf Schaltflächen[345] oder die unternehmerseitige Voreinstellung zahlungspflichtiger Zusatzleistungen beim Abschluss von Verträgen im Internet[346].

Wird *Nudging* intransparent, manipulativ und/oder ohne Rücksicht auf die Interessen der betroffenen Person eingesetzt, so spricht man auch von „dark patterns“[347] oder „dark nudges“[348] oder –

---

341 Vgl. etwa *Heidbrink/Klonschinski*, Nudges, Transparenz und Autonomie – Eine normativ gehaltvolle Kategorisierung von Maßnahmen des Nudgings, Vierteljahrshefte zur Wirtschaftsforschung 2018, 15, abrufbar unter https://elibrary.duncker-humblot.com/zeitschriften/id/25/vol/87/iss/1906/art/9838/.

342 Vgl. *Schmidt/Engelen*, The Ethics of Nudging: An overview, 2020, 7, abrufbar unter https://onlinelibrary.wiley.com/doi/epdf/10.1111/phc3.12658; *Meske/Amojo*, Status Quo, Critical Reflection, and the Road Ahead of Digital Nudging in Information Systems Research: A Discussion with Markus Weinmann and Alexey Voinov, Communications of the Association for Information Systems 2020, 402, 405, abrufbar unter https://aisel.aisnet.org/cgi/viewcontent.cgi?article=4194&context=cais.

343 Vgl. *Thaler*, The Power of Nudges, for Good and Bad (nytimes.com, 31.10.2015), abrufbar unter https://www.nytimes.com/2015/11/01/upshot/the-power-of-nudges-for-good-and-bad.html.

344 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates v. 25.10.2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, Abl. EU Nr. L 304 v. 22.11.2011, S. 64 (kurz Verbraucherrechte-Richtlinie).

345 Hier sieht die Verbraucherrechte-Richtlinie in Art. 8 Abs. 2 UAbs. 2 die sog. *Button-Lösung* vor, derzufolge ein Bestellvorgang eines Verbrauchers im Internet nur über eine Schaltfläche mit den Wörtern "zahlungspflichtig bestellen" oder einer gleichermaßen klaren Beschriftung abgeschlossen werden kann. Die *Button-Lösung* wurde in § § 312j Abs. 3 BGB umgesetzt. Ausführlich hierzu *Brönnecke* in Tamm/Tonner/Brönnecke, Verbraucherrecht, 3. Aufl. 2020, § 10 E-Commerce, Rn. 35 d. ff.

346 Art. 22 der Verbraucherrechte-Richtlinie verbietet im elektronischen Geschäftsverkehr eine unternehmerseitige Voreinstellung, mit der eine Zahlung, die das Entgelt für die Hauptleistung übersteigt, vereinbart werden soll. In Deutschland wurde die Richtlinienvorgabe umgesetzt in § 312a Abs. 3 S. 2 BGB.

347 Vgl. *Brignull*, What are dark patterns? (darkpatterns.org, undatiert), abrufbar unter https://www.darkpatterns.org/.

348 S. insb. *Newall*, Dark nudges in gambling, Addiction Research & Theory 2019, S. 65, abrufbar unter https://www.tandfonline.com/doi/full/10.1080/16066359.2018.1474206.

im Fall exzessiver Erschwerung des Zugangs zu oder der Nutzung eines Produkts oder Services[349] – „sludges“[350].

a) Ermittlungsergebnisse

Auch im Zusammenhang mit Smart-TVs stößt man auf *Nudges*. Dies zeigt sich bereits bei der Ersteinrichtung des Geräts, wie folgende Beispiele veranschaulichen:

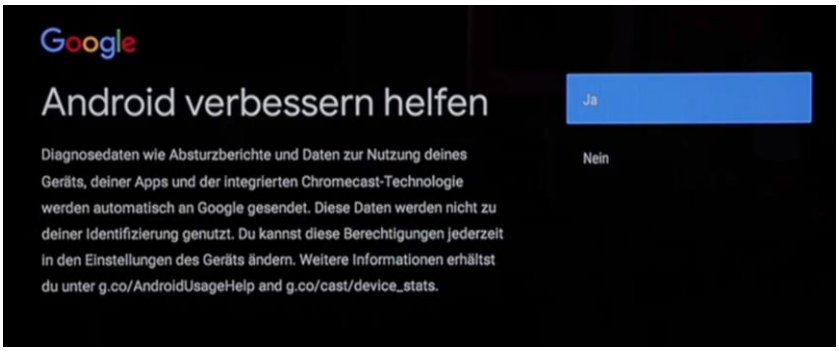
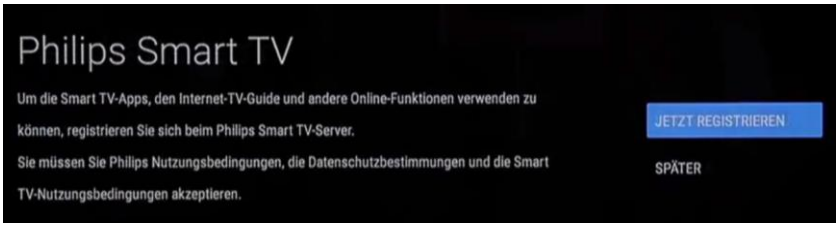
	Die Vorauswahl ist bereits auf „Ja“ (= Zustimmung) eingestellt.

Abbildung 26:Screenshot Ersteinrichtung eines Smart-TVs von *TP Vision* (*Philips*) mit *Android TV*[351]

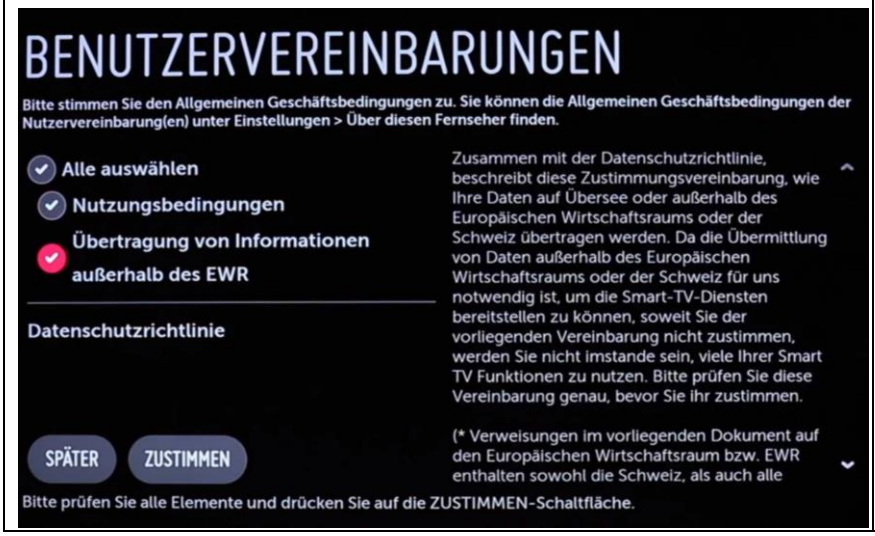
 Der obige Text lautet: „Um die Smart TV-Apps, den Internet-TV-Guide und andere Online-Funktionen verwenden zu können, registrieren Sie sich beim *Philips* Smart TV-Server. Sie müssen Sie [sic] *Philips* Nutzungsbedingungen, die Datenschutzbestimmungen und die Smart TV-Nutzungsbedingungen akzeptieren.“	Die Vorauswahl ist bereits auf „Jetzt registrieren“ (= Zustimmung) eingestellt. Dem Nutzer wird suggeriert, die Verwendung von Apps setze eine Registrierung voraus (dabei können ohne Registrierung nur die Smart-TV-Apps von *Philips* nicht genutzt werden, die für den Nutzer wesentlich bedeutenderen *Android*-Apps sind hiervon nicht betroffen). Zudem gibt es keine Schaltfläche „Ablehnen“, sondern nur die Option „Später“.

349 S. *Reisch*, a. a. O. (Fn. 339), 87, 90.

350 *Thaler*, Nudge, not sludge – Editorial, Science 2018, S. 431; abrufbar unter https://science.sciencemag.org/content/sci/361/6401/431.full.pdf.

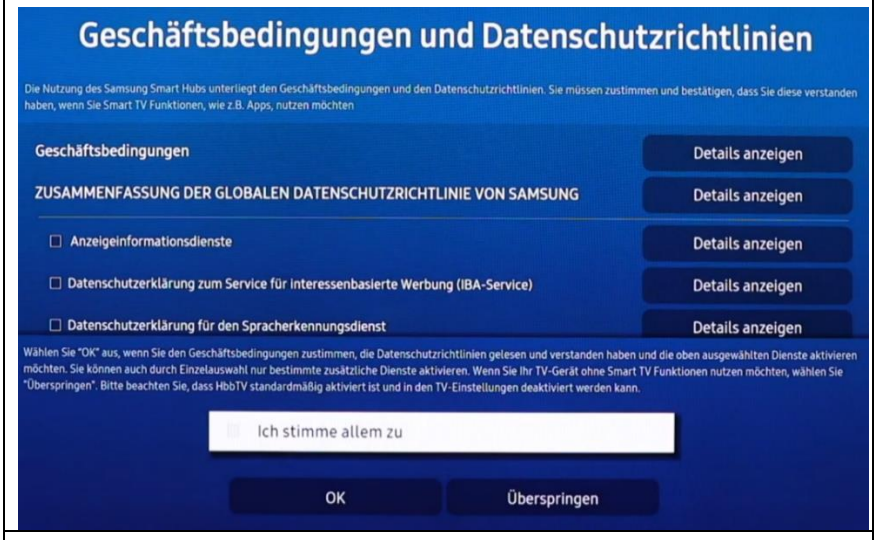
351 Entnommen aus dem Video *Philips TV Ersteinrichtung Thomas Electronic Online Shop Erstinstallation Philips TV LineUp 2019* https://www.youtube.com/watch?v=-1CasBn9EnE (Minute 3:00).

Abbildung 27:Screenshot Ersteinrichtung eines Smart-TVs von *TP Vision* (*Philips*) mit *Android TV*[352]



Bei Durchlesen des relevanten Textes wird das Auswahlfeld bereits aktiviert. Dem Nutzer wird in Aussicht gestellt, ohne Zustimmung viele – nicht näher bezeichnete – „Smart TV Funktionen“ nicht nutzen zu können. Es gibt zudem keine Schaltfläche „Ablehnen“, sondern nur „Später“ oder „Zustimmen“. Der Text unten auf der Seite („Bitte prüfen Sie alle Elemente und drücken Sie auf die ZUSTIMMEN-Schaltfläche“) suggeriert ebenfalls, dass eine Zustimmung erforderlich ist.

Abbildung 28:Screenshot Ersteinrichtung eines Smart-TVs von *LG*[353]



Der obige kleingedruckte Text lautet:

„Die Nutzung des Samsung Smart Hubs unterliegt den Geschäftsbedingungen und den Datenschutzrichtlinien. Sie müssen zustimmen und bestätigen, dass Sie diese verstanden haben, wenn Sie Smart TV Funktionen, wie z. B. Apps, nutzen möchten.

Hier tritt eine für den Nutzer nicht klar erkennbare Vermengung von Kenntnisnahme-/Zustimmungsszenarien ein: Eine Zustimmung zu den Geschäftsbedingungen als grundlegende Voraussetzung für die Nutzung von Smart-TV-Funktionen, eine Kenntnisnahme der globalen Datenschutzrichtlinie sowie jeweils eine optionale Zustimmung zur Aktivierung der drei genannten Zusatzdienste und den hiermit verbundenen Datenverarbeitungen. Durch die begleitende Formulierung „Die Nutzung des Smart Hubs unterliegt … den Datenschutzrichtlinien“ kann zudem der Eindruck entstehen, es müsste in alle Daten-

352 Entnommen aus dem Video *Philips TV Ersteinrichtung Thomas Electronic Online Shop Erstinstallation Philips TV LineUp 2019* https://www.youtube.com/watch?v=-1CasBn9EnE (Minute 1:30).

353 Entnommen aus dem Video *LG TV 2019 Ersteinrichtung Thomas Electronic Online Shop Erstinstallation LG LineUp 2019* vom 21.11.2019, abrufbar unter https://www.youtube.com/watch?v=Vqsa-wIPlaKs (Minute 1:39).

[…] Wählen Sie „OK“ aus, wenn Sie den Geschäftsbedingungen zustimmen, die Datenschutzrichtlinien gelesen und verstanden haben und die ausgewählten Diesnte aktivieren möchten. Sie können auch durch Einzelauswahl nur bestimmte zusätzliche Dienste aktivieren. Wenn Sie Ihr TV-Gerät ohne Smart TV Funktionen nutzen möchten, wählen Sie „überspringen“. Bitte beachten Sie, dass HbbTV standardmäßig aktiviert ist und in den TV Einstellungen deaktiviert werden kann.“	schutztexte eingewilligt werden. Die Schaltfläche „Ich stimme allem zu“ ist bereits vorausgewählt und prominent hervorgehoben.

Abbildung 29:Screenshot Ersteinrichtung eines Smart-TVs von *Samsung*[354]

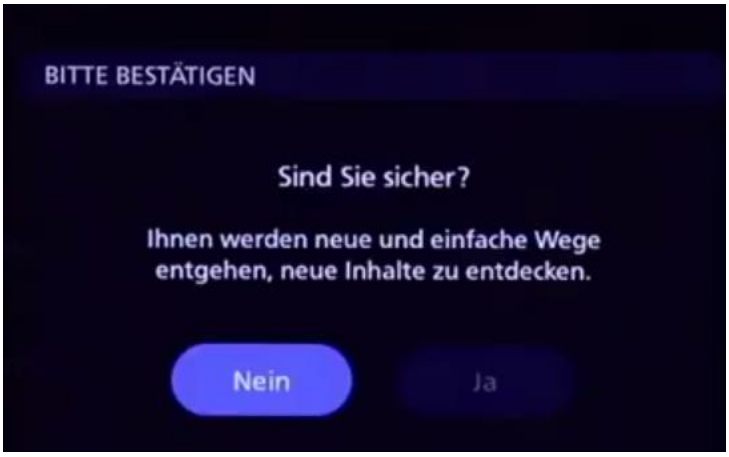
	Will der Nutzer Samba-TV im Rahmen der Erstinstallation deaktivieren, so muss er dies nochmals separat bestätigen, wobei die „Nein“-Schaltfläche vorausgewählt ist.

Abbildung 30:Screenshot Ersteinrichtung eines Smart-TVs von *Panasonic*[355]

b) Rechtliche Beurteilung

Inwieweit unternehmerisches Nudging zulässig ist, wird als übergreifende Frage bislang eher selten aufgeworfen. Dies mag zum einen daran liegen, dass das Thema Nudging großteils noch immer im Kontext der Verantwortbarkeit entsprechender staatlicher Maßnahmen erörtert wird.[356] Zum anderen weist der Begriff des *Nudgings* Unschärfen auf, und es kann in vielerlei Formen in

354 Entnommen aus dem Video *Ersteinrichtung Samsung QLED 2020 Onlineshop Thomas Electronic* vom 25.03.2020, abrufbar unter https://www.youtube.com/watch?v=dDd9_JL9HQk&list=PLO6t7DBoZlu0s4TwuZXxBCqCaodCht1LC (Minute 2:37).

355 Entnommen aus dem Video *Ersteinrichtung + Sendersortierung Panasonic OLED oder LED 2020 Onlineshop Thomas Electronic*, abrufbar unter https://www.youtube.com/watch?v=rYhWuAmCevM (Minute 4:27).

356 S. etwa *Kirchhof*, Nudging – zu den rechtlichen Grenzen informalen Verwaltens, ZRP 2015, 136; Hufen, Rechtsformen, Möglichkeiten und Grenzen der sanften Beeinflussung des Menschen durch den Staat, JuS 2020, 193.

Erscheinung treten. Trotz Bemühungen um die Festlegung von Nudging-Kategorien sowie Transparenz- und Fairness-Kriterien ist daher in Anbetracht der vielfältigen Nudging-Sachverhalte stets eine Einzelfallbetrachtung vonnöten.[357]

Der norwegische *Forbrukerrådet* hatte im Jahr 2018 in einer Studie angeprangert, dass insbesondere *Google* und *Facebook* „dark patterns" einsetzten, um an Nutzerdaten zu gelangen.[358] Es sei zweifelhaft, ob die Methoden im Einklang stünden mit den Prinzipien der DSGVO. Insbesondere könne eine Zustimmung unter diesen Bedingungen nicht als freiwillige und unmissverständliche Einwilligung angesehen werden.[359]

Im Hinblick auf die Ersteinrichtung von Smart-TVs – oder IoT-Geräten im Allgemeinen – stellt sich das Problem, dass der Verbraucher nicht immer ohne Weiteres auf den ersten Blick erkennt, ob er über realistische Wahlmöglichkeiten verfügt, wenn ihm Texte zur Kenntnisnahme oder Zustimmung vorgelegt werden. Aufgrund der Vielzahl faktisch alternativloser Zustimmungserteilungen tritt ein gewisser Gewöhnungseffekt ein und mit ihm die Praxis, sich möglichst zügig durch Verbrauchertexte zu klicken.[360] Vor diesem Hintergrund kann ein zusätzliches Verleiten der Verbraucher in Richtung Zustimmung durchaus kritisch gesehen werden. Ob tatsächlich ein rechtlich missbilligtes Verhalten vorliegt, muss jedoch im Einzelfall beurteilt werden.

Was die Rechtmäßigkeit erteilter Einwilligungen anbelangt, so wurden oben bereits Beispiele genannt, in denen es an einer ausreichenden Information des Verbrauchers fehlte (s. dazu E. V. 1. c) bb) (2), S. 133). Auch das Hervorrufen von Fehlvorstellungen beim Verbraucher kann dazu führen, dass er seine Einwilligungserklärung nicht in (korrekt) informierter Weise abgibt und die Einwilligung daher nicht wirksam ist. Hierzu wird es jedoch nicht alleine ausreichen, dass etwa Schaltflächen farblich unterlegt und/oder anderweitig hervorgehoben sind. Auch eine Nachfrage im Sinne von „Sind Sie sicher?" wird für sich genommen im Regelfall nicht Fehlinformationen oder eine die Freiwilligkeit ausschließende Drucksituation hervorrufen. Etwas anderes kann sich hingegen ergeben, wenn als Auswahlalternativen beispielsweise nur „Zustimmung" und „Später" angegeben werden, da beim Verbraucher so die Fehlvorstellung entstehen kann, eine Zustim-

---

357 Vgl. *Schmidt/Engelen* (Fn. 342), 7, 9.

358 *Forbrukerrådet*, Deceived by design – How tech companies use dark patterns to discourage us from exercising our rights to privacy, 2018, abrufbar unter https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

359 *Forbrukerrådet*, a. a. O. (vorhergehende Fußnote), insb. S. 8 ff.

360 Vgl. *Schaub/Alebako/Durity/Cranor*, A Design Space for Effective Privacy Notices, USENIX Association 2015 Symposium on Usable Privacy and Security, 1, 2 f., abrufbar unter https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf;

mung könnte nicht komplett verweigert werden. Die in Abbildung 28 bzw. Abbildung 29 dargestellten Einwilligungsersuchen vereinigen mehrere Nudging-Elemente in sich, die zusammen genommen – über das bereits festgestellte Fehlen wesentlicher Informationen hinaus – Zweifel an der Informiertheit der Verbraucherauswahlentscheidung aufkommen lassen.

Schwer fassen lässt sich eine Auswahlentscheidung wie in Abbildung 27. Wird der Nutzer zur Inanspruchnahme von Zusatzdienstleistungen verleitet, die er womöglich nicht benötigt, ohne dass eine Einwilligung in Datenverarbeitungen verlangt wird, sind jedenfalls die Regelungen der DSGVO zur Freiwilligkeit von Einwilligungen grundsätzlich nicht einschlägig.

Im Hinblick auf die oben beschriebenen *Nudging*-Beispiele könnte man jeweils die Frage stellen, inwieweit diese mit den DSGVO-Grundsätzen des Datenschutzes durch Technikgestaltung bzw. der datenschutzfreundlichen Voreinstellungen in Einklang stehen.[361] Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen, bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DS-GVO erfüllt werden.[362] Es erscheint möglich, die Konzeption der Gerätesoftware nach Art. 25 Abs. 1 DSGVO (i. V. m. Art. 5 Abs. 1 DSGVO) im Hinblick auf eine transparente und faire Nutzerführung hin zu untersuchen. Dabei muss jedoch berücksichtigt werden, dass Art. 25 Abs. 1 DSGVO etliche Faktoren enthält, die bei der Beurteilung des erforderlichen Pflichtenniveaus im Rahmen einer Abwägung zu berücksichtigen sind.[363] Art. 25 Abs. 2 DSGVO ist Ausdruck des Datensparsamkeitsprinzips und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten“ Voreinstellungen zu setzen.[364] Auch die Ausgestaltung von Entscheidungssituationen ist immer bereits eine Voreinstellung. Der Wortlaut von Art. 25 Abs. 2 S. 1 DSGVO[365] legt jedoch nahe, dass die Vorschrift solche Situationen (und Datenverarbeitungen) nicht erfasst, in denen die betroffene Person gerade um Zustimmung zu einer (zusätzlichen) Datenverarbeitung ersucht wird, die über den ursprünglichen Vertragszweck hinausgeht.

---

361 Dies war ein wesentlicher Aspekt in der Studie des norwegischen *Forbrukerrådet,* s. *Forbrukerrådet*, a. a. O. (Fn. 358), S. 8 f.

362 *Baumgartner* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 25 Rn. 3.

363 Vgl. *Martini* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 25 DSGVO Rn. 36.

364 *Baumgartner* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 25 Rn. 3; Voreinstellungen sind ein besonders wirksames Nudginginstrument, s. *Thaler*, Do you need a nudge? (Yale Insights, 04.11.2009), abrufbar unter https://insights.som.yale.edu/insights/do-you-need-nudge.

365 „Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“

Je nach Grad und Art und Weise des Hervorrufens von Fehlvorstellungen beim Verbraucher könnten neben dem Datenschutzrecht ggf. auch Normen des Lauterkeitsrechts wie insb. § 5 UWG (Irreführung) oder in extremeren Fällen auch § 4a UWG (aggressive Geschäftspraktiken) zur Anwendung kommen. Daneben kommt – etwa bei bereits vorausgewählten Antwortboxen – das Fehlen einer wirksamen Einwilligung als Rechtsgrundlage (Art. 6 abs. 1 UAbs. 1 lit. a) DSGVO) infrage, was wiederum auch einen Verstoß gegen 307 BGB (unangemessene Benachteiligung des Verbrauchers) bedeuten kann.[366]

Aufgrund der Vielfalt der *Nudging*-Situationen, die man zudem im Zusammenhang mit dem jeweiligen Ablauf der Nutzerführung und ggf. auch Besonderheiten der verwendeten Hardware (z. B. lange Ladezeiten oder langsame Reaktionsgeschwindigkeit) betrachten muss, lassen sich an dieser Stelle keine abschließenden rechtlichen Bewertungen treffen. Dies gilt umso mehr, als insbesondere die in Art. 25 Abs.1 bzw. Abs. 2 DSGVO verankerten Prinzipien bislang nur wenig konturiert sind. Soweit ersichtlich mangelt es hinsichtlich *Nudges* an einschlägiger Behördenentscheidungspraxis und Rechtsprechung.[367] Eindeutig manipulative *Nudges* oder solche mit offensichtlichem Bagatellcharakter lassen sich rechtlich mutmaßlich ohne größere Schwierigkeiten einordnen. In anderen Fällen wären zur Unterstützung normativer Bewertungen[368] wissenschaftliche Erkenntnisse dazu hilfreich, wie Verbraucher in bestimmten *Nudging*-Situationen reagieren.

Festzuhalten bleibt somit zum einen, dass *Nudges* in der rechtlichen Beurteilung keine eigenständige Kategorie bilden, sondern je nach Fallgestaltung durchaus unterschiedliche Normen verletzen können. Dabei rücken insbesondere Vorschriften der DSGVO und des Lauterkeitsrechts in den Blickpunkt. Zum anderen kann die Verwendung von *Nudges* je nach Umfang, Häufigkeit und Manipulationspotential keinesfalls als unbedenklich gelten. Unter Transparenzgesichtspunkten wäre in jedem Fall wünschenswert, dass dem Verbraucher Entscheidungsersu-

366 S. dazu BGH, Urteil vom 28. Mai 2020 - I ZR 7/16 (zum Zeitpunkt der Publikation dieses Berichts noch nicht veröffentlicht), Pressemitteilung des BGH Nr. 67/2020 vom 28.05.2020 – *Cookie-Einwilligung II*. Die Entscheidung des BGH basierte auf einer Vorabentscheidung des EuGH, s. EuGH, Urteil vom 01.10.2019, Az. C-673/17, EU:C:2019:801.

367 Soweit ersichtlich beziehen sich beispielsweise die meisten bislang zu Art. 25 DSGVO ergangenen Entscheidungen auf Einzelfälle, in denen die Sicherheit personenbezogener Daten vor unberechtigten Zugriffen nicht gewährleistet wurde.

368 Vgl. dazu *Podszun* in Harte-Bavendamm/Henning-Bodewig [Hrsg], UWG, 4. Aufl. 2016, § 3 Rn. 127 f.

chen jeweils einzeln unter Mitteilung oder wenigstens direkter Abrufbarkeit aller wesentlichen Informationen und mit einer klar erkennbaren und optisch gleichrangigen Ablehnungsoption[369] vorgelegt werden[370].

3. Verantwortlichkeiten

Bei der Untersuchung der potentiell haftungsrelevanten Beteiligten im Bereich der Smart-TVs sind wie bereits dargestellt (unter D. III.) verschiedene Akteure zu unterscheiden:

Bereits bis zum Inverkehrbringen der Geräte sind unter Umständen eine Vielzahl von Unternehmen in den Herstellungsprozess involviert, und zwar als (End-)Hersteller, Teilhersteller, sog. Assembler, Lizenzgeber, Quasi-Hersteller, Importeure oder Lieferanten.[371] Je nach den Umständen des Einzelfalles und vertretener rechtlicher Ansicht können sie alle potentiell nach § 4 ProdHaftG mit seinem weiten Herstellerbegriff als „Hersteller“ haften.

Auf der „Plattform Smart-TV“ ist daneben eine Vielzahl von Diensteanbietern tätig. Da wäre zum einen der Hersteller des Smart-TVs, der meistens – aber nicht zwingend – auch für das Betriebssystem des Geräts verantwortlich zeichnet. Hinzu kommen insbesondere HbbTV-Fernsehsender, Anbieter von TV-Portalen oder einzelner Apps sowie für elektronische Programmführer. Jeder dieser Diensteanbieter kann vertragliche Beziehungen mit dem Nutzer eingehen und diesem im Rahmen der Vertragsanbahnung Nutzungs- und/oder Datenschutzbedingungen zur Kenntnisnahme oder ggf. Einwilligung vorlegen.

Die Beiträge dieser Akteure sind sehr heterogen. Sie können einerseits Standardteile oder -leistungen umfassen, sowie andererseits speziell für bestimmte Smart-TVs konzipierte Bauteile oder Software. Zudem ist zu beobachten, dass etwa Samsung – nach Absatzzahlen Marktführer in Deutschland und weltweit – seine Fernseher weitestgehend unternehmensintern entwickelt, während kleinere Hersteller bestimmte Leistungen (etwa TV-Portale) als standardisiertes „Komplettpaket“ zukaufen, ohne hierauf inhaltlich wesentlichen Einfluss auszuüben. In diesem Zusammen-

---

369 Aus der Vorgabe des Art. 7 Abs. 3 S.3 DSGVO, demzufolge der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung sein muss, lässt sich jedenfalls für das Datenschutzrecht der allgemeine Rechtsgedanke ableiten, dass auch die Verweigerung einer Einwilligung ebenso einfach möglich sein muss wie deren Erteilung.

370 Noch weitergehend der norwegische *Forbrukerrådet*, der als datenschutzfreundlichste Voreinstellung ein vorausgewähltes Ankreuzfeld für die datenschutzfreundlichste Auswahloption fordert*, s. Forbrukerrådet*, a. a. O. (Fn. 358), S. 9.

371 Vgl. die Aufzählung bei *Littbarski* in Kilian/Heussen [Hrsg.], Computerrechts-Handbuch, Teil 18 – Produkthaftung, Rn. 146 ff. m. w. N.

hang zeigt sich auch eine höchst unterschiedliche Machtposition bei Verhandlungen mit Zulieferern, insbesondere was das Verhältnis zwischen Herstellern und Anbietern sog. Over-the-top-Inhalte wie *Netflix* oder *Amazon Prime Video* anbelangt.

Für die Prüfung der datenschutzrechtlichen Verantwortlichkeiten durch den Nutzer bedeutet diese Ausgangssituation bei Smart-TVs, dass mehrere Parteien in einen datenbezogenen Sachverhalt organisatorisch eingebunden sein und entsprechende Beiträge leisten können. Im Einzelnen kann es für den Verbraucher kaum mehr nachvollziehbar sein, wer für einen bestimmten Datenverarbeitungsvorgang verantwortlich ist.

Es ist daher für den Nutzer schwer zu beurteilen, welche Vorschriften der DSGVO einschlägig sind und insbesondere welche Beteiligten als „Verantwortliche“ im Sinne der datenschutzrechtlichen Vorschriften anzusehen sind oder anderweitig bei Rechtsverstößen haften.

a) Ermittlungsergebnisse

Bei Smart-TVs kann man im Wesentlichen drei verschiedene Konstellationen unterscheiden, wobei Mischformen durchaus vorkommen und auch bei einem Hersteller Unterschiede je nach Modellreihe bestehen können. Zum einen gibt es den Fernseher, bei dem alle wesentliche Hard- und Software aus einer Hand stammt. Dies ist etwa bei den Herstellern *Samsung, LG* und *Panasonic* der Fall. Zum anderen gibt es Fernseher, bei denen die Systemsoftware von einem Drittanbieter bezogen wird. Dies betrifft etwa Gerätemodelle von *TP Vision (Philips)* oder *Sony*, bei denen *Android TV* von *Google* vorinstalliert ist. Schließlich besteht die Möglichkeit, auf dem Fernsehgerät nur rudimentäre Software vorzuinstallieren und sämtliche wesentlichen Smart-Funktionen über ein webbasiertes, auf den jeweiligen Fernsehhersteller zugeschnittenes TV-Portal anzubieten. Zu den Anbietern solcher Portale zählen insbesondere die Unternehmen *Foxxum* und *Netrange*.

Je nachdem, welcher der o. g. Ansätze gewählt wurde, unterscheiden sich auch die Datenflüsse – und die Kenntnisse über Datenflüsse – erheblich. Unternehmen, bei denen „alles aus einer Hand stammt“, sind naturgemäß am besten in der Lage, Datenflüsse nachzuverfolgen. Umgekehrt verhält es sich bei Fernsehern, die praktisch nur das Eingangstor zu TV-Portalen anderer Anbieter darstellen. Hierbei lässt sich wiederum beobachten, dass diejenigen Hersteller, deren Geräte nur auf webbasierte TV-Portale zugreifen, am wenigsten Kenntnisse über Datenströme besitzen.

aa) Vorinstallierte Apps

Abbildung 31:App-Icons[372]

Die befragten Unternehmen gaben nahezu durchgängig an, dass sie über Dritt-Apps keinerlei Nutzerdaten erhielten. Sie hatten auch keine oder jedenfalls keine detaillierten Kenntnisse darüber, welche Daten zwischen Nutzer und App-Anbieter fließen.[373] Soweit die befragten Unternehmen die Übermittlung bestimmter Daten zwischen Nutzer und App-Anbieter ausschlossen, ließ sich dies darauf zurückführen, dass die betreffenden Daten bereits nicht auf dem Fernsehgerät in gespeicherter Form vorhanden waren und die betreffende App die Eingabe dieser Daten nicht vom Nutzer verlangte. Soweit eine Übermittlung von lokal auf dem Gerät vorhandenen Daten möglich war oder die App selbst Dateneingaben verlangte, war den Smart-TV-Herstellern in der Regel nicht bekannt, ob diese Daten tatsächlich erhoben wurden, d. h. sie hatten keinen Einblick in den Datenverkehr zwischen Nutzer und App-Anbieter. Ein Hersteller beantwortete die hierauf gerichtete Frage schlicht mit „Wir haben keine Ahnung“[374]. Ein anderer gab an: „Diese Apps sind außerhalb unserer Kontrolle, die Aktionen von Endverbrauchern innerhalb dieser Apps unterliegen den Endnutzer- und Lizenz- sowie Datenschutzbestimmungen zwischen Endverbraucher und App-Anbieter“.[375] Ein weiteres Unternehmen antwortete: „Apps (Internet Apps, HbbTV Apps, etc) kommunizieren direkt mit den Servern der entsprechenden App-Anbieter. [Wir haben] keine Kenntnis über die Inhalte eben dieser Kommunikation.“

Die vorinstallierten Dritt-Apps sind jedoch nicht völlig losgelöst von Entscheidungen und Interessen der Hersteller zu sehen. Zum einen können sie bei manchen Anbietern durch den Verbraucher nicht deinstalliert und z. T. nicht einmal deaktiviert werden (siehe dazu E. VII. 4., S. 207). Zum anderen sind die Hersteller mitunter über *Revenue Sharing Agreements* und andere Vergütungen an dem Erfolg der Dritt-Apps beteiligt (siehe dazu unter cc), S. 153).

372 Bildnachweis: *geralt/pixabay*.

373 Teilweise wurde (bei Einwilligung des Nutzers) erfasst, welche Apps benutzt wurden und ggf. auch für wie lange.

374 Im englischsprachigen Original: „We have no idea“.

375 Im englischsprachigen Original: “Those apps are out of [our] control, the actions of end users in those apps are under the EULA and [privacy policy] between end user and app owner.”

Unternehmenseigene Apps der Smart-TV-Hersteller fanden sich nur selten und waren ganz überwiegend datensparsam, d. h. es wurden, wenn überhaupt, nur in geringem Umfang personenbezogene Daten übermittelt. Auch waren die Datentransfers in der Regel nachvollziehbar (z. B. Übermittlung der bereits installierten Apps bei Aufrufen des App-Stores).

Vor der Nutzung einer App wird der Nutzer im Regelfall mit den einschlägigen Datenschutzbestimmungen konfrontiert. Dies geschieht zum einen bereits im Rahmen der Ersteinrichtung des Fernsehers, insbesondere im Hinblick auf die Apps des Herstellers selbst. Zum anderen werden Datenschutzbestimmungen, vor allem bei Apps von Drittanbietern, beim ersten Aufrufen der App angezeigt.

bb) Andere vorinstallierte Software

Im Rahmen der Sektoruntersuchung wurden zu der sonstigen Software, die auf den jeweiligen Fernsehgeräten verwendet wird, im Wesentlichen die gleichen Fragen gestellt wie zu Apps. Dies war schon deshalb geboten, weil in manchen Fällen eine Anwendung als (System-)Software oder als für den Nutzer sichtbare App umgesetzt werden kann.

Die befragten Hersteller konnten zum Datentransfer durch die vorinstallierte Software aussagekräftigere Angaben machen als bei den – zumeist von Dritten angebotenen – Apps. Dies galt jedoch nicht oder nur sehr eingeschränkt für die Unternehmen, deren Fernsehgeräte von OEM-Herstellern[376] stammten oder deren Geräte ein unternehmensfremdes Betriebssystem oder TV-Portal hatten. Bei etlichen Herstellern gibt es vorinstallierte Softwarekomponenten, die nicht als Apps ausgestaltet sind, aber ebenso wie Apps Zusatzfunktionen bereitstellen und nicht im engeren Sinne systemrelevant sind, z. B. Sprachassistenten oder Empfehlungsdienste.

Betrachtet man die Software-Architektur von Smart-TVs im Hinblick auf mögliche Datenschutzverletzungen, so geht von der systemnahen Software in aller Regel deutlich weniger Gefahr aus als von Zusatzdiensten und (Dritt-)Apps.

cc) Verträge zwischen Herstellern und Anbietern von Software (einschließlich Apps)

Generell sind die Hersteller bemüht, ihre eigene Verantwortlichkeitssphäre zu begrenzen. Dies gilt einerseits für das Verhältnis zum Nutzer. So findet sich etwa in den Datenschutzbestimmungen *Samsungs* die Aussage

---

376 Sog. *Original Equipment Manufacturer* (OEM) oder auch Erstausrüster stellen Produkte oder Produktkomponenten her, die sie an andere Unternehmen liefern, die die Produkte dann unter ihrem Markennamen auf den Markt bringen. Im Bereich der Smart-TVs gibt es OE-Hersteller, die sowohl Vorlieferant für andere Hersteller als auch unter eigener Marke Fernseher in den Verkehr bringen.

> „Denken Sie daran, dass einige Drittanbieter interessenbasierte Werbung in ihren Apps auf Ihrem Samsung Smart TV anzeigen können. Diese Drittanbieter sind für ihre Datenschutzpraktiken selbst verantwortlich, z.B. für die Rechtsgrundlage der Verarbeitung Ihrer personenbezogenen Daten."[377]

Ferner sind die Verträge zwischen Herstellern und Software-Anbietern dadurch gekennzeichnet, dass Verantwortlichkeitssphären abgegrenzt werden. Im Regelfall soll nach den vertraglichen Regelungen jeweils (nur) derjenige für die Einhaltung aller gesetzlichen Vorgaben einstehen, der die betreffenden personenbezogenen Daten empfängt. Eine gemeinsame Verantwortung, ggf. einhergehend mit der Zuweisung von Informationspflichten gegenüber den Nutzern, ist in den Verträgen nicht angelegt. Mitunter wird die Einhaltung von Datenschutzgesetzen auch explizit angemahnt. Die Verträge enthalten indessen keinerlei spezifische Verbote zum Umgang mit Nutzerdaten. Auch ansonsten sind keine verstärkten Bemühungen erkennbar, dass Hersteller Software-Anbieter mit Nachdruck zur Einhaltung von Datenschutzstandards auffordern und dies ggf. auch durchsetzen, ohne dass ein konkreter Datenschutzverstoß bekannt geworden wäre. *LG* hält in seinen Allgemeinen Geschäftsbedingungen für seine *Seller Lounge* App-Entwickler immerhin dazu an, ihren Kunden eine Datenschutzerklärung zur Verfügung zu stellen, die vollumfänglich offenlegt, wie App-Anbieter Kundendaten sammeln, verwenden und verwalten.[378]

Zugleich verdeutlichen die Verträge, dass häufig eine enge wirtschaftliche Interessengemeinschaft zwischen den Herstellern und den Software-Anbietern besteht. Etliche Verträge beinhalten sog. Revenue Sharing Agreements. Diese legen fest, dass der Fernseherhersteller einem Diensteanbieter die Möglichkeit des Nutzerkontakts verschafft (insbesondere durch die Vorinstallation einer App) und im Gegenzug an den hieraus resultierenden Geschäftsabschlüssen, Abo-Gebühren oder Werbeeinkünften beteiligt wird. Diese Beteiligung kann bei vorinstallierten Streaming-Anbietern durchaus bei über 10 % des erzielten Umsatzes liegen. Über die Vorinstallation hinaus kann der Hersteller auch eine hervorgehobene Darstellung der App im Home Screen, im Menü oder in der Favoritenliste vornehmen sowie die Integration eines eigenen „Buttons" für die direkte Anwahl in der Fernbedienung anbieten. Teilweise ist die Vorinstallation von Software sogar mit dem Einbau spezifischer Hardware (Chip) verbunden.

---

377 *Samsung*, Globale Datenschutzrichtlinie – Datenschutzhinweis für interessenbasierte Werbung, unter *Was ist interessenbasierte Werbung?*

378 S. Punkt 8.2 der *LG Seller Lounge Terms & Conditions*, abrufbar unter http://seller.lgappstv.com/seller/footer/terms.lge?lang=en.

b) Rechtliche Würdigung

Angesichts dieses Zusammenwirkens stellt sich die Frage, ob der Hersteller für die Datenverarbeitung durch die Dritten (mit-)verantwortlich sein kann. Eine solche Verantwortlichkeit könnte sich aus dem Datenschutzrecht (unter aa)), dem allgemeinen Zivilrecht (unter bb) oder dem Lauterkeitsrecht (unter cc)) ergeben.

aa) Verantwortlichkeit im Sinne der DSGVO

Zentraler Anknüpfungspunkt der DSGVO ist die Qualifizierung einer natürlichen oder juristischen Person als „Verantwortlicher". Verantwortlich ist, so Art. 4 Nr. 7 DSGVO, „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet." Art. 24 S. 1 DSGVO statuiert konkrete Pflichten für den Verantwortlichen. Dieser muss „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um[setzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß [der Datenschutzgrundverordnung] erfolgt." Der Verantwortliche hat im Rahmen eines sog. „risikobasierten Ansatzes" einzustehen für die Sicherstellung der zulässigen Datenverarbeitung durch den Einsatz von technischen und organisatorischen Maßnahmen, die regelmäßig zu überprüfen sind.[379]

Im Hinblick auf die Vielzahl von Akteuren, die dem Verbraucher bei der Benutzung eines Smart-TVs gegenübertreten (siehe S. 120), verdient die Frage, wer als Verantwortlicher zu gelten hat, besondere Aufmerksamkeit. Unzweifelhaft können für gesonderte Datenverarbeitungsvorgänge, die personenbezogene Daten betreffen, jeweils unterschiedliche Personen allein verantwortlich sein. In Art. 4 Nr. 7 DSGVO angelegt ist darüber hinaus aber auch die Möglichkeit einer gemeinsamen Verantwortlichkeit für ein und dieselben Datenverarbeitungsvorgänge (hierzu nachfolgend unter (1)). In Betracht kommt ferner eine grundsätzliche (Mit-)Verantwortlichkeit des Auftragsdatenverarbeiters (hierzu nachfolgend unter (2)). Diese Fragen sind von hoher praktischer Relevanz, da betroffene Personen bzw. Verbraucherverbände oder Aufsichtsbehörden die Unterlassung von Datenschutzverletzungen oder Schadensersatzansprüchen bei Annahme gemeinsamer Verantwortlichkeit wesentlich einfacher durchsetzen können.

---

379 Vgl. *Gola* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 4 Rn. 49.

(1) Gemeinsame Verantwortlichkeit in der Rechtsprechung des EuGH

Entscheidend für die Annahme gemeinsamer Verantwortlichkeit ist gem. Art. 4 Nr. 7 DSGVO, dass eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[380] Ob dies der Fall ist, ist nach einem objektiven Maßstab zu entscheiden. Einlassungen der Vertragsparteien können allenfalls einen Anhaltspunkt darstellen.[381] Die Annahme einer gemeinsamen Verantwortlichkeit hat weitreichende Folgen. So ist etwa nach Art. 5 Abs. 2 DSGVO jeder der gemeinsam Verantwortlichen rechenschaftspflichtig für die in Art. 5 Abs. 1 DSGVO niedergelegten Voraussetzungen einer rechtmäßigen Datenverarbeitung. Art. 26 Abs. 3 DSGVO sieht vor, dass die betroffene Person ihre Rechte nach der DSGVO gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.

Der Europäische Gerichtshof hat zur gemeinsamen Verantwortlichkeit[382] in der Entscheidung *Wirtschaftsakademie Schleswig-Holstein* festgestellt, dass der Betreiber einer *Facebook*-Fanpage gemeinsam mit *Facebook* für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich ist. Die Betreiber von Fanpages können mit Hilfe der Funktion *Facebook Insight*, die ihnen *Facebook* zur Verfügung stellt, anonymisierte statistische Daten über die Nutzer dieser Seiten erhalten. Die Datensammlung erfolgt dabei über Cookies. Dem EuGH zufolge ist es für die Annahme gemeinsamer Verantwortlichkeit mehrerer Personen für dieselbe Verarbeitung nicht notwendig, dass jeder Zugang zu den betreffenden personenbezogenen Daten hat.[383] Der Betreiber einer auf *Facebook* unterhaltenen Fanpage sei durch die von ihm vorgenommene Vorgabe bestimmter Auswertungsparameter an der Entscheidung über die Zwecke

---

380 Hier liegt ein Unterschied zur alten Gesetzeslage nach dem BDSG. § 3 Abs. 7 BDSG a. F. verwendete den Begriff der „verantwortlichen Stelle“, ohne den Aspekt der Möglichkeit der Kooperation mehrerer Verantwortlicher anzusprechen; S. *Gola* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 4 Rn. 48.

381 S. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (WP 169 vom 16.02.2010), S. 23, abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf; *Golland*, K & R 2019, 533.

382 Die Entscheidung des EuGH bezog sich zwar auf Art. 2 Buchstabe d) der Datenschutz-Richtlinie. Die Regelung ist jedoch hinsichtlich der Definition der gemeinsam Verantwortlichen in Art. 4 Nr. 7 DSGVO deckungsgleich.

383 EuGH, Urteil vom 5.6. 2018, Az. C-210/16, EU:C:2018:388, Rn. 38 – *Wirtschaftsakademie Schleswig-Holstein*; wiederholt in EuGH, Urteil vom 10.07.2018, Az. C-25/17, EU:C:2018:551 – *Zeugen Jehovas*, Rn. 69.

und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt.[384]

In seiner Entscheidung *Zeugen Jehovas* stellte der EuGH klar, dass das Bestehen einer gemeinsamen Verantwortlichkeit nicht zwangsläufig eine *gleichwertige* Verantwortlichkeit der verschiedenen Akteure bedeute. Vielmehr könnten die Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein.[385] Eine datenschutzrechtliche Verantwortlichkeit könne bereits dann vorliegen, wenn eine Person aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nehme und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirke.[386]

In seinem Urteil in der Rechtssache *Fashion ID* äußerte sich der EuGH abermals zur Frage der gemeinsamen Verantwortlichkeit.[387] In dem Ausgangssrechtsstreit ging es im Kern darum, ob das Unternehmen *Fashion ID*, welches *Facebooks* „Gefällt mir"-Button in seine Website eingebunden hatte, hinsichtlich Datenverarbeitungen durch *Facebook* ebenfalls als Verantwortlicher angesehen werden konnte. Der EuGH bejahte diese Frage. Für eine gemeinsame Entscheidung über die Mittel sah der EuGH es als ausreichend an, dass Fashion ID den „Gefällt mir"-Button von *Facebook* in dem Wissen in seine Website eingebunden hatte, dass dieser als Werkzeug zum Erheben und zur Übermittlung von personenbezogenen Daten der Besucher der Website fungieren konnte.[388] Die gemeinsame Entscheidung über den Zweck der Datenverarbeitung bejahte der Gerichtshof ebenfalls. So habe *Fashion ID* mit der Einbindung des „Gefällt mir"-Buttons zumindest stillschweigend in das Erheben personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung eingewilligt. Die Verarbeitungsvorgänge lägen im wirtschaftlichen Interesse sowohl von *Fashion ID* als auch von *Facebook*. *Facebook* biete *Fashion ID* einen wirtschaftlichen Vorteil und erhalte als Gegenleistung die Möglichkeit, die empfangenen Daten für eigene wirtschaftliche Zwecke nutzen zu können.[389] Der EuGH stellte jedoch auch klar, dass die gemeinsame Verantwortlichkeit nur den initialen Datenfluss vom Website-Besucher an

---

384 EuGH, Urteil vom 5.6. 2018, Az. C-210/16, EU:C:2018:388, Rn. 39 – *Wirtschaftsakademie Schleswig-Holstein*.

385 EuGH, Urteil vom 10.07.2018, Az. C-25/17, EU:C:2018:551, Rn. 66 – *Zeugen Jehovas*.

386 EuGH, Urteil vom 10.07.2018, Az. C-25/17, EU:C:2018:551, Rn. 68 – *Zeugen Jehovas*.

387 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 68 – *Fashion ID*; wiederum betraf der Ausgangsrechtsstreit zwar Normen der Datenschutz-Richtlinie. Aber auch hier können insoweit die Ausführungen des EuGH zu den weitgehend deckungsgleichen Vorschriften der DSGVO gelten.

388 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 77 – *Fashion ID*.

389 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 80 – *Fashion ID*.

Facebook betreffe; für die sich anschließende weitere Verarbeitung der Daten sei *Facebook* allein verantwortlich.[390]

Die bisher ergangene Rechtsprechung des EuGH ist indessen in einigen Punkten unscharf. So begründet der EuGH nicht, worin er im Fall *Fashion ID* über ein Erheben von Daten hinaus auch eine Weitergabe von Daten durch Übermittlung an *Facebook* sieht. Der Website-Betreiber *Fashion ID* hatte zu keinem Zeitpunkt Zugriff auf die Nutzerdaten, die über seine Internetseite direkt an *Facebook* flossen. Man könnte den EuGH dahin gehend verstehen, dass er bereits das bloße Ermöglichen eines Datenzugriffs durch *Fashion ID* als Unterfall der Datenverarbeitung, nämlich Datenweitergabe durch Übermittlung, genügen lässt. Jedoch selbst bei weiter Auslegung des Verarbeitungsbegriffs in Art. 4 Nr. 2 DSGVO muss man konstatieren, dass die Norm bei allen Fallbeispielen – und seien diese nur exemplarisch[391] – ihrem Wortlaut nach verlangt, dass zumindest kurzzeitig tatsächliche Gewalt über die betreffenden Daten besteht. Der EuGH selbst scheint auch nicht davon auszugehen, dass eine Datenweitergabe durch *Fashion ID* erfolgt. Hierfür spricht die folgende Passage im Urteil Fashion ID:

> „[…] Fashion ID [scheint] […] in das Erheben personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung eingewilligt zu haben.“ [392]

Diese Formulierung zeigt, dass der EuGH *nicht* von einer (eigenen) Verarbeitung durch Weitergabe von Daten durch *Fashion ID* ausgeht, sondern von einer bloßen Billigung der konkret ermöglichten Datenverarbeitung durch *Facebook*. Einer gemeinsamen Verantwortlichkeit steht dies freilich nicht entgegen.[393]

---

390 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 76 und 85 – *Fashion ID*.

391 S. *Roßnagel* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 4 Nr. 2 DSGVO Rn. 14 m. w. N.

392 S. EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 80 – *Fashion ID*. Offen bleibt freilich, wer dann überhaupt Daten an *Facebook* „weitergibt“. Der Nutzer selbst scheidet hier aus, da nur weitergegeben werden kann, was man zuvor selbst erhalten hat. Jedenfalls aber müsste eine Weitergabe *gezielt* erfolgen (also zumindest mit Wissen des Nutzers), S. *Roßnagel* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 4 Nr. 2 DSGVO Rn. 26. Dies wäre hier nicht der Fall, da der Nutzer sich der Datenweitergabe ggf. nicht einmal bewusst ist.

393 S. *Petri* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO Rn. 20 mit Fußnotenhinweis auf die EuGH-Entscheidung in *Wirtschaftsakademie Schleswig-Holstein*.

Es spricht daher vieles dafür, dass der EuGH eine Verantwortlichkeit von *Fashion ID* für eine Datenverarbeitung annahm, die zwar von *Fashion ID* mit ermöglicht, aber ausschließlich von einer anderen Person (*Facebook* Ireland) durchgeführt wurde.[394] Der Wortlaut des Art. 4 Nr. 7 DSGVO lässt dies durchaus zu. Diese Lesart lässt sich zudem gut mit den Ausführungen des EuGH im Urteil *Zeugen Jehovas* vereinbaren. Auch dort stellte der EuGH nicht auf eine eigene Datenverarbeitung durch die Religionsgemeinschaft der Zeugen Jehovas selbst ab. Er sah dennoch eine (gemeinsame) Verantwortlichkeit der Religionsgemeinschaft für die Datenverarbeitung durch einzelne Verkünder.

In *Zeugen Jehovas* stellte der EuGH zwar fest, dass die Datenverarbeitung der Verbreitung des Glaubens der Zeugen Jehovas diene.[395] In *Wirtschaftsakademie Schleswig-Holstein* bemerkte der EuGH, dass die Datenerhebung über das *Facebook*-Plugin durch den Website-Betreiber u. a. in dessen Interesse erfolge, später statistisch relevante Daten über seine Kunden zu erhalten.[396] In Fashion ID schließlich stellte der EuGH sinngemäß darauf ab, dass der Website-Betreiber in *Facebooks* Datenverarbeitung über den „Gefällt mir"-Button stillschweigend einwillige, damit im Gegenzug seine Produkte in dem sozialen Netzwerk sichtbarer würden.[397] Der EuGH hat bislang aber nicht ausdrücklich entschieden, ob ein (ggf. auch nur mittelbares) Eigeninteresse am infrage stehenden Datenverarbeitungsvorgang konstitutiv für die Annahme gemeinsamer Verantwortlichkeit ist. Dogmatisch gesehen lassen sich die vorgenannten Interessenserwägungen am ehesten im Rahmen des Merkmals des „gemeinsamen Entscheidens" über die Mittel und Zwecke der Datenverarbeitung fruchtbar machen. Ein Entscheiden in diesem Sinne setzt stets eine Einflussnahme voraus.[398] Dies wird noch deutlicher, wenn man andere Sprachfassungen der DSGVO

---

394 Vgl. hierzu auch Stellungnahme des Generalanwalts *Bot* v. vom 24.10.2017 in der Rs. C-210/16, EU:C:2017:796 – *Wirtschaftsakademie Schleswig-Holstein,* Rn. 54. Generalanwalt *Bot* geht hier davon aus, dass der Website-Betreiber selbst keine Datenverarbeitung durchführt, aber gleichwohl gemeinsam mit *Facebook* verantwortlich ist für *Facebooks* Datenverarbeitung.

395 EuGH, Urteil vom 10.07.2018, Az. C-25/17, EU:C:2018:551, Rn. 71 – *Zeugen Jehovas*.

396 EuGH, Urteil vom 05.06. 2018, Az. C-210/16, EU:C:2018:388, Rn. 34 – *Wirtschaftsakademie Schleswig-Holstein*.

397 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 80 – *Fashion ID*.

398 Generalanwalt *Bot* hat das Entscheiden über Mittel und Zwecke der Datenverarbeitung (in der französischen Fassung „détermine[r] les finalités et les moyens du traitement") als Ausübung rechtlichen oder tatsächlichen Einflusses auf Mittel und Zwecke der Datenverarbeitung definiert, S. Stellungnahme des Generalanwalts Yves Bot v. vom 24.10.2017 in der Rs. C-210/16, EU:C:2017:796, Rn. 54 – *Wirtschaftsakademie Schleswig-Holstein*.

betrachtet.[399] Der tatsächliche Einfluss auf die Datenverarbeitungs*mittel* lässt sich bei Plattform-Konstellationen in der Regel relativ einfach feststellen, da eine Datenverarbeitung oftmals nur durch das Zusammenwirken der Akteure technisch realisiert werden kann.[400] Wer hingegen Einfluss auf die Datenverarbeitungs*zwecke* nimmt, lässt sich schwerer nachweisen. Liegen jedoch die Zwecke der konkreten Datenverarbeitung im Interesse des jeweiligen Akteurs – auch des verarbeitungsferneren –, so lässt sich hieraus schließen, dass dieser auch Einfluss auf die Zwecke der Datenverarbeitung ausgeübt hat. Nach der Rechtsprechung des EuGH scheint es für eine solche Einflussnahme zu genügen, dass die verfolgten Zwecke zumindest mittelbar auch für den verarbeitungsfernen Akteur vorteilhaft sind und dieser in die Datenverarbeitung stillschweigend eingewilligt hat.[401] Im Hinblick auf den Wortlaut des Art. 2 lit. d) der Datenschutz-Richtlinie[402] (und die gleichlautende Regelung in Art. 4 Nr. 7 DSGVO) erscheint dieser Ansatz sehr weitgehend. Der EuGH hat jedoch keinen Zweifel daran gelassen, dass er eine weite Definition des Begriffs des „Verantwortlichen“ anstrebt, um einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten.[403] Ein solcher an der objektiven Interessenlage orientierter Ansatz vermeidet insbesondere, dass eine Verantwortlicheneigenschaft in den Fällen ausscheidet, in denen einer der Akteure die Verarbeitungszwecke bereits vorteilhaft für den anderen ausgestaltet, so dass dieser nicht aktiv werden muss, um seine Interessen einzubringen. Um einem Ausufern des Verantwortungsbegriffs zu begegnen, wird man indessen nicht jegliches mittelbare (i. d. Regel wirtschaftliche) Interesse an der Datenverarbeitung genügen lassen können. Andernfalls müsste man etwa eine Einflussnahme eines Auftragsverarbeiters auf die Datenverarbeitung bejahen, da diese letztlich die Grundlage für seine Entlohnung darstellt. Sachgerecht ist es daher

---

399 Die Formulierungen „determines“ (englisch) bzw. „détermine“ (französisch) oder „vaststellt“ (Niederländisch“ legen – eher als das deutsche „entscheiden über“ eine echte Einwirkung auf Mittel und Zweck nahe. In Art. 26 Abs. 1 spricht die DSGVO denn auch von einer gemeinsamen Festlegung von Mitteln und Zwecken.

400 Generalanwalt Bot stellt in *Wirtschaftsakademie Schleswig-Holstein* darauf ab, dass der Website-Betreiber die Datenverarbeitung durch Schließung seiner Fanpage beenden kann, S. Stellungnahme des Generalanwalts Yves Bot v. vom 24.10.2017 in der Rs. C-210/16, EU:C:2017:796, Rn. 56 – *Wirtschaftsakademie Schleswig-Holstein*. Er differenziert an dieser Stelle zwar nicht zwischen Mitteln und Zwecken. Die Möglichkeit der Schließung der Fanpage betrifft aber erkennbar die Einflussnahme auf das Mittel der Datenerhebung.

401 S. EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 80 – *Fashion ID*.

402 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG Nr. L 281 vom 23.11.1995, S. 31 (im Folgenden bezeichnet als „Datenschutz-Richtlinie“).

403 EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 66 – *Fashion ID*, unter Verweis auf die ergangene Rechtsprechung.

zu fragen, ob der betreffende Datenverarbeitungsvorgang zur Schaffung einer *Basis von Daten*[404] führt, an denen der jeweils andere Verantwortliche zumindest teilweise ein Eigeninteresse hat. Dieses Interesse kann auch darin liegen, dass die Schaffung einer solchen Basis *conditio sine qua non* ist für einen sich anschließenden Verarbeitungsschritt, der im Interesse des betreffenden Akteurs liegt, z. B. die Durchführung und Übermittlung einer Analyse bestimmter Daten, selbst wenn diese keinen Personenbezug mehr enthalten. Mit anderen Worten: Ist es für einen Akteur irrelevant, welche Daten in dieser Datenbasis enthalten sind, so kann auch nicht von einer Einflussnahme ausgegangen werden. Sähe man dies anders, dann wäre eine Person selbst dann als verantwortlich anzusehen, wenn ein anderer Akteur die Zwecke der Datenverarbeitung autonom vollständig ändern könnte, solange die über die Datenverarbeitungsmittel mitentscheidende Person weiterhin irgendeinen Vorteil aus der Datenverarbeitung erhielte (z. B. eine finanzielle Beteiligung an den Erträgen aus der Datenverwertung). Sowohl in Wirtschaftsakademie Schleswig-Holstein als auch in Fashion ID bestand jeweils bereits ein Interesse des Website-Betreibers an der durch die initiale Datenverarbeitung geschaffenen Datenbasis. Bei *Wirtschaftsakademie Schleswig-Holstein* diente diese Datenbasis dazu, dem Website-Betreiber nach seinen Vorgaben differenzierte Informationen über die Besucher seiner Website bereitzustellen. Bei *Fashion ID* war die Datenbasis jedenfalls notwendiges Zwischenziel für die erstrebte Werbung, denn die Erhebung bestimmter Nutzerdaten durch *Facebook* war notwendig, um dann im Newsfeed der Freunde eines Nutzers auf die von diesem gelikte Website hinweisen zu können.

Legt man einen solchen Maßstab zugrunde, dann fallen Konstellationen nicht unter die gemeinsame Verantwortlichkeit, in denen kein originäres Interesse an zumindest einem Teil der verarbeiteten Daten besteht. Erhielte demnach ein Website-Betreiber unabhängig von der konkreten Datenverarbeitung eine Entlohnung für das Einbinden eines personenbezogene Daten erhebenden Plugins, wäre der Website-Betreiber nicht als Verantwortlicher anzusehen. Auch wäre in einem Fall wie *Wirtschaftsakademie Schleswig-Holstein* eine gemeinsame Verantwortung abzulehnen, wenn der Fanpage-Betreiber keinerlei Auswertungsdaten zur Verfügung gestellt bekäme, sondern lediglich die Möglichkeit, mit einfachen Mitteln eine Fanpage zu erstellen. Dieser Ansatz führt ggf. zu aus Nutzersicht unbefriedigenden Ergebnissen. Da der Nutzer im Zweifelsfall nicht weiß, ob aus den erhobenen Daten ein datenspezifischer Vorteil für den Website-Betreiber erwächst, wäre für ihn nicht ohne Weiteres ersichtlich, ob eine gemeinsame Verantwortung vorliegt oder nicht. Dieses Resultat ist insbesondere der Tatsache geschuldet, dass die DSGVO in diesem Punkt nicht die Perspektive des Verbrauchers einnimmt. Zudem ist die Definition der gemeinsamen Verantwortung bereits rund 25 Jahre alt. Ungeachtet der enormen zwischenzeitlich

404 Ähnlich *Hanloser*, Keine gemeinsame Verantwortlichkeit für Datenspeicherung durch *Facebook* – Fashion ID – Anm. zu EuGH, Urteil vom 29.7.2019 – C-40/17, ZD 2019, 455, 459, der auf das Ergebnis des Datenverarbeitung abstellt.

eingetretenen technischen Entwicklungen – gerade in der Plattformökonomie – wurde diese Definition aus der Datenschutz-Richtlinie in die DSGVO übernommen. Die DSGVO selbst regelt auch keine Störerhaftung, die bei der Ermöglichung des Datenzugriffs durch Nichtverantwortliche Durchsetzungslücken füllen könnte.

(2) Gemeinsame Verantwortlichkeit bei Smart-TVs

Bezogen auf Smart-TVs oder vergleichbare IoT-Geräte ergeben sich hieraus etliche Fragen. Aufgrund der Vielzahl möglicher Konstellationen, in denen Plattformbetreiber und Dritte im Ökosystem Smart-TV aufeinandertreffen, wird man hier nur schwerlich allgemeingültige Aussagen treffen können. Ungeklärt scheint insbesondere, ob der Betreiber eines TV-Portals (oftmals, aber nicht immer der Fernseherhersteller) und Drittunternehmen, deren Apps über das TV-Portal abrufbar sind, als gemeinsam Verantwortliche angesehen werden können. Fest steht, dass Apps häufig personenbezogene Daten verarbeiten. Dies ist in besonderem Maße bei Apps der Fall, die Nutzerverhalten oder -präferenzen erfassen. Beispielsweise kann dies bei einer Video-Streaming-App dazu dienen, dass diese erkennt, welche Filme ein Nutzer gerne sieht, um diesem dann entsprechende Vorschläge für ähnliche Sendungen zu unterbreiten. Eine gemeinsame Entscheidung über die Mittel der Datenerhebung dürfte in diesen Konstellationen unproblematisch zu bejahen sein. TV-Portal-Betreiber und App-Anbieter sind sich darüber einig, dass der App-Anbieter seine App auf der zur Verfügung gestellten Plattform (TV-Portal) anbietet und so Nutzerdaten erhebt. Fraglich ist jedoch, ob darüber hinaus auch eine gemeinsame Entscheidung über die Zwecke der Nutzung vorliegt. In diesem Zusammenhang ist von Bedeutung, dass dem TV-Portal-Betreiber in vielen Fällen nicht einmal bekannt ist, welche Daten übermittelt und zu welchen Zwecken diese verarbeitet werden. Dies muss zwar nicht notwendig gegen die Annahme gemeinsamer Verantwortlichkeit sprechen. In der Entscheidung *Fashion ID* hat der EuGH es genügen lassen, dass dem Website-Betreiber bewusst war, dass *Facebook* die empfangenen Daten zu (nicht weiter spezifizierten) wirtschaftlichen Zwecken verwendet und er dies – im eigenen wirtschaftlichen Interesse – in Kauf genommen hatte. Nach den oben getroffenen Feststellungen muss jedoch ein spezifisches Interesse an den verarbeiteten Daten selbst bestehen, um eine Einflussnahme auf den Datenverarbeitungszweck und damit eine gemeinsame Verantwortlichkeit unterstellen zu können.

Aus Sicht eines TV-Portal-Betreibers gibt es grundsätzlich mehrere denkbare Vorteile aus der Aufnahme einer App in das Portal. So kann er vom App-Anbieter aus der Datenverarbeitung stammende statistische Daten, eine Art Listungsentgelt oder eine finanzielle Beteiligung aus dessen Werbemaßnahmen erhalten. Jedenfalls bei populären Apps könnte man darüber hinaus in der Erhöhung der Attraktivität des TV-Portals einen Vorteil sehen. Ein Interesse an den verarbeiteten Daten selbst (und nicht nur ein hieraus mittelbar abgeleiteter Vorteil) besteht jedoch nur bei der ersten Konstellation. Die Ermittlungen des Bundeskartellamts haben ergeben, dass nur in

wenigen Einzelfällen der TV-Portal-Betreiber Primär- oder Sekundärdaten aus der Datenverarbeitung durch den App-Anbieter erhält. Nur in diesen Fällen läge nach dem oben Gesagten eine gemeinsame Verantwortung vor. Gemeinsam Verantwortliche treffen für die betreffende Datenverarbeitung die Verpflichtungen aus der DSGVO. Sie sind mithin jeweils Adressat von Betroffenenrechten und müssen insbesondere die Hinweispflichten nach Art. 13 DSGVO erfüllen. Art. 26 Abs. 1 S. 2 DSGVO sieht verbindlich vor, dass die gemeinsam Verantwortlichen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung aus der DSGVO erfüllt. Dies gilt insbesondere für die Informationspflichten gegenüber den betroffenen Personen. Entsprechende Vereinbarungen wurden dem Bundeskartellamt im Rahmen der Ermittlungen nicht vorgelegt, sodass insoweit von einzelnen Verstößen gegen die DSGVO auszugehen ist.

Festzuhalten bleibt, dass neben dem App-Anbieter der TV-Portal-Betreiber mutmaßlich nur in wenigen Fällen (Erhalt von verarbeiteten oder hieraus abgeleiteten Daten vom App-Anbieter) als – gemeinsam – Verantwortlicher gelten kann. Es ist durchaus nicht auszuschließen, dass der EuGH in künftigen Fällen eine weitere Auslegung vertreten könnte.[405] Dies hätte zwar den unbestreitbaren Vorteil, dass nicht dem Verbraucher oftmals unbekannte Datenflüsse über die Verantwortlicheneigenschaft mitentscheiden würden. Andererseits würde ein solch weitgehender Ansatz die Trennlinie zum Auftragsverarbeiter verwischen. Zudem würden die Wortlautgrenzen des Art. 4 Nr. 7 DSGVO (bzw. des insoweit wortgleichen Art. 2 lit. d) der Datenschutz-Richtlinie) sehr stark aus- oder gar überdehnt.[406]

---

405 So sah etwa die Artikel-29-Datenschutzgruppe den Online-Inhalteanbieter, der Werbefenster für Dritte bereitstellt, ebenso wie den Datenempfänger als verantwortlich für die initiale Datenerhebung an. Der Online-Inhalteanbieter bestimme über den Zweck der Datenerhebung mit, nämlich die Datenverwendung zur Schaltung gezielter Onlinewerbung, S. Art.-29-Gruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioral *Targeting* (WP 171 vom 22.06.2010), S. 14, abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_de.pdf. Wie oben ausgeführt, begegnet diese Auffassung insoweit Bedenken, als der Online-Inhalteanbieter selbst nicht an den Daten interessiert ist, sondern an der Zahlung einer „Miete“ für bereitgestellte Werbefenster. Ob und welche Daten der Datenempfänger erhält, ist für den Online-Inhalteanbieter nicht unmittelbar relevant.

406 Es gibt durchaus Präzedenzfälle, in denen der EuGH im Hinblick auf das Schutzgut eine extrem weite, über den Wortlaut hinausgehende Auslegung der betreffenden Norm vorgenommen hat, so etwa die Qualifizierung des Verkaufs eines Medienabspielgeräts als „öffentliche Wiedergabe“ im Sinne von Art. 3 Abs. 1 der Urheberrechtsrichtlinie (Richtlinie 2001/29/EG), S. EuGH, Urteil vom 26.04.2017, Az. C-527/15, EU:C:2017:300, Rn. 23 ff. – *Stichting Brein/Jack Frederik Wullems*. Der EuGH hatte eine öffentliche Wiedergabe zudem für das bloße Setzen von Hyperlinks bejaht, wenn dies mit Gewinnerzielungsabsicht geschieht und mit Kenntnis (oder Kennenmüssen) der Rechtswidrigkeit der Veröffentlichung der Werke auf der verlinkten Zielseite, s. EuGH, Urteil des Gerichtshofs vom 08.09.2016, Az. C-160/15, EU:C:2016:644 – *GS Media BV/Sanoma Media Netherlands BV u. a.*

(3) Auftragsverarbeitung

Vom „Verantwortlichen“ abzugrenzen ist der bloße „Auftragsverarbeiter“. Bei diesem handelt es sich gem. Art. 4 Nr. 8 DSGVO um „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Der „Auftragsverarbeiter“ wird also bei der Verarbeitung personenbezogener Daten lediglich als verlängerter Arm des Verantwortlichen[407] tätig – ohne eigene Entscheidungskompetenz hinsichtlich der Zwecke[408]. Gekennzeichnet wird der Auftragnehmer durch seine Weisungsgebundenheit (vgl. Art. 29 DSGVO). Nur wenn ein Auftragsverarbeiter die weisungsgebundene Funktion unerlaubt verlässt und über Zwecke und Mittel der Verarbeitung selbst bestimmt, tritt er in die Rolle eines (rechtswidrig handelnden) Verantwortlichen ein (Art. 28 Abs. 10 DSGVO).[409] Im Falle eines durch die Datenverarbeitung entstandenen Schadens haften Verantwortlicher und Auftragsverarbeiter gegenüber dem Geschädigten als Gesamtschuldner (Art. 82 Abs. 4 DSGVO), wobei sich der Auftragsverarbeiter exkulpieren kann, wenn er nachweist, dass er entsprechend den Vorgaben der DSGVO und des Verantwortlichen gehandelt hat (Art. 82 Abs. 3 i. V. m. Abs. 2 S. 2 DSGVO). Im Rahmen der Sektoruntersuchung waren bzgl. der Abgrenzung von Verantwortlichem und Auftragsverarbeiter keine Probleme zu beobachten.

bb) Zivilrechtliche Haftung des TV-Portal-Betreibers

Nach hier vertretener Auffassung sind die meisten App-Anbieter für die von ihnen veranlassten Datenverarbeitungen datenschutzrechtlich allein verantwortlich. Gleichwohl stellt sich die Frage nach einer Haftung des TV-Portal-Betreibers bei einer rechtswidrigen Verarbeitung der Daten durch den – nach DSGVO verantwortlichen – App-Anbieter.

In Betracht kommen unter Umständen zivilrechtliche Ansprüche des Nutzers gegen den TV-Portal-Betreiber. Wenn der Portal-Betreiber Apps auf dem Gerät vorinstalliert, die erkennbar die Gefahr von Datenschutzverletzungen auf Seiten der Nutzer begründen, könnte dies deliktische An-

---

407 Vgl. *Ernst* in: Paal/Pauly [Hrsg.], 2. Aufl. 2018, DSGVO Art. 4 DSGVO Rn. 56, wo zur Veranschaulichung der Begriff „‘Marionette‘ des Verantwortlichen“ verwendet wird.

408 Im Bereich der eingesetzten Mittel kann dem Auftragsverarbeiter hingegen eine gewisse Entscheidungsfreiheit zukommen, S. *Hartung* in: Kühling/Buchner/Bäcker [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 4 DSGVO Nr. 8, Rn. 7.

409 Vgl. *Gola* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 4 Rn. 75 m. w. N.

sprüche oder quasinegatorische Beseitigungs- und Unterlassungsansprüche aus dem allgemeinen Persönlichkeitsrecht begründen.[410] Denn dieses umfasst das Recht auf informationelle Selbstbestimmung, das eine konkrete Ausprägung im Recht auf Schutz personenbezogener Daten findet.

Soweit Verletzungshandlungen des App-Anbieters vorliegen, ist zunächst an eine Haftung des Portals als Teilnehmer (Anstifter oder Gehilfe, § 830 Abs. 2 BGB) zu denken. Als Gehilfe haftet, wer zumindest bedingt vorsätzlich die Rechtsverletzung eines anderen fördert, wobei zum erforderlichen Vorsatz nicht nur die Kenntnis der objektiven Tatbestandsmerkmale, sondern auch das Bewusstsein der Rechtswidrigkeit der Haupttat gehört.[411] Dies kann etwa vorliegen, wenn ein Portalbetreiber trotz deutlicher Hinweise auf Datenschutzverstöße von Apps oder anderer Software diese vorinstalliert. Regelmäßig wird sich ein entsprechender Vorsatz aber nicht nachweisen lassen. Ist der Portalbetreiber danach nicht selbst Täter oder Teilnehmer, so kann er aber unter Umständen als Störer auf Unterlassung in Anspruch genommen werden, wenn es in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt.[412] Der EuGH hat erkennen lassen, dass er einer zivilrechtlichen Störerhaftung außerhalb des

---

410 Soweit vertragliche Beziehungen des Nutzers zum Portal-Betreiber bestehen, ist auch an eine mögliche Verletzung vertraglicher Schutzpflichten (§ 241 Abs. 2 BGB) zu denken. Diese betreffen die Integrität absolut geschützter Rechte und Rechtsgüter, die im Rahmen des Zumutbaren vor Schäden zu bewahren sind. Hieraus kann z. B. die Pflicht folgen, vor Gefahren, die vom Vertragsgegenstand ausgehen, zu warnen. Weitergehende Prüf- und Unterlassungspflichten sind insbesondere dort vorstellbar, wo die freie Entscheidung des Vertragspartners zur Nutzung der App eingeschränkt wird, etwa weil diese ohne weitere Handlung seinerseits Aktivitäten entfaltet oder nicht ohne Weiteres deinstallierbar ist. Regelmäßig wird in den AGB der Portal-Betreiber allerdings jede Haftung für die Apps Dritter ausgeschlossen. Es stellt sich dann die Frage, ob eine solche Freizeichnung auch wirksam möglich ist, wenn das Portal nicht nur den Zugang zur App eröffnet, sondern diese bereits auf dem Gerät vorinstalliert hat (insb. wenn eine Deinstallation nicht möglich ist). Hierin könnte eine unangemessene Benachteiligung des Vertragspartners liegen (§ 307 Abs. 1 BGB). Bedenklich erscheint der Haftungsausschluss unter dem Gesichtspunkt der Risikobeherrschung (soweit der Verbraucher keine Möglichkeit hat, die Verwirklichung des Risikos zu verhindern), angesichts der tatsächlich vorhandenen aktiven Rolle des Portals (wenn dieses nicht nur den Zugang eröffnet, sondern die App bereits vorinstalliert) sowie im Hinblick auf die Gewährleistung absolut geschützter Rechtsgüter (allgemeines Persönlichkeitsrecht).

411 Vgl. z. B. BGH, Urteil vom 11.03.2004, Az. I ZR 304/01, BGHZ 158, 236, Rn. 45 – *Internet-Versteigerung I*.

412 Vgl. hierzu etwa BGH, Urteil vom 27.02.2018, Az. VI ZR 489/16, BGHZ 217, 350, Rn. 31– *Internetforum*.

DSGVO-Regimes nicht abgeneigt ist.[413] Auch das OLG Düsseldorf hätte im Fall *Fashion ID* die betreffende Frage dem EuGH nicht vorgelegt, hätte es eine Störerhaftung von vornherein für ausgeschlossen gehalten.[414] In der Literatur finden sich ebenfalls befürwortende Stimmen.[415] Soweit der abschließende Charakter der DSGVO betont wird, die über ein umfassendes Rechtsbehelfs- und Sanktionsmodell verfüge[416], geschieht dies zumeist im Hinblick auf die Möglichkeit einer lauterkeitsrechtlichen Haftung neben der DSGVO. Bei den hier einschlägigen Fallgestaltungen haftet der Störer jedoch nicht nach den Vorschriften der DSGVO, so dass Datenschutzbehörden oder Private nicht auf dieser Basis gegen ihn vorgehen könnten. Jedenfalls in dieser Konstellation verfängt der Hinweis auf das Rechtsbehelfs- und Sanktionenmodell der DSGVO nicht. So sieht DSGVO-Erwägungsgrund 146 S. 4 auch vor, dass eine Schadensersatzhaftung gegen Verantwortliche oder Auftragsverarbeiter auch außerhalb des DSGVO-Regimes möglich ist.

Die von der Rechtsprechung bislang entwickelten Grundsätze zur Störerhaftung verlangen indessen positive Kenntnis einer Rechtsverletzung; in Unkenntnis einer Rechtsverletzung kommt eine Störerhaftung grundsätzlich nur in Betracht, wenn eine Pflicht zur Prüfung von Rechtsverletzungen Dritter missachtet wurde. Eine solche Prüfpflicht wird aber im Regelfall nur nach einem vorhergehenden qualifizierten Hinweis angenommen.[417] Der Nachweis der Kenntnis einer Datenschutzverletzung oder auch nur das Erteilen eines qualifizierten Hinweises dürfte zumindest für

---

413 S. dazu EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 74 – *Fashion ID*: „[…] Dagegen kann, **unbeschadet einer etwaigen insoweit im nationalen Recht vorgesehenen zivilrechtlichen Haftung**, diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als im Sinne dieser Vorschrift verantwortlich angesehen werden." (Hervorhebung hinzugefügt). Das vorlegende OLG Düsseldorf hatte die Störerhaftung in seiner dritten (vom EuGH nicht beantworteten) Vorlagefrage thematisiert. Es kann daher davon ausgegangen werden, dass der EuGH die Störerhaftung bei Abfassung des Urteils vor Augen hatte.

414 S. Vorlagefrage 3, EuGH, Urteil vom 29.07.2019, Az. C-40/17, EU:C:2019:629, Rn. 42 – *Fashion ID*. Hätte das OLG Düsseldorf eine Störerhaftung von vornherein ausgeschlossen, hätte es die Frage mangels Entscheidungserheblichkeit nicht vorgelegt.

415 *Mantz*, Störerhaftung für Datenschutzverstöße Dritter -Sperre durch DS-RL und DSGVO?, ZD 2014, 62, 66; *Schantz* in Schantz/Wolff [Hrsg.], Das neue Datenschutzrecht, 2017, Rn. 363; *Wolff*, UWG und DSGVO: Zwei separate Kreise?, ZD 2018, 248; *Specht-Riemenschneider*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73.

416 S. etwa *Köhler* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 3a Rn. 1.40a f.; den insoweit abschließenden Charakter der DSGVO hingegen verneinend OLG Stuttgart, Urteil vom 27.02.2020, Az. 2 U 257/19, Rn. 41 ff. m. w. N.

417 S. etwa BGH, Urteil vom 31.03.2016, Az. VI ZR 34/15, BGHZ 209, 139, Rn. 23.

private Kläger nur schwer zu bewerkstelligen sein.[418] Dort, wo das Portal über die Eröffnung des Zugangs hinaus durch die Vorinstallation eine Gefahrenquelle eröffnet und so einen aktiven Beitrag zur möglichen Verletzung des Rechts auf informationelle Selbstbestimmung leistet, erscheint – jedenfalls, wenn der Portalbetreiber durch finanzielle Beteiligung o. Ä. profitiert – eine weitergehende eigenständige Prüfpflicht jedoch angemessen.[419] Es bleibt abzuwarten, inwieweit dieser Ansatz von der Rechtsprechung aufgegriffen werden wird.

cc) Lauterkeitsrechtliche Verantwortlichkeit des TV-Portal-Betreibers

Verstößt der App-Anbieter gegen datenschutzrechtliche Bestimmungen (beispielsweise Informationspflichtverstöße oder Erhebung personenbezogener Daten ohne Rechtsgrundlage), so könnte darin zugleich eine unlautere Handlung nach § 3a UWG liegen. Voraussetzung hierfür wäre zunächst, dass man die verletzten Vorschriften der DSGVO als Marktverhaltensregelungen im Sinne des § 3a UWG einstuft[420] und der Verstoß geeignet ist, die Interessen von Verbrauchern spürbar zu beeinträchtigen.

Aus einer solchen lauterkeitsrechtlichen Zuwiderhandlung des App-Anbieters könnte auch eine Verantwortlichkeit des Portal-Betreibers folgen. Grundsätzlich kommt eine Verantwortlichkeit des Vermittlers nach der Rechtsprechung unter dem Aspekt der Verletzung einer wettbewerbsrechtlichen Verkehrspflicht in Betracht. Wer durch sein Handeln im geschäftlichen Verkehr die Gefahr schafft, dass Dritte durch das Wettbewerbsrecht geschützte Interessen von Marktteilnehmern

---

418 Vgl. hierzu auch *Mantz*, Störerhaftung für Datenschutzverstöße Dritter – Sperre durch DS-RL und DSGVO?, ZD 2014, 62, 66. Die nunmehr in Kraft befindliche DSGVO sieht Auskunftsmöglichkeiten und Informationspflichten vor, so dass im Einzelfall die Feststellung eines offenkundigen Rechtsverstoßes erleichtert werden könnte. Voraussetzung wäre jedenfalls, dass der Verantwortliche diesen Pflichten auch umfassend nachkommt.

419 Specht-Riemenschneider befürwortet in diesem Zusammenhang etwa eine Pflicht des Herstellers zur datenschutzkonformen Ausgestaltung von Produkten, *Specht-Riemenschneider*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73, 75.

420 Dies ist umstritten und von der Rechtsprechung bisher nicht abschließend geklärt, bejahend für diverse Informationspflichten des Art. 13 DSGVO OLG Stuttgart, Urteil vom 27.02.2020, Az. 2 U 257/19, juris Rn. 77 ff., allgemein bejahend für DSGVO-Vorschriften zur Nutzung von Daten zu Werbezwecken sowie speziell für Art. 9 DSGVO OLG Naumburg, Urteil vom 7.11.2019, Az. 9 U 39/18, juris Rn. 52 ff., ablehnend etwa *Köhler* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 3a Rn. 1.74b. Mitunter wird auch das Vorliegen einer Marktverhaltensregel nicht grundsätzlich abgelehnt, jedoch eine Sperrwirkung des Rechtsbehelfs- und Sanktionenregimes der DSGVO angenommen, s. dazu Fn. 416. Die Frage einer möglichen abschließenden Natur des Durchsetzungsregimes der DSGVO hat der BGH dem EuGH zur Vorabentscheidung vorgelegt, vgl. BGH, Beschluss vom 28.05.2020, Az. I ZR 186/17, noch nicht veröffentlicht, dazu Pressemitteilung des BGH Nr. 66/2020 vom 28.05.2020.

verletzen, ist wettbewerbsrechtlich dazu verpflichtet, diese Gefahr im Rahmen des Möglichen und Zumutbaren zu begrenzen.[421] Diese wettbewerbsrechtliche Verkehrspflicht konkretisiert sich bei Intermediären, die den Zugang zu Angeboten Dritter vermitteln, als Prüfungspflicht, deren Bestehen und Umfang sich im Einzelfall nach einer Abwägung aller betroffenen Interessen und relevanten rechtlichen Wertungen richtet. Entscheidend kommt es darauf an, ob und inwieweit dem in Anspruch Genommenen eine Prüfung zuzumuten ist.[422]

Hier sprechen einige materielle Gesichtspunkte für eine Prüfpflicht in Bezug auf vorinstallierte Apps. Denn mit der Vorinstallation geht das Portal über das bloße Bereitstellen einer Infrastruktur hinaus und nimmt eine aktive Rolle ein.[423] Durch die Beteiligung an den Erlösen über Listungsentgelte oder Revenue Sharing Agreements hat es ein eigenes finanzielles Interesse an der Nutzung der Apps durch die Endkunden. Die Vorinstallation bestimmter Apps kann zudem als Marketingargument für den Verkauf des Produkts genutzt werden. Auf der anderen Seite ist mit dem Recht auf informationelle Selbstbestimmung ein gewichtiges Rechtsgut gefährdet. Verletzungen der Datenschutzregeln durch App-Anbieter sind naheliegend und für das Portal regelmäßig leichter zu erkennen und abzustellen als für den einzelnen Verbraucher. Aufwand und Kosten halten sich angesichts der begrenzten Zahl vorinstallierter Apps in Grenzen. Hinzu kommt, dass die Möglichkeiten des Verbrauchers, sich selbst zu schützen unter Umständen eingeschränkt sind, etwa wenn eine Deinstallation oder effektive Deaktivierung der Apps nicht möglich ist.

Entscheidend ist jedoch, dass die wettbewerbsrechtliche Verkehrspflicht im Hinblick auf den Kreis der Verpflichteten nicht weiter reichen kann als die datenschutzrechtliche Verantwortlichkeit. Die Rechtsprechung verlangt, dass dort, wo die Marktverhaltensregelung eine besondere Normad-

---

421 BGH, Urteil vom 12.07.2007, Az. I ZR 18/04, BGHZ 173, 188, Rn. 35 – *Jugendgefährdende Medien bei eBay*.

422 Ebenda, Rn. 38.

423 Bereits deshalb stehen auch die Wertungen der § 7 Abs. 2, §§ 8 bis 10 des Telemediengesetzes v. 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Art. 11 des Gesetzes v. 11.07.2019 (BGBl. I S. 1066) - TMG, einer Prüfpflicht nicht grundsätzlich entgegen. Dort ist eine Privilegierung für reine Access- oder Host-Provider vorgesehen, die auf der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Abl. EG Nr. L 178 v. 17.07.2000, S. 1 (kurz E-Commerce-Richtlinie), beruht. Im Rahmen der „Digital Services Act"-Initiative werden diese europaweiten Regeln zur beschränkten Verantwortlichkeit der Anbieter digitaler Dienste derzeit einer Evaluierung im Hinblick auf eine mögliche Überarbeitung unterzogen, vgl. die „Roadmap" der Europäischen Kommission unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

ressatenstellung voraussetzt, diese auch beim Vermittler vorliegen muss, um seine täterschaftliche Haftung begründen zu können.[424] Der TV-Portal-Betreiber ist hier aber gerade nicht als Verantwortlicher selbst Adressat der besonderen Datenschutzregeln der DSGVO (siehe dazu unter aa), S. 155). Für denjenigen, der nicht selbst Adressat der Verbotsnorm ist, kommt nach der Rechtsprechung lediglich eine Haftung als Teilnehmer (Anstifter oder Gehilfe) in Betracht. Wie bereits dargestellt, setzt eine Haftung als Gehilfe voraus, dass das der Portalbetreiber zumindest bedingt vorsätzlich den Wettbewerbsverstoß eines anderen fördert, wobei zum erforderlichen Vorsatz nicht nur die Kenntnis der objektiven Tatbestandsmerkmale, sondern auch das Bewusstsein der Rechtswidrigkeit der Haupttat gehört. Jedenfalls soweit unstreitige Datenschutzverstöße von Anbietern vorinstallierter Apps nicht öffentlich bekannt sind, dürfte somit nach aktueller Rechtsprechung eine Gehilfenhaftung ausscheiden.

Zusammenfassung

Hersteller von Smart-TVs und Diensteanbieter können eine Verarbeitung personenbezogener Nutzerdaten im Wesentlichen auf Basis dreier Rechtsgrundlagen rechtfertigen: die Erforderlichkeit für den mit dem Nutzer abgeschlossenen Vertrag, das Vorliegen berechtigter Interessen oder die Einwilligung des Nutzers. Von diesen Rechtsgrundlagen machen die befragten Unternehmen in unterschiedlichem Ausmaß Gebrauch. Soweit für Datenverarbeitungen berechtigte Interessen angeführt werden, bestehen erhebliche Zweifel. Eine Auseinandersetzung mit den Interessen der von der Datenverarbeitung betroffenen Personen findet nicht erkennbar statt. Darüber hinaus wird als ein berechtigtes Interesse zumeist die Verbesserung des eigenen Produkts bzw. der eigenen Dienstleistung ins Feld geführt. Dabei wird jedoch insbesondere nicht erkennbar, weshalb diese nicht im Wesentlichen ebenso gut mit anonymisierten Daten erreicht werden kann oder welche der verarbeiteten Daten für diese Verbesserung überhaupt herangezogen werden.

Eine Verarbeitung personenbezogener Daten zu Werbezwecken wird in der Regel nicht als berechtigtes Interesse deklariert, sondern von der Einwilligung des Nutzers abhängig gemacht. Dies ist insofern sinnvoll, als eine Abwägung der berührten Interessen jedenfalls bei bezahlten Produkten im Regelfall zuungunsten des datenverarbeitenden Unternehmens ausgehen würde. Das Einholen einer Einwilligung stellt in solchen Fällen zudem unter Transparenzgesichtspunkten die deutlich vorzugswürdige Variante dar.

[424] OLG Düsseldorf, Urteil vom 27.03.2019, Az. I-15 U 18/18, juris Rn. 26; BGH, Urteil vom 12.03.2015, Az. I ZR 84/14, GRUR 2015, 1025 – *TV-Wartezimmer* (betr. berufsrechtliche Regelung für Apotheker); BGH, Urteil vom 3.07.2008, Az. I ZR 145/05, BGHZ 177, 150, Rn. 13 f. – *Kommunalversicherer* (betr. Eigenschaft als öffentlicher Auftraggeber).

Eine wirksame Einwilligung scheitert dabei zumeist nicht am Vorliegen einer Drucksituation. Hingegen fehlt es den Einwilligungsersuchen praktisch durchgängig an einer Darstellung aller wesentlichen Angaben, die der Nutzer für eine informierte Einwilligung benötigen würde.

Nutzermenüs sind häufig nicht neutral ausgestaltet, sondern lenken den Nutzer in Richtung bestimmter Auswahlentscheidungen, die mit einer umfangreicheren Verarbeitung personenbezogener Daten einhergehen. Die Zulässigkeit eines solchen Vorgehens lässt sich zwar grundsätzlich durchaus nach geltendem Recht, insbesondere dem Datenschutz- und Lauterkeitsrecht, beurteilen. Einschlägige Behörden- oder Gerichtsentscheidungen, die als Orientierungspunkte dienen könnten, sind jedoch bislang Mangelware.

In Einzelfällen, in denen eine gemeinsame Verantwortlichkeit i. S. d. Datenschutzrechts vorliegt, verstoßen TV-Portal-Betreiber und App-Anbieter gegen Art. 26 Abs. 1 S. 2 und 3 sowie Abs. 2 DSGVO, da sie keinerlei Regelungen zur gemeinsamen Verantwortlichkeit getroffen haben. Hinzu kommen ggf. Verstöße gegen Informations- und Transparenzpflichten (insb. aus Art. 13 DSGVO), da für etwaige Versäumnisse beide Verantwortliche gleichermaßen einstehen müssen.

Nach hier vertretener Auffassung besteht aber im Regelfall keine datenschutzrechtliche Verantwortung des TV-Portal-Betreibers. Eine weiter gehende Auslegung des Verantwortlichenbegriffs durch den EuGH in der Zukunft erscheint indessen nicht ausgeschlossen.

Die Tatsache, dass womöglich ein Akteur – ohne selbst Verantwortlicher zu sein – einen DSGVO-widrigen Zugriff auf personenbezogene Nutzerdaten ermöglicht, kann zwar nach den Grundsätzen der Störerhaftung betrachtet werden. Vermutlich wird es jedoch noch eine geraume Zeit dauern, bis sich zu dieser Problematik eine gefestigte Rechtsprechung herausgebildet haben wird. Eine behördliche Durchsetzung in diesem Bereich dürfte jedenfalls mangels einschlägiger Eingriffsbefugnisse grundsätzlich nicht möglich sein.

VI. Binnenorganisation in Datenschutzfragen

Die DSGVO ordnet in Art. 5 Abs. 2 i. V. m. Art. 24 Abs. 1 eine Rechenschafts- sowie Nachweispflicht an[425], die Behörden die Aufsicht ermöglicht bzw. erleichtert. Dies erfordert ein nachhaltiges internes Datenschutzmanagementsystem des Verantwortlichen.[426] Für dessen Implementierung

---

425 Vgl. *Datenschutzkonferenz (DSK)*, Kurzpapier Nr.1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO, S.1 f., abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf.

426 *Frenzel* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 5 DSGVO Rn. 50 ff.

sieht die DSGVO eine Reihe von Maßnahmen vor, von denen die für den Bereich der Smart-TVs wichtigsten nachfolgend behandelt werden.

1. Verzeichnis von Verarbeitungstätigkeiten

Die zentrale Dokumentationspflicht ist das Führen eines Verzeichnisses von Datenverarbeitungstätigkeiten nach Art. 30 DSGVO. Wie DSGVO-Erwägungsgrund 82 zu entnehmen ist, soll es die zentrale Dokumentation zum Nachweis der Einhaltung der DS-GVO und Grundlage für Kontrollen der Aufsichtsbehörden bilden.[427] Art. 30 DSGVO verpflichtet den Verantwortlichen zu einer *generellen Dokumentation*[428] aller vorgenommenen personenbezogenen Datenverarbeitungsvorgänge. Dieser Pflicht müssen grundsätzlich alle Unternehmen nachkommen, sofern sie als datenschutzrechtlich Verantwortliche handeln (s. dazu E. V. 2., S. 142 ff.). Sie trifft dabei eine Aktualisierungsobliegenheit[429]. Die Aufsichtsbehörden erhalten ihrerseits die Befugnis zur Einsichtnahme (Art. 31 DSGVO i. V. m. Erwägungsgrund 82 S. 2).

Art. 30 Abs. 1 S.2 DSGVO stellt umfangreiche Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten. Damit werden zu wesentlichen Teilen die gleichen Informationen in das interne Verzeichnis eingetragen, wie sie in Datenschutzbestimmungen gegenüber Verbrauchern oder bei einer Anfrage eines Betroffenen nach Art. 15 DSGVO angegeben werden sollen. Die tatsächlichen Auskunftsansprüche Betroffener können jedoch weit über die Angaben im Verzeichnis der Verarbeitungstätigkeiten hinausgehen.[430]

a) Ermittlungsergebnisse

Von den untersuchten 21 Smart-TV-Anbietern hatten 9 Datenverarbeitungsverzeichnisse angelegt. Diese unterschieden sich deutlich in Umfang und Detailtiefe. Als Grund für den Verzicht auf ein Datenverarbeitungsverzeichnis gaben die Unternehmen zumeist an, keine personenbezogenen Daten zu speichern. Dies ist auch glaubhaft. Zum einen Teil handelte es sich hierbei um

---

427 *Haag* in: Forgó/Helfrich/Schneider [Hrsg.], Betrieblicher Datenschutz, 3. Aufl. 2019, Art. 30 DSGVO Rn. 17 f.

428 *Ingold* in Sydow [Hrsg.], Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 30 Rn. 4.

429 Vgl. *Spoerr* in: BeckOK DatenschutzR, 32. Ed., 01.05.2020, DSGVO, Art. 30 Rn. 10a.

430 Vgl. OLG Köln, Urteil vom 26.07.2019, Az. I-20 U 75/18, juris Rn. 304. Das OLG Köln verwies der Entscheidung[430], in der es das Auskunftsrecht der betroffenen Person sehr weit auslegte, auf das Volkszählungsurteil des Bundesverfassungsgerichts. Letzteres hatte befunden, dass es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr gebe (BVerfG, Urteil vom 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1, Rn. 152).

Hersteller, die bereits vorgefertigte Fernseher beziehen, um diese dann unter ihrem Markennamen zu vertreiben. Falls es bei den betreffenden Smart-TVs zu Datentransfers kommt, ist in der Regel der OEM-Hersteller Datenempfänger. Zum anderen Teil waren Fernsehgeräte betroffen, deren Smartfunktionen im Wesentlichen über ein webgestütztes TV-Portal gewährleistet werden. Bei solchen Geräten ist Datenempfänger der Betreiber des TV-Portals.

Verantwortlicher und Datenschutzbeauftragter des jeweiligen Unternehmens ließen sich den Verzeichnissen in der Regel entnehmen, jedoch in etwa der Hälfte der Fälle nicht mit konkreten Kontaktdaten. Die Zwecke der Verarbeitung, die die betreffende Datenverarbeitung legitimieren sollen, wurden durchgehend genannt. Dabei traten jedoch teilweise Unschärfen, die bereits im Rahmen der Datenschutzbestimmungen erörtert wurden (pauschale Zweckangaben, mangelhafte Erkennbarkeit der für den jeweiligen Zweck benötigten personenbezogenen Daten; s. dazu E. II. 4. c), S. 74). Die Kategorien Betroffener waren durchweg eingetragen; es handelte sich stets um Endverbraucher. Auch die Kategorien von Datenempfängern wurden in den übersandten Verzeichnissen angegeben. In der Regel handelte es sich hierbei um Konzerngesellschaften in den USA und Asien.

In allen Verzeichnissen fanden sich mitunter nach Datumstyp differenzierte vorgesehene feste Löschfristen. Ergänzend wurde jedoch oftmals ausgeführt, die Daten würden solange wie benötigt gespeichert, so dass insoweit doch keine konkrete Löschfrist bestand. Das gesetzliche Petitum, technisch-organisatorische Maßnahmen zum Datenschutz anzugeben (Art. 30 Abs. 1 lit. g) DSGVO), wurde überwiegend befolgt.

b) Rechtliche Würdigung

Soweit Fernseherhersteller keine Daten aus dem Betrieb des Smart-TVs erhalten, ist auch das Führen eines Verzeichnisses von Verarbeitungstätigkeiten nicht erforderlich. Art. 30 Abs. 1 DSGVO gilt ausdrücklich nur für datenschutzrechtlich Verantwortliche. Wer keine personenbezogenen Daten verarbeitet und keine diesbezüglichen Entscheidungen trifft, gilt nicht als Verantwortlicher i. S. v. Art. 7 Abs. 1 DSGVO. Daran ändert nach hier vertretener Ansicht[431] auch die Tatsache nichts, dass die TV-Hersteller die Datenverarbeitung Dritter erst ermöglichen, indem sie ihnen das Fernsehgerät als Plattform zur Verfügung stellen.

Soweit die Hersteller von Smart-TVs selbst Daten verarbeiten, müssen sie ein Verzeichnis von Verarbeitungstätigkeiten nach den Vorgaben von Art. 30 Abs. 1 DSGVO führen. Es muss gem. Art. 30 Abs. 1 S.2 DSGVO jedenfalls folgende Angaben beinhalten:

---

431 S. dazu S. 156 ff.

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

sowie „falls möglich“

- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Absatz 1 DSGVO.

Lediglich Unternehmen und Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sind gem. Art. 30 Abs. 5 DSGVO grundsätzlich von dieser Pflicht ausgenommen. Bei den im Rahmen der Sektoruntersuchung befragten Unternehmen lag die konzernweite Beschäftigtenzahl jedoch fast immer über dieser Grenze.

Die untersuchten Datenverarbeitungsverzeichnisse hielten die o. g. Anforderungen der DSGVO im Wesentlichen ein. Bei der bei der Angabe von Verwendungszwecken besteht mitunter noch Konkretisierungsbedarf. Zudem gab es Versäumnisse bei der Nennung erforderlicher Kontaktdaten. Die Angabe von Löschfristen mit Erforderlichkeitsvorbehalt mag unbefriedigend erscheinen. Die Formulierung der DSGVO („falls möglich“) lässt hier jedoch Spielraum für Fälle, in denen eine Frist aufgrund besonderer Umstände nicht fixiert werden kann.[432] Zudem geht es im Rahmen von Art. 30 DSGVO in erster Linie um die Prinzipien Transparenz und Rechenschaftspflicht.[433] Die

---

[432] So ist etwa denkbar, dass bestimmte Kundendaten während der Nutzung eines bestimmten Services gespeichert werden müssen. Das verantwortliche Unternehmen wäre in diesem Fall nur in der Lage, eine exakte Speicherdauer nach Beendigung der Inanspruchnahme des Services durch den Nutzer anzugeben.

[433] S. *Petri* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 30 DSGVO Rn. 1.

Einhaltung der Dokumentationsvorschriften des Art. 30 DSGVO sagt mithin nichts aus über die materiellrechtliche Zulässigkeit der jeweiligen Datenverarbeitung selbst.[434]

2. Datenschutz-Folgenabschätzung

Mit einer sog. Datenschutz-Folgenabschätzung wird die Verarbeitung personenbezogener Daten beschrieben und ihre Notwendigkeit und Verhältnismäßigkeit bewertet. Zudem sollen die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung mit sich bringt, durch eine entsprechende Risikoabschätzung und die Ermittlung von Gegenmaßnahmen besser kontrolliert werden.[435] Die Datenschutz-Folgenabschätzung dient als Frühwarnsystem für spätere Datenschutzverletzungen. Sie soll dem Verantwortlichen das Gefahrenpotential der Datenverarbeitung vor Augen führen.

a) Ermittlungsergebnisse

Drei der 21 überprüften Smart-TV-Hersteller hatten eine Datenschutz-Folgenabschätzung vorgenommen, darunter war ein Unternehmen, welches Nutzerprofile verarbeitet. Ein weiteres Nutzerprofile verarbeitendes Unternehmen hatte keine Datenschutz-Folgenabschätzung vorgenommen.

Die entsprechenden Dokumente enthielten Angaben zu Verarbeitungsvorgängen und deren Zwecke, Verhältnismäßigkeitserwägungen, Risikobewertungen im Hinblick auf die betroffenen Personen sowie Erwägungen hinsichtlich möglicher Gefahren und deren Eintrittswahrscheinlichkeit sowie möglicher Gefährdungsverringerungsmaßnahmen.

b) Rechtliche Würdigung

aa) Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung

Wie oben dargestellt, verarbeiten 12 TV-Hersteller nach eigenen Angaben überhaupt keine personenbezogenen Daten. Für diese erübrigt sich somit bereits mangels Verantwortlicheneigenschaft die Erstellung einer Datenschutz-Folgenabschätzung.

---

434 Zur Angabe von Speicherdauern s. auch unten E. V. 4. i), S. 85.

435 *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248 rev. 01. vom 04.10.2017), abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Ansonsten definiert Art. 35 Abs. 3 DSGVO drei Szenarien, bei denen stets eine Folgenabschätzung vorzunehmen ist. Für den Bereich der Smart-TVs ist hiervon allenfalls lit. a) einschlägig, nämlich die „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, […] die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen". Das Unternehmen, das trotz Profilings keine Datenschutz-Folgenabschätzung vorgenommen hat, erhebt zwar Nutzungsmuster und verarbeitet damit sensible Daten. Eine Rechtswirkung lässt sich indessen nicht feststellen, da gegenüber der betroffenen Person keinerlei profilbasierte Entscheidung getroffen wird. Auch eine Beeinträchtigung in ähnlich erheblicher Weise ist insoweit zu verneinen, da das Profiling nicht der Ausstrahlung von Werbung, sondern der Produktweiterentwicklung dient.

Für Aufsichtsbehörden sieht Art. 35 Abs. 4 DSGVO ferner die Möglichkeit vor festzulegen, welche Datenverarbeitungsvorgänge stets die Aufstellung einer Datenschutz-Folgenabschätzung erfordern. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat gemeinsam eine entsprechende Liste für Datenverarbeitungen im nicht-öffentlichen Bereich verabschiedet.[436] Unter Punkt 7 findet sich hier

> „Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen."

Dieser Punkt entspricht in wesentlichen Teilen der Formulierung des Art. 35 Abs. 3 lit. a) DSGVO. Eine Verpflichtung zur Datenschutz-Folgenabschätzung lässt sich hieraus vorliegend ebenfalls nicht ableiten, weil es an einer Rechtswirkung bzw. ähnlich gravierenden Konsequenzen fehlt.

Der Generalklausel in Art. 35 Abs. 1 DSGVO zufolge besteht für Verantwortliche stets eine Pflicht zur Durchführung einer Folgenabschätzung, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für personenbezogene Daten zur Folge hat. Anhand der bekannten Informationen muss der Verantwortliche zu einer fundierten Analyse hinsichtlich eines Risikos gelangen. Dabei kommt ihm kein Entscheidungsspielraum zu: Ob eine Risikofolgenabschätzung erforderlich war, kann

---

436 *Datenschutzkonferenz (DSK)*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_VerarbeitungsvorgaengeDSK.pdf?__blob=publicationFile&v=4.

ein Gericht im Nachhinein vollumfänglich auf der Tatsachenbasis überprüfen, die der Prognoseentscheidung zugrunde lag. Dabei kann also die Entscheidung, keine Risiko-Folgenabschätzung vorzunehmen, immer noch rechtmäßig sein, auch wenn sich im Nachhinein herausstellt, dass das Risiko dennoch vorhanden war.[437] Ob die Prognose eines hohen Risikos zu bejahen ist, bemisst sich im Wesentlichen anhand der Eintrittswahrscheinlichkeit und der Schwere eines ggf. eintretenden Schadens.[438] Die Artikel-29-Datenschutzgruppe hat bereits 2017 Leitlinien zum Begriff des hohen Risikos und zur Datenschutz-Folgenabschätzung veröffentlicht[439]. In den Leitlinien werden unter Berücksichtigung der Vorgaben der DSGVO (u. a. Erwägungsgründe 71, 75 und 91) neun Kriterien für Datenverarbeitungsvorgänge mit hohem Risiko aufgestellt. Sofern mindestens zwei dieser Kriterien erfüllt sind, ist nach Auffassung der Artikel-29-Datenschutzgruppe in der Regel die Durchführung einer Datenschutz-Folgenabschätzung notwendig.

Vorliegend wären als Kriterien jedenfalls das Erstellen von Profilen (Nr. 1) sowie der große Umfang der Datenverarbeitung (Nr. 5) einschlägig. Aufgrund dessen ist davon auszugehen, dass mindestens ein Smart-TV-Anbieter verbindlich zu einer Datenschutz-Folgenabschätzung angehalten war und sie trotzdem nicht durchgeführt hat. Für die anderen Unternehmen, die keine Datenschutzfolgenabschätzung durchgeführt haben, wäre ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen i. S. d. Art. 35 Abs. 1 DSGVO eher zu verneinen und es bestünde insofern keine Verpflichtung.

bb) Notwendiger Inhalt einer Datenschutz-Folgenabschätzung

Der Mindestinhalt einer rechtmäßigen Datenschutz-Folgenabschätzung ist in Art. 35 Absatz 7 DSGVO angelegt:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

---

437 *Martini* in: Paal/Pauly [Hrsg.], DSGVO BDSG, 2. Aufl. 2018, Art. 35 DSGVO Rn. 19.

438 *Karg* in: Simitis/Hornung/Spiecker [Hrsg.], Datenschutzrecht, 2019, Art. 35 DSGVO Rn. 23, unter Verweis auf DSGVO-Erwägungsgrund 75 S. 1.

439 *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248 rev. 01, abrufbar über https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Alle vorgelegten Datenschutz-Folgenabschätzungen entsprachen grundsätzlich den o. g. Vorgaben. So wurden insbesondere die Verarbeitungsstationen aufgezeigt. Bei einer Folgenabschätzung fehlte allerdings eine nachvollziehbare Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung. Bei einer Datenschutz-Folgenabschätzung fehlte die Benennung möglicher Schäden, womit ein konkreter Abwägungsprozess zwischen Zweck und Risiken nicht zu erkennen war.

3. Benennung eines Datenschutzbeauftragten

Unter bestimmten Voraussetzungen sieht Art. 37 Abs.1 DSGVO eine Verpflichtung vor, einen Datenschutzbeauftragten zu benennen. Dieser soll gem. DSGVO-Erwägungsgrund 97 S.1 a. E. über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügen und den Verantwortlichen unterstützen.

a) Ermittlungsergebnisse

Von den 21 überprüften Smart-TV-Anbietern verfügten lediglich drei über keinen Datenschutzbeauftragten.

b) Rechtliche Würdigung

Eine Pflicht, einen Datenschutzbeauftragten zu benennen, besteht nach Art. 37 Abs.1 lit. b) DSGVO insbesondere dann, wenn die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Der deutsche Gesetzgeber hat zudem von der Öffnungsklausel in § 37 Abs. 4 S. 1 Hs. 2 DSGVO Gebrauch gemacht und in weiteren Fällen eine Verpflichtung zur Benennung eines Datenschutzbeauftragten statuiert. Gemäß § 38 Abs. 1 BDSG soll der Verantwortliche ergänzend zu Art. 37 Abs. 1 unter bestimmten Bedingungen einen Datenschutzbeauftragten benennen (z. B.

wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind).

Bei den wenigen Unternehmen ohne Datenschutzbeauftragten lag für den Bereich der Smart-TVs bereits keine nennenswerte Verarbeitung personenbezogener Daten vor. Solche Datenverarbeitungen erfolgten vielmehr durch Drittsoftware, die auf den Geräten installiert war bzw. durch ein webbasiertes TV-Portal, ohne dass die betreffenden Hersteller selbst in den Besitz übermittelter Daten gelangt wären. Es fehlt daher bereits an der Verantwortlicheneigenschaft der betreffenden Unternehmen bzw. es kann jedenfalls ausgeschlossen werden, dass eine Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht. Verstöße gegen eine Pflicht zur Benennung eines Datenschutzbeauftragten liegen mithin nicht vor.

Zusammenfassung

Einige der untersuchten Unternehmen speichern selbst keine personenbezogenen Daten und unterliegen insoweit nicht den Pflichten der DSGVO und des BDSG.

Die übrigen Unternehmen kommen ihren in der DSGVO ausdrücklich niedergelegten internen Datenschutz-Organisationspflichten im Wesentlichen nach. Zur Durchführung einer Datenschutz-Folgenabschätzung war nur ein Unternehmen verpflichtet, andere Unternehmen nahmen diese auf freiwilliger Basis vor. Insoweit gibt es nur vereinzelt Kritikpunkte.

VII. Nachhaltigkeit der Produktpflege

Da der smarte Fernseher ähnlich wie ein Computer funktioniert und sich mit dem Internet verbinden kann, ist er den gleichen Sicherheitsrisiken ausgesetzt wie andere internetfähige Geräte. Das Bundeskartellamt hat die Hersteller von Smart-TVs daher befragt, welche Vorkehrungen sie treffen, um die Funktionsfähigkeit ihrer Geräte zu sichern und sie gegen Angriffe von außen zu schützen. Dabei können konzerninterne wie auch externe Maßnahmen sowohl vor als auch nach dem Inverkehrbringen des Geräts zum Einsatz kommen. Da der Smart-TV eine Plattform für viele verschiedene Dienstleister bietet, sind auch mögliche Vereinbarungen zur Sicherheit der Software zwischen Herstellern und den verschiedenen Zulieferern und Diensteanbietern für eine sichere Anwendung der Geräte von Interesse. Wenn der Verbraucher einen Smart-TV anschafft, dürfte er davon ausgehen, das Gerät einige Jahre ohne Sicherheitsrisiko nutzen zu können. Für eine sichere Anwendung ist daher maßgeblich, über welchen Zeitraum die Hersteller die Software ihrer Geräte aktualisieren und durch regelmäßige Aktualisierungen gegen neu bekanntgewordene Sicherheitsrisiken schützen. Das Bundeskartellamt hat schließlich die Garantiebestimmungen der Hersteller verglichen, um zu erfahren, wie der Verbraucher bei Hard- und Softwareschäden abgesichert ist.

1. Datensicherheitsvorkehrungen

Nur wenige Hersteller verhalten sich vollständig passiv und verlassen sich allein auf Vereinbarungen zur Compliance u. Ä. mit Zulieferern, um ihre Software sicher zu machen. Fast alle Hersteller treffen konzerninterne Vorkehrungen, um Sicherheitslücken zu vermeiden oder aufzuspüren. Die Mehrheit der Hersteller geht vor allem nach dem Verkauf des Produkts an den Verbraucher aktiv mit Sicherheitsmängeln um. Deutlich weniger Hersteller sorgen auch vor und setzten bereits in der Produktentwicklung an, um Sicherheitsmängel zu verhindern. Umfassende Qualitätssicherungssysteme über alle Marktstufen sind die Ausnahme. Insgesamt sind die Maßnahmen der Hersteller – was Aufwand, Intensität und Regelmäßigkeit angeht – sehr unterschiedlich.

a) Ermittlungsergebnisse

aa) Konzerninterne spezielle Vorkehrungen

Viele Hersteller wenden **vor dem Inverkehrbringen** grundlegende technische Sicherheitsvorkehrungen wie Secure Boot, Firewalls, verschlüsselte Software Images, Standard-Web-Sicherheitsimplementierungen wie sichere http-Verbindungen mit Verschlüsselungsverfahren wie SSL-Handshaking[440] für die internetbasierten Anwendungsfunktionen auf Smart-TVs an. Hersteller führen auch automatische Viren-Scans durch. Viele Hersteller richten ihre Smart-TVs so ein, dass nur vom Hersteller signierte und verschlüsselte oder autorisierte Anwendungen genutzt werden können.

Einige Hersteller verstehen unter Softwaresicherheit hauptsächlich die **Sicherheit von Diensten**, z. B. indem ein *Trusted Execution Environment* (TEE), also eine vertrauenswürdige Laufzeitumgebung für Applikationen eingerichtet wird. Auf dem TEE können nur speziell dafür freigeschaltete Applikationen ausgeführt werden.

Nur wenige Hersteller haben ein umfassendes **Qualitätssicherungssystem** über alle Marktstufen eingerichtet. Von der **Produktentwicklung** bis zur endgültigen **Marktreife** werden regelmäßige Kontrollen durchgeführt und als Milestone im Entwicklungsprozess verankert. Dabei wird auch die Robustheit der eigenen Software überprüft, so dass sie von Dritten nicht verändert werden kann. Ein Hersteller erläutert, dass das interne Netzwerk für die Entwicklung der Produkte von anderen Netzwerken getrennt wird, bevor das Produkt in den Markt geht.

---

[440] SSL (*Secure Sockets Layer*) Handshake ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, weiterentwickelt unter dem neuen Namen TLS (*Transport Layer Socket*).

Ein weltweit führender Hersteller überprüft seine Produkte auf allgemein bekannte Schwachstellen, die auf der sog. **CVE**-Webseite[441] (*Common Vulnerabilities and Exposure*, CVE, häufige Schwachstellen und Risiken) gelistet sind. Hierbei handelt es sich um eine weltweite Sammlung bekannt gewordener Schwachstellen. Der Hersteller besitzt ein automatisches Tool, das die Schwachstellen von der Website abruft und prüft, ob diese für Smart-TVs relevant sein können. Er führt außerdem eine Codierungsprüfung durch, um Sicherheitslücken im Quellcode der verwendeten Software zu finden, sowie einen Penetrationstest. Dabei wird ein autorisierter simulierter Cyberangriff auf das Computersystem durchgeführt und die Sicherheit des Systems anschließend bewertet. Die Testergebnisse können zu organisatorischen Veränderungen führen, die das Risiko reduzieren sollen, z. B. zusätzliche Überprüfungen der Sicherheit.

Fast alle Hersteller werden aktiv, sobald **Sicherheitsmängel nach dem Kauf** in der Software von Kunden oder Zulieferern entdeckt werden. Die jeweiligen Maßnahmen sollen auch neu entwickelten Produkten zu Gute kommen, da Fehler so nicht wiederholt werden können. Die Hersteller werten beispielsweise „häufig gestellte Fragen" der Kunden, Produkttests (z. B. Stiftung Warentest), Internetforen für Produkte, Blogs zur Sicherheit sowie Sicherheitsmitteilungen von Betriebssystemherstellern, wie z. B. das *Android Security Bulletin* aus, führen stichprobenartige Tests der aufgespielten Software durch oder veranlassen Software-Updates in Folge von Fehlern. Hersteller wenden sog. *Patches* an, eine Software, die entwickelt wird, um ein Computerprogramm und/oder seine unterstützenden Daten zu aktualisieren, zu optimieren oder Fehler zu beheben (z. B. *Google Security Patch* für *Android*). Ein Hersteller hat ein **Belohnungsprogramm** eingeführt, um Anreize zu setzen, Sicherheitslücken auf seinen Geräten zu melden.

Einzelne Anbieter, die ihre Geräte von OEM-Herstellern[442] erhalten, geben Meldungen über Sicherheitslücken an diese Hersteller weiter, die dann ggf. entsprechende Updates zur Verfügung stellen. Einige Hersteller stehen dazu nicht nur mit den Nutzern in Kontakt, sondern auch mit Dritten, z. B. Anbietern von Apps.

---

441 Common Vulnerabilities and Exposures (CVE, häufige Schwachstellen und Risiken) ist ein Industriestandard, dessen Ziel die Einführung einer einheitlichen Benennung für Sicherheitslücken und andere Schwachstellen in Computersystemen ist. Dadurch ist ein reibungsloser Informationsaustausch zwischen den verschiedenen Datenbanken einzelner Hersteller möglich. Die CVE-Nummern werden seit 1999 vergeben. Die Liste der „häufigen Schwachstellen und Risiken" wird von der Mitre Corporation in Zusammenarbeit mit den CVE Numbering Authorities (Sicherheitsexperten, Bildungseinrichtungen, Behörden und Herstellern von Sicherheitssoftware etc.) verwaltet, vgl. https://www.itwissen.info/CVE-common-vulnerabilities-and-exposures.html.

442 S. Fn. 376.

Einige Hersteller geben an, ihre Sicherheitsmaßnahmen auch an den **Anforderungen der Diensteanbieter auf ihrer Plattform** auszurichten. Diese Anforderungen umfassen offenbar z. B. den Schutz vor Manipulationen und Hacken der Software sowie sichere Softwareschlüssel.

bb) Zertifizierungen

Nur zwei der befragten Hersteller geben an, eine **konzerninterne Zertifizierung** im eigentlichen Sinne entwickelt zu haben, um die eigene Software sicher zu machen. Es gibt bei einigen Unternehmen aber **Qualitätssicherungssysteme mit festgeschriebenen Abläufen** (wie im vorherigen Abschnitt beschrieben), was vom Ergebnis her einer Zertifizierung entsprechen kann. Wurde der Prozess erfolgreich durchlaufen, kann das Produkt freigegeben werden. So betont einer der führenden Hersteller, dass er auch ohne Zertifizierung interne Prüfungen durchführt, um sicherzustellen, dass die jeweils verwendete Software in Übereinstimmung mit den jeweils gültigen herstellerspezifischen technischen Anforderungen ist. Zusätzlich führt der Hersteller für sämtliche Software-Module eine Risiko-Einschätzung durch.

Zertifizierungen durch **externe Prüfungsinstanzen** werden bisher wenig genutzt. Nur 30% der befragten Hersteller haben bisher eine Zertifizierung erhalten oder streben diese an. Nach Einschätzung des Bundeskartellamts hat sich für die Softwaresicherheit unter den Zertifizierungen bisher **kein Marktstandard** etabliert. Ein Hersteller hat seine Software vom **TÜV Rheinland** zertifizieren lassen. Mehrere andere Hersteller haben ein Sicherheitszertifikat des privaten US-amerikanischen Sicherheitsunternehmens *Underwriters Laboratories Inc.* [443] oder **die sog. *CC certification (Common Criteria for Information Technology Security Evaluation)*** erhalten. Das *UL Cybersecurity Assurance Program (UL CAP)* zielt nach Angaben von UL darauf ab, Sicherheitsrisiken zu managen. Es arbeitet auf Basis von standardisierten Kriterien, um Schwachstellen der Software aufzudecken und zu beurteilen. *CC* sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten.[444] Diese *Allgemeinen Kriterien*

---

443 UL ist ein weltweit tätiges Unternehmen, das Dienstleistungen in den Bereichen Zertifizierung, Validierung, Prüfung, Verifizierung, Inspektion, Audit sowie Beratung und Ausbildung erbringt. Das Zertifizierungsprogramm UL CAP bezieht sich auf die UL 2900 Normenreihe, die mithilfe von Interessenvertretern aus Regierung, Universität und Industrie entwickelt wurde. Vgl. https://germany.ul.com/.

444 Die *Common Criteria* unterscheiden zwischen der Funktionalität (Funktionsumfang) des betrachteten Systems und der Vertrauenswürdigkeit (Qualität). Die Vertrauenswürdigkeit wird nach den Gesichtspunkten der Wirksamkeit der verwendeten Methoden und der Korrektheit der Implementierung betrachtet. Den *Common Criteria* liegt ein Vier-Augen-Prinzip bei der Prüfung der Sicherheitseigenschaften eines Produktes zugrunde. Das Produkt muss zuerst von einer akkreditierten Prüfstelle evaluiert werden und kann dann bei einer Zertifizierungsstelle – in Deutschland ist dies das Bundesamt für

für die Bewertung der Sicherheit von Informationstechnologie sollen garantieren, dass schädliche Apps von Dritten nicht installiert werden können.

Hersteller berufen sich ferner auf Zertifizierungen von Dienstleistern, wie z. B. verschiedenen Videoportalen, die auch Sicherheitsanforderungen enthalten, die vom Hersteller erfüllt werden müssen.

cc) Vereinbarungen zwischen Herstellern, Zulieferern, Diensteanbietern

Die Hälfte der befragten Unternehmen trifft keine besonderen Vorkehrungen **in Verträgen mit Zulieferern oder externen Dienstleistern**.

Mehrere Hersteller fordern Zulieferer zumindest auf, **Checklisten für die Robustheit** der Dienste umzusetzen, bei denen es um die Verschlüsselung von Digital-TV und die sichere Verbreitung von Inhalten, Kopierschutz und Jugendschutz geht.[445]

Soweit Software Dritter personenbezogene Daten erfasst, verpflichten manche Hersteller den Lizenzgeber, Datensicherheit in dem gesetzlich vorgeschriebenen Umfang durch entsprechende **technische und organisatorische Maßnahmen** zu gewährleisten.

Ein Unternehmen trifft **keine speziellen Regelungen für Sicherheitsthemen**, ordnet Probleme mit Software oder Software-Updates aber allgemeinen Regelungen zu Verstößen oder Fehlfunktionen zu.

Nur wenige Hersteller schließen mit ihren Zulieferern **Qualitätssicherungsvereinbarungen** ab, die sehr umfangreiche Vorschriften enthalten können. Bei einem dieser Hersteller müssen Zulieferer jede Anwendung einreichen, die Sie über den App-Store des Herstellers oder eines seiner Partnerunternehmen verteilen möchten. Der Hersteller prüft und zertifiziert die Anwendung gemäß den Zertifizierungsanforderungen. Er prüft außerdem die Dokumentation entsprechend den

---

Sicherheit in der Informationstechnik (BSI) – zertifiziert werden, vgl. z. B. https://www.tuev-nord.de/explore/de/erklaert/was-sind-die-common-criteria/ oder https://de.wikipedia.org/wiki/Common_Criteria_for_Information_Technology_Security_Evaluation.

445 Sie nennen vor allem Anforderungen des Digital Rights Management und des CI-Plus-Standards. CI-Plus ist ein erweiterter Standard der Schnittstelle Common Interface (CI) bei DVB-Empfangsgeräten für die Verschlüsselung von Digital-TV. CI-Plus betrifft die sichere Verbreitung von Inhalten, Kopierschutz und Jugendschutz. Der CI-Plus-Standard wurde von der Gesellschaft für Unterhaltungs- und Kommunikationselektronik (gfu) und der Consumer Electronics im ZVEI vorangetrieben. Vgl.https://de.wikipedia.org/wiki/Common_Criteria_for_Information_Technology_Security_Evaluation, Stand: 22.07.2019.

Vorgaben, die den Dienstleistern vom Hersteller oder seiner Partner zur Verfügung gestellt wurden.

Vereinzelt werden Softwarepflegevereinbarungen abgeschlossen, die insbesondere dem Erhalt der Sicherheitsstandards dienen. Bei einem weiteren Hersteller müssen Zulieferer erklären, nicht nur alle gesetzlichen Regelungen einzuhalten (*Compliance*), sondern auch Vereinbarungen und Verpflichtungen, die in den Bedingungen und/oder anderen Unterlagen des Herstellers aufgeführt sind, z. B. zur Konfiguration der Systeme, technische Spezifikationen, Werberichtlinien und Dokumentation. Zulieferer dürfen ferner keine Anwendung entwickeln oder bereitstellen, die Hacking[446]-Funktionen oder -Eigenschaften besitzt. Wenn der Hersteller nach eigenem Ermessen feststellt, dass eine Anwendung über Hacking-Fähigkeiten, -Zwecke oder -Eigenschaften verfügt, behält er sich das Recht vor, diese Vereinbarung zu kündigen.

Hersteller orientieren sich nach eigenen Angaben auch an den Vorgaben zur Sicherheit der verschiedenen Diensteanbieter auf ihrer Plattform. Die Ermittlungen des Bundeskartellamts bestätigen, dass auch Diensteanbieter sicherheitstechnische Anforderungen stellen, bevor ihre Apps installiert werden dürfen. Die Anforderungen der Diensteanbieter sind sehr unterschiedlich. Um die Sicherheit der Dienste und den Schutz vor Hacking geht es allen Diensteanbietern, die Dichte der Maßnahmen ist aber uneinheitlich. Einzelne App-Anbieter setzen vor allem auf regelmäßige Updates, die teilweise mit dem Hersteller abgestimmt und innerhalb einer bestimmten Frist durchgeführt werden müssen und fordern Maßnahmen für die Robustheit der Systeme ein. Im Vergleich dazu betreibt ein führender Video-Streaming-Anbieter ein umfassendes Zertifizierungsprogramm. Teilnehmende Hersteller müssen nicht nur die bereits erwähnten Software-Updates und Regeln für die Robustheit abstimmen, sondern auch Berichtspflichten mit kumulierten, nicht personenbezogenen Angaben zur App-Nutzung bei den Geräten erfüllen.

b) Rechtliche Würdigung

Die Sicherheitsvorkehrungen der einzelnen Hersteller von Smart-TVs stellen sich uneinheitlich dar. Die Ermittlungen des Bundeskartellamts bei den Herstellern auf Basis von bußgeldbewehrten Auskunftsverlangen haben aber keine augenfälligen Anhaltspunkte dafür ergeben, dass aktuell Hersteller von Smart-TVs technisch unsichere Geräte in den Verkehr bringen. Eine Untersuchung möglicherweise einschlägiger Haftungstatbestände erübrigt sich daher.

---

446 Hacking bezeichnet den unbefugten Zugriff auf oder die Umgehung von Sicherheitsmaßnahmen bei einer Website, einem Gerät, einem Netzwerk oder einem Server, um den Betrieb und die Nutzung eines solchen Geräts, Computersystems, Netzwerks, Servers oder Website zu unterbrechen, zu stören, zu beschädigen, zu behindern oder auf andere Art darauf zuzugreifen.

2. Ausbleiben von Software-Updates

Bedenken bzgl. Sicherheitsstandards ergeben sich in erster Linie nach dem Inverkehrbringen[447] von Smart-TVs. Dies betrifft den Fall, dass Hersteller (oder anderweitig Verantwortliche) bei öffentlich bekannt gewordenen Sicherheitslücken der Gerätesoftware keine Updates zu deren Behebung zur Verfügung stellen. Dies kann einerseits dazu führen, dass bereits im Gebrauch befindliche Fernsehgeräte angreifbar werden. Andererseits besteht die Gefahr, dass Smart-TVs aus Modellreihen, die bereits seit längerer Zeit vertrieben werden, bereits beim Verkauf im Einzelhandel nicht mehr dem aktuellen Sicherheitsstandard entsprechen.

a) Ermittlungsergebnisse

Sicherheits-Updates werden zu unterschiedlichen Zeitpunkten durchgeführt. Die meisten Hersteller werden sofort aktiv, wenn Sicherheitsmängel auftreten. Bei anderen Herstellern dauert es länger. Entweder müssen Gremien oder verschiedene Abteilungen passiert werden oder Updates werden grundsätzlich nur zum nächstmöglichen Firmware-Release-Zeitpunkt vorgenommen.

Der Großteil der Hersteller stellt Updates für Chipsatzsoftware, Betriebssystem, HbbTV-Software, Smart-Portal, Web-Browser, vorinstallierte konzerneigene Apps, vorinstallierte konzernexterne Apps bereit. Der weit überwiegende Teil der Hersteller sieht für seine TV-Modelle einheitliche Zeiträume für die Versorgung mit Sicherheitsupdates vor. Nach außen werden diese Fristen in aller Regel aber nicht kommuniziert.

Die Sektoruntersuchung hat ergeben, dass – im Durchschnitt aller Anbieter – bei im Jahr 2018 neu in den Verkehr gebrachten Geräten für ca. 27 Monate mit Software-Sicherheitsupdates gerechnet werden konnte. Dabei versorgen die meisten Hersteller ihre Geräte innerhalb von **24 bis 36 Monaten** nach dem ersten Inverkehrbringen des betreffenden Modells noch mit Updates. Zwei Hersteller aktualisieren die Gerätesoftware auch noch 60 Monate nach diesem Zeitpunkt. Ein kleiner Teil der Anbieter stellt Sicherheitsupdates oder andere geeignete Gegenmaßnahmen nur reaktiv dann bereit, wenn diese – offenbar aufgrund eines entdeckten Sicherheitsmangels – notwendig werden. Ein periodisches Update führen diese Hersteller nicht durch. Dass überhaupt keine Updates bereitgestellt werden, ist die Ausnahme, kommt aber vor.

Wer also im Jahr 2020 ein TV-Modell des vorletzten Jahres erwirbt, kann in vielen Fällen bereits nicht mehr davon ausgehen, dass dieses überhaupt Updates erhält. Der Verbraucher muss sich also ggf. bereits nach relativ kurzer Nutzung fragen, ob er einen neuen Smart-TV oder ein neues

---

447 Mit Inverkehrbringen ist die erstmalige Belieferung von Groß- und Einzelhändlern durch den Hersteller in Deutschland oder das erstmalige Bereitstellen im (Online-)Direktvertrieb gemeint, nicht der Moment des tatsächlichen Verkaufs an den Endverbraucher.

externes Gerät mit Smartfunktionalität kaufen soll, um Risiken durch nicht behobene Softwaresicherheitslücken zu vermeiden.

b) Rechtliche Würdigung

Ob und in welchen Konstellationen beim Vorliegen von Sicherheitsdefiziten auch Verbraucherrechtsverstöße zu bejahen sind, ist nicht einfach zu beantworten. Für eine Haftung kommen grundsätzlich mehrere Grundlagen in Betracht, die nachfolgend dargestellt werden.[448]

aa) Updatepflicht

Dies gilt zunächst für die Updatepflicht.

(1) Gewährleistungsrecht

Das Kaufrecht ist auch auf Mängel der *S*oftware eines Smart-TVs anwendbar. Zwar sind Kaufgegenstände nach § 90 BGB Sachen, also körperliche Gegenstände. Jedenfalls nach herrschender Ansicht genügt für diese Körperlichkeit, dass die Software auf einem Datenträger gespeichert und damit verkörpert wird.[449] Nach aktueller Rechtslage deckt das Gewährleistungsrecht jedoch

---

448 Aufgrund der unterschiedlichen Ausgestaltung und der unterschiedlichen Reichweite von Garantieverträgen werden diese unter 3. gesondert behandelt. Eine strafrechtliche Haftung ist selbst bei geplanter Obsoleszenz nur in Extrembeispielen möglich und wird daher hier nicht erörtert, S. dazu etwa *Hoven*, Der „eingebaute" Produktverschleiß – Die Strafbarkeit geplanter Obsoleszenz, NJW 2019, 3113. Aufgrund geringer unmittelbarer Verbraucherrelevanz wird ebenfalls nicht eingegangen auf das Problem möglicher Botnetz-Attacken, die von unsicheren IoT-Geräten ausgehen, S. hierzu *Klein-Henning/Schmidt*, Zurück auf Los – Die IT-Sicherheit zurück in der Steinzeit, DuD 2017, 605. Eine Updateverpflichtung aufgrund des Produktsicherheitsgesetzes kommt bei Smart-TVs nicht infrage, da deren fehlerhafte Software nicht die Sicherheit oder Gesundheit von Personen gefährdet (Haftungsvoraussetzung gem. § 3 Abs. 2 S. 1 des Gesetzes über die Bereitstellung von Produkten auf dem Markt v. 08.11.2011 (BGBl. I S. 2178, 2179; 2012 I S. 131), zuletzt geändert durch Art. 16 des Gesetzes v. 28.04.2020 (BGBl. I S. 960) – Produktsicherheitsgesetz (ProdSG)). Die ohnehin erst bis 01.01.2022 umzusetzende EU-Richtlinie über digitale Inhalte (Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates v. 20.05.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. EU Nr. L 136 v. 22.05.2019, S. 1), ist nicht einschlägig, denn der vorliegende Bericht beleuchtet nur die rechtliche Situation bei vorinstallierter Software (s. dazu *Schippel*, Die Pflicht zur Bereitstellung von Software, Updates und Upgrades nach der Richtlinie über digitale Inhalte und Dienstleistungen, K&R 2020, 117, 120).

449 BGH, Urteil vom 15.11.2006, Az. XII ZR 120/04, juris Rn. 15 m. w. N.

nur die Mangelfreiheit der Kaufsache im Zeitpunkt des Gefahrübergangs ab.[450] Ist die Gerätesoftware zu diesem Zeitpunkt frei von erkennbaren Sicherheitslücken, scheidet insoweit eine Gewährleistung des Verkäufers im Regelfall wohl aus, wenn später Sicherheitslücken bekannt werden, die im Zeitpunkt des Gefahrübergangs nicht erkennbar waren.[451] Das Gewährleistungsrecht erfasst ebenfalls nur die Beziehung zwischen Verkäufer und Käufer, Ansprüche gegen den Hersteller lassen sich hieraus nicht herleiten.[452] Im Falle ausbleibender notwendiger Software-Updates kann das Gewährleistungsrecht mithin aktuell allenfalls dann herangezogen werden, wenn ein Verkäufer Smart-TVs verkauft, die bei Gefahrübergang bereits bekannte Sicherheitslücken aufweisen.

Beim Kauf eines Smart-TVs werden in der Regel weder eine Beschaffenheit noch vertraglich eine Eignung für eine bestimmte Verwendung vereinbart. Das Vorliegen eines Sachmangels bemisst sich daher nach § 434 Abs. 1 S. 2 Nr. 2 BGB. Demzufolge ist eine Sache mangelfrei, soweit sich der Gegenstand „für die gewöhnliche Verwendung eignet und eine Beschaffenheit aufweist, die bei Sachen der gleichen Art üblich ist und die der Käufer nach der Art der Sache erwarten kann“. Die vom Verkäufer zu erwartende Beschaffenheit der Kaufsache ist hierbei nach dem Empfängerhorizont eines Durchschnittskäufers zu beurteilen und richtet sich nach der objektiv berechtigten Käufererwartung.[453] Diese kann § 434 Abs. 1 S. 3 BGB zufolge grundsätzlich auch durch Werbung beeinflusst sein.

Das Vorliegen von Sicherheitslücken schließt die Verwendung eines Smart-TVs für das Fernsehen unter Nutzung von Smartfunktionen nicht aus. Man könnte aber bezweifeln, ob die Gebrauchsfähigkeit („für die gewöhnliche Verwendung“) durch die Sicherheitslücken nicht zumindest beeinträchtigt ist, was zur Bejahung eines Sachmangels führen würde.[454] Jedenfalls stellt sich die Frage, ob bei einem solchen Fernsehgerät noch eine Beschaffenheit vorliegt, die bei vergleichbaren Gegenständen üblich ist und den Käufererwartungen entspricht. Abzustellen ist

---

450 Gefahrübergang ist der Zeitpunkt, in dem die Gefahr von Verlustes oder Beschädigung der Sache auf den Käufer übergeht. Beim Versendungskauf findet der Gefahrübergang erst dann statt, wenn der Verbraucher die Sache erhalten hat (§ 475 Abs. 2 BGB als Ausnahme zu § 447 Abs. 1 BGB).

451 Vgl. *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1843. Zu einer nachvertraglichen Nebenleistungspflicht zur Bereitstellung ggf. kostenpflichtiger Updates s. *Schrader/Engstler*, Anspruch auf Bereitstellung von Software-Updates?, MMR 2018, 356, 358.

452 Normalerweise vertreiben Hersteller ihre Smart-TVs nicht oder nur in sehr begrenztem Umfang direkt an den Endverbraucher.

453 BGH, Urteil vom 20.05.2009, Az. VIII ZR 191/07, juris Rn. 14.

454 Vgl. BGH, Beschluss vom 08.01.2019 – VIII ZR 225/17, juris Rn. 5; BGH, Urteil vom 29.06. 2016 – VIII ZR 191/15, juris Rn. 40 m. w. N.

dabei auf die Verkehrsauffassung[455] unter Berücksichtigung des Standes der Technik[456]. Vergleichsmaßstab sind Produkte des betreffenden Unternehmens und der Konkurrenz, die derselben Preisklasse angehören.[457] In die Betrachtung wird man auch mit einfließen lassen müssen, wie lange sich die Geräte-Modellreihe bereits auf dem Markt befindet, sofern dies für den Käufer ohne Weiteres erkennbar ist. Vor diesem Hintergrund dürfte es, mit Ausnahme eklatanter Sicherheitslücken, zumeist schwerfallen, einen Sachmangel zu bejahen. Im Bereich der meisten IoT-Geräte besteht zumindest außerhalb des Premiumsegments keine allgemeine Praxis, dass Gerätesoftware nach[458] dem erstmaligen Inverkehrbringen regelmäßig durch Sicherheitsupdates aktualisiert wird. Die Anwendbarkeit des Gewährleistungsrechts bei Sicherheitsmängeln, die sich erst nach dem Inverkehrbringen manifestieren, dürfte damit ausgeschlossen sein.

Die Rechtslage wird sich in Zukunft allerdings grundlegend ändern. Bis 01.07.2021 müssen die EU-Mitgliedstaaten die Warenkaufrichtlinie[459] in nationales Recht umsetzen und sie ab dem 01.01.2022 anwenden. Die Warenkaufrichtlinie erweitert die Gewährleistungshaftung deutlich. Art. 7 Abs. 3 lit. a) der Richtlinie sieht für einmalige Käufe von Waren mit digitalen Elementen erweiterte Verkäuferpflichten vor. Der Verkäufer muss dafür sorgen, dass der Verbraucher bei Aktualisierungen, einschließlich Sicherheitsaktualisierungen, die für den Erhalt der Vertragsmäßigkeit dieser Waren erforderlich sind, informiert wird und solche erhält. Dies gilt für den gesamten Zeitraum, während dessen der Verbraucher solche Aktualisierungen in Anbetracht der Umstände und der Besonderheiten des Vertrags vernünftigerweise erwarten kann. Gemäß Erwägungsgrund 31 der Warenkaufrichtlinie ist dies zumindest während des regulären Gewährleistungszeitraums der Fall. Für Deutschland bestünde somit eine Sicherheitsupdate-Pflicht für wenigstens zwei Jahre nach dem Warenkauf.

Die Umsetzung der Warenkaufrichtlinie wird einen Paradigmenwechsel bzgl. der Haftung des Verkäufers mit sich bringen. Mit ihrem Inkrafttreten besteht eine grundsätzliche Verpflichtung des

---

455 Vgl. *Faust* in: BeckOK BGB, 54. Edition, 01.05.2020, § 434 BGB Rn. 66 i. V. m. 59 („Erwartungshorizont eines vernünftigen Durchschnittskäufers“).

456 Vgl. *Westermann* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, § 434 BGB Rn. 24.

457 Vgl. *Faust*, a a. O. (Fn. 455), § 434 BGB Rn. 66 i. V. m. 61 f.

458 Erwirbt der Käufer hingegen ein erst seit kurzer Zeit auf dem Markt befindliches Neugerät mit wesentlichen – bereits im Zeitpunkt des Inverkehrbringens öffentlich bekannten – Sicherheitslücken, ließe sich das Vorliegen eins Sachmangels durchaus bejahen, da der Käufer vernünftigerweise erwarten darf, dass dies bei einem solchen Gerät nicht der Fall ist.

459 Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG, Abl. EU Nr. L 136 v. 22.05.2019, S. 28 (kurz Warenkaufrichtlinie).

Verkäufers zum Erhalt der vertragsgemäßen Gebrauchsfähigkeit des Kaufgegenstands weit über den Zeitpunkt des Gefahrübergangs hinaus. Dies ist umso bemerkenswerter, als der Verkäufer selbst faktisch nicht in der Lage ist, Software-Updates zum „Erhalt der Vertragsmäßigkeit der Waren“ ohne entsprechende Kooperation des Geräteherstellers (oder ggf. des vom Hersteller abweichenden TV-Portalbetreibers[460]) zur Verfügung zu stellen.

Allerdings sieht Art. 7 Abs. 5 der Warenkaufrichtlinie auch die Möglichkeit vor, dass der Käufer u. a. einem Abweichen von der Updateverpflichtung ausdrücklich und gesondert zustimmen kann. Es besteht daher die Gefahr, dass die jeweils betroffene Branche im Wege bewussten Parallelverhaltens[461] die Updateverpflichtung umgeht, indem dem Verbraucher stets Updateverzichtsregelungen vorgelegt werden. Es bleibt mithin abzuwarten, welche tatsächlichen Veränderungen die Warenkaufrichtlinie – auch entlang der Lieferkette – auslösen wird.

(2) Datenschutzrecht

Eine Updatepflicht des Herstellers könnte sich aus dem Datenschutzrecht ergeben. Die Datensicherheit betreffenden Vorschriften der DSGVO nehmen den jeweiligen für eine Datenverarbeitung Verantwortlichen in die Pflicht.[462] Der Verkäufer eines IoT-Geräts, der (mit Ausnahme des Herstellerdirektvertriebs) bei Betrieb des Geräts im Regelfall keinerlei personenbezogenen Daten erhält, ist hiervon nicht betroffen. Art. 5 Abs. 1 lit. f) DSGVO zufolge müssen Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um bei der Verarbeitung von personenbezogenen Daten ein angemessenes Sicherheitsniveau zu gewährleisten. So sollen die Daten insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung geschützt werden. Art. 25 Abs. 1 DSGVO verlangt, dass dies sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung gilt. Art. 32 Abs. 1 DSGVO schließlich sieht hierfür beispielhaft Maßnahmen des Verantwortlichen vor. Dies bedeutet einerseits, dass bei der Verarbeitung personenbezogener Daten kontinuierlich Schutzmaßnahmen zu ergreifen sind. Andererseits steht diese Verpflichtung unter dem Vorbehalt der „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und

460 Ein im Rahmen der Sektoruntersuchung befragtes Unternehmen wies ausdrücklich darauf hin, es gebe derzeit nur beschränkte Möglichkeiten, Vereinbarungen, die eine zeitlich beschränkte Behebung von Softwarefehlern garantieren, von Drittanbietern einzufordern. Die Verhandlungsmacht sei insoweit abhängig von den Kräfteverhältnissen und insbesondere dem eigenen Umsatzvolumen.

461 Entsprechende explizite Absprachen wären nach § 1 GWB natürlich verboten.

462 S. insb. Art. 5 Abs. 2 DSGVO.

Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen […]“.[463]

Grundsätzlich kann man aus den vorgenannten Bestimmungen eine Verpflichtung des jeweiligen Verantwortlichen für Sicherheitsupdates herauslesen.[464] Zwar sieht der Beispielskatalog des Art. 32 Abs. 1 DSGVO dies nicht ausdrücklich vor. Dieser Katalog ist aber erkennbar nicht abschließend ausgestaltet. Mit Ausnahme der Einhaltung gesetzlicher Mindeststandards wird man dem Verantwortlichen indessen einen gewissen Ermessensspielraum zugestehen müssen.[465] Die erforderliche Interessenabwägung kann so ergeben, dass Aufwand und Implementierungskosten für den Verantwortlichen angesichts eines nur geringen Risikos für die betreffenden Daten zu hoch sind. Dies kann insbesondere der Fall sein, wenn ein Gerät bereits älter oder wenig verbreitet und daher das Risikopotential begrenzt ist.

Soweit ersichtlich gibt es bislang keinerlei Rechtsprechung zur Frage einer Updateverpflichtung auf Grundlage der DSGVO. Soweit die Gerichte eine solche Verpflichtung im Grundsatz bejahen sollten, wäre diese immer einer Interessenabwägung unterworfen. In praktischer Hinsicht besteht zudem das Problem, dass die Datengefährdung je nach Lage des Falls gar nicht durch den verantwortlichen Datenempfänger behoben werden kann, sondern etwa durch einen Plattformbetreiber, der selbst nicht Verantwortlicher ist (zur Frage der Verantwortlichkeit bei Datenverarbeitungen siehe unter E. V. 3., S. 150). Es ist daher schwer zu prognostizieren, welche Rolle eine Sicherheitsupdate-Pflicht nach der DSGVO in der Praxis spielen könnte und ob diese einen echten Mehrwert für den Verbraucher bedeuten würde.

(3) Lauterkeitsrecht

Vereinzelt wird in der Literatur eine lauterkeitsrechtliche Updatepflicht des Herstellers in Analogie zur Rechtsprechung des BGH in der Sache *Jugendgefährdende Medien auf eBay befürwortet*[466]. Das Unternehmen, das die benötigten Updates nicht zur Verfügung stelle, schaffe – jedenfalls bei weit verbreiteter Massensoftware – die konkrete und ernsthafte Gefahr der Verletzung lauterkeitsrechtlich geschützter Interessen.[467] In Frage kämen in diesem Zusammenhang (zurechenbare) Verstöße Dritter gegen § 4a Abs. 1 Nr. 2 UWG (Nötigung durch *Ransomware* oder Drohung

---

463 S. Art. 25 Abs. 1, 32 Abs. 1 DSGVO.

464 Alternativ könnte der Datenempfänger auch auf die Verarbeitung personenbezogener Daten verzichten, soweit dies möglich ist.

465 *Mantz* in Sydow [Hrsg.], Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 25 DSGVO Rn. 48.

466 *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1845 f.

467 *Raue*, a. a. O. (Fn. 466), 1841, 1846.

mit DDoS-Attacken), § 7 Abs. 1 S. 1 UWG (Installation von Schadsoftware als unzumutbare Beeinträchtigung) und § 7 Abs. 2 Nr. 3 UWG (unaufgeforderte Zusendung von Werbung).[468]

In dem Urteil *Jugendgefährdende Medien auf eBay* hatte der BGH ausgeführt, dass die Beklagte mit ihrer Internetplattform die ernsthafte Gefahr einer Verletzung des Jugendschutzrechts und damit auch der lauterkeitsrechtlich geschützten Verbraucherinteressen eröffnet habe. Es komme daher unter dem Aspekt der Verletzung einer wettbewerbsrechtlichen Verkehrspflicht eine Haftung der Beklagten als Täterin nach § 3 UWG [in der Fassung des UWG 2004] in Betracht. Auch im Lauterkeitsrecht gelte der in anderen Rechtsbereichen entwickelte Rechtsgedanke der Verkehrspflichten, dass der Verantwortung für eine Gefahrenquelle in den Grenzen der Zumutbarkeit eine Pflicht zu gefahrverhütenden Maßnahmen entspreche.[469] Hieraus folgerte der BGH, dass *eBay* eine Prüfungspflicht obliege, deren Umfang im Einzelfall nach einer Abwägung aller betroffenen Interessen und relevanten rechtlichen Wertungen zu bestimmen sei.[470] In seiner Entscheidung befand der BGH, dass *eBay* bei konkreten Hinweisen auf jugendgefährdende Medien das betreffende Angebot sperren und Sorge dafür tragen müsse, dass es in Zukunft nicht zu gleichartigen Rechtsverletzungen komme.[471]

Die BGH-Entscheidung *Jugendgefährdende Medien auf eBay* fußte auf § 3 UWG 2004 („Unlautere Wettbewerbshandlungen, die geeignet sind, den Wettbewerb zum Nachteil der Mitbewerber, der Verbraucher oder der sonstigen Marktteilnehmer nicht nur unerheblich zu beeinträchtigen, sind unzulässig“). In der aktuellen Fassung des UWG wäre auf geschäftliche Handlungen gegenüber Verbrauchern § 3 Abs. 2 UWG anzuwenden, demzufolge geschäftliche Handlungen, die sich an Verbraucher richten oder diese erreichen, unlauter sind, wenn sie nicht der unternehmerischen Sorgfalt entsprechen und dazu geeignet sind, das wirtschaftliche Verhalten des Verbrauchers wesentlich zu beeinflussen. Schutzgut des § 3 Abs. 2 UWG (i. V. m. § 2 Abs. 1 Nr. 8 UWG) ist indessen nicht das vertragliche Leistungsinteresse auf Verbraucherseite, sondern die Fähigkeit des Verbrauchers zu einer informierten Entscheidung.[472] Diese wird nicht durch ein faktisches Unterlassen von Updates beeinträchtigt, sondern allenfalls durch eine unterbleibende Information hierüber. § 3 Abs. 2 UWG in seiner heutigen Fassung ist mithin keine passende Norm, um ein rein tatsächliches Nicht-Handeln zu beurteilen, welches für sich genommen keine Auswirkung auf die Informationslage oder die Entscheidungsfreiheit des Verbrauchers hat.

---

468 *Raue*, a. a. O (Fn. 466), 1841, 1845.

469 BGH, Urteil vom 12.07.2007, Az. I ZR 18/04, BGHZ 173, 188, Rn. 36 f.

470 BGH, a. a. O. (Fn. 469), Rn. 38.

471 BGH, a. a. O. (Fn. 469), Rn. 42.

472 Vgl. *Bähr* in: Münchener Kommentar zum Lauterkeitsrecht, 3. Aufl. 2020, § 2 UWG Rn. 354.

Bei anderen lauterkeitsrechtlichen Normen wie § 4a Abs. 1 Nr. 2 UWG, § 7 Abs. 1 S. 1 UWG oder § 7 Abs. 2 Nr. 3 UWG ließe sich zwar ein täterschaftliches Unterlassen aufgrund der Verletzung einer wettbewerbsrechtlichen Verkehrspflicht (zur Gefahrenbeseitigung durch Bereitstellung von Software-Updates) annehmen. Es ist aber fraglich, ob Verstöße Dritter gegen diese Vorschriften konkret drohen und ob daraus ein gerichtlich durchsetzbarer Anspruch auf Updates hergeleitet werden kann. Insofern bestünde zunächst die Schwierigkeit, dass vom Hersteller ein positives Handeln – die Beseitigung von Software-Sicherheitslücken – verlangt würde. Es müsste daher ein „vorbeugender Beseitigungsanspruch“[473] geltend gemacht werden. [474] Die bloße Existenz eines solchen Anspruchs ist bereits umstritten[475]; mitunter wird gefordert, dass zumindest eine abgeschlossene Zuwiderhandlung und ein auf ihr beruhender Störungszustand vorliegen müsse[476]. Eine abgeschlossene Zuwiderhandlung ist aber erst dann gegeben, wenn ein Dritter bestehende Sicherheitslücken auch ausnutzt. Selbst wenn man die Existenz eines vorbeugenden Beseitigungsanspruchs annähme, so müsste – im Einklang mit der vorbeugenden Unterlassungsklage – eine Erstbegehungsgefahr nachgewiesen werden.[477] Während eine Wiederholungsgefahr bei Vorliegen einer bereits begangenen Verletzung *vermutet* wird[478], muss der Kläger die tatsächlichen Umstände, die eine Erstbegehungsgefahr begründen, im Einzelnen nachweisen, worin eine besondere Schwierigkeit liegt.[479] Der BGH stellt an einen entsprechenden Nachweis sehr hohe Anforderungen und verlangt, dass ernsthafte und greifbare tatsächliche Anhaltspunkte für eine in naher Zukunft konkret drohende Rechtsverletzung bestehen. Dabei müsse sich

---

473 Ein vorbeugender Unterlassungsanspruch würde sich dagegen gegen den unmittelbaren Täter der eigentlichen Verletzungshandlung – hier also den Hacker – richten.

474 Zur Abgrenzung von Unterlassungs- und Beseitigungsanspruch S. *Bornkamm* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 8 Rn. 1.69.

475 Ablehnend etwa *Bornkamm* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 8 Rn. 1.110; *Goldmann* in Harte-Bavendamm/Henning-Bodewig [Hrsg], UWG, 4. Aufl. 2016, § 8 Rn. 166; bejahend nur für die Fallgruppe der Zeichenanmeldungen *Büscher* in: Fezer/Büscher/Obergfell [Hrsg.], Lauterkeitsrecht: UWG, 3. Aufl. 2016, § 8 UWG Rn. 11.

476 S. *Fritzsche* in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 8 Rn. 153.

477 S. *Fritzsche* in: Münchener Kommentar zum Lauterkeitsrecht, 2. Aufl. 2014, § 8 Rn. 21.

478 Bei *Jugendgefährdende Medien auf eBay* handelte es sich um einen Fall, in dem „nur“ eine Wiederholungsgefahr bzgl. desselben Beklagten belegt werden musste; ein erster Verstoß gegen das Jugendschutzgesetz war durch das Einstellen eines Angebots jugendgefährdender Medien bereits einmal erfolgt. Zu einem solchen Verletzungsunterlassungsanspruch S. *Bornkamm* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 8 Rn. 1.40, 1.43.

479 *Bornkamm* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 8 Rn. 1.18.

die Erstbegehungsgefahr auf eine konkrete Verletzungshandlung beziehen. Die die Erstbegehungsgefahr begründenden Umstände müssten die drohende Verletzungshandlung so konkret abzeichnen, dass sich für alle Tatbestandsmerkmale zuverlässig beurteilen lasse, ob sie verwirklicht seien.[480]

In einem Szenario, in dem sich die Rechtsverletzung erst durch ein mögliches strafbares Handeln eines Dritten realisiert, wäre ein entsprechender Nachweis kaum zu führen. Bereits 2016 hatte die niederländische Verbraucherorganisation *Consumentenbond* ein Verfahren gegen *Samsung* angestrengt. Mit der Klage wollte der *Consumentenbond* insbesondere erreichen, dass *Samsung* regelmäßige Updates für seine Smartphones bereitstellt. Die *Rechtbank Den Haag* wies die Klage ab. Sie stellte fest, dass der *Consumentenbond* das von den nicht aktualisierten Smartphones ausgehende Risiko nicht konkret genug nachgewiesen habe.[481]

Das Lauterkeitsrecht in seiner aktuellen Fassung und Anwendung bietet somit grundsätzlich keine Grundlage für Ansprüche von Verbrauchern auf Software-Sicherheitsupdates.

(4) Produzentenhaftung des Herstellers (§ 823 Abs. 1 BGB i. V. m. § 1004 BGB analog)

Gem. § 823 Abs. 1 BGB[482] haftet auf Schadensersatz, wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt. Als sonstiges verletztes Recht kommt dabei grundsätzlich auch das Recht auf informationelle Selbstbestimmung infrage.[483] Selbst wenn die Gefahr noch nicht zu einer

480 BGH, Versäumnisurteil vom 10.03.2016, Az. I ZR 183/14, juris Rn. 21.

481 Rechtbank Den Haag, Urteil vom 30.05.2018, Az. C-09-525464-HA ZA 17-85, Rn. 4.16, abrufbar unter https://www.recht.nl/rechtspraak/uitspraak/?ecli=ECLI:NL:RBDHA:2018:6310 (nur auf Niederländisch erhältlich).

482 Ansprüche aus dem ProdHaftG wurden hier nicht geprüft. Voraussetzung für einen Anspruch aus dem Produkthaftungsgesetz wäre das Vorliegen einer Rechtsgutverletzung im Sinne von § 1 Abs. 1 S. 1. ProdHaftG. Dieser erfasst Schäden an Körper, Gesundheit oder Sachen, jedoch nicht an dem infrage stehenden Produkt selbst (s. § 1 Abs. 1 S. 2 ProdHaftG). Der Schutzbereich der Norm ist somit eng gefasst und erstreckt sich insbesondere nicht auf über Sachschäden hinausgehende Schäden an Eigentum, Vermögen oder immateriellen Rechtsgütern. Nach herrschender Ansicht sind auch die sog. „Weiterfresserschäden“ am fehlerhaften Produkt selbst nicht abgedeckt, S. *Förster* in: BeckOK BGB, 54. Ed., 01.05.2020, ProdHaftG § 1 Rn. 23 f.

483 S. etwa *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 295; *Raff* in: Münchener Kommentar zum BGB, 8. Aufl. 2020, § 1004 Rn. 37.

Rechtsgutsverletzung geführt hat, besteht daneben grundsätzlich ein Gefahrenabwendungsanspruch analog § 1004 Abs. 1 S. 1 BGB gegen den Hersteller.[484]

Ab dem Bekanntwerden von Sicherheitslücken in der Gerätesoftware werden die betreffenden Geräte angreifbar und damit unsicher. Typischerweise tritt hierdurch zwar unmittelbar noch kein Schaden ein. Dies wäre erst dann der Fall, wenn Dritte die bestehenden Sicherheitslücken auch ausnutzen und beispielweise private Daten ausspionieren.[485] In Literatur und Rechtsprechung ist jedoch anerkannt, dass den Hersteller[486] als eine Form der allgemeinen Verkehrssicherungspflichten nach dem Inverkehrbringen eine Produktbeobachtungspflicht[487] trifft. Er ist gehalten, in angemessenem Umfang „alles zu tun, was ihm nach den Umständen zumutbar ist, um Gefahren abzuwenden, die sein Produkt erzeugen kann."[488] Aus der Produktbeobachtungspflicht kann wiederum eine Reaktionspflicht erwachsen, soweit sich Produktfehler manifestieren.[489] Der Umfang der grundsätzlich bestehenden Gefahrenabwendungspflicht des Herstellers ist jedoch nicht klar umrissen und lässt sich nur unter Berücksichtigung aller Umstände des Einzelfalls bestimmen.[490] Je nach Fallgestaltung wurden in der Rechtsprechung insbesondere Warnhinweise[491] oder Produktrückrufe[492] für erforderlich erachtet.

---

484 Vgl. *Spindler* in: Kullmann/Pfister/Stöhr/Spindler [Hrsg.], Produzentenhaftung, 01/18, Produktverantwortung und Haftung im IT-Bereich – (7) Rückrufpflichten; Pflicht zu Patches?; zur analogen Anwendbarkeit von § 1004 BGB auf Beeinträchtigungen jeglicher absoluten Rechte bzw. des allgemeinen Persönlichkeitsrechts S. etwa *Thole* in: Staudinger [Hrsg.], BGB, Neubearbeitung 2019, § 1004 Rn. 13, 8.

485 Die Gefahrabwendungspflicht besteht auch dann, wenn sich die Gefahr erst durch Eingreifen eines Dritten realisiert, S. *Hager* in: Staudinger [Hrsg.], Das Recht der unerlaubten Handlungen, Rn. 513, unter Verweis auf BGH, Urteil vom 19.12.1989, Az. VI ZR 182/89, juris Rn. 11.

486 In Literatur und Rechtsprechung wird eine deliktische Haftung des Verkäufers insoweit nicht diskutiert; im Regelfall dürfte dieser nicht über die Mittel verfügen, unabhängig vom Hersteller die Sicherheit eines Produkts kontinuierlich zu überprüfen.

487 Die Intensität der Produktbeobachtungspflichten ist einerseits abhängig vom Umfang des drohenden Schadens und dem Grad der Gefahr, andererseits von der Möglichkeit und wirtschaftlichen Zumutbarkeit von Beobachtungsmaßnahmen, S. *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 838.

488 BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 10 m. w. N.

489 *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 840, spricht insoweit davon, dass die Produktbeobachtungspflicht letztlich bloßes „Mittel zum Zweck der Reaktion“ sei.

490 BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 13.

491 S. dazu *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 846 f. m. w. N.

492 S. dazu *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 848 ff. m. w. N.

Geht es um Software-Sicherheitslücken bei Smart-TVs oder anderen IoT-Geräten, so stellt sich die Frage, ob aus einer Produktbeobachtungspflicht eventuell eine Gefahrabwendungsverpflichtung des Herstellers erwächst und wie weit diese reicht. Grundsätzlich wird man eine Reaktionspflicht bejahen können, wenn dem Unternehmen von Nutzerseite ernstliche Sicherheitsbedenken mitgeteilt werden oder öffentlich (etwa durch das Bundesamt für Sicherheit in der Informationstechnik) vor Sicherheitslücken in der Gerätesoftware gewarnt wird.

Aus Sicht des Verbrauchers spricht vieles für die Durchführung von Software-Sicherheitsupdates als Gefahrbeseitigungsmaßnahme.[493] Updates lassen sich unkompliziert und schnell durchführen und stellen effektiv die risikofreie Nutzbarkeit des Geräts wieder her. Mit einer Update-Verpflichtung des Herstellers könnte auch vermieden werden, dass unsichere Geräte Teil von Botnetzen[494] werden können, von denen eine reelle Gefahr für Dritte ausgeht.[495]

Es ist jedoch nicht ausgeschlossen, dass die Gefahrenlage auch durch alternative Maßnahmen ausgeräumt werden könnte. Der Hersteller ist grundsätzlich frei in der Wahl der Mittel zur Beseitigung der Beeinträchtigung oder Bedrohung fremder Rechte.[496] In der Entscheidung *Pflegebetten* stellte der BGH fest, dass der Hersteller aufgrund der deliktischen Produzentenhaftung regelmäßig nur die von dem fehlerhaften Produkt ausgehenden Gefahren für die in § 823 Abs. 1 BGB

493 Ein Rückruf wäre für alle Beteiligten deutlich aufwendiger und in Anbetracht der Möglichkeit ständig neuer Sicherheitslücken kaum praktikabel. Ein Rückruf einschließlich Nachrüstung würde mutmaßlich auch von weniger Nutzern befolgt als die Nachinstallation eines Software-Updates und würde mithin nicht zu einer effektiveren Beseitigung der Gefahrenquelle führen.

494 Ein *Botnet* oder *Botnetz* ist eine Gruppe automatisierter Schadprogramme, sogenannter *Bots*. Die *Bots* (von englisch: robot „Roboter“) laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen. Der Betreiber eines Botnetzes kann dieses z. B. für den Versand von Spam-Mails oder DDos-Attacken verwenden (vgl. *Wikipedia*, Botnet, abrufbar unter https://de.wikipedia.org/wiki/Botnet).

495 Auch Smart-TVs sind in der Vergangenheit bereits in Botnetze einbezogen worden, S. etwa *DoubleVerify*, DoubleVerify Fraud Lab Identifies First Scaled CTV Botnet Attack, Pressemitteilung von DoubleVerify vom 16.11.2018, abrufbar unter https://www.doubleverify.com/newsroom/doubleverify-fraud-lab-identifies-first-scaled-ctv-botnet-attack-extending-quality-coverage-across-emerging-high-growth-channel/.

496 S. dazu *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, vor § 823 BGB Rn. 42.

genannten Rechtsgüter so effektiv wie möglich und zumutbar ausschalten müsse. Selbst bei einer Verletzung von Konstruktions-[497] oder Instruktionspflichten müsse er dem Erwerber oder Nutzer nicht ein fehlerfreies, in jeder Hinsicht gebrauchstaugliches Produkt zur Verfügung stellen.[498] Der deliktsrechtliche Schutz erfasse nicht das Äquivalenz-, sondern das Integritätsinteresse des Geschädigten. Eine kostenlose Reparatur sei nur ausnahmsweise erforderlich, wenn die Produktgefahr nicht anderweitig effektiv abgewehrt werden könne.[499] In dem entschiedenen Fall hielt der BGH einen qualifizierten Warnhinweis daher für ausreichend.[500]

Im Hinblick auf Smart-TVs oder andere IoT-Geräte wäre ebenfalls die Frage zu stellen, ob möglicherweise eine Herstellerwarnung vor bestimmten Nutzungen bereits als ausreichend angesehen werden könnte. Zwar ist der durchschnittliche Nutzer nicht in der Lage, in Reaktion auf einen Warnhinweis Software-Patches selbst zu entwickeln und so sein Gerät wieder sicher zu machen.[501] Paradoxerweise kann eine Warnung auch erst dazu führen, dass eine bestehende Sicherheitslücke in den Fokus von Hackern gerät.[502] Ein Warnhinweis könnte aber insoweit erfolgversprechend sein, als durch den Verzicht auf bestimmte nicht zentrale Funktionen die Sicherheit

---

497 Von einem sog. Konstruktionsfehler wird gesprochen, wenn ein Produkt bereits im Zeitpunkt des Inverkehrbringens schon seiner Konzeption nach unter dem gebotenen Sicherheitsstandard des Stands der Technik bleibt, S. BGH, Urteil vom 16.06.2009, Az. VI ZR 107/08, BGHZ 181, 253, Rn. 15 m. w. N. Zum Kennen bzw. Kennen müssen des Konstruktionsfehlers S. *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI (2007), Rn. 123, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2.

498 BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 18 f.

499 BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 12.

500 Da die betroffene Pflegekasse aufgrund der eigenen sozialversicherungsrechtlichen Leistungsverpflichtungen die Pflegebedürftigen vor drohenden Gefahren schützen müsse, sei zu erwarten, dass sie auf Warnhinweise reagieren und die Betten entsprechend dem Warnhinweis nachrüsten werde, S. BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 16.

501 Darüber hinaus wäre dies in urheberrechtlicher Hinsicht problematisch, S. dazu *Raue*, NJW 2017, Haftung für unsichere Software, 1841, 1842.

502 *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI (2007), Rn. 130, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2.

des betroffenen Geräts gewährleistet werden könnte.[503] Eventuell käme gar eine teilweise ferngesteuerte Außerfunktionsetzung anfälliger Software in Betracht.[504] Ferner muss man in Rechnung stellen, dass die Verpflichtung des Herstellers zur Gefahrbeseitigung unter dem Vorbehalt der Zumutbarkeit steht.[505] Schwierig zu beurteilen ist dabei in erster Linie, wie lange dem Hersteller eine Updatepflicht[506] zumutbar wäre. In der Literatur wird eine Updateverpflichtung zumindest für den Zeitraum befürwortet, in dem der Hersteller weiterhin (Geräte mit) Software mit Sicherheitslücken aktiv in den Verkehr bringt. Darüber hinaus könne dies nur im Einzelfall beurteilt werden.[507] Bei einer Einzelfallbetrachtung müsste man indessen primär die Dimension der tatsächlichen Gefährdung – insbesondere unter Berücksichtigung von Schadenswahrscheinlichkeit, Schadensausmaß, Anzahl betroffener Personen – dem Aufwand für Entwicklung und Verbreitung des konkret erforderlichen Updates gegenüberstellen.

Es lässt sich somit festhalten, dass nach aktuellem Stand der Rechtsprechung jedenfalls keine auf Deliktsrecht beruhende allgemeingültige Pflicht des Herstellers zur Versorgung mit Software-

---

503 Es wäre hingegen wahrscheinlich i. d. R. aussichtslos, an die Nutzer des betroffenen Geräts zu appellieren, dieses in Zukunft überhaupt nicht mehr zu benutzen. Wegen Unzumutbarkeit trifft die Nutzer auch keine entsprechende Verkehrspflicht, S. *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1844.

504 Zur Problematik einer im Ergebnis regelmäßig nicht zu rechtfertigenden ferngesteuerten vollständigen Produktstilllegung S. *Grünvogel u. Dörrenbächer*, Smartere Anforderungen an smarte Hausgeräte?, ZVertriebsR 2019, 87, 90 f.

505 BGH, Urteil vom 16.12.2008, Az. VI ZR 170/07, juris Rn. 15; *Förster* in: BeckOK BGB, 54. Ed., 01.05.2020, § 823 Rn. 52.

506 Nicht zu verwechseln mit der Produktbeobachtungspflicht, die sich durchaus über einen langen Zeitraum erstrecken kann, S. *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI (2007), Rn. 133 ff., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2.

507 *Grünvogel u. Dörrenbächer*, Smartere Anforderungen an smarte Hausgeräte?, ZVertriebsR 2019, 87, 89 f.; *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1844.

Sicherheitsupdates angenommen werden kann. Höchstens in – mutmaßlich seltenen – Einzelfällen[508] könnte die Bereitstellung eines solchen Updates die einzig realistische und effektive Maßnahme zur Gefahrbeseitigung darstellen.[509]

bb) Informationspflicht

Eine Pflicht des Verkäufers zur Information über die künftige (Nicht-)Bereitstellung von Software-Sicherheitsupdates könnte sich zunächst aus dem Verbrauchervertragsrecht ergeben.

(1) Verbrauchervertragsrechtliche Informationspflichten

Für Verbraucherverträge erlegt das BGB dem Unternehmer diverse Informationspflichten auf. Dies gilt sowohl beim Verkauf in einem stationären Geschäft (§ 312a Abs. 2 BGB i. V. m. Art. 246 Abs. 1 EGBG) als auch im Fernabsatz (§ 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 EGBGB). Die einschlägigen Normen erfassen erkennbar nur die am Vertrag unmittelbar beteiligten Parteien, der Hersteller wird hierdurch nicht verpflichtet. In beiden Fällen ist der Verbraucher über die „wesentlichen Eigenschaften der Waren“ zu informieren. Soweit ersichtlich, haben weder EuGH noch BGH bislang eine Definition der „wesentlichen Eigenschaften“ im Sinne von Art. 5 Abs 1 lit. a) bzw. Art. 6 Abs. 1 UAbs. 1 lit. a) Verbraucherrechte-Richtlinie[510] vorgenommen, welche die Grundlage der o. g. Vorschriften des EGBGB bildet.

Allerdings sind die genannten Vorschriften der Verbraucherrechte-Richtlinie im Wesentlichen mit Art. 7 Abs. 4 Buchstabe a) UGP-Richtlinie identisch[511]. Es ist daher davon auszugehen, dass der europäische Gesetzgeber in der vier Jahre nach der UGP-Richtlinie verabschiedeten Verbraucherrechte-Richtlinie einen zumindest weitestgehend vergleichbaren Regelungsgegenstand der identisch formulierten Normen vor Augen hatte. Art. 7 Abs. 4 Buchstabe a) der UGP-Richtlinie

---

508 Dies für mobile Updates im Ergebnis bejahend *Reusch*, Mobile Updates, BB 2019, 904, 909, ähnlich wie hier *Grünvogel u. Dörrenbächer*, Smartere Anforderungen an smarte Hausgeräte?, ZVertriebsR 2019, 87, 90 m. w. N.

509 Zwar wäre der Hersteller für eintretende Schäden aufgrund der Verletzung seiner Gefahrabwendungspflicht schadensersatzpflichtig, die Durchsetzbarkeit eines Update-Anspruchs durch einzelne Kläger wäre indessen zweifelhaft, S. *Wagner* in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 854; *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1845.

510 S. Fn. 344.

511 Die begriffliche Unterscheidung zwischen „Eigenschaften“ (Verbraucherechte-Richtlinie) und „Merkmalen“ (UGP-Richtlinie) findet sich in den anderen Sprachfassungen nicht wieder (Englisch: jeweils „main characteristics“, Französisch: „caractéristiques principales“ bzw. „principales caractéristiques“). Es dürfte sich hier schlicht um eine inkonsistente Übersetzung handeln.

hat wiederum Niederschlag gefunden in § 5a Abs. 3 Nr. 1 UWG[512]. Eine Bestimmung der Begriffe „Eigenschaften“ und „Wesentlichkeit“ kann somit auch in Anlehnung an § 5a Abs. 3 Nr. 1 UWG erfolgen. Hierfür spricht auch, dass insoweit ein weitgehender Gleichlauf der Informationspflichten im Verbraucherrecht sowie im verbraucherbezogenen Lauterkeitsrecht gewährleistet ist.[513]

In Literatur und Rechtsprechung zu § 5a Abs. 3 Nr. 1 UWG wird zumeist nicht problematisiert, was der Eigenschaftsbegriff konkret beinhaltet. Einen groben Orientierungspunkt bietet allenfalls die Aufzählung in § 5 Abs. 2 S. 1 Nr. 1 UWG[514]. Diese Vorschrift umfasst jedoch auch die Lieferung oder Beschwerdeverfahren – Aspekte, die bei der Irreführung durch Unterlassen bereits in § 5a Abs. 3 Nr. 4 UWG abgedeckt sind und daher nicht mehr unter die wesentlichen Eigenschaften subsumiert werden müssten. Dennoch steht in Anbetracht des weiten Katalogs des § 5 Abs. 2 S. 1 Nr. 1 UWG und des mit der UGP-Richtlinie und der Verbraucherrechte-Richtlinie angestrebten hohen Verbraucherschutzniveaus[515] zu erwarten, dass die Gerichte den Eigenschaftsbegriff sehr weit – über die eigentliche Wortlautgrenze des Begriffs „Eigenschaft“ hinaus – auslegen werden. Vor diesem Hintergrund ließe sich mutmaßlich auch die (Nicht-)Erwartbarkeit von Software-Sicherheitsupdates als Eigenschaft einstufen. Sicherheitslücken eines Produkts (bzw. dessen Software) dürften ohnehin unstreitig eine Eigenschaft darstellen.

Geht man von einer weiten Interpretation des Eigenschaftsbegriffs aus, kommt dem Kriterium der „Wesentlichkeit“ entscheidende Bedeutung zu. Die Wesentlichkeit einer Eigenschaft bemisst sich danach, ob der angesprochene Durchschnittsverbraucher deren Mitteilung billigerweise erwarten darf, um eine informierte geschäftliche Entscheidung treffen zu können.[516] Naturgemäß kann dies

---

512 Für den speziellen Fall der Aufforderung zum Kauf.

513 Vgl. dazu Leitfaden der GD Justiz vom Juni 2014 zur Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25.10.2011 über die Rechte der Verbraucher, S. 21, abrufbar unter https://ec.europa.eu/info/sites/info/files/crd_guidance_de_updated.pdf, Leitlinien der Kommission vom 25.05.2016 zur Umsetzung/Anwendung der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken – COM 2016 (320) final, S. 22 f., abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016SC0163&from=EN.

514 Dessen Wortlaut entspricht Art. 6 Abs. 1 UAbs. 1 lit. b) der UGP-Richtlinie.

515 S. etwa Erwägungsgründe 7 und 65 sowie Art. 1 der Verbraucherrechte-Richtlinie und Erwägungsgründe 5, 11 und 23 sowie Art. 1 der UGP-Richtlinie.

516 Vgl. BGH, Beschluss vom 15.12.2016, Az. I ZR 241/15, juris Rn. 16.

nur im Rahmen einer Einzelfallbetrachtung beurteilt werden.[517] Das OLG Köln hat in einem Verfahren der *Verbraucherzentrale Nordrhein-Westfalen* gegen *Media Markt*[518] eine Informationspflicht über den Sicherheitsstand der Gerätesoftware und die Verfügbarkeit von Updates abgelehnt. Die Entscheidung betraf Smartphones, kann aber für andere IoT-Geräte, also auch Smart-TVs, gleichermaßen herangezogen werden. Eine „wesentliche Eigenschaft" i. S. d. § 246 Abs. 1 Nr. 1 EGBGB sei im Rahmen der Einzelfallprüfung aus den gleichen Gründen abzulehnen wie das Vorliegen einer „wesentlichen Information" i. S. d. § 5a Abs. 2 S. 1 UWG.[519] Es ist einerseits bemerkenswert, dass das Gericht insoweit eine inhaltsgleiche Prüfung ausreichen lässt.[520] Andererseits erscheint es grundsätzlich nachvollziehbar, auch bei der Beurteilung der Informationspflichten im Rahmen von § 312a Abs. 2 BGB i. V. m. Art. 246 Abs. 1 EGBG bzw. § 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 EGBGB ein Korrektiv zugunsten des Unternehmers zuzulassen wie es etwa in Art. 246 Abs. 1 Nr. 8 EGBG[521] und Art. 246a § 1 Abs. 1 S. 1 Nr. 15 EGBGB[522] vorgesehen ist. Es lässt sich daher vertreten, dass in analoger Anwendung der betreffenden Vorschriften eine Pflicht zur Information des Verbrauchers über wesentliche Eigenschaften der angebotenen Waren oder Dienstleistungen insoweit nicht besteht, wie der Unternehmer hiervon keine Kenntnis hat und diese auch nicht vernünftigerweise haben müsste.[523] Die

---

517 S. auch *Busch* in: BeckOGK, Stand 01.07.2019, Art. 246 EGBGB Rn. 18.

518 Beklagte in dem Fall war die *Media Markt TV-HiFi-Elektro GmbH Köln Hohe Straße.*

519 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 78.

520 Das OLG wendet so im Ergebnis die Rechtsprechung des BGH zu „wesentlichen Informationen" auf „wesentliche Eigenschaften" an. Es ist allerdings nicht geklärt, ob den Unternehmerinteressen bei Auslegung des Begriffs der wesentlichen Eigenschaften ein gleichermaßen starkes Gewicht zukommen sollte, zumal es sich auch in den jeweiligen europäischen Richtlinientexten um unterschiedliche Begriffe handelt. Art. 7 Abs. 1 der UGP-Richtlinie spricht von einer „wesentlichen Information" (Englisch: „material information", Französisch: „information substantielle"), Art. 5 Abs. 1 lit. a) der Verbraucherrechte-Richtlinie hingegen von „wesentlichen Eigenschaften" (Englisch: „main characteristics", Französisch: „principales caractéristiques"). Der EuGH hat in den Rechtssachen *Konsumentenombudsmannen/Ving Sverige AB* und *Verband Sozialer Wettbewerb e. V./DHL Paket GmbH* jeweils eine wesentliche Eigenschaft bejaht und eine Korrektur insbesondere im Hinblick auf die in Art. 7 Abs. 1 UGP-Richtlinie vorgesehene Gesamtbetrachtung vorgenommen, S. EuGH, Urteil vom 12.05.2011, Az. C-122/10, EU:C:2011:299, Rn. 52 ff. – *Konsumentenombudsmannen/Ving Sverige AB;* EuGH, Urteil vom 30.03.2017, Az. C-146/16, EU:C:2017:243, Rn. 26 – *Verband Sozialer Wettbewerb e. V./DHL Paket GmbH*.

521 Basierend auf dem wortgleichen Art. 5 Abs. 1 lit. h) der Verbraucherrechte-Richtlinie.

522 Basierend auf dem wortgleichen Art. 6 Abs. 1 UAbs. 1 lit. s) der Verbraucherrechte-Richtlinie.

523 Ähnlich das LG Köln, welches mit dieser Argumentation jedoch bereits das Vorliegen einer wesentlichen Eigenschaft verneinte, S. LG Köln, Urteil vom 30.04.2019, Az. 31 O 133/17, juris Rn. 37.

Kernfrage ist daher, ob der Verkäufer sich beim Hersteller über den Sicherheitsstand der verkauften Geräte erkundigen bzw. diesbezüglich zumindest angemessene Anstrengungen unternehmen muss. Wie unter (2) weiter ausgeführt wird, hat das OLG Köln dies in der Entscheidung *Verbraucherzentrale Nordrhein-Westfalen gegen Media Markt* abgelehnt. Den Unternehmerinteressen wird nach der aktuellen Rechtsprechung somit ein hoher Wert beigemessen; eine Klärung durch den EuGH ist derzeit nicht absehbar.

Die Durchsetzung einer Informationspflicht des Verkäufers auf der Grundlage von § 312a Abs. 2 BGB i. V. m. Art. 246 Abs. 1 EGBG (bzw. im Fernabsatz § 312d Abs. 1 BGB i. V. m. Art. 246a § 1 Abs. 1 EGBGB) erscheint daher momentan wenig aussichtsreich.

(2) Lauterkeitsrechtliche Informationspflichten

Es gibt zwei unterschiedliche Ansatzpunkte für mögliche lauterkeitsrechtliche Informationspflichten des Verkäufers. Zum einen die Nichtinformation des Verbrauchers über Software-Sicherheitslücken, die (insbesondere bei älteren Smart-TVs) bereits im Verkaufszeitpunkt bestehen können. Zum anderen die Nichtinformation des Verbrauchers darüber, dass ein verkaufter Smart-TV nicht mehr mit Sicherheitsupdates versorgt wird. Beides könnte eine Irreführung durch Unterlassen gem. § 5a Abs. 2 S. 1 UWG darstellen. Eine solche Irreführung begeht, „wer im konkreten Fall unter Berücksichtigung aller Umstände dem Verbraucher eine wesentliche Information vorenthält, die dieser je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und deren Vorenthalten geeignet ist, ihn zu einer geschäftlichen Entscheidung zu veranlassen, die er anderenfalls nicht getroffen hätte."

Haftung des Verkäufers im Einzelhandel

Das OLG Köln hatte in dem Verfahren der Verbraucherzentrale Nordrhein-Westfalen gegen *Media Markt* den Fall zu beurteilen, dass das Unternehmen im Juli 2016 Smartphones mit dem damals nicht mehr aktuellen[524] Betriebssystem *Android* 4.4 vertrieben hatte. Zwei zu Testzwecken erworbene Smartphones hatten eine bzw. 15 schwere Sicherheitslücken aufgewiesen. *Media Markt* hatte weder über die bestehenden Sicherheitslücken noch darüber informiert, dass für die betreffenden Smartphones keine Sicherheitsupdates mehr zu erwarten waren.

---

[524] Zum damaligen Zeitpunkt aktuell waren seit Veröffentlichung von Android 4.4 zwölf Android-Updates/Upgrades erschienen, zuletzt Android 6.0.1; Android 7.0 wurde einen knappen Monat später veröffentlicht, s. *Wikipedia*, Liste von Android-Versionen, abrufbar unter https://de.wikipedia.org/wiki/Liste_von_Android-Versionen.

Das OLG Köln wies die Klage ab. In seiner Begründung stellte es darauf ab, dass die vorenthaltene Information für den Verbraucher nicht „wesentlich“ sei.[525] Zwar ging das Gericht zunächst davon aus, dass die Information über das Vorliegen von Sicherheitslücken und die Nichtbereitstellung von Sicherheitsupdates für den Verbraucher von großer Bedeutung sei. Durch Sicherheitslücken könnten Daten des Verbrauchers bei der Nutzung des Smartphones erlangt werden, was eine erhebliche Verletzung dessen Privatsphäre bedeuten könne. Auch könnten die erlangten Daten zu betrügerischen Zwecken missbraucht und der Verbraucher hierdurch massiv geschädigt werden.[526] Im Rahmen der Prüfung, ob einer vorenthaltenen Information wesentliche Bedeutung zukommt, ist jedoch nach ständiger Rechtsprechung des BGH eine Abwägung der Interessen von Unternehmer und Verbraucher vorzunehmen.[527] Das OLG Köln stellte in diesem Zusammenhang sinngemäß fest, dass ein Unternehmer zur Beurteilung des Sicherheitsstandards bei jedem einzelnen Smartphone umfangreiche Tests durchführen müsse.[528] Ob ein Gerät Sicherheitsupdates erhalte, sei dem Verkäufer im Verkaufszeitpunkt in der Regel nicht bekannt. Die entsprechenden Informationen könnten sich zudem ständig ändern.[529] Vor diesem Hintergrund hielt das Gericht es für unverhältnismäßig, dem Unternehmer eine Informationspflicht gegenüber dem Verbraucher aufzuerlegen, wie die Verbraucherzentrale Nordrhein-Westfalen sie gefordert hatte. Die Informationen zu bestehenden Sicherheitslücken und der Nichtbereitstellung von Sicherheitsupdates erachtete es infolgedessen als nicht wesentlich. Des Weiteren wertete das OLG Köln das Verhalten von *Media Markt* auch nicht als „Vorenthalten“ von Informationen. Die betreffenden Informationen gehörten weder zum Geschäfts- und Verantwortungsbereich des Unternehmers noch seien sie für diesen zumutbar beschaffbar.[530]

---

525 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 65.

526 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 69.

527 S. dazu *Köhler* in: Köhler/Bornkamm/Feddersen [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 38. Aufl. 2020, § 5a Rn. 3.11 m. w. N. In sprachlicher Hinsicht erscheint es zwar zweifelhaft, die Wesentlichkeit für den Verbraucher in Abhängigkeit von Interessen des Unternehmers zu bestimmen. Die Notwendigkeit einer Berücksichtigung der Unternehmerinteressen ist unter Verhältnismäßigkeitsgesichtspunkten jedoch geboten und könnte alternativ auch bei den Tatbestandsmerkmalen „im konkreten Fall unter Berücksichtigung aller Umstände“ sowie „Vorenthalten“ verortet werden. Kritisch insoweit auch *Obergfell* in: Fezer/Büscher/Obergfell [Hrsg.], Lauterkeitsrecht: UWG, 3. Aufl. 2016, § 5a Rn. 76.

528 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 70.

529 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 73.

530 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 74.

Die Argumentation des OLG Köln ist insoweit bemerkenswert, als das Gericht selbst bzgl. eines Smartphones, welches 15 Sicherheitslücken aufwies und dem das BSI ein „eklatantes Sicherheitsrisiko“ bescheinigte, jegliche Informationspflicht verneinte. Da Smartphones nicht nur zum Telefonieren genutzt werden, sondern der Verbraucher typischerweise auch sensible Daten auf dem Gerät oder über das Gerät verarbeitet (z. B. zur Nutzung seines Terminkalenders oder von Fitness-Apps), ist die Eignung eines eklatant unsicheren Smartphones für die gewöhnliche Verwendung durchaus diskutabel. Eine Prüf- und Informationspflicht des Verkäufers zumindest bei älteren Gerätemodelle, die öffentlich bekannte Sicherheitsmängel aufweisen, erscheint – auch unter dem Gesichtspunkt des hierfür notwendigen Rechercheaufwands – für den Verkäufer nicht unzumutbar. Es erschiene daher durchaus vorstellbar, in solchen Fällen die Unsicherheit des Geräts selbst als wesentliche Eigenschaft einzustufen, über die der Verbraucher informiert werden müsste.[531]

Es steht zu vermuten, dass das OLG Köln den Sachverhalt anders beurteilen würde, wäre die Warenkaufrichtlinie[532] in Deutschland bereits umgesetzt und anwendbar. So weist das Gericht in seinem Urteil darauf hin, dass dem Verkäufer nach der Warenkaufrichtlinie gerade bis zum 01.01.2022 Zeit gegeben werden soll, sich auf die neue Rechtslage einzustellen.[533] Obgleich die Warenkaufrichtlinie in erster Linie das Kaufrecht betrifft, kann sie doch maßgeblichen Einfluss darauf haben, was der Verbraucher von der Kaufsache erwarten darf. Man wird insofern davon ausgehen dürfen, dass es dem Unternehmer angesichts der neuen Rechtslage eher möglich und daher zuzumuten sein wird, sich bzgl. der Planung von Software-Sicherheitsupdates umfassend zu informieren. Es ist auch nicht unwahrscheinlich, dass von Herstellerseite entsprechende Informationen regelmäßig zum Abruf bereitgestellt werden.

Haftung des Herstellers

Im Gegensatz zum Einzelhändler ist der Hersteller ohne Weiteres in der Lage, bei seinen IoT-Geräten Sicherheitsaspekte und Update-Notwendigkeit regelmäßig zu prüfen und hierüber zu informieren. Angaben zu Updates und Updatezeiträume haben unmittelbaren Verbraucherbezug, da sie für die Einschätzung der Langlebigkeit der verkauften Produkte hohe Relevanz haben.

---

531 Man kann auch davon ausgehen, dass bei eklatant unsicheren Geräten eine Verkehrserwartung bzgl. einer Aufklärung besteht, vgl. dazu *Sosnitza* in Ohly/Sosnitza [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 7. Auflage, § 5a Rn. 55 f.

532 S. Fn. 459.

533 OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19, juris Rn. 76.

Soweit der Hersteller hierzu keine oder lückenhafte Angaben veröffentlicht, stellt dies eine geschäftliche Handlung gegenüber dem Verbraucher dar (in Form des Unterlassens)[534]. Da die Update-Informationen dem Geschäfts- und Verantwortungsbereich des Unternehmers zuzurechnen bzw. von diesem im Regelfall beschaffbar sind, kann auch ein „Vorenthalten“ dieser Informationen bejaht werden. Die Informationen sind auch nötig, damit der Verbraucher eine informierte geschäftliche Entscheidung treffen kann (§ 5a Abs. 2 S. 1 Nr. 1 UWG). Ob das Vorenthalten schließlich auch geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte (§ 5a Abs. 2 S. 1 Nr. 2 UWG), bedarf der Klärung im konkreten Fall. Eine Irreführung durch Unterlassen ließe sich jedenfalls bzgl. Geräten annehmen, die bereits mit Sicherheitslücken in den Verkehr kommen oder bei denen keine Sicherheitsupdates geplant sind oder wenn die Versorgungsphase mit Updates deutlich hinter der Lebenserwartung des Produkts zurückbleibt. Zumindest bei höherpreisigen Produkten kann durchaus von der Verbrauchervorstellung ausgegangen werden, dass eine angemessene Versorgung mit Sicherheitsupdates stattfindet.

Vor diesem Hintergrund erscheint es somit zumindest möglich, eine lauterkeitsrechtliche Informationsverpflichtung des Herstellers über die Updatepolitik für einzelne Gerätemodelle anzunehmen. Bei Bejahung einer solchen lauterkeitsrechtlichen Update-Informationsverpflichtung stellen sich naturgemäß einige Folgefragen. Mangels konkreter gesetzlicher Vorgaben müssten die Gerichte insbesondere klären, wie lange nach Inverkehrbringen der Hersteller über den verbleibenden Mindestzeitraum für Aktualisierungen informieren muss.[535] Vorstellbar wären zum einen fixe Zeitspannen, zum anderen aber auch Zeiträume, die sich an der Lebensdauer des Produkts ori-

---

534 Der Verbraucherbezug ist in Unterlassensfällen zu bejahen, sofern die unterlassene Pflicht – wie bei der Nichtbereitstellung von Software-Updates für Massen-IoT-Produkte der Fall – Verbrauchern geschuldet war, s. *Podszun* in Harte-Bavendamm/Henning-Bodewig [Hrsg], UWG, 4. Aufl. 2016, § 3 UWG, Rn. 20.

535 In dem oben auf S. 192 angesprochenen Gerichtsverfahren der niederländischen Verbraucherorganisation *Consumentenbond* gegen *Samsung* hatte es die Rechtbank Den Haag ausreichen lassen, dass *Samsung* die aktuellen Updateintervalle – ohne Angabe eines verbleibenden Mindestzeitraums für Updates – kommuniziert , S. Urteil der Rechtbank Den Haag vom 30.05.2018, Az. C-09-525464-HA ZA 17-85, Rn. 2.16, 4.20 f., abrufbar unter https://www.recht.nl/rechtspraak/uitspraak/?ecli=ECLI:NL:RBDHA:2018:6310 (nur auf Niederländisch erhältlich).

entieren. Es ist schließlich zu beachten, dass Ansprüche nach dem UWG vom einzelnen Verbraucher bisher nicht geltend gemacht werden können, sondern allenfalls von Verbraucherverbänden[536].

3. Reichweite von Garantien

Das Bundeskartellamt hat von den Unternehmen Garantiebestimmungen angefordert, um zu überprüfen, ob und ggf. inwieweit Verbrauchern über die gesetzlichen Vorschriften hinaus Leistungen gewährt werden.

a) Ermittlungsergebnisse

Insgesamt gewähren 18 der befragten 21 Unternehmen dem Verbraucher eine solche freiwillige Garantie. Die Garantiedauer betrug bei 13 Unternehmen zwei Jahre, also ebenso lange wie die geltende Gewährleistungsfrist. Bei 3 Unternehmen hing die Garantiefrist von Modell bzw. Verkaufsmodalitäten ab und betrug je nachdem 2 oder 3 Jahre. Nur zwei Unternehmen gaben eine Garantie für 3 Jahre ab.

Von den 18 freiwilligen Garantieerklärungen enthielten 9 einen Hinweis auf die gesetzlichen Rechte des Verbrauchers sowie darauf, dass diese durch die Garantie nicht eingeschränkt werden. Bei weiteren 6 Garantieerklärungen wurde nur auf den Nichtausschluss der gesetzlichen Gewährleistung verwiesen. In drei Fällen fehlte ein entsprechender Hinweis vollständig.

Aus den Ermittlungsergebnissen der Erstbefragung hatte sich der Eindruck ergeben, dass einige Unternehmen mit ihren Garantiebestimmungen nur Hardwaremängel abdecken wollten. Unzulänglichkeiten der Software können für den Verbraucher jedoch gleichermaßen einschneidend sein. Einerseits können Softwaremängel zur Beeinträchtigung des Funktionsumfangs führen. Andererseits besteht die Gefahr, dass es zu Datenverlusten und/oder Fremdzugriffen auf – unter

536 § 8 Abs. 3 Nr. 3 UWG i. V. m. § 4 Abs. 1 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen in der Fassung der Bek. v. 27.08.2002 (BGBl. I S. 3422, 4346), zuletzt geändert durch Art. 4 des Gesetzes v. 17.07.2017 (BGBl. I S. 2446) – Unterlassungsklagengesetz (UKlaG). Im Rahmen des „New Deal for Consumers“ wurden Ende 2019 unter anderem Änderungen in der Richtlinie über unlautere Geschäftspraktiken beschlossen, die von den Mitgliedstaaten verlangen, bis Mai 2022 wirksame Rechtsbehelfe für Verbraucher einzuführen, die durch unlautere Geschäftspraktiken geschädigt wurden (vgl. Artikel 3 Ziffer 5 der Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union, Abl. EU Nr. L 328 vom 18.12.2019, S. 7).

Umständen sensible – Daten kommt. Bei der Zweitbefragung hat das Bundeskartellamt die Unternehmen daher ausdrücklich danach befragt, ob die gewährte Garantie neben Hardwarekomponenten auch für Software gilt.

11 der 18 garantiegebenden Unternehmen gewährten nach eigenen Angaben eine Garantie sowohl auf die Hardwarekomponenten[537] als auch auf die (mutmaßlich gesamte) Software des Smart-TVs.

2 Unternehmen gaben ihren Angaben zufolge eine Garantie ausschließlich auf Hard- und nicht auf Software. Nur bei einem dieser Unternehmen kam dies auch in den Garantiebedingungen eindeutig zum Ausdruck.

5 Unternehmen sahen neben Hardwaremängeln Softwarefehler nur dann als von der Garantie umfasst an, wenn die Software nicht von Dritten[538] stammt. Jedoch wird diese Unterscheidung in keiner der Garantiekarten/-bestimmungen explizit getroffen. Der eine Teil der Garantiebedingungen enthält gar keinen Ausschluss von Softwarefehlern, der andere Teil hingegen schließt sämtliche Softwarefehler aus.

Bei drei Garantieerklärungen fiel auf, dass die Unterscheidung zwischen gesetzlicher Gewährleistung und vertraglicher Garantie nicht sauber getroffen wurde.

In zwei Fällen wurden z. T. weitreichende Einschränkungen der „Gewährleistung“ formuliert.[539]

b) Rechtliche Würdigung

Die den Verkäufer treffende gesetzliche Gewährleistung für Produktmängel oder das Vorhandensein zugesicherter Eigenschaften greift bis 24 Monate nach dem Kauf eines neuen Produkts ein.[540] Die Garantie für ein Produkt ist hingegen nicht gesetzlich vorgeschrieben. Sie ist eine freiwillige Leistung des Herstellers (Herstellergarantie), des Händlers (Händlergarantie) oder eines

---

537 Zwei kleinere Hersteller schlossen Display- bzw. Rahmenbruch von der Garantie aus, bei den anderen Unternehmen erfolgte keinerlei Ausschluss von Hardwarekomponenten.

538 Je nach Konfiguration des Fernsehers können z. B. Webbrowser, App-Portal oder Apps von Dritten stammen.

539 Von einem Unternehmen, welches keinerlei Garantie anbot und von einem Unternehmen, welches in seinen Garantiekarten mutmaßlich versehentlich den Begriff „Gewährleistung“ anstelle von „Garantie“ benutzte.

540 Während der ersten sechs Monate der Gewährleistungsfrist gilt in Deutschland zugunsten des Verbrauchers grundsätzlich eine Beweislastumkehr, d. h. es wird vermutet, dass ein Sachmangel bereits bei Gefahrübergang vorlag (§ 477 BGB).

Dritten[541]. Bei der Garantie können Hersteller oder Händler selbst entscheiden, was die Garantie abdeckt und wie lange sie gilt. In diesem Rahmen haftet der Garantiegeber für die versprochene Beschaffenheit und ggf. sonstige Anforderungen (§ 443 Abs. 1 BGB) bzw. Haltbarkeit (§ 443 Abs. 2 BGB). Eine Haltbarkeitsgarantie greift auch in Fällen ein, in denen ein Mangel erst nach Gefahrübergang eintritt.[542]

Der Garantievertrag kommt durch ein Angebot des Garantiegebers (vorliegend also des Herstellers) und dessen Annahme durch den Garantienehmer zustande. Die Annahme muss dabei nicht erklärt werden, da die Beifügung der Garantieerklärung zum Produkt als Angebot unter Verzicht auf den Zugang einer Annahmeerklärung des Kunden nach § 151 BGB anzusehen ist.[543] Das Angebot des Garantiegebers ist dabei, wie jede empfangsbedürftige Willenserklärung im deutschen Zivilrecht, so auszulegen, wie der Empfänger die ihm zugegangene Äußerung nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte verstehen durfte (§§ 133, 157 BGB).[544]

Legt man diesen Maßstab zugrunde, so ist zunächst festzustellen, dass durchweg keine Haltbarkeitsgarantien vorlagen. Ein entsprechender Garantiewille, der auch nach dem Kauf auftretende Softwaremängel abgedeckt hätte, war den Garantieerklärungen der untersuchten Hersteller nicht zu entnehmen. Der Kunde kann sich daher insbesondere dann nicht auf die Garantie berufen, wenn sich Softwarefehler manifestieren, die zum Kaufzeitpunkt noch nicht bekannt waren (und die deshalb auch keinen Sachmangel darstellen).

In drei Garantieerklärungen kam der (von den Unternehmen jeweils behauptete) Garantieausschluss für Drittsoftware nicht zum Ausdruck. Bei Auslegung nach dem objektiven Empfängerhorizont ist ein solcher Ausschluss daher nicht Bestandteil des Garantieangebots des Garantiegebers. Der Kunde kann somit auch bei (anfänglichen) Softwaremängeln seine Rechte aus dem abgeschlossenen Garantievertrag einfordern und durchsetzen. Ein bloß einseitiger Vorbehalt des Garantiegebers ist insoweit irrelevant.

In drei der untersuchten Herstellergarantieerklärungen fehlte der Hinweis auf die gesetzlichen Rechte des Verbrauchers sowie darauf, dass sie durch die Garantie nicht eingeschränkt werden. Dies stellt einen Verstoß gegen § 479 Abs. 1 S. 2 Nr. 1 BGB dar. Dieser erfordert eine Klarstellung, dass die gesetzlichen Rechte des Verbrauchers durch die Garantie nicht eingeschränkt werden. Die in fünf Erklärungen enthaltene Formulierung, dass die Garantie nicht die gesetzliche

---

541 S. *Faust* in: BeckOK BGB, 54. Ed., 01.05.2020, § 443 BGB Rn. 12.

542 S. *Faust*, a. a. O. (vorhergehende Fußnote), Rn. 14

543 Vgl. *Westermann* in: Münchener Kommentar zum BGB, 8. Aufl. 2019, § 443 Rn. 6.

544 S. *Ellenberger* in: Palandt, Bürgerliches Gesetzbuch, 79. Aufl. 2020, § 133 Rn. 9 m. w. N.

Gewährleistung ausschließe, ist ebenfalls nicht ausreichend. Denn neben der gesetzlichen Gewährleistung bleibt insbesondere die Produkthaftung oder allgemeine deliktische Haftung als Anspruchsgrundlage gegen den Hersteller unberührt.

Der fehlende oder fehlerhafte Hinweis kann dazu führen, dass bei dem Verbraucher der Eindruck entsteht, er habe nur die in der Garantieerklärung definierten Ansprüche, und er so von der Geltendmachung bestehender Rechte abhalten wird. Da es sich bei § 479 Abs. 1 S. 2 Nr. 1 BGB um eine Marktverhaltensregel handelt, stellt deren Verletzung gleichzeitig einen Verstoß gegen § 3a UWG dar.[545]

In zwei Fällen lag auch eine Verletzung von § 5 Abs. 1 Nr. 7 UWG vor. Diese Vorschrift greift ein bei einer Täuschung oder bei zur Täuschung geeigneten Angaben über Rechte des Verbrauchers, insbesondere solchen auf Grund von Garantieversprechen oder Gewährleistungsrechten bei Leistungsstörungen.[546] Da es sich bei der Herstellergarantie um eine freiwillige Leistung handelt, ist es grundsätzlich möglich, diese einzuschränken. Es ist daher beispielsweise zulässig, sämtliche Software oder Software Dritter aus der Garantie auszunehmen. Eine Irreführung des Verbrauchers kann aber darin liegen, dass falsche Aussagen zu den Gewährleistungsrechten getroffen und diese mutmaßlich eingeschränkt oder ausgeschlossen werden.[547] Dies war in zwei Garantieerklärungen der Fall.

4. Nichtlöschbarkeit vorinstallierter Software

Wie andere IoT-Geräte auch (insbesondere Smartphones und Tablets) werden Smart-TVs oftmals mit vorinstallierter Software ausgeliefert, die sich vom Verbraucher nicht entfernen lässt. Bedenklich ist dies insbesondere bei Dritt-Apps, für deren feste Integration in den Fernseher keine technische Notwendigkeit besteht und an deren Verwendung der Verbraucher unter Umständen überhaupt kein Interesse hat.

a) Ermittlungsergebnisse

Die Praxis der Hersteller in Bezug auf die Vorinstallation von Software und deren Löschbarkeit durch den Nutzer ist nach den Ermittlungsergebnissen sehr unterschiedlich. Bei den Herstellern, die sich webbasierter TV-Portale bedienen, stellt sich die Frage einer „Deinstallation“ von Apps

---

545 Vgl. BGH, Urteil vom 14.04.2011, Az. I ZR 133/09, juris Rn. 22.

546 Die in § 5 Abs. 1 S. 1 UWG vorausgesetzte „geschäftliche Entscheidung“ des Verbrauchers läge in den vorliegenden Fällen darin, aufgrund der irreführenden Angaben gesetzliche Gewährleistungsrechte nicht geltend zu machen, vgl. *Keller* in Harte-Bavendamm/Henning-Bodewig [Hrsg], UWG, 4. Aufl. 2016, § 2 Rn. 320.

547 Vgl. *Diekmann* in: Ullmann [Hrsg.], jurisPK-UWG, 4. Aufl. 2016, § 5 Rn. 783.

von vornherein nicht, weil diese dort schon nicht auf dem Fernseher selbst installiert werden, sondern der Fernseher im Wesentlichen nur einen Link zum Web-TV-Portal aufruft. Bei den anderen Herstellern ist die Vorinstallation einer erheblichen Anzahl von Dritt-Apps jedoch der Regelfall, wohingegen unternehmenseigene Apps seltener und weniger zahlreich sind. Einige dieser Hersteller ermöglichen nach eigenen Angaben dem Verbraucher das vollständige Löschen der vorinstallierten Apps. Teilweise sind einzelne Apps hiervon ausgenommen, z.B. solche die einen eigenen „Button" auf der Fernbedienung des Fernsehers erhalten haben. Andere Hersteller, insbesondere *Sony*, schließen eine Deinstallation aus, ermöglichen aber eine Deaktivierung[548] der Programme. Bei *Samsung* als dem größten Anbieter im Markt sind Dritt-Apps durchgehend weder deinstallierbar noch deaktivierbar.

Auf die Frage nach den Gründen für die fehlende Löschbarkeit von Software gaben einige Hersteller an, dass diese sehr eng mit dem Betriebssystem verbunden oder notwendig für das Funktionieren des Fernsehgeräts sei. Eine Deinstallation oder Deaktivierung sei daher technisch nicht möglich. Naturgemäß kommt eine Deinstallation oder auch nur Deaktivierung von (System-)Software grundsätzlich nicht in Betracht. Allerdings gibt es bei einigen Herstellern vorinstallierte Softwarekomponenten, die nicht als Apps ausgestaltet sind, aber ebenso wie Apps Zusatzfunktionen bereitstellen und nicht im engeren Sinne systemrelevant sind. Zu nennen wären hier etwa Sprachassistenten oder Empfehlungsdienste. Bei den Apps stellen wirklich systemrelevante Programme den absoluten Ausnahmefall dar. Zumindest eine Deaktivierungsmöglichkeit ließe sich in der Regel ohne übermäßigen technischen Aufwand einrichten. Grundsätzlich wäre es auch möglich, die Gerätesoftware so einzurichten, dass nicht systemrelevante Apps einzeln deinstalliert werden können. Auffällig ist, dass etliche Apps bei den Geräten einiger Hersteller deinstalliert werden können, bei anderen hingegen nicht. Bei *LG* etwa werden sämtliche Apps von Drittanbietern nicht auf den Smart-TVs vorinstalliert, sondern dem Nutzer zunächst lediglich als Link-Icon zum Download angeboten. Die heruntergeladenen Apps können vom Nutzer ohne Weiteres auch wieder deinstalliert werden. Von *Sony* werden für die Beschränkung auf die Deaktivierung Sicherheitsgründe geltend gemacht. Die Originalversion würde in einem dem Nutzer nicht zugänglichen Bereich gespeichert, um Änderungen durch unbefugte Dritte zu verhindern.

---

548 Deaktivierung ist in dem Sinne zu verstehen, dass eine App zwar auf dem Gerät installiert bleibt, jedoch keinerlei Aktivitäten entfaltet, nicht aktualisiert wird, in der Standard-Nutzeroberfläche nicht mehr auftaucht und vor einer Nutzung in einem separaten Schritt erst wieder reaktiviert werden müsste. Die Deaktivierung von Apps ist vor allem aus dem Bereich der Smartphones bekannt, wo häufig vorinstallierte Apps nicht vollständig deinstalliert, sondern nur deaktiviert werden können. Im Hinblick auf Gerätesicherheit und Datensouveränität ist das Deaktivieren nicht systemrelevanter Apps gegenüber der Deinstallation die schlechtere Lösung.

Aus den Antworten mancher Hersteller ist aber auch ersichtlich, dass es wirtschaftliche Gründe für den Ausschluss der Löschbarkeit gibt. So wird etwa darauf verwiesen, dass es sich um Anwendungen von „Schlüsselpartnern“ handele. Insoweit ist zu beachten, dass die Hersteller regelmäßig über Revenue Sharing Agreements oder auf andere Weise an den mit einer vorinstallierten App erzielten Erlösen beteiligt werden. Dies erhöht den Anreiz, die Verfügbarkeit solcher Apps langfristig zu sichern und sie dem Nutzer auf der Benutzeroberfläche zu präsentieren.

b) Rechtliche Würdigung

Die fehlende Löschbarkeit vorinstallierter Apps kann zu einer relevanten Beeinträchtigung von Verbraucherinteressen führen. Eine aktuelle Befragung zu vorinstallierten Apps auf Smartphones hat gezeigt, dass die Mehrheit der Befragten den überwiegenden Teil der ab Werk enthaltenen Apps nicht nutzt und es wichtig findet, diese entfernen zu können.[549] Zwar sind einige der Punkte, die zu der kritischen Haltung der Verbraucher führen, vorliegend nicht in gleicher Weise relevant. So haben die Belegung von Speicherplatz oder ein erhöhter Strom- und Datenvolumenverbrauch nicht die gleiche Bedeutung wie bei mobilen Endgeräten. Aber auch hier kann die Nichtentfernbarkeit nicht gewünschter Software nicht nur die Bedienung stören, sondern auch ein Sicherheitsrisiko und eine Beeinträchtigung des Datenschutzes bedeuten. Ein Sicherheitsrisiko kann insbesondere dann entstehen, wenn die nicht genutzte Software nicht oder nicht im erforderlichen Umfang aktualisiert wird. Datenschutz rechtlich wäre es zudem bedenklich, wenn es unabhängig von einer Aktivierung und Einwilligung zu Datenübertragungen kommen würde.

Im letztgenannten Fall, für den die vorliegende Untersuchung allerdings keine konkreten Anhaltspunkte festgestellt hat, würde ein Verstoß gegen die Bestimmungen der DSGVO vorliegen, für den sich die Frage der Verantwortlichkeit des Herstellers stellen würde (hier sowohl datenschutz- als auch lauterkeitsrechtlich i. d. R. zu verneinen, siehe unter E. V. 3. b) aa) (1), S. 156 bzw. E. V. 3. b) cc), S. 167.). Auch ansonsten dürfte die fehlende Löschbarkeit höchstens in Ausnahmefällen rechtliche Konsequenzen haben. Ein Sachmangel liegt bei Fehlen einer anderweitigen Vereinbarung nur vor, wenn der Smart-TV sich für die gewöhnliche Verwendung nicht eignet oder nicht die übliche und vom Käufer erwartbare Beschaffenheit aufweist (§ 434 Abs. 1 S. 2 Nr. 2 BGB). Eine Mangelhaftigkeit wird danach nur anzunehmen sein, wenn wesentliche Funktionen oder die grundlegende Gerätesicherheit beeinträchtigt werden; die bloße „Lästigkeit“ der

549 Vgl. *Verbraucherzentrale Bundesverband e.V. (vzbv)*, Vorinstallierte Apps auf Smartphones: Kaum genutzt und schwer loszuwerden, Pressemitteilung des *vzbv* vom 27.08.2019, abrufbar unter https://www.vzbv.de/pressemitteilung/vorinstallierte-apps-auf-smartphones-kaum-genutzt-und-schwer-loszuwerden.

nicht löschbaren Programme dürfte hingegen nicht genügen.[550] Die Bedeutung für die Kaufentscheidung der Verbraucher wird regelmäßig auch nicht so erheblich sein, dass etwa in einem fehlenden Hinweis auf die Nichtlöschbarkeit ein Vorenthalten wesentlicher Informationen nach §§ 5, 5a UWG gesehen werden könnte.

Unabhängig von dieser rechtlichen Einschätzung wären transparente Angaben über vorinstallierte Apps aber wünschenswert, um dem Verbraucher eine informierte Entscheidung zu ermöglichen. Noch besser wäre es, dem Nutzer die Hoheit über die installierte Software einzuräumen und Deinstallationen nur dann auszuschließen, soweit hierdurch die Systemstabilität gefährdet würde.

Zusammenfassung

Nachdem das Bayerische Landesamt für Datenschutzaufsicht noch im Jahr 2015 erhebliche Datensicherheitsmängel bei Smart-TVs ermittelt hatte, ist aktuell ein Bemühen der Hersteller um ein hohes Datensicherheitsniveau erkennbar. Der Aufwand für Sicherungsmaßnahmen ist dabei durchaus unterschiedlich.

Bei etlichen Herstellern ist keinesfalls gesichert, dass der Sicherheitsstandard der Geräte bei Inverkehrbringen auch in den Folgejahren durch Software-Aktualisierungen aufrechterhalten wird. Bislang veröffentlicht kein Hersteller verbindliche Angaben dazu, wie lange seine Produkte mit Sicherheits-Patches versehen werden. Dieses Problem betrifft andere IoT-Geräte und insbesondere Smartphones in gleicher Weise.

Für den Kunden ist die Information, ob und ggf. bis zu mindestens welchem Zeitpunkt ein Gerät Sicherheits-Updates erhält, unerlässlich, um einschätzen zu können, wie lange eine uneingeschränkte Verwendung des Geräts gefahrlos möglich ist. Wenn der Kunde dies nicht weiß, fällt es ihm auch schwerer, die Angemessenheit des Kaufpreises zu beurteilen.

Nach aktueller Rechtslage sind jedoch keine rechtlichen Ansprüche gegen Smart-TV-Hersteller oder Verkäufer auf Bereitstellung von Software-Sicherheitsupdates ersichtlich.

Das Gewährleistungsrecht ist darauf ausgerichtet, die Mangelfreiheit nur für den Zeitpunkt des Gefahrübergangs der Kaufsache sicherzustellen. Ob die Umsetzung der Warenkaufrichtlinie für den Verbraucher in diesem Punkt spürbare Verbesserungen erbringen wird, bleibt abzuwarten. Auch die Regelungen zu verpflichtenden Verbraucherinformationen helfen den Käufern von Smart-TVs nicht weiter; jedenfalls bei den aktuellen Gegebenheiten dürfte dem Verkäufer nicht

[550] Vgl. zum teilweise recht weiten Verständnis des Sachmangels bei Software *Redeker*, in: Redeker [Hrsg.], IT-Recht, 6. Aufl. 2017, Rn. 319 ff.

zuzumuten sein, sich jeweils aktuelle Informationen über vorgesehene oder nicht vorgesehene Software-Aktualisierungen für die angebotenen Produktpalette zu besorgen und diese dem Kaufinteressenten zu präsentieren.

Die DSGVO fordert zwar grundsätzlich die Datensicherheit bei Datenverarbeitungsvorgängen ein. Eine Pflicht zu Software-Sicherheitsupdates ist aber nicht explizit vorgesehen und könnte sich erst über eine jahrelange Fortentwicklung der Rechtsprechung herausbilden. Ansätze hierzu sind bislang nicht erkennbar. Hinzu kommt, dass nicht immer gewährleistet ist, dass Software-Sicherheitslücken überhaupt vom (verantwortlichen) datenverarbeitenden Unternehmen behoben werden könnten.

Aus den Vorschriften des Lauterkeitsrechts in ihrer derzeitigen Fassung lässt sich ebenfalls kein Update-Anspruch des Verbrauchers ableiten. Ein solcher Update-Anspruch gegen den Hersteller ist aufgrund der schwierigen Dreieckskonstellation *Hersteller – Verbraucher – Dritter als Täter der Rechtsgutverletzung* kaum zu begründen. Zum einen würde die eigentliche Rechtsgutverletzung von einer Person begangen, mit der der Hersteller als Anspruchsgegner in keinerlei Geschäftsbeziehung steht. Zum anderen erfolgt die Rechtsverletzung typischerweise durch nicht näher bestimmbare Dritte. Sie ist daher i. d. R. nicht einmal in Umrissen absehbar und eine konkret bevorstehende Rechtsgutverletzung somit nicht nachweisbar.

Eine auf Lauterkeitsrecht fußende gegenüber dem Verbraucher bestehende Informationspflicht des Herstellers über Updates erscheint hingegen nicht ausgeschlossen. Praktische Schwierigkeiten ergeben sich aber aus dem Erfordernis, dass der Verbraucher durch die unterbliebene Information zu einer geschäftlichen Entscheidung veranlasst worden sein müsste, die er andernfalls nicht getroffen hätte. Auch müsste sich erst noch eine Rechtsprechung dazu herausbilden, für welchen Zeitraum Update-Informationen bereitgestellt werden müssten und ob und ggf. unter welchen Umständen eine entsprechende Verbrauchererwartung hinsichtlich der gesamten Produktpalette nur einzelner Geräte besteht. Da das Lauterkeitsrecht dem einzelnen Verbraucher keine rechtlichen Durchsetzungsmöglichkeiten an die Hand gibt, müssten insoweit Verbraucherverbände tätig werden.

Soweit im Rahmen der Sektoruntersuchung Herstellergarantien vorgelegt wurden, greifen diese auch bei Softwaremängeln ein, soweit sich nicht aus der Garantieerklärung eindeutig etwas anderes ergibt. Allerdings decken die Garantien nur solche Mängel ab, die bereits im Zeitpunkt des Gefahrübergangs auf den Verbraucher bestanden. Kein Unternehmen gewährte eine Haltbarkeitsgarantie. Mitunter waren die Garantien insofern nicht fehlerfrei, als sie nicht auf die vollständige Geltung des Gewährleistungsrechts hinwiesen oder dieses sogar einzuschränken vorgaben.

Die Nichtlöschbarkeit von Apps stellt grundsätzlich ein weniger großes Problem dar als bei Smartphones. Auch bei Smart-TVs können hierdurch jedoch Sicherheitsprobleme entstehen. Apps sind

bei manchen Herstellern löschbar, bei anderen hingegen nicht. Das zeigt, dass es durchaus technisch machbar wäre, dem Verbraucher die Entscheidung zu überlassen, welche Apps er auf seinem Fernsehgerät haben möchte. Ein Rechtsverstoß ist mit der Vorinstallation nicht löschbarer Apps – jedenfalls bei dem festgestellten Ausmaß an Vorinstallationen – jedoch nicht verbunden.

VIII. Sonstige Problemfelder

Im Verlauf der Ermittlungen stieß das Bundeskartellamt auf weitere kritische Punkte. Diese standen zwar nicht im Fokus der Ermittlungen, sind aber unter Verbraucherschutzgesichtspunkten dennoch von Interesse.[551]

1. Unaufgeforderte Werbeeinblendungen

Es gibt vereinzelt Berichte, dass Smart-TV-Hersteller oder Betriebssystembetreiber auf der Benutzeroberfläche des Smart-TVs (konkret: auf der Startseite des TV-Portals) Werbung einblenden.

a) Sachverhalt

Es handelt sich in den beschriebenen Fällen nicht um hervorgehobene Empfehlungen für Apps oder andere Angebote im Zusammenhang mit dem Smart-TV, sondern um allgemeine Werbebanner für Konsumgüter, etwa bei *Samsung*

551 Mehrere Unternehmen verwenden in ihren Nutzungsvereinbarungen Rechtswahl- und/oder Gerichtsstandsvereinbarungen, die mutmaßlich rechtswidrig sind, da der Verbraucher in den betreffenden AGB-Klauseln nicht oder nicht in der nötigen Klarheit auf den Vorrang zwingenden nationalen Verbraucherrechts hingewiesen und ihm ein falsches Bild von den ihm zustehenden Rechtsschutzmöglichkeiten vermittelt wird, s. dazu etwa BGH, Urteil vom 19.07.2012, Az. I ZR 40/11, juris Rn. 32 ff. Mangels spezifischen Bezugs zu Smart-TVs wurde hier auf eine vertiefte Darstellung verzichtet.

Abbildung 32:Teil-Screenshot von computerbild.de[552]

oder beim erst seit Herbst 2019 auf dem Markt befindlichen Fire-TV-Betriebssystem von Amazon:

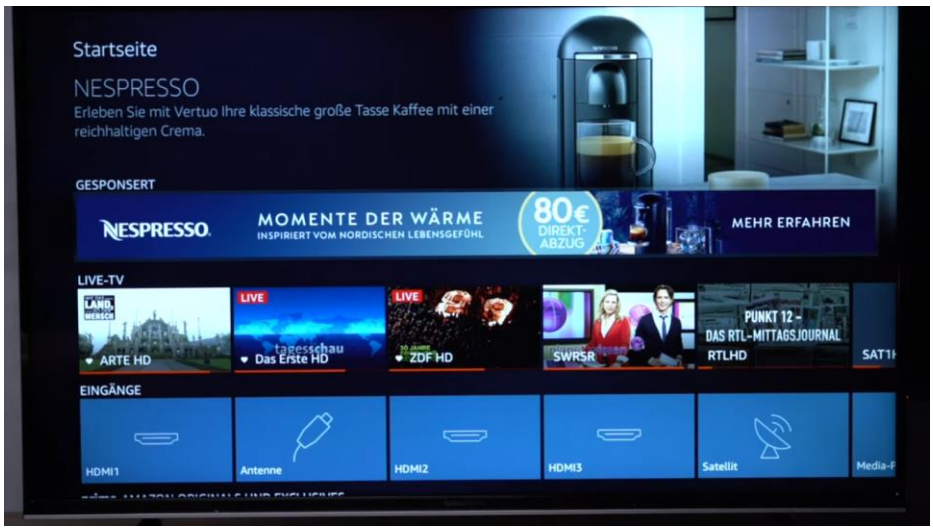


Abbildung 33:Teil-Screenshot von computerbild.de[553]

552 *Samsung nervt mit Zwangswerbung und verhöhnt die Kunden* (computerbild.de, 06.03.2020), abrufbar unter https://www.computerbild.de/Art./avf-News-Fernseher-*Samsung*-Fernseher-Zwangswerbung-25279989.html.

553 Grundig Vision 7 Fire TV Edition: Erster Alexa-Fernseher im Test; abrufbar unter https://www.computerbild.de/Art./avf-Tests-Fernseher-Grundig-Vision-7-Fire-TV-Edition-Alexa-24202121.html (Minute 4:11 des eingebetteten youtube-Videos).

Bei TP Vision gab es Überlegungen, personalisierte Werbung einzublenden, die jedoch nach Intervention der niederländischen Datenschutzbehörde nicht fortgeführt wurden.[554] *Google* hatte die Einblendung von Werbung im *Android-TV*-Portal zumindest zwischenzeitlich getestet.[555]

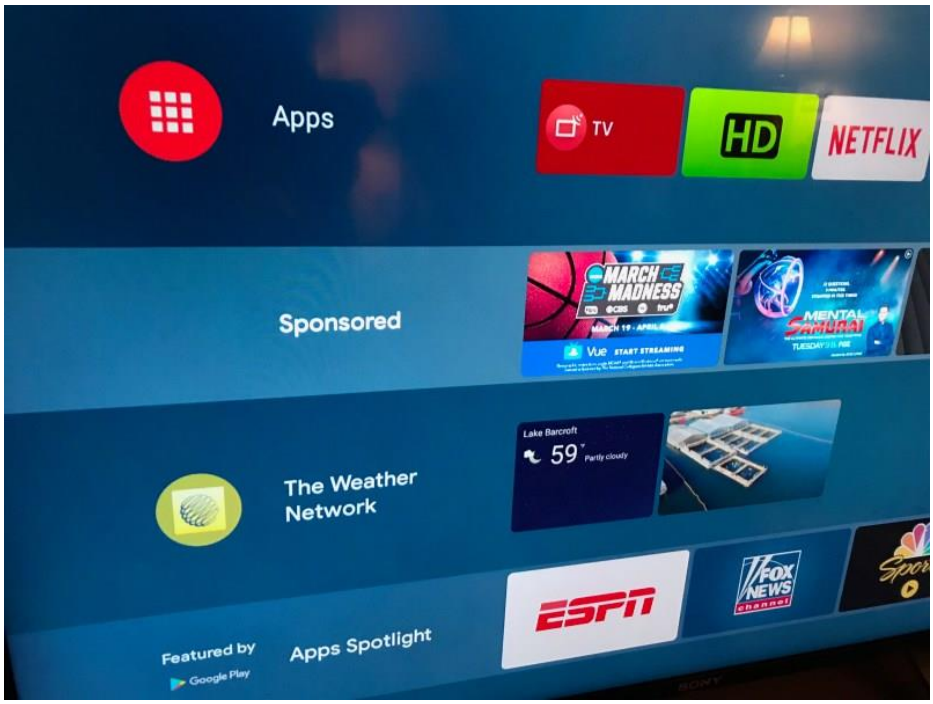


Abbildung 34:Teil-Screenshot von xda-developers.com[556]

b) Rechtliche Würdigung

Diese Praxis kann gegen Vorschriften des UWG verstoßen, wenn der Verbraucher beim Kauf des Smart-TVs nicht über die Möglichkeit dieser Form von Werbung informiert wird und mit ihr auch nicht rechnen muss. Zum einen kann in dem fehlenden Hinweis bei Vertragsschluss ein unlauteres Vorenthalten wesentlicher Informationen liegen (dazu unter aa)). Zum anderen kann die spätere Einblendung der Werbung eine unzumutbare Belästigung darstellen (dazu unter bb).

---

554 *Autoriteit Persoonsgegevens*, AP spreekt TP Vision aan op reclame op smart-tv's, Pressemitteilung vom 26.01.2017, abrufbar unter https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-spreekt-tp-vision-aan-op-reclame-op-smart-tv%E2%80%99s. (nur auf Niederländisch verfügbar).

555 *Many Android TV users are seeing sponsored posts in the launcher after the latest update* (xda-developers.com, Meldung aktualisiert am 09.04.2019), abrufbar unter https://www.xda-developers.com/android-tv-sponsored-posts-launcher/; *Google verpestet Android TV Oberfläche mit „Werbung"*, (4k-filme.de, 06.04.2019), abrufbar unter https://www.4kfilme.de/*Google*-verpestet-android-tv-oberflaeche-mit-werbung/.

556 S. vorhergehende Fußnote.

aa) Unlauteres Vorenthalten wesentlicher Informationen, § 5a Abs. 2 UWG

Nach § 5a Abs. 2 UWG handelt unlauter, wer dem Verbraucher eine wesentliche Information vorenthält, die dieser den Umständen nach benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und deren Vorenthalten geeignet ist, ihn zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. In § 5a Abs. 3 UWG wird dies für den Fall eines Angebots zum Geschäftsabschluss dahingehend konkretisiert, dass zu den wesentlichen Informationen u.a. „alle wesentlichen Merkmale der Ware oder Dienstleistung in dem dieser und dem verwendeten Kommunikationsmittel angemessenen Umfang“ gehören.

Von zentraler Bedeutung ist danach, ob die Information über die mögliche Einblendung von Werbung als in diesem Sinne „wesentlich“ angesehen werden kann. Dies hängt nach der Rechtsprechung des Bundesgerichtshofs insbesondere von einer Abwägung der Interessen des Verbrauchers einerseits sowie des Unternehmens andererseits ab (s. dazu oben, S. 94).

Vorliegend lassen sich einige Argumente für eine Informationspflicht anführen. Zunächst handelt es sich bei dem Kauf eines Smart-TV um den Erwerb eines komplexen Produkts von einigem Wert. Vom Erwartungs- und Verständnishorizont eines Durchschnittsverbrauchers ist dabei nicht mit der Einblendung entsprechender Werbeanzeigen im Bedienungsmenü zu rechnen. Werbung wird typischerweise bei kostenlosen, werbefinanzierten Angeboten oder in Medien erwartet (z. B. bei der Ausstrahlung privater Fernsehsender). Bei technischen Geräten, für die ein erheblicher Kaufpreis erbracht wird, ist dies hingegen nicht der Fall. Da großflächig eingeblendete Werbung vielfach als störend empfunden wird und bei einer Werbung in der Benutzeroberfläche (anders als bei Werbung im TV-Programm) ein Ausweichen nicht möglich ist, dürfte die Information über solche Werbung für die Kaufentscheidung des durchschnittlichen Verbrauchers von besonderem Gewicht sein. Auf der anderen Seite wäre ein entsprechender Hinweis für das Unternehmen nicht mit besonderem Aufwand verbunden. Zwar muss ein Unternehmen nicht jede Eigenschaft seines Produkts aktiv benennen, selbst wenn diese von einem Teil der Nutzer kritisch gesehen werden könnte. Hier handelt es sich jedoch um eine gezielt eingefügte Funktionalität, mit der der Verbraucher nicht zu rechnen braucht und die erhebliche Bedeutung für die vertragliche Leistungsverteilung hat. Dies lässt sich am Beispiel eines anderen smarten Geräts verdeutlichen. So verkauft Amazon Modelle seines eBook-Readers *Kindle* in einer Variante mit Werbung („Spezialangeboten“) zu einem gegenüber den werbelosen Readern mehr als 10 % günstigeren Preis.

Als Verantwortlicher für das unlautere Vorenthalten der Information kommen je nach den Umständen des Falles sowohl der verkaufende Händler als auch der Hersteller des Smart-TVs in Betracht. Auf der Ebene des Händlers ist zu berücksichtigen, dass ein „Vorenthalten“ von Informationen auch gegeben sein kann, wenn die entsprechenden Informationen dem Unternehmen

noch überhaupt nicht vorliegen, es sich diese aber mit zumutbaren Aufwand beschaffen kann.[557] Den Hersteller trifft eine Verantwortlichkeit, wenn er in der Werbung, etwa der Darstellung des Smart-TVs auf der eigenen Website, zumutbare Hinweise auf die Werbeeinblendungen unterlässt. Auch kann ihn eine mittelbare Verantwortung für das Unterlassen des Händlers treffen. So kann er, wenn er dessen Zuwiderhandlung im eigenen Interesse veranlasst und sein Handeln kontrolliert, unter Umständen als mittelbarer Täter oder ansonsten wegen der Verletzung einer Verkehrspflicht haften.

bb) Unzumutbare Belästigung, § 7 Abs. 1 UWG

Die Einblendung von Werbung in das Benutzermenü des Smart-TVs kann, wenn beim Kauf nicht ausdrücklich auf diese Möglichkeit hingewiesen wurde, auch eine unzumutbare Belästigung darstellen. Nach § 7 Abs. 1 S. 1 UWG ist eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, unzulässig. Nach § 7 Abs. 1 S. 2 UWG gilt dies insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.

(1) Unerwünschte Werbung

Ob die hier betrachtete Form der Werbung dem nicht abschließend zu verstehenden Beispielstatbestand des § 7 Abs. 1 S. 2 UWG unterfällt, ist fraglich.[558] Denn dieser setzt voraus, dass von der Werbung konkrete Marktteilnehmer angesprochen werden. Hieraus wird gefolgert, dass es sich um eine Individualwerbung handeln muss. Allgemeine Werbung, die sich an einen unbestimmten Personenkreis richtet (etwa Plakat-, Fernseh- oder Internetwerbung), wird hingegen nicht erfasst.[559] Allerdings soll es ausreichen, dass die Werbung einem Verbraucher in einer Weise nahegebracht wird, die seine private Sphäre berührt, auch wenn er nicht individuell-persönlich angesprochen wird.[560] Beispiele hierfür sind die nichtadressierte Briefkastenwerbung[561] oder Scheibenwischerwerbung.[562]

---

557 BGH, Urteil vom 02.03.2017, Az. I ZR 41/16, juris Rn. 27 – *Komplettküchen*.

558 Dies gilt erst recht für das per se-Verbot des § 7 Abs. 2 Nr. 1 UWG, das eingreift, wenn ein Verbraucher durch Werbung mit Fernkommunikationsmitteln „hartnäckig angesprochen" wird, obwohl er dies erkennbar nicht wünscht, vgl. *Köhler i*n: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 104 ff.

559 *Köhler* in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 33.

560 *Köhler*, ebenda.

561 So *Köhler* in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 91d; die Rechtsprechung zieht insoweit § 7 Abs. 2 Nr. 1 UWG heran.

562 *Köhler* in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 117.

Hierzu können durchaus Parallelen gesehen werden. Denn es geht vorliegend nicht um Werbung im TV-Programm, die an eine unbestimmte Allgemeinheit gerichtet ist, sondern um Einblendungen in der Menüführung eines technischen Geräts, welches der konkrete Verbraucher gekauft hat. Dieser Werbung kann er nicht durch Wahl des Programms oder „Umschalten" entkommen. Soweit er bei dem Kauf nicht auf die Möglichkeit solcher Werbung hingewiesen wurde, kann diese sich für ihn auch als unerwartete Beeinträchtigung seiner Fernsehernutzung darstellen.

Geht man davon aus, dass eine Werbung im Sinne des § 7 Abs. 1 S. 2 UWG vorliegt, so ist diese unzulässig, wenn sie erfolgt, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer sie nicht wünscht. Dies bedeutet, dass der entgegenstehende Wille, soweit er nicht bereits aus den äußeren Umständen erkennbar ist, vom Empfänger zum Ausdruck gebracht werden muss. Ein solcher entgegenstehender Wille könnte etwa durch Abstellen entsprechender Werbung im TV-Menü vorgenommen werden. Wo eine solche oder andere wirkungsgleiche Option nicht vorhanden, kann der Nutzer seinen entgegenstehenden Willen nicht effektiv[563] zum Ausdruck bringen. Ein Verstoß gegen § 7 Abs. 1 S. 2 UWG dürfte daher in Ermangelung der Erkennbarkeit eines entgegenstehenden Willens ausscheiden.

(2) Sonstige unzumutbare Belästigung

Soweit § 7 Abs.1 S. 2 UWG nicht einschlägig ist, kann dennoch der Grundtatbestand der unzumutbaren Belästigung (§ 7 Abs.1 S. 1 UWG) erfüllt sein, der u. a. darauf zielt, das Eindringen in die Privatsphäre von Verbraucherinnen und Verbrauchern zu verhindern. Belästigend im Sinne dieser Vorschrift ist eine geschäftliche Handlung, die dem Empfänger aufgedrängt wird und die bereits wegen der Art und Weise, wie sie den Empfängerkreis erreicht, unabhängig von ihrem Inhalt als störend empfunden wird.[564] Das soll anzunehmen sein, wenn der Handelnde die Aufmerksamkeit und/oder die Einrichtungen und Ressourcen eines Marktteilnehmers gegen seinen erkennbaren oder mutmaßlichen Willen in Anspruch nimmt und ihn damit zwingt, sich mit der Handlung auseinanderzusetzen.[565]

So wird z. B. für Internetwerbung in Form von Pop-ups und vergleichbaren Werbeformen angenommen, dass eine unzumutbare Belästigung vorliegt, wobei teilweise auf die Dauer der Anzeige

563 Ein Anschreiben des TV-Portal-Betreibers wäre zwar theoretisch möglich, aber aufwendig und mutmaßlich nicht erfolgversprechend, wenn ein Abschalten von Werbung für den einzelnen Fernseher softwareseitig nicht vorgesehen ist.

564 BGH, Urteil vom 25.04.2019, Az. I ZR 23/18, GRUR 2019, 750, Rn. 12 – *WifiSpot*.

565 So *Köhler* in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 19.

oder die Möglichkeit des „Wegklickens“ abgestellt wird.[566] Auch die (un)gestörte Menünutzung kann ein Anhaltspunkt für die Zumutbarkeit von Werbung sein. Hierbei ist allerdings zu beachten, dass im Kontext vollständig oder teilweise werbefinanzierter Internetangebote eine höhere Zumutbarkeitsschwelle anzusetzen ist als bei der Nutzung eines zuvor käuflich erworbenen hochpreisigen Produkts.

Hier kann die Belästigung darin gesehen werden, dass der Verbraucher bei der Bedienung eines von ihm erworbenen technischen Geräts mit Werbung konfrontiert wird, ohne dass er beim Kauf darauf hingewiesen wurde oder sonst vorher damit rechnen musste. Im Hinblick auf die Unzumutbarkeit dieser Beeinträchtigung ist ferner zu berücksichtigen, dass die Werbeeinblendungen im TV-Portal selbst, also dem Kernstück der Nutzeroberfläche, stattfinden. Hinzu kommt, dass solche TV-Portale jedenfalls bislang typischerweise als werbungsfreie Zonen ausgestaltet sind.

Sieht der Fernseherhersteller bzw. TV-Portal-Betreiber eine Möglichkeit vor, eingeblendete Werbung einfach und effektiv abzustellen (z. B. durch eine einfach zu aktivierende Opt-out-Funktion), kann er einer Haftung nach § 7 Abs.1 UWG entgehen.

2. Standby-Stromverbrauch

a) Ermittlungsergebnisse

Gemäß § 1 Nr. 8 EVPGV[567] zur Durchführung des EVPG[568] i. V. m. Verordnung (EG) Nr. 642/2009[569] [Anhang I Nr. 2.2a bzw. Nr. 2.2b sowie Nr. 3.3] werden aktuell je nach Art der Bildschirmanzeige als maximale Stromverbrauchswerte 0,3 Watt / 0,5 Watt im Aus-Zustand bzw. 0,5 Watt / 1 Watt im Bereitschaftszustand und 2 Watt im Zustand des vernetzten Bereitschaftsbetriebs festgelegt. Zwar halten alle Hersteller nach den übermittelten Angaben diese Grenzwerte

---

566 Vgl. *Mankowski* in: Fezer/Büscher/Obergfell, UWG, 3. Aufl. 2016, S 12 – Wettbewerbsrecht des Internets, Rn. 149 ff., *Ohly* in Ohly/Sosnitza [Hrsg.], Gesetz gegen den unlauteren Wettbewerb, 7. Auflage, § 7 Rn. 95; im Einzelnen str.

567 Verordnung zur Durchführung des Gesetzes über die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte vom 14.08.2013 (BGBl. I S. 3221), geändert durch Art. 1 der Verordnung v. 18.01.2017 (BGBl. I S. 85) - EVPG-Verordnung (EVPGV).

568 Gesetz über die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte v. 27.02.2008 (BGBl. I S. 258), zuletzt geändert durch Art. 332 der Verordnung v. 31.08.2015 (BGBl. I S. 1474) - Energieverbrauchsrelevante-Produkte-Gesetz (EVPG).

569 Verordnung (EG) Nr. 642/2009 der Kommission vom 22.07.2009 zur Durchführung der Richtlinie 2005/32/EG des Europäischen Parlaments und des Rates im Hinblick auf die Festlegung von Anforderungen an die umweltgerechte Gestaltung von Fernsehgeräte, ABl. EU Nr. L 191 vom 23.07.2009, S. 42.

ein. Die Smart-TV-Geräte von sechs Herstellern „erwachen“ im Auslieferungszustand jedoch regelmäßig aus dem Standby-Modus. Sie verbrauchen dann wesentlich mehr Strom als für den Standby-Modus gesetzlich maximal vorgesehen. Bei den Smart-TV-Geräten von fünf dieser Hersteller kann der Nutzer durch Änderung der Einstellungen ohne Weiteres dafür sorgen, dass der Smart-TV den Standby-Modus nicht unterbricht. Sony hatte im ersten Fragebogen angegeben, dass die Fernsehgeräte des Unternehmens, sobald sie mit dem Internet verbunden seien, stets für „interne Prozesse“ aus dem Standby-Modus aufgeweckt werden könnten. Später relativierte Sony die Aussage dahin gehend, dass es durchaus möglich sei, Sony-Smart-TVs in mehreren Schritten aus dem aktiven Standby- in den „deep“-Standby“-Modus zu versetzen und so ein Aufwachen für Updateprüfungen o. Ä. zu unterbinden.

b) Rechtliche Würdigung

Rechtlich gesehen stellt das Aufwachen aus dem Standby-Modus keinen Verstoß gegen die aktuell geltenden Vorschriften dar. Dies gilt selbst für den Fall, dass sich die Aufwachfunktion nicht abstellen lässt, denn im Standby-Modus werden die Grenzwerte ja eingehalten. Dass der Standby-Modus ggf. unnötig oft unterbrochen wird, ist insoweit ohne Relevanz. In der ab dem 1. März 2021 geltenden neuen VO 2019/2021 ist jedoch für neu in Verkehr gebrachte Fernsehgeräte vorgesehen, dass der Nutzer den „vernetzten Bereitschaftsbetrieb“, in dem eine Aktivierung des Geräts aus der Ferne möglich ist, abschalten können muss.[570]

3. Haftungsfreizeichnung

a) Ermittlungsergebnisse

Ein Anbieter schließt in seinen Datenschutzbedingungen gegenüber Endverbrauchern die „Haftung für die Preisgabe von persönlichen Informationen aufgrund von Fehlern in der Übertragung oder unautorisierten Zugriffen oder gesetzeswidrigen Handlungen Dritter“ aus. Die Datenschutzbestimmungen eines anderen Anbieters enthalten die Formulierung „Soweit gesetzlich zulässig, lehnen wir ausdrücklich jegliche Verantwortung oder Haftung für die Nutzung oder den Missbrauch solcher Funktionen durch Kinder unter vierzehn Jahren ab.“

---

570 Die Verordnung (EG) Nr. 642/2009 der Kommission wird mit Wirkung zum 01.03.2021 abgelöst durch die Verordnung (EU) 2019/2021 der Kommission v. 01.10.2019 zur Festlegung von Ökodesign-Anforderungen an elektronische Displays gemäß der Richtlinie 2009/125/EG des Europäischen Parlaments und des Rates, zur Änderung der Verordnung (EG) Nr. 1275/2008 der Kommission und zur Aufhebung der Verordnung (EG) Nr. 642/2009 der Kommission, Abl. EU Nr. L 315 v. 05.12.2019, S. 241. In dieser Verordnung wird das Problem des „Aufwachens aus dem Standby-Betrieb“ nicht thematisiert; der Nutzer muss jedoch den vernetzten Bereitschaftszustand des Fernsehgeräts komplett deaktivieren können (s. Anhang II, C. 2 Abs. 4 u. 5 der genannten Verordnung).

Haftungsfreizeichnungen finden sich auch in den Nutzungsbedingungen mehrerer Hersteller für ihre Smart-TV-Dienste:

- „…lehnt sämtliche Verantwortung im Hinblick auf Handlungen, fehlende Informationen und Gebaren von Drittanbietern im Zusammenhang mit oder im Bezug auf Ihren Zugriff oder der Verwendung des Portals, der Websites, Dienste oder Inhalte ab. Sie tragen daher das alleinige Risiko für den Zugriff und die Verwendung, einschliesslich, jedoch nicht beschränkt auf, jegliche erhaltenen Informationen. Ihr einziges Rechtsmittel gegen … im Falle von Schäden, Kosten oder Unzufriedenheit beim Zugriff oder der Verwendung des Portals oder jeglicher Apps, Websites oder Inhalte, ist die Einstellung der Verwendung des Portals oder der jeweiligen Apps, Websites, Dienste oder Inhalte."

- "to the extent allowed by applicable law, … shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, which may be incurred by you as a result of the use of the portal, including but not be limited to loss of profit, loss of goodwill or business reputation, cost of procurement of substitute goods or services, etc."

- Ein anderer Hersteller begrenzt in seinen Nutzungsbedingungen die Haftung grundsätzlich auf 500 USD,

  „mit der Ausnahme dass nichts die Haftung … für Tod oder Körperverletzung berührt oder begrenzt die durch Fahrlässigkeit … verursacht wird, oder die Haftung … für betrug oder betrügerische Fehldarstellung oder jegliche andere Haftung, die nach geltendem Recht nicht ausgeschlossen oder begrenzt werden kann."

b) Rechtliche Würdigung

Soweit Haftungsfreizeichnungen in Datenschutzbestimmungen enthalten sind, stellt sich die Frage, ob es sich bei solchen Formulierungen in Datenschutzbestimmungen überhaupt um allgemeine Geschäftsbedingungen handeln kann. Dies ist in Rechtsprechung und Literatur umstritten. Folgte man der Ansicht, dass Datenschutzbestimmungen generell keine Allgemeinen Geschäftsbedingungen enthalten können, so müsste man jedenfalls zu dem Ergebnis gelangen, dass die Haftungsfreizeichnung bereits nicht wirksam als AGB in das Vertragsverhältnis mit dem Endverbraucher einbezogen ist und somit ein rechtliches Nullum darstellt. Wollte man Datenschutzbestimmungen – und sei es nur im Einzelfall – hingegen eine AGB-Qualität zusprechen, so würden die vorgenannten Haftungsfreizeichnungsklauseln – ob in Datenschutzbestimmungen oder Nutzungsbedingungen enthalten – jedenfalls am absoluten Klauselverbot des § 309 Nr.

7 BGB scheitern, wenn selbst die Haftung für grobe Fahrlässigkeit und Vorsatz ausgeschlossen wird. Dies gilt ebenso für die Haftungsfreizeichnungen, die von vornherein in Nutzungsbedingungen festgeschrieben sind.

Der Vorbehalt „soweit dies gesetzlich zulässig ist“ ändert hieran nichts. Der Bundesgerichtshof hat bereits mehrfach entschieden, dass ein solcher Zusatz die Unwirksamkeitsfolge der gegen die gesetzlichen Regelungen über Allgemeine Geschäftsbedingungen verstoßenden Klauseln nicht beseitigt. Vielmehr seien solche salvatorische Klauseln ihrerseits unwirksam, weil sie gegen das Verständlichkeitsgebot verstießen.[571]

Zusammenfassung

Die Sektoruntersuchung hat einige Rechtsverstöße zutage gefördert, die zwar nicht die gesamte Branche betreffen, aber gleichwohl bemerkenswert sind.

Aufgrund der immer weiteren Zunahme personalisierter Werbung steht zu befürchten, dass unaufgeforderte Werbeeinblendungen im TV-Portal zunehmen werden. Werbung zu schalten, ohne dass der Verbraucher hierauf bereits beim Kauf des Fernsehers hingewiesen worden wäre, ist nach Auffassung des Bundeskartellamts unzulässig.

F. Fazit und Handlungsempfehlungen

Die Sektoruntersuchung Smart-TVs gibt über ihre Ermittlungsergebnisse und deren rechtliche Einordnung hinaus wichtige Hinweise für den künftigen Umgang mit der verbraucherrechtlich unbefriedigenden Situation in diesem Wirtschaftszweig sowie ganz allgemein bei IoT-Geräten.

Ungeachtet ihrer praktischen Vorteile für den Nutzer sind Smart-TV-Geräte auch dafür einsetzbar, in großer Intensität Daten über die Verbraucher und deren Nutzungsverhalten zu erheben und für Werbezwecke zu verwenden, auch wenn diese Möglichkeiten von den betreffenden Smart-TV-Anbietern zurzeit bei Weitem noch nicht ausgeschöpft werden.

Bereits auf Basis des aktuellen Verhaltens der Anbieter von Smart-TVs hat die Untersuchung eine Reihe von Verbraucherrechtsverstößen, und zwar gegen Bestimmungen des Datenschutz-, Lauterkeits- und bürgerlichen Rechts, ausgemacht und darüber hinaus Schutzlücken im geltenden Verbraucherrecht aufgezeigt.

Die Situation bei der Verfolgung der identifizierten Verstöße ist wenig befriedigend. Der eigenen Ausübung von Rechten und Rechtsschutzmöglichkeiten durch den Verbraucher stehen dessen

571 BGH, Urteil vom 04.02. 2015, Az. VIII ZR 26/14, juris Rn. 17 m. w. N.

informationelle Überforderung und rationale Apathie im Wege. Die an sich bewährte Rechtsdurchsetzung durch Verbände stößt aufgrund von Nachweisschwierigkeiten und fehlender Breitenwirkung in wichtigen von der Untersuchung erfassten Problemsachverhalten an Grenzen. Behördliche Rechtsdurchsetzung ist bislang entweder nicht effektiv genug (Datenschutzrecht) oder fehlt völlig (Lauterkeits- und bürgerliches Recht).

Um dem Verbraucherschutz im Bereich der Smart-TVs gleichwohl zu mehr Breitenwirkung zu verhelfen, sollte der verbraucherschutzfreundliche Umgang mit Nutzerdaten als Wettbewerbsparameter beim Absatz von Smart-TVs etabliert werden. Dazu müssen dem Verbraucher allerdings weitaus besser als bisher die wesentlichen Informationen über die Datenschutzqualität vermittelt werden. Es müssen neue Wege beschritten werden, um das zu Lasten des Verbrauchers bestehende Informationsgefälle abzumildern. Zu denken ist zunächst an visuelle Instrumente der Verbraucherinformation bei der Angebotsdarstellung in der Werbung, im Shop oder auf der Geräteverpackung. Mögliche Lösungsansätze wären Selbstverpflichtungen oder auch eine Kooperation von Behörden und Herstellern (Co-Regulierung). Außerdem könnte eine sinnvolle Verbraucherinformation und Datensouveränität durch digitale Technologien wie Datenschutz-Apps und -„Cockpits“ befördert werden.

Zumindest für die Erteilung bzw. Verwendung visueller Instrumente der Informationsvermittlung ist der rechtliche Rahmen durchaus gegeben. So ermöglicht zumindest die DSGVO den Unternehmen die freiwillige Verwendung von Zertifikaten oder standardisierten Bildsymbolen. Der Aufbau der hierfür vorgesehenen Strukturen ist allerdings zeitintensiv und noch nicht abgeschlossen.

Das Bundeskartellamt empfiehlt deshalb Entscheidern, Unternehmen und Wissenschaft, in Anknüpfung an den vorliegenden Bericht

- das Bewusstsein der Verbraucher für die extensiven Datenverarbeitungsmöglichkeiten von Smart-TVs und IoT-Geräten insgesamt weiter zu schärfen,
- Haftungsfragen beim Zusammenspiel der verschiedenen Akteure im IoT-Bereich gesetzgeberisch zu klären und einen Anspruch des Verbrauchers auf Software-Updates durch den Hersteller gesetzlich zu verankern,
- auf die Ergänzung bestehender Transparenzanforderungen durch aussagekräftige, einfach zu erfassende und bereits vor dem Kauf verfügbare Datenschutzinformationen hinzuwirken, die dem Verbraucher ermöglichen, den Weg preisgegebener Daten konkret nachzuvollziehen,
- dem Verbraucher die Möglichkeit an die Hand zu geben, Verarbeitungen seiner personenbezogenen Daten tagesaktuell effektiv nachzuvollziehen, anzupassen und ggf. zu beenden,
- durch Kennzeichnung und neue Technologien Datenschutzqualität als Wettbewerbsparameter zu etablieren und

- die Verwendung visueller Informationsinstrumente durch die Smart-TV-Anbieter voranzutreiben und dafür die gesetzlich bereitgestellten Akkreditierungs- und Zertifizierungsverfahren abzuschließen.

Im Einzelnen:

I. Rolle der Smart-TVs im Geschäft mit den Daten

Smart-TVs eröffnen dem Verbraucher Nutzungsmöglichkeiten, die weit über den klassischen Fernsehkonsum hinausgehen. Sie sind aber nach dem Ergebnis der Ermittlungen von ihren technischen Möglichkeiten und der Weite mancher Datenschutzbestimmungen her in einem Ausmaß in das Geschäft mit den Daten integrierbar, wie es dem Verbraucher bisher nur bezüglich mobiler Endgeräte bewusst war. Gerätehersteller, HbbTV-Anbieter, TV-Portal- und App-Store-Betreiber, App-Anbieter und Betreiber von Empfehlungsdiensten sammeln Nutzerdaten und verwenden diese für eigene Zwecke.

Die Sektoruntersuchung hat ein sehr heterogenes Bild der Datenverarbeitungen durch Smart-TV-Hersteller gezeigt. Während einzelne Anbieter bereits in bedeutendem Umfang Nutzungsdaten erheben, zeigen sich andere datensparsam. Auf den Geräten der letzteren befindet sich jedoch oftmals Drittsoftware, die nicht Gegenstand der Untersuchung war, welche jedoch mutmaßlich ebenfalls Nutzungsdaten erhebt. Aufgrund der nahezu durchgängig unklaren Datenschutzbestimmungen stellt sich das Problem, dass die von Nutzereinwilligungen umfassten Daten oder deren Speicherdauer nicht konkret erkennbar sind. Selbst wenn die Nutzer Einwilligungen verweigern können, lässt sich oftmals nicht feststellen, welche konkreten Nutzungsdaten ggf. auf der Grundlage sog. berechtigter Interessen erfasst werden, die von den Verantwortlichen einseitig definiert werden.

Von der technischen Seite und der Weite der Datenschutzbestimmungen her wären Smart-TVs für eine noch umfassendere Datenverarbeitung geeignet.

In technischer Hinsicht hat sich aus der Befragung der Gerätehersteller, der Konsultation von Stellen mit entsprechender technischer Expertise sowie eigenen Recherchen des Bundeskartellamts ergeben, dass Smart-TVs die erforderlichen Bauteile und Software enthalten, um die geschilderte Analyse des TV-Nutzungsverhaltens mittels automatisierter Inhaltserkennung (Automatic Content Recognition, kurz ACR) vorzunehmen.

In rechtlicher Hinsicht hat die im Rahmen der Untersuchung vorgenommene Analyse von Datenschutzbestimmungen ergeben, dass sich viele Smart-TV-Hersteller heute schon die Möglichkeit zu der geschilderten Analyse des TV-Nutzungsverhaltens einräumen lassen. Dies erfolgt in den Datenschutzbestimmungen entweder im Wege der Nutzereinwilligung oder durch sehr weit gefasste Nutzungszwecke bzw. berechtigte Interessen. Außerdem sehen einige der vom Bundeskartellamt angeforderten Verträge von Smart-TV-Herstellern mit Empfehlungsdiensten und mit

TV-Portal- bzw. App-Store-Betreibern die Verarbeitung von Nutzerdaten zu Marketing-Zwecken vor.

Das TV-Nutzungsverhalten des Verbrauchers kann somit detailliert ausgelesen werden. Die Erhebung statistischer Daten zur Reichweitenmessung, individueller Daten zur Interaktion mit Programmen oder Apps zum tatsächlichen Fernsehverhalten ist ohne Weiteres technisch machbar. Dies erlaubt das Ausspielen zielgerichteter Werbung, sei es im TV-Portal selbst oder als Teil- oder Vollüberblendung im Fernsehprogramm. Beim Anklicken von Werbe-Spots kann der Nutzer direkt auf die Website des Werbetreibenden weitergeleitet werden. Durch Analyse des TV-Nutzungsverhaltens lässt sich die Werbung je nach Standort des Geräts oder Zuschauerinteressen passgenau zuschneiden, ein verpasster Werbespot kann wiederholt werden. Bislang weniger genutzt, aber ebenfalls grundsätzlich möglich ist das Ausspielen zielgerichteter Werbung auf verschiedenen Geräten des Verbrauchers unter Zuhilfenahme eindeutiger Identifikatoren.

Dass diese Möglichkeiten der automatischen Inhaltserkennung zwecks zielgerichteter Werbung bei Smart-TVs weithin ungenutzt bleiben, ist nicht zu erwarten. Ansätze für eine praktische Umsetzung dieser Möglichkeiten durch Smart-TV-Hersteller sind bereits zu beobachten. Der Verbraucher muss sich daher bewusst sein, dass nicht nur Mobilgeräte in großem Umfang personenbezogene Daten verarbeiten, sondern dass auch Alltagsgeräte wie Fernseher technisch und juristisch dafür bereit stehen.

II. Verbraucherrechtsverstöße und Verbraucherrechtslücken

Legt man das gegenwärtige, verglichen mit den beschriebenen Möglichkeiten noch als moderat zu bezeichnende Datensammelverhalten der Smart-TV-Anbieter zugrunde, wurden im Laufe der Sektoruntersuchung gleichwohl eine Reihe von Verbraucherrechtsverstößen identifiziert und daneben auch Lücken im Verbraucherrecht aufgezeigt.

1. Datenschutzrecht

Dies gilt zunächst in Bezug auf die DSGVO.

Nach dem Ergebnis der Ermittlungen verarbeiten die Smart-TV-Hersteller selbst in erster Linie gerätebezogene Basisdaten und nur in geringerem Umfang Nutzungsdaten. Sensiblere personenbezogene Daten werden zumeist bei Aktivierung von Zusatzdiensten (z. B. Sprachassistent) oder (Dritt-)Apps erhoben. Man mag diese gegenwärtige Datenverarbeitungspraxis der Smart-TV-Hersteller überwiegend noch als gemäßigt einstufen; sie verstößt jedoch mutmaßlich auch auf dem gegenwärtigen Eingriffsniveau in vielen Fällen gegen die Vorgaben der DSGVO. Dies liegt insbesondere an intransparenten Datenschutzbestimmungen und vielfach nicht nachvollziehbaren Rechtfertigungsgründen für die Verarbeitung. Die Transparenzprobleme sind in erster Linie auf den „one fits all“-Ansatz zurückzuführen, auf dem die meisten Datenschutzbestimmungen basieren. Eine Datenschutzerklärung soll möglichst für alle aktuellen und künftigen Dienste

und Geräte eines Herstellers herhalten, auch wenn der Nutzer einen Großteil hiervon gar nicht nutzt. Selbst wo dies nicht der Fall ist oder (jedenfalls ansatzweise) nach Nutzungsprozessen und verwendeten Geräten differenziert wird, führen pauschalierende, schwammige Formulierungen, überflüssige Informationen und inkohärente Gliederungen zu unverständlichen Verbrauchertexten. Hinzu kommt, dass die Ausübung der Verbraucherrechte zuweilen ineffektiv ausgestaltet ist, weil die Informationen hierüber in Datenschutzbestimmungen nicht immer zutreffend sind oder Hürden für die Kontaktaufnahme aufgebaut werden.

Wie die Ermittlungen gezeigt haben, entfällt indessen der größere Teil der Datenverarbeitungsaktivitäten auf Akteure, die neben dem Hersteller am Funktionieren des Smart-TVs beteiligt sind. Zu denken ist hier vor allem an TV-Portal-Betreiber, App-Anbieter (z. B. Streamingdienste) und Dienstleister wie Anbieter elektronische Empfehlungsdienste. Die datenschutzbezogene Haftung des Herstellers für die Handlungen dieser (nicht zum untersuchten Wirtschaftszweig zählenden) Akteure ist jedoch rechtlich völlig ungeklärt. Für den Verbraucher, der im Wesentlichen auf den Hersteller und den Einzelhändler zugreifen kann, stellt dies eine beachtliche Schutzlücke dar.

2. Lauterkeits- und bürgerliches Recht

Des Weiteren sind einzelne Rechtsverstöße und Schutzlücken in Bezug auf das Lauterkeits- und das bürgerliche Recht erkennbar geworden.

Normalerweise sind die Datenschutzbestimmungen des Smart-TV-Anbieters oder des TV-Portal-Betreibers erstmals bei der Erstinbetriebnahme des Geräts einsehbar. Verbraucher werden so erst zu einem Zeitpunkt über den Umfang und die Zwecke der Datenverarbeitung informiert, an dem sie ihre Kaufentscheidung faktisch nicht mehr rückgängig machen. Hierin kann unter Umständen ein Transparenzpflichtverstoß nach § 5a Abs. 2 UWG liegen, vor allem, wenn bestimmte nicht-smarte Basisfunktionen des Fernsehens an eine in technischer Hinsicht nicht erforderliche Preisgabe personenbezogener Daten geknüpft sind.

Punktuell kommt es vor, dass der Gerätehersteller oder ein Dritter Konsumgüterwerbung auf der Startseite des TV-Portals (Homescreen) einblendet. Dies verstößt gegen § 7 Abs. 1 Satz 1 UWG, wenn beim Kauf nicht ausdrücklich auf diese Möglichkeit hingewiesen und der Kunde auch aufgrund der Gesamtumstände nicht damit rechnen musste.

Bei manchen Herstellern entsprechen die Garantieerklärungen nicht den gesetzlichen Vorgaben des § 479 Abs. 1 Satz 2 Nr. 1 BGB, was wegen des Charakters dieser Bestimmung als Marktverhaltensregel zugleich einen Verstoß gegen § 3a UWG darstellt. In Ausnahmefällen liegt eine Verletzung von § 5 Abs. 1 Nr. 7 UWG vor, weil der Verbraucher durch falsche Aussagen zu den Gewährleistungsrechten in die Irre geführt wird.

3. Datensicherheit

Kein Verbraucherrechtsverstoß, aber doch eine bedeutende Schutzlücke liegt in der teilweise sehr geringen Zeitspanne, in der die Smart-TV-Anbieter die verkauften Geräte aktuell halten. Auch wenn die Untersuchung keine augenfälligen Anhaltspunkte dafür ergeben hat, dass momentan Smart-TV-Hersteller technisch unsichere Geräte in den Verkehr bringen, so hat die Befragung doch ein kritisches Bild dazu ergeben, wie nach dem ersten Inverkehrbringen der Geräte deren Aktualität gewährleistet wird. Danach versorgen zwar die meisten Hersteller die Geräte nach dem Inverkehrbringen für 2 bis 3 Jahre mit Sicherheitsupdates, doch schmilzt diese Spanne beim Erwerb von Modellen aus dem Vor- oder Vorvorjahr rasch zusammen. In wenigen Ausnahmefällen werden die Geräte gar nicht aktualisiert – auch nicht im Falle öffentlich bekannt gewordener Sicherheitslücken der Gerätesoftware. Hinsichtlich der Information der Verbraucher mit vollständigem Inkrafttreten der Verordnung (EU) 2019/2013[572] zum 01.03.2021 eine gewisse Verbesserung eintreten. Diese sieht in Art. 3 lit. h) vor, dass der Lieferant eines Geräts mit einer Displaygröße von über 100 cm^2 dem Händler ein Produktdatenblatt zur Verfügung stellt. Im Fernabsatz muss der Händler dieses Produktdatenblatt gem. Anhang VIII. Nr. 4 in der Nähe des Produktpreises anzeigen. Anhang V. Tabelle 4 der Verordnung sieht für das Produktdatenblatt u. a. folgende Pflichtangabe vor:

	Angaben	Wert und Genauigkeit	Einheit	Anmerkungen
21.	Mindestens garantierte Software- und Firmware-Aktualisierungen (bis):	TT. MM. AAAA	Datum	Gemäß Anhang II Buchstabe E Nummer 1 der Verordnung (EU)

Abbildung 35:Auszug aus Anhang V der VO 2019/2013

Ein Anspruch gegen Smart-TV-Hersteller nicht nur auf Information, sondern auf tatsächliche Bereitstellung jeweils aktueller Software-Sicherheitsupdates zumindest für eine bestimmte Dauer lässt sich nach geltendem Recht nicht belastbar begründen. Weder das Gewährleistungsrecht, noch das Verbrauchervertragsrecht, noch DSGVO oder UWG, noch Produkt- oder Produzentenhaftung geben solch einen Anspruch her.

Gemessen an der Wichtigkeit aktueller Gerätesoftware für die Datensicherheit ist dies eine ernstzunehmende Schutzlücke im Hinblick auf die Datensicherheit des Verbrauchers. Es besteht auch ein starker Wunsch der Verbraucher nach Sicherheitsupdates bzw. diesbezüglichen Informationen. So ergab eine Befragung im Auftrag der Verbraucherzentrale Rheinland-Pfalz, dass jeweils

572 Delegierte Verordnung (EU) 2019/2013 der Kommission vom 11.03.2019 zur Ergänzung der Verordnung (EU) 2017/1369 des Europäischen Parlaments und des Rates in Bezug auf die Energieverbrauchskennzeichnung elektronischer Displays und zur Aufhebung der Delegierten Verordnung (EU) Nr. 1062/2010 der Kommission.

rund 90 % der Verbraucher Informationen über die Nichtaktualisierung von Smartphone-Betriebssystemen sowie eine Updateverpflichtung der Hersteller befürworteten. Als gewünschte Update-Zeitspanne gaben die Befragten im Durchschnitt 5,4 Jahre an.[573]

III. Unbefriedigende Rechtsdurchsetzung

Wo nicht bereits Schutzlücken im Verbraucherrecht bestehen, sondern Verstöße gegen geltendes Verbraucherrecht identifiziert wurden, stellt sich die Situation in der Rechtsdurchsetzung nach dem in der Sektoruntersuchung gewonnenen Eindruck in Teilen als unbefriedigend dar.

1. Der einzelne Verbraucher

Der einzelne Verbraucher selbst macht von seinen datenschutzrechtlichen Auskunfts-, Widerrufs- und sonstigen Rechten in aller Regel nur wenig bis keinen Gebrauch.[574] Die Gründe dafür liegen in seiner informationellen Überforderung sowie einer rationalen Apathie gegenüber dem Ergreifen rechtlicher Maßnahmen.

Exemplarisch hierfür ist die Vorgehensweise der Smart-TV-Hersteller, extensive Datenverarbeitungen durch eine Nutzereinwilligung oder schlicht über die Geltendmachung weit gefasster berechtigter Interessen abzusichern. Selbst wenn die genannten Rechtfertigungsgründe einer rechtlichen Überprüfung nicht standhalten, besteht kaum ein Sanktionsrisiko. Der Verbraucher befindet sich zunächst in dem Dilemma, dass eine Nichtakzeptanz von Datenschutzbestimmungen bzw. Nichteinwilligung in bestimmte Datenverarbeitungen dazu führen kann, dass der soeben erst erworbene Fernseher nicht oder nicht wie gewünscht benutzt werden kann. Zudem kann der Verbraucher im Preisgabezeitpunkt einen mit der Datenverarbeitung verbundenen, ggf. in fernerer Zukunft liegenden Nachteil nicht ermessen. Dies gilt umso mehr, als er im Regelfall überhaupt nicht genau erkennen kann, welche ihn betreffenden personenbezogenen Daten überhaupt erhoben und wo und wie lange diese gespeichert werden und welche Daten beispielsweise von

---

573 S. Verbraucherzentrale Rheinland-Pfalz, Verbraucher wünschen sich fünf Jahre lang Smartphone-Updates, Pressemitteilung der Verbraucherzentrale Rheinland-Pfalz vom 21.05.2019, abrufbar unter https://www.verbraucherzentrale-rlp.de/pressemeldungen/digitale-welt/verbraucher-wuenschen-sich-fuenf-jahre-lang-smartphoneupdates-36517.

574 Die Bundesregierung verzeichnete innerhalb von ca. 10 Monaten nach Inkrafttreten der DSGVO für sämtliche bundesministerialen Internetauftritte lediglich 76 Fälle der Geltendmachung von Betroffenenrechten. Da die Aufstellung nach fünf unterschiedlichen Betroffenenrechten differenzierte, ist davon auszugehen, dass deutlich weniger als 76 Personen Anträge stellten, s. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Müller-Böhm, Thomae, Aggelidis u. a. der Fraktion der FDP*, BT-Drucksache 19/8618 vom 05.04.2019, S. 6, abrufbar unter http://dipbt.bundestag.de/doc/btd/19/091/1909168.pdf.

einem Einwilligungswiderruf erfasst wären. Zwar könnte er diese Informationen durch Geltendmachung ihm zustehender Auskunftsansprüche in Erfahrung bringen. Für den Verbraucher ist dies aber nicht nur mit Aufwand, sondern womöglich auch mit der Preisgabe weiterer personenbezogener Daten verbunden, soweit er sich ggf. gegenüber dem Smart-TV-Hersteller identifizieren muss. Zudem ist nicht gewährleistet, dass der Verbraucher die einschlägigen Informationen stets in der gebührenden Detailtiefe erhält.[575] So wird der Verbraucher ohne einen monetär bezifferbaren Schaden normalerweise vor einer Rechtsverfolgung, insbesondere einer mit hohem Zeitaufwand und Kosten verbundenen Beschreitung des Rechtswegs, zurückschrecken. Dies gilt umso mehr, als es in diesem Bereich so gut wie keine Entscheidungen höherer Gerichte gibt.

2. Rechtsdurchsetzung durch Verbände

Was Verbände betrifft, so können diese einige wichtige Problemsachverhalte aus der Sektoruntersuchung durchaus ohne größere Schwierigkeiten verfolgen. Zu denken ist hier etwa an fehlerhafte Garantieerklärungen. Bei den komplexen in der Sektoruntersuchung beleuchteten Fragestellungen stoßen Verbände jedoch an Grenzen.

So können sich Nachweisschwierigkeiten ergeben, weil aus verschlüsselten Datenströmen nicht klar nachzuvollziehen ist, welche Daten an welchen konkreten Empfänger übermittelt werden.[576] Die Aufklärung der tatsächlich stattfindenden Datenverarbeitung bzw. der technischen Möglichkeiten für solche Datenflüsse, auch wenn sie noch nicht genutzt werden, ist Verbänden ohne Zugriff auf die technischen Zertifikate oder Schlüssel nicht möglich. Wie vom Bundeskartellamt nachvollzogen wurde, lassen sich selbst unter Einsatz von Analyse-Software im Wesentlichen nur die IP-Adresse des Datenempfängers, die Menge der übermittelten Daten sowie der Zeitpunkt der Übermittlung feststellen. Belastbare Schlüsse auf Verstöße lassen sich hieraus aber nicht, auch nicht im Indizienwege, ziehen. Derartige Sachverhalte können hingegen mit behördlichen Mitteln aufgeklärt werden. Zum einen bieten sich hierfür Auskunftsersuchen an, wie sie auch in der vorliegenden Sektoruntersuchung zum Einsatz gekommen sind. Zum anderen sind eigenständige technische Untersuchungen der betreffenden Geräte sinnvoll, wie sie etwa das Bundesamt für Sicherheit in der Informationstechnik unter den Voraussetzungen des § 7a BSIG[577] durchführen kann.

---

575 Siehe hierzu etwa das Negativbeispiel der unbefriedigenden Auskunftserteilung durch Video-Streamingdienste, welche zu acht Beschwerden der Organisation NOYB führte: https://noyb.eu/de/netflix-spotify-youtube-acht-strategische-beschwerden-zum-recht-auf-zugang-eingereicht.

576 S. dazu LG Frankfurt, Urteil vom 10.06.2016, Az. 2-3 O 364/15, juris Rn. 147 ff. – *VZ NRW/Samsung*.

577 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik v. 14.08.2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 13 des Gesetzes v. 20.11.2019 (BGBl. I S. 1626) – BSI-Gesetz (BSIG).

Daneben werden Verbände Verbraucherrechtsverstöße bei Smart-TVs nicht immer in der erforderlichen Breite verfolgen können. Sie können zwar die Datenschutzbestimmungen der Smart-TV-Hersteller einer gerichtlichen Überprüfung unterziehen. In der Praxis sind hier aber höchstens einzelne Musterverfahren realistisch. So sind die Datenschutzbestimmungen nämlich nur für wenige (wenngleich absatzstarke) Hersteller im Internet abrufbar, in der großen Mehrzahl muss man hingegen zunächst ein Gerät anschaffen, um die entsprechenden Texte dann während der Installation angezeigt zu bekommen. Dies erschwert die private Rechtsdurchsetzung deutlich. Behörden wie das Bundeskartellamt können die Unternehmen im Rahmen von Auskunftsersuchen verpflichten, Datenschutzbestimmungen, AGB und andere für den Verbraucher relevante Texte in Papier- oder elektronischer Form einzureichen und sich über Aktualisierungen fortlaufend informieren.

3. Behördliche Rechtsdurchsetzung

Die behördliche Durchsetzung von Verbraucherrechten in Bezug auf die hier relevanten Problem-Sachverhalte ist bislang wenig effektiv gewesen bzw. gar nicht vorgesehen.

Hinsichtlich der DSGVO-Vorgaben ist mit den Datenschutzbehörden grundsätzlich eine Durchsetzungsstruktur etabliert. Gleichwohl sind, soweit ersichtlich, keine durchgreifenden Interventionen von dieser Seite erfolgt. Möglicherweise spielen hier auch die Zuständigkeitsregeln der DSGVO eine Rolle. Denn bei – wie hier – grenzüberschreitender Datenverarbeitung[578] ist die Datenschutzbehörde am Sitz der Hauptniederlassung des Verantwortlichen federführend; die Hauptniederlassungen der Smart-TV-Anbieter sind aber über die EU verstreut mit der Folge, dass ein koordiniertes Vorgehen der federführenden Datenschutzbehörden der Mitgliedstaaten nötig wäre. Es ist auch nicht auszuschließen, dass die Aufsichtsbehörden angesichts der großen Masse von DSGVO-Verstößen zunächst andere Prioritäten setzen.

Gar keine behördliche Rechtsdurchsetzung gibt es, soweit Verstöße gegen das Lauterkeitsrecht und das bürgerliche Recht in Rede stehen. Denn verbraucherschützende Vorschriften aus diesen Rechtsgebieten werden in Deutschland traditionell durch private Kläger durchgesetzt. Bemühungen des Bundeskartellamts, im Rahmen der 10. GWB-Novelle zumindest ergänzende Eingriffskompetenzen zu erhalten,[579] sind erfolglos geblieben.

---

578 Vgl. zur Auslegung des Begriffs der grenzüberschreitenden Datenverarbeitung *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, S. 314 ff.

579 Vgl. *Bundeskartellamt*, Stellungnahme des Bundeskartellamts zum Referentenentwurf zur 10. GWB-Novelle v. 25.02.2020, S. 25, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Stellungnahmen/Referentenentwurf_10_GWB_Novelle.html.

IV. Smarte Informationen für Smart-TVs

Um die identifizierten Rechtsdurchsetzungsdefizite bzw. verbraucherrechtlichen Schutzlücken zu schließen und um dem Datenschutz bei Smart-TVs zu mehr Breitenwirkung zu verhelfen, befürwortet das Bundeskartellamt vor allem marktbezogene Lösungen. Inwieweit es gelingt, Datenschutzqualität als Wettbewerbsvorteil voranzubringen, hängt maßgeblich von der Wahrnehmung der Verbraucher ab. Das Bewusstsein der Verbraucher für die extensiven Datenverarbeitungsmöglichkeiten von Smart-TVs und IoT-Geräten sollte daher weiter geschärft werden. Die subjektive Wahrnehmung der Verbraucher ist es letztendlich, die die Art der Informationsaufnahme und die Aktivitäten zur Informationssuche bestimmt.[580]

1. Ein smartes Instrumentenset für mehr wettbewerblichen Datenschutz

Mögliche Maßnahmen zur Informationsvermittlung sind sorgfältig auf ihre **Eignung** zu prüfen. Die marktbezogenen Abhilfemaßnahmen müssen zunächst den Wahrnehmungen und Verhaltensweisen der Verbraucher – wie sie das *Privacy Paradox* beschreibt – Rechnung tragen. Inwieweit dies der Fall ist, ist im Zeitverlauf immer wieder zu überprüfen.

Vieles spricht dafür, dass die Menge und vor allem Ungenauigkeit und Unübersichtlichkeit der von Smart-TV-Herstellern zur Verfügung gestellten Informationen den Verbraucher schon jetzt überfordert.[581] Deshalb sollten Entscheider in Politik und Rechtsdurchsetzung, wann immer sie mit Datenschutz-Bestimmungen befasst sind, auf vereinfachte Informationsvermittlung durch die Unternehmen hinwirken.

Wenn also neue Wege der Informationsvermittlung beschritten werden sollen, so bietet die Forschung eine Vielzahl von Maßnahmen an, mit denen Informationsasymmetrien zum Wohle der Verbraucher gemildert werden können (s. dazu auch E. IV., S. 98).

Als Screening-Maßnahme wäre beispielsweise auf mittlere Sicht denkbar, bei der Datenschutzqualität ein differenziertes Selbstwahl-Angebot entsprechend der Risikoneigung des Verbrauchers zu schaffen. Dies setzt aber zum einen ein klar entwickeltes Bewusstsein für die eigene Zielvorstellung und die Wechselwirkung zwischen Risiko und Preis bei den Verbrauchern voraus. Da viele Verbraucher bisher ihren Informationsbedarf nicht und den Wert ihrer persönlichen Daten nur schwer einschätzen können, sind diese Voraussetzungen noch nicht gegeben. Zum anderen brauchen die infrage kommenden Instrumente noch Entwicklungszeit (s. hierzu die Ausführungen unter E. IV. 3. a), S. 104) zu ersten Projekten, die den Verbraucher beim Treffen von Entscheidungen unterstützen können).

---

580 Vgl. *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 203.

581 Vgl. zum „information overload“ bzw. „Informationsverdruss“ bei Finanzprodukten *Buck-Heeb/Lang* in: BeckOGK, Stand 01.03.2020, § 675 BGB Rn. 237 – 239 m. w. N. aus Rechtsprechung und Literatur.

Kurzfristig können die verbraucherrechtlichen Problemfelder eher mit Signaling-Maßnahmen angegangen werden. Datenschutzqualität könnte von den Anbietern erfolgversprechend vor allem über Zertifizierungen/Prüfsiegel und Bildsymbole an die Verbraucher signalisiert werden. Der Mehrwert einer Zertifizierung für Verwender und Verbraucher hängt maßgeblich davon ab, dass das mit der Zertifizierung bestätigte Datenschutzniveau als anspruchsvoll angesehen wird und die zertifizierende Institution selbst Vertrauen beim Verbraucher genießt. Voraussetzung für einen effektiven Einsatz von Bildsymbolen ist insbesondere, dass es sich um nicht bereits anderweitig etablierte Zeichen handelt und sie aus sich heraus hinreichend aussagekräftig sind (s. die Ausführungen unter E. IV. 3. b) und d), S. 106 bzw. S. 109).

Marktbezogene Maßnahmen müssen nicht nur alle relevanten Informationen über die zusammengesetzte Transaktion – den Erwerb des Produktes und das Datengeschäft – zielgruppengerecht übermitteln, damit Angebot an und Nachfrage nach datenschutzfreundlichen Smart-TVs entstehen können. Für den Verbraucher ist auch Vertrauen in die Fairness des Anbieters nach Vertragsabschluss ein wichtiger Gesichtspunkt, über den er entsprechend informiert werden sollte. So ist beispielsweise die regelmäßige Aktualisierung von Software und das Bereitstellen von Updates für die Datensicherheit und langfristige Funktionsfähigkeit von IoT-Geräten wie Smart-TVs von wesentlicher Bedeutung. Sofern Updates nicht oder nicht lange genug bereitgestellt werden, ist das smarte TV-Gerät ab einem gewissen Zeitpunkt ggf. nur noch stark eingeschränkt verwendbar. Wenn der Verbraucher sich darüber vor Vertragsschluss nicht im Klaren ist und ihn erst nach Vertragsabschluss die Erfahrung entsprechend belehrt, ist verborgenen Absichten (sog. *Hidden Intention* oder *Hold-up*) der Hersteller Tür und Tor geöffnet. Wie bereits festgestellt, besteht bislang im Regelfall keine realistische Möglichkeit, einen Anspruch gegen den Verkäufer oder Gerätehersteller auf Software-Updates durchzusetzen.

2. Fünf Symbole für ausgewählte Datenschutzaspekte

Das Bundeskartellamt möchte mit diesem Bericht einen weiteren Impuls für eine verbrauchergerechte Informationsvermittlung setzten, die zur Implementierung von Datenschutzqualität als Wettbewerbsparameter dienlich sein kann. Aus dem oben genannten Set hat es dafür auf das – neben dem Datenschutz-Zertifikat – bereits kurzfristig erfolgversprechende Instrument der Bildsymbole zurückgegriffen. Dabei sind beispielhaft für vier Datenschutzeigenschaften eines Smart-TVs, deren Kenntnis für den Verbraucher nach dem Ergebnis der Sektoruntersuchung besonders wichtig ist, eingängige Piktogramme entwickelt worden. Zudem sollte der Verbraucher über ein Symbol mit QR-Code und Internetlink sämtliche datenschutzrelevanten Informationen über ein Gerät online abrufen können. Hierfür geeignete Bildsymbole könnten schon im Vorfeld des Kaufs verwendet werden, um dem Verbraucher bereits frühzeitig einen schnellen Eindruck von diversen Datenschutzaspekten des betreffenden Geräts zu vermitteln. Auf diese Weise könnte sie der Verbraucher als Kriterium in seine Kaufentscheidung mit einfließen lassen.

Wie Befragungen zeigen, sind der Speicherort für persönliche Daten und der Mindestversorgungszeitraum mit Software-Sicherheitsupdates für Verbraucher von großer Bedeutung. Des Weiteren hat sich herausgestellt, dass die Möglichkeiten, bereits vor dem Kauf Nutzungs- und Datenschutzbestimmungen und ggf. ergänzende wichtige Detailinformationen (z. B. eine aktuelle Liste von datenempfangenden Drittunternehmen) zur Kenntnis zu nehmen, verbesserungsbedürftig sind. Außerdem ist – vor dem Kauf oder spätestens im Rahmen eines Einwilligungsersuchens – von Belang, ob das Fernsehverhalten per automatischer Inhaltserkennung (ACR) erfasst und ob ggf. biometrische Daten verarbeitet werden (s. dazu die Ausführungen unter E. IV. 3. d), S. 109).

Eine Bildsymbolik für die o. g. Aspekte könnte wie folgt aussehen:

Abbildung 36: Beispielhafte Symbolik zu fünf Datenschutzaspekten

V. Rechtlicher Rahmen für die Einführung einer smarten Symbolik

Hoheitliche Eingriffe zur Durchsetzung speziell von Bildsymbolen und Datenschutz-Zertifizierung erscheinen derzeit nicht zwingend. Immerhin besteht mit der DSGVO ein rechtlicher Rahmen, um einen freiwilligen Einsatz von Datenschutzzertifikaten und standardisierten Bildsymbolen zu befördern. Datenschutz- und Lauterkeitsrecht verpflichten die Smart-TV-Hersteller zwar, wie gesehen, zu geschäftlicher Transparenz. Einen Zwang, diese speziell mit den genannten Informationsinstrumenten zu erreichen, gibt es jedoch nicht.

1. Datenschutzrecht

Im Datenschutzrecht unterliegen die Unternehmen umfassenden Transparenzpflichten, wie sie vor allem in Art. 7 Abs. 3 Satz 3 DSGVO (Hinweis auf Widerrufsrecht bezüglich der Einwilligung), in Art. 13, 14 DSGVO (Informationspflichten bei Erhebung von personenbezogenen Daten) sowie in Art. 15 ff. DSGVO (Betroffenenrechte) normiert sind. Hierüber muss nach Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form informiert werden. Die Möglichkeit einer visuellen Vermittlung solcher und anderer Informationen ist in der DSGVO an zwei Stellen vorgesehen, nämlich in Art. 42, 43 (Datenschutzzertifikat) und Art. 12 Abs. 7, 8 (standardisierte Bildsymbole für Informationen nach Art. 13, 14, DSGVO). Beide Möglichkeiten sind allerdings in der Praxis bislang nicht zur Anwendung gekommen.

a) Zertifizierung nach Art. 42 DSGVO

Die DSGVO sieht in Art. 42 die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegeln und -prüfzeichen auf europäischer Ebene vor. Die – freiwillige – Zertifizierung bestätigt, dass ein Datenverarbeitungsvorgang DSGVO-konform ist.

Bestehende Zertifizierungen können sich für den Verantwortlichen selbst unmittelbar positiv auswirken.[582] Für den Verbraucher können sie eine wertvolle Orientierungshilfe bei der Anschaffung eines Geräts oder Inanspruchnahme einer Dienstleistung darstellen.

b) Standardisierte Bildsymbole nach Art. 12 Abs. 7 DSGVO

In Art. 12 Abs. 7 stellt die DSGVO Unternehmen anheim, mittels standardisierter Bildsymbole ihre in Abs. 1 dieser Vorschrift normierte Verpflichtung zur Information über die Datenverarbeitung in präziser, transparenter, verständlicher und leicht zugänglicher Form (zumindest in Bezug auf die Informationen nach Art. 13, 14 DSGVO) zu erfüllen. Einerseits liegt hierin eine große Chance. Da ein Großteil der Verbraucher überhaupt keine Datenschutzbestimmungen liest oder diese allenfalls überfliegt (s. dazu die obigen Ausführungen auf S. 52 f.), kann mit Bildsymbolen zumindest partiell eine bessere Orientierung erreicht werden.[583] Andererseits ist eine solche Transparenz-Symbolik nicht universell einsetzbar. So wird berechtigterweise bezweifelt, dass sich alle Informationspflichten sinnvoll und verständlich als Bildsymbole darstellen lassen.[584] Umgekehrt erwähnt Art. 12 Abs. 7 DSGVO nur Bildsymbole, die der Darstellung der Informationen in Art. 13 und 14 DSGVO dienen. Die Vorschrift erstreckt sich damit nicht auf bildlich gut darstellbare Informationen, die für den Verbraucher unter Datenschutz- bzw. Datensicherheitsgesichtspunkten zentral sind, die aber in Art. 13, 14 DSGVO keinen direkten Anknüpfungspunkt haben, z. B. Mindest-Updatezeiträume (s. dazu Abbildung 17 auf S. 110).

c) Anlaufschwierigkeiten

Die genannten Institute der visuellen Informationsvermittlung sind für die Unternehmen optional. Die DSGVO sieht hierfür bestimmte Verfahren vor.

---

582 S. Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 28 Abs. 5 und 6, Art. 32 Abs. 3, Art. 46 Abs. 2 lit. f), Art. 83 Abs. 2 lit. j DSGVO.

583 Dies gerade für den begrenzten Darstellungsumfang mobiler Anzeigen betonend *Nink* in Spindler/Schuster [Hrsg.], Recht der elektronischen Medien, 4. Aufl. 2019, Art. 12 DSGVO Rn. 27.

584 Vgl. *Specht-Riemenschneider/Bienemann*, Informationsvermittlung durch standardisierte Bildsymbole, in: Specht-Riemenschneider/Werry/Werry [Hrsg.], Datenrecht in der Digitalisierung, 2019, S. 324, 338 u. 343 m. w. N.

Das Datenschutz-Zertifizierungsregime steckt derzeit noch in den Kinderschuhen. So ist vor allem die Akkreditierung von Zertifizierungsstellen auf der Basis vom Europäischen Datenschutzausschuss (EDSA) genehmigter[585] Kriterien bislang noch nicht in Gang gekommen.[586] In Deutschland bedarf ein Tätigwerden als Zertifizierungsstelle der Befugniserteilung der zuständigen Datenschutzaufsichtsbehörde; die Akkreditierung selbst nimmt die vom Bund beliehene *Deutsche Akkreditierungsstelle GmbH* vor.[587] Anforderungen für Zertifizierungsverfahren kann die Europäische Kommission gem. Art. 43 Abs. 8 und 9 DSGVO in Form von delegierten Rechtsakten bzw. Durchführungsrechtsakten vorgeben, was jedoch – soweit ersichtlich – bislang nicht geschehen ist. Die Billigung der von einer Zertifizierungsstelle schließlich vorgelegten konkreten Kriterien für die Erteilung eines Zertifikates obliegt gem. Art. 58 Abs. 3 lit. f) DSGVO der zuständigen Aufsichtsbehörde (mit Genehmigung des Europäischen Datenschutzausschusses[588]). Es ist daher nicht damit zu rechnen, dass kurzfristig Zertifizierungen, Datenschutzsiegel und -prüfzeichen weithin verfügbar sein werden. Umgekehrt lässt die lange Startphase darauf hoffen, dass die Beteiligten ambitionierte Zertifizierungsmaßstäbe entwickeln, die ein hohes Datenschutzniveau nicht nur suggerieren, sondern wirklich sicherstellen.

---

585 Der Entwurf der Akkreditierungsregeln ist dem EDSA gem. Art. 64 Abs. 1 lit. c), 2. Alt. DSGVO vorzulegen, der dann ggf. Einwände geltend und seine Position im Bedarfsfall nach Art. 65 Abs. 1 lit. c) DSGVO auch durchsetzen kann, s. etwa die Stellungnahme des EDSA zu den vorgelegten deutschen Akkreditierungsregeln: EDSA, Opinion on the draft decision of the competent supervisory authorities of Germanyregarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR) vom 25.05.2020, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202015_de_requirementscertificationbodies_en.pdf (nur auf Englisch verfügbar).

586 Der EDSA hat hierfür wiederum Leitlinien vorgegeben: EDSA, Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Version 3.0 vom 04.06.2019, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf (noch nicht auf Deutsch verfügbar). Die Aufsichtsbehörden könnten ihrerseits ebenfalls Zertifizierungen vergeben, wie sich insbesondere aus Art. 58 Abs. 3 lit. f), 2. Fall DSGVO ergibt. Sie müssen in diesem Fall Vorkehrungen zur Vermeidung von Interessenkonflikten treffen, s. Rn. 42 f. der vorgenannten Leitlinien.

587 S. dazu § 9 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 30.06.2017 (BGBl. 2017 I, S. 2097) - Datenschutz-Anpassungs- und -Umsetzungsgesetz – EU (DSAnpUG-EU). Detaillierte Darstellung hierzu bei *Richter*, Zertifizierung unter der DSGVO, ZD 2020, 84, 85.

588 Art. 64 Abs. 1 lit. c), 3. Alt. DSGVO. Der EDSA kann ggf. auch selbst Kriterien genehmigen, s. Art. 42 Abs. 5 DSGVO, etwa wenn ihm eine Aufsichtsbehörde Zertifizierungskriterien für Datenverarbeitungsvorgänge vorlegt, die mehrere Mitgliedstaaten betreffen, s. *Lepperhoff* in: Gola u. a. [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 42 Rn. 24; *Will* in: Ehmann/Selmayr [Hrsg.], DSGVO, 2. Aufl. 2018, Art. 42 Rn. 35 ff.

Soweit ersichtlich existieren bislang auch keine delegierten Rechtsakte der Europäischen Kommission nach Art. 12 Abs. 8 DSGVO, auf deren Grundlage standardisierte Datenschutz-Bildsymbole erarbeitet worden wären, auf die etwa Smart-TV-Anbieter zurückgreifen könnten.

Inwieweit sich Zertifizierungen, Datenschutzsiegel und -prüfzeichen sowie Bildsymbole etablieren werden, lässt sich kaum prognostizieren. Es kann zwar davon ausgegangen, dass früher oder später entsprechende auf IoT-Geräte zugeschnittene Auszeichnungen am Markt erhältlich sein werden. Deren Erfolg wird jedoch einerseits maßgeblich davon abhängen, ob sie aus Verbrauchersicht verlässlich und aussagekräftig sind. Andererseits spielt eine entscheidende Rolle, welches Gewicht die Hersteller dem Datenschutz als Wettbewerbsfaktor beimessen.

2. Lauterkeitsrecht

Auch das Lauterkeitsrecht zwingt Unternehmen zu geschäftlicher Transparenz. Insbesondere gilt es als Irreführung durch Unterlassen, wenn Unternehmen nach § 5a Abs. 2 Satz 2 UWG wesentliche Informationen in unklarer, unverständlicher oder zweideutiger Weise oder nicht rechtzeitig bereitstellen. Mit dem Datenschutzrecht vergleichbare Regulierungsansätze zu visuellen Instrumenten zwecks Herstellung der geforderten Transparenz kennt das Lauterkeitsrecht nicht.

Gleichwohl ließe sich solche lauterkeitsrechtlich wünschenswerte Transparenz mit smarter Symbolik auf der Verkaufsverpackung bzw. in der Werbung und im Verkaufsprozess in effektiver Weise befördern. So könnte vor allem die Situation aufgelöst werden, wonach der Verbraucher bei der Mehrheit der Hersteller erst im Zeitpunkt der Geräteinstallation die Einzelheiten der beabsichtigten Datenverarbeitung zur Kenntnis nehmen kann bzw. in Ausnahmefällen dann auch erst erfährt, inwieweit die Nutzung des Geräts und seiner Grund- oder Smartfunktionen an die Preisgabe personenbezogener Daten gekoppelt ist und in welchem Ausmaß diese verarbeitet werden. Indem der Smart-TV-Hersteller dem Verbraucher Informationen über den Datenumgang eines Geräts – unabhängig davon, ob es sich um wesentliche Informationen im Sinne von § 5a Abs. 2 Satz 1 UWG handelt – mit einem Blick der Werbung, dem Online-Angebot oder der Verkaufsverpackung entnehmen kann, beugt er Lauterkeitsrechtsverstößen jedenfalls vor.

Bislang fehlt es an einer behördlichen Durchsetzung des UWG, mit deren Hilfe die Verwendung einer entsprechenden, branchenweit einheitlichen Bildsymbolik begleitet werden könnte. Dies ist insofern bedauerlich, als mit der vorgeschlagenen Einführung einer smarten Symbolik für Smart-TVs nicht nur den Verbrauchern gedient wäre, sondern auch den sich datenschutzrechtlich lauter verhaltenden Anbietern. Deren Konkurrenten können zurzeit ihre Geräte ohne Datenschutzinvestitionen günstiger anbieten oder über die werbliche Nutzung von Daten ihre Produkte quersubventionieren.

3. Umsetzung und Durchsetzung

Gesetzgeber, Gerichte und Behörden sollten immer dann, wenn sie mit der Transparenz von Datenschutzbestimmungen befasst sind, einfordern, dass für jedes – konkret zu bezeichnende – verarbeitete Datum

- der Nutzungsprozess genannt wird, bei dem das Datum erhoben wird,
- ein aussagekräftiger Verwendungszweck genannt wird,
- eine eindeutige DSGVO-Rechtsgrundlage genannt wird,
- konzerninterne und -externe Datenweiterleitungen und Drittlandtransfers erkennbar sind,
- wann immer möglich eine maximale Speicherdauer genannt wird.

Bei der Umsetzung ausgewählter marktbezogener Maßnahmen sind alle Akteure einzubeziehen: Entscheider, Unternehmen und Wissenschaft stehen in der Verantwortung, die notwendigen Voraussetzungen für informierte Entscheidungen der Verbraucher zu schaffen bzw. den Handlungsrahmen zu verbessern.

Die **betroffenen Anbieter** müssten ein Interesse daran haben, die möglichen ökonomischen Nachteile mangelnden Verbrauchervertrauens für sie selbst möglichst früh zu erkennen und ihnen vorzubeugen. Eine besonders wichtige Rolle kommt der Kommunikation von zielgerichteten Signalen zu. So könnten zum Beispiel Selbstbindungen in Sachen Datenschutz als marktgetriebene Abhilfemaßnahmen kommuniziert werden. Des Weiteren könnten Smart-TV-Anbieter visuelle Informationsinstrumente in der Werbung, im Verkaufsprozess und auf der Verkaufsverpackung wie etwa **Datenschutz-Zertifikate** und **standardisierte Bildsymbole** verwenden. Auch um möglichen Transparenzverstößen nach dem UWG vorzubeugen, könnten Smart-TV-Hersteller im eigenen Interesse eine smarte Bildsymbolik zu den für eine informierte Verbraucherentscheidung wichtigsten Themen verwenden. Hierzu gibt es auch bereits Ansätze.[589]

Hoheitliche Maßnahmen zur Durchsetzung speziell der visuellen Informationsinstrumente erscheinen derzeit nicht zwingend. Sollte sich nach einem Beobachtungszeitraum herausstellen, dass eigene Initiativen der Smart-TV-Hersteller – ggf. in Ergänzung zu künftigen Vorgaben der Europäischen Kommission – zu aussagekräftigen Datenschutzzertifikaten, standardisierten Bildsymbolen oder anderweitiger smarter Bildsymbolik nicht hinreichend ehrgeizig und effektiv sind, kann auch eine Begleitung des Prozesses durch den Gesetzgeber bzw. durch eine Behörde erwogen werden.

589 Siehe hierzu die Beispiele auf *Smart Media – Zahlen, Fakten, News* (tv-plattform.de, undatiert), abrufbar unter https://www.tv-plattform.de/de/service/thema/thema-smart-media.

VI. Zehn Handlungsempfehlungen

Nach alledem lassen sich folgende zehn Empfehlungen für den untersuchten Wirtschaftszweig Smart-TVs an Verbraucher, Entscheider, Unternehmen und Wissenschaft aussprechen:

(1) Das Bewusstsein der Verbraucher für die extensiven Datenverarbeitungsmöglichkeiten von Smart-TVs sollte geschärft werden, um einen bewussteren Umgang mit diesen und anderen IoT-Geräten zu fördern. Mit dem vorliegenden Bericht möchte das Bundeskartellamt einen Beitrag zu mehr Transparenz zu diesem Thema leisten und konkrete Hinweise für Verbesserungen des Verbraucherschutzes geben.

(2) Soweit in der Sektoruntersuchung verbraucherrechtliche Defizite bei der Haftung im Zusammenspiel der verschiedenen Smart-TV-Akteure deutlich geworden sind, sollte der Gesetzgeber ein Tätigwerden erwägen.

(3) In Ermangelung eines belastbaren Anspruchs des Verbrauchers gegen den Hersteller auf Software-Updates für seinen Smart-TV sollte der Gesetzgeber ebenfalls ein Nachsteuern in Betracht ziehen.

(4) Zielsetzung von Datenschutzbestimmungen sollte es sein, die Verwendung, Speicherung und ggf. Weitergabe jedes einzelnen personenbezogenen Datums für den Verbraucher konkret nachvollziehbar zu machen. Pauschalierungen sind zu vermeiden. Hier sollten Aufsichtsbehörden und Verbände rasch geeignete Fälle aufgreifen und für Rechtsprechung sorgen, die aussagekräftige Datenschutzbestimmungen befördert.

(5) Der Verbraucher sollte bereits vor dem Kauf eines Geräts Einsicht in Datenschutzbestimmungen und sämtliche Allgemeine Geschäftsbedingungen haben, die bei der Nutzung des Geräts einschlägig sind. Entsprechende Internetseiten müssen ihrerseits frei von Trackern sein. Bei Datenschutz-Fragen muss sich der Verbraucher unkompliziert und ohne Preisgabe nicht erforderlicher personenbezogener Daten an das datenverarbeitende Unternehmen wenden können.

(6) Der Verbraucher muss jederzeit die Möglichkeit haben, seine datenschutzrechtlichen Entscheidungen nachzuprüfen und ggf. nachzujustieren. Es muss daher eine einfache Möglichkeit geben, wie der Verbraucher die einschlägigen Verbrauchertexte einsehen und Verarbeitungen personenbezogener Daten ggf. beenden kann, z. B. durch Widerrufen von Einwilligungen und/oder Beenden von Nutzungen, die Datentransfers auslösen oder den Entzug von Berechtigungen, welcher für jede Anwendung individuell durchführbar sein sollte. Dies kann im Menü des IoT-Geräts verankert werden, z. B. durch ein Datenschutz-Cockpit.

(7) Zur Vermeidung von Informationsüberflutung der Verbraucher sollten Entscheider in Politik und Rechtsdurchsetzung, wann immer sie mit Datenschutz-Bestimmungen befasst sind, auf vereinfachte Informationsvermittlung durch die Unternehmen hinwirken, z. B. mittels gestufter bzw. geschichteter Darstellungsarten.

(8) Um Datenschutzqualität als Wettbewerbsparameter zu etablieren und damit dem Datenschutz bei Smart-TVs mehr Breitenwirkung zu verschaffen, sind neue Wege der Informationsvermittlung vonnöten. Zu nennen sind hier visuelle Informationsinstrumente, die die Unternehmen – möglichst auf der Basis effektiver Selbstverpflichtungen und nur nachrangig durch hoheitlichen Zwang – in der Werbung, im Verkaufsprozess und auf der Verkaufsverpackung verwenden sollten. Dazu zählt aber auch der Einsatz digitaler Technologien für Verbraucherschutz und Verbraucherbefähigung; diesbezügliche Forschungsvorhaben und Entwicklungen, die es teilweise bereits gibt, sollten (weiter) gefördert werden.

(9) Europäische Kommission und Datenschutz-Aufsichtsbehörden sollten die bestehenden Möglichkeiten der DSGVO zur Verwendung von Datenschutz-Zertifikaten und standardisierter Bildsymbole durch die Smart-TV-Anbieter vorantreiben und den Aufbau der hierfür in der DSGVO vorgesehenen Akkreditierungs- und Zertifizierungsverfahren abschließen.

(10) Gleichermaßen sollten die Transparenzgebote des UWG von den Smart-TV-Anbietern zum Anlass genommen werden, eine smarte Bildsymbolik zur Vermittlung der nach dem Ergebnis der Sektoruntersuchung relevantesten Informationen zu etablieren. Anders als im Datenschutzbereich kann dieser Prozess nach derzeitiger Rechtslage allerdings nicht behördlich begleitet werden.

G. Anhang: Analyse von Datenschutzbestimmungen im Überblick

I. Umsetzung zentraler DSGVO-Informationspflichten

	Anzahl der Unternehmen, die in ihren Datenschutzbestimmungen die einschlägigen DSGVO-Informationspflichten…				
	 …hervorragend…	 …gut…	 …mittelmäßig	 unzureichend	 stark mangelhaft
	…umgesetzt haben:				
Erkennbarkeit der erhobenen Daten	1	4	1	7	1
Erkennbarkeit der Zweckbestimmung(en) der Datenverarbeitungsvorgänge	2	--	3	3	6
Erkennbarkeit der Rechtsgrundlage/n der Datenverarbeitungsvorgänge	1	1	2	2	8
Erkennbarkeit der berechtigten Interessen[590]	--	--	4	1	5
Erkennbarkeit der Datenempfänger[591]	2	1	2	4	4
Erkennbarkeit von Datentransfers in Drittländer[592]	--	--	1	--	9

590 Vier Unternehmen stützten Verarbeitungen personenbezogener Daten nicht auf berechtigte Interessen gestützt; die Datenschutzbestimmungen dieser Unternehmen wurden insoweit nicht bewertet.

591 Ein Unternehmen übermittelte laut seinen Datenschutzbestimmungen keine personenbezogenen Daten an Dritte; die Datenschutzbestimmungen dieses Unternehmens wurden insoweit nicht bewertet.

592 Vier Unternehmen nahmen laut ihren Datenschutzbestimmungen keine Übermittlungen personenbezogener Daten in Drittländer vor; die Datenschutzbestimmungen dieser Unternehmen wurden insoweit nicht bewertet.

Darstellung der Datenschutzgarantien und Auskunftsmöglichkeiten bzgl. Datentransfers in Drittländer[593]	--	1	3	3	3
Erkennbarkeit der Speicherdauern	2	2	1	1	8

Tabelle 12: Überblick Umsetzung zentraler DSGVO-Informationspflichten

593 S. vorhergehende Fußnote.

II. Umsetzung von DSGVO-Informationspflichten zu Kontaktpersonen/Rechten

	Anzahl der Unternehmen, die in ihren Datenschutzbestimmungen die einschlägigen DSGVO-Informationspflichten über Kontaktpersonen bzw. Rechte betroffener Personen…				
	 …hervorragend…	 …gut…	 …mittelmäßig…	 …unzureichend…	 …stark mangelhaft…
	…umgesetzt haben:				
Hinweis auf Verantwortlichen	4	4	3	2	1
Hinweis auf Datenschutzbeauftragten	4	4	--	5	1
Hinweis auf Recht auf Auskunftserteilung	6	1	2	4	1
Hinweis auf Recht auf Datenlöschung	6	1	2	4	1
Hinweis auf Recht auf Einschränkung der Datenverarbeitung	3	3	2	2	4
Hinweis auf Recht auf Widerspruch gegen die Verarbeitung[594] [muss vom übrigen Text abgesetzt werden]	--	--	6	5	1
Hinweis auf Recht auf Widerruf erteilter Einwilligungen	4	6	1	3	--
Hinweis auf Beschwerdemöglichkeit bei einer Aufsichtsbehörde	4	4	1	2	3

Tabelle 13: Überblick Umsetzung von Hinweispflichten zu Kontaktpersonen/Rechten

[594] Bei zwei Unternehmen wurden Verarbeitungen personenbezogener Daten weder auf berechtigte Interessen gestützt noch betrieben diese Unternehmen Direktwerbung auf Basis der erhobenen Nutzerdaten; es gab somit keinen Bedarf für eine Widerspruchsregelung und eine Bewertung fand nicht statt.