



Sektoruntersuchung Smart-TVs zeigt Verbraucherschutz-Defizite auf

Schriftenreihe „Wettbewerb und Verbraucherschutz
in der digitalen Wirtschaft“

Dezember 2020



Sektoruntersuchung Smart-TVs zeigt Verbraucherschutz-Defizite auf
Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“
Dezember 2020

Kontakt

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

Inhaltsverzeichnis

A. Einleitung	4
B. Erkenntnisse aus der Untersuchung.....	5
I. Datenerhebungen durch Smart-TVs	5
II. Verbraucherrechtliche Problemfelder	7
1. Intransparente Verbraucherinformationen in Datenschutzbestimmungen	7
2. Fehlende Rechtsgrundlagen für Datenverarbeitungen	11
3. Lückenhafte Information des Verbrauchers vor dem Kauf	12
4. Ausbleiben von Software-Updates	12
C. Handlungsbedarf und Lösungsansätze	13
I. Handlungsbedarf trotz (oder wegen?) des Privacy Paradox.....	14
II. Datenschutz als Wettbewerbsfaktor etablieren	14
1. Mehr Transparenz schaffen.....	15
2. Datenschutzregeln durchsetzen	17

A. Einleitung

Im Dezember 2017 leitete die Beschlussabteilung Verbraucherschutz des Bundeskartellamts eine verbraucherrechtliche Sektoruntersuchung des Wirtschaftszweigs Smart-TVs ein.¹

Fernsehgeräte werden i. d. R. dann als „smart“ bezeichnet, wenn sie mehr als nur rudimentäre Online-Funktionalitäten aufweisen. D. h. Nutzer können mit Smart-TVs beispielsweise Videos streamen, soziale Netzwerke und Apps nutzen. Jedenfalls Smart-TVs neueren Datums verfügen zudem über einen roten Fernbedienungsknopf zum Aufrufen von HbbTV²-Inhalten (*Red-Button-Funktion*). Über HbbTV kann der Zuschauer zusätzliche programmabhängige Informationen erhalten, wie z. B. Angaben zu einer laufenden Sendung, passende Werbung oder gleich die Verlinkung zu einschlägigen Teleshopping-Angeboten. Aufgrund der Online-Funktionalitäten zählen Smart-TVs auch zum Bereich des Internet of Things (IoT).

Smart-TVs sind in den letzten Jahren zur Standardausstattung in den deutschen TV-Haushalten avanciert. Der Anteil von Smart-TVs am gesamten TV-Absatz in Deutschland steigt beständig und betrug 88 Prozent in den Monaten Januar bis September 2020.³ Insgesamt wurden seit 2012 in Deutschland über 44 Millionen Smart-TVs verkauft.⁴

Nach den Ermittlungen des Bundeskartellamts wurden im Referenzjahr 2017 deutschlandweit über 5,2 Mio. Smart-TVs abgesetzt. Marktführer war *Samsung* mit einem Marktanteil von ca. 30 bis 35 Prozent. Danach folgten *Panasonic*, *Sony* und *Vestel*⁵, die auf Marktanteile zwischen 10 und 15 Prozent kamen. Jeweils 5 bis 10 Prozent entfielen auf *Arçelik*⁶, *LG* und *TP Vision*⁷. Alle anderen kamen gemeinsam nur auf einen Marktanteil von deutlich weniger als 5 Prozent. Neben den Smart-TV-Herstellern sind weitere Unternehmen am Funktionieren des Smart-TVs beteiligt, die im Rahmen der Sektoruntersuchung nicht erfasst wurden. Dazu zählen etwa HbbTV-Anbieter, selbstständige TV-Portalbetreiber, App-Anbieter und Betreiber von Empfehlungsdiensten.

Dass das Bundeskartellamt nicht nur im Bereich des Kartellrechts, sondern auch im Verbraucherrecht Sektoruntersuchungen durchführen kann, ist eine Neuerung, die mit Inkrafttreten der 9. Novelle im Juni 2017 Eingang ins Gesetz gegen Wettbewerbsbeschränkungen (GWB) gefunden hat.⁸ Voraussetzung für die Einleitung einer Sektoruntersuchung ist der begründete Verdacht auf erhebliche, dauerhafte oder wiederholte

¹ Siehe Pressemitteilung vom 13.12.2017, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/13_12_2017_SU_SmartTV.html?nn=3591568. **Stand sämtlicher Internetquellen ist der 26.10.2020.**

² *Hybrid Broadcast Broadband TV*.

³ *Deutsche TV-Plattform*, Smart-TV Absatz in Deutschland wächst um 14 Prozent (nicht datiert), abrufbar unter <https://tv-plattform.de/smart-tv-absatz-in-deutschland-wachst-um-14-prozent/>.

⁴ *Deutsche TV-Plattform*, Smart-TV Absatz in Deutschland Q1-Q3 2020, abrufbar unter <https://tv-plattform.de/m Medien-center/infografiken/>.

⁵ In Deutschland bekannteste TV-Marken von *Vestel*: *Hitachi*, *Telefunken*, *Toshiba*.

⁶ *Arçelik* vertreibt seine Fernseher in Deutschland unter dem Markennamen *Grundig*.

⁷ *TP Vision* vertreibt seine Fernseher unter der Marke *Philips*.

⁸ Siehe § 32e Abs. 5 des Gesetzes 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.

Verstöße gegen verbraucherrechtliche Vorschriften, die nach ihrer Art oder ihrem Umfang die Interessen einer Vielzahl von Verbraucherinnen und Verbrauchern beeinträchtigen. Im Vorfeld der Sektoruntersuchung hatte es in den Medien immer wieder Meldungen über mögliche verbraucherrechtliche Verstöße durch Smart-TVs gegeben. Entsprechenden Verstößen kommt somit eine hohe Reichweite zu, was einer der Beweggründe des Bundeskartellamts für die Durchführung der Sektoruntersuchung war. Sektoruntersuchungen richten sich nicht gegen bestimmte Unternehmen, sondern dienen der Untersuchung eines Wirtschaftszweigs im Hinblick auf mögliche verbraucherrechtliche Verstöße.

Im Rahmen der Untersuchung befragte das Bundeskartellamt zunächst in einer ersten Runde ca. 30 Unternehmen. 20 dieser Unternehmen, bei denen sich herausgestellt hatte, dass ihre Smart-TVs in nennenswertem Umfang in Deutschland vertrieben wurden, erhielten einen zweiten noch detaillierteren Fragebogen. Ganz überwiegend zeigten sich die Unternehmen kooperations- und auskunftsbereit. Aufgrund von Sprachbarrieren und internationaler Unternehmensstrukturen gestalteten sich die Ermittlungen jedoch mitunter schwierig.

Die nachfolgenden Ausführungen stützen sich zu einem wesentlichen Teil auf Erkenntnisse, die im Rahmen der Unternehmensbefragungen gewonnen wurden. Der Abschlussbericht der Sektoruntersuchung wurde am 1. Juli 2020 veröffentlicht.⁹

B. Erkenntnisse aus der Untersuchung

Nachfolgend werden zunächst Erkenntnisse zu Datenerhebungen durch Smart-TVs vorgestellt (I.), um darauf aufbauend verbraucherrechtliche Problemfelder (II.) zu skizzieren.

I. Datenerhebungen durch Smart-TVs

Während manche Unternehmen ihre Smart-TVs praktisch vollständig unternehmensintern mit selbst produzierten Komponenten fertigen, beziehen andere das Gerät samt vorinstallierter Software bereits vollständig vormontiert von Vorlieferanten. Innerhalb dieser Bandbreite sind alle Variationen möglich. Nicht selten kommt es vor, dass Dritte das Betriebssystem und/oder das TV-Portal¹⁰ zur Verfügung stellen. So zeichnet etwa *Google* für das gesamte Betriebssystem *Android TV* samt Nutzeroberfläche verantwortlich. Unternehmen wie *Foxxum* oder *Netrange* bieten ein internetbasiertes TV-Portal an, über welches Web-Apps aufgerufen werden können. Daneben treten die HbbTV-Sender sowie mitunter Betreiber von Empfehlungsdiensten als weitere Akteure in Erscheinung. Auf Smart-TVs bereits vorinstallierte Apps wiederum stammen zumeist nicht vom Gerätehersteller, sondern von unabhängigen App-Anbietern. Angesichts dieser Vielzahl von Akt-

⁹ *Bundeskartellamt*, Sektoruntersuchung Smart-TVs – Bericht, Juli 2020, abrufbar über die Website des Bundeskartellamts: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.html?nn=11563702.

¹⁰ Als TV-Portal wird hier die Bedienoberfläche mit den wesentlichen Apps bezeichnet, die dem Nutzer standardmäßig nach dem Start des Geräts angezeigt wird.

euren fällt es mitunter schwer, Verantwortlichkeiten abzugrenzen und Haftbarkeitsvoraussetzungen zu prüfen. Aus den Angaben der befragten TV-Hersteller ergab sich einerseits, dass diese in aller Regel keine Kenntnis darüber besitzen, welche Daten andere Akteure von Nutzern erheben. Soweit Verträge, etwa zwischen Hersteller und App-Anbieter, existieren, regeln diese zumeist, dass jede Partei für die Einhaltung aller einschlägigen rechtlichen Vorgaben in ihrem Bereich verantwortlich sein soll.

Eine gemeinsame Haftung mehrerer Akteure hätte für private Kläger wie Behörden den Vorteil, dass auch die Betreiber der „Plattform Smart-TV“ belangt werden können. Diese sind zum einen oft einfacher ausfindig zu machen als Drittanbieter auf dieser Plattform. Sie sind außerdem meistens gut geeignet, einen Verstoß (auch von Dritten) effektiv abzustellen. Die Voraussetzungen für eine gemeinsame Haftung liegen indessen normalerweise nicht vor. Für eine gemeinsame Verantwortlichkeit im Sinne der Datenschutzgrundverordnung (DSGVO) fehlt es zumeist an einer gemeinsamen Entscheidung über den Zweck der Datenverarbeitung. Eine Haftung nach Deliktsrecht scheidet im Regelfall an einem entsprechenden Teilnehmervorsatz. Eine lauterkeitsrechtliche Störerhaftung würde entweder Kenntnis oder jedenfalls eine Prüfpflicht bezüglich der Rechtsverletzung eines Anderen erfordern. Es ist durchaus möglich, dass durch eine Fortentwicklung der Rechtsprechung die Anforderungen an eine gemeinsame Verantwortlichkeit gesenkt oder weitergehende Prüfpflichten für Hersteller von IoT-Geräten formuliert werden. Momentan gibt es jedoch keine konkreten Anzeichen für eine solche Entwicklung.

Die Analyse der von den Herstellern angegebenen Datenverarbeitungen hat ergeben, dass über die vorinstallierte systemnahe Software vor allem gerätebezogene Daten erhoben werden (IP-Adresse, Geräte-ID(s), MAC-Adresse, Gerätestandort, individuelle Gerätekonfiguration, verbundene Geräte, installierte Apps etc.), nur in Einzelfällen werden Nutzungsdaten zu Zwecken der Statistik bzw. Weiterentwicklung der Software verarbeitet. Hingegen übermitteln Zusatzdienste wie z. B. Sprachassistenten und Empfehlungsdienste, in beachtlichem Umfang Nutzungsdaten, insbesondere auch solche aus automatisierter Inhaltserkennung (*Automatic Content Recognition, ACR*). Entsprechende ACR-Software ist mittlerweile auf den meisten Smart-TVs vorinstalliert. Sie dient dazu, 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. Anhand der – ggf. auch über weitere IoT-Geräte im selben WLAN-Netz – ermittelten Vorlieben des Fernsehzuschauers kann dann z. B. für diesen maßgeschneiderte Werbung auf seinem Smart-TV ausgespielt werden.

Nutzer in Deutschland können die Aktivierung von ACR-Funktionen auf ihrem Fernsehgerät in aller Regel ablehnen, ohne hierdurch wesentliche Leistungsumfangseinbußen hinnehmen zu müssen. Problematisch ist indessen, dass der Nutzer in der Regel hierfür nicht sensibilisiert ist und sich zumeist auf dem schnellsten Weg durch die Ersteinrichtung seines neuen Fernsehgeräts klickt. Die Nutzerführung bei der Ersteinrichtung des Smart-TVs trägt dazu ihren Teil bei, indem die Auswahl datensparsamer Optionen erschwert oder optisch in den Hintergrund gerückt wird.

Betrachtet man die Software-Architektur von Smart-TVs im Hinblick auf mögliche Datenschutzverletzungen, so geht für den besonders umsichtigen Verbraucher mutmaßlich die größte Gefahr von (Dritt-)Apps aus. In diesem Zusammenhang war es bemerkenswert, dass die Smart-TV-Hersteller durchweg erklärten, keinerlei

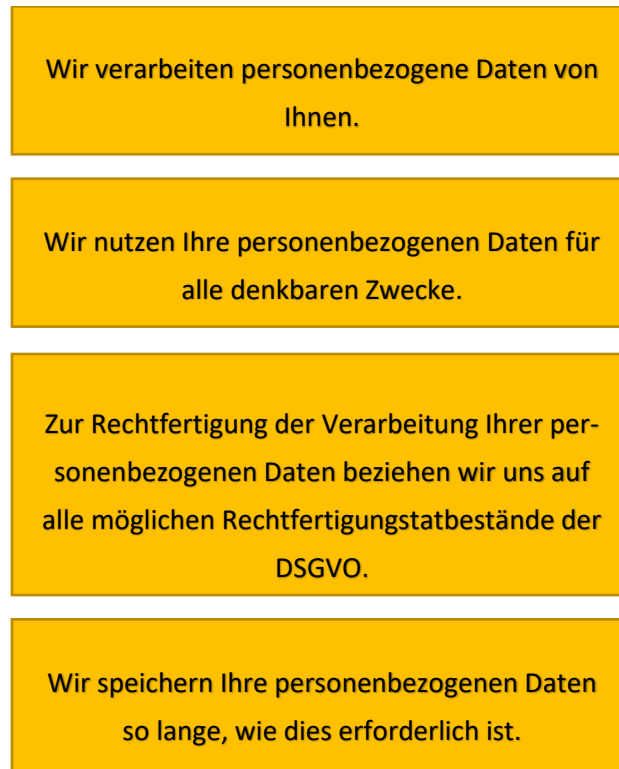
Kenntnis von den Datenverarbeitungen zu haben, die mit der Nutzung bestimmter vorinstallierter Apps einhergehen.

II. Verbraucherrechtliche Problemfelder

Die Sektoruntersuchung hat Hinweise auf verschiedene rechtswidrige Verhaltensweisen ergeben, die allerdings nicht immer gleichzeitig und nicht bei jedem untersuchten Smart-TV-Anbieter aufgetreten sind. Vier dieser Verhaltensweisen sollen nachfolgend beleuchtet werden.

1. Intransparente Verbraucherinformationen in Datenschutzbestimmungen

Eines der größten Probleme bei der Erstellung von Datenschutzbestimmungen ist die unterschiedliche Erwartungshaltung von Verbraucher und Unternehmen. Der Verbraucher wünscht sich verständliche, schnell erfassbare und möglichst konkrete Informationen, die sich auf diejenigen Datenverarbeitungen beschränken, die die Nutzung eines bestimmten Produkts oder einer bestimmten Dienstleistung tatsächlich auslöst. Aus unternehmerischer Perspektive kann es hingegen als vorteilhaft erscheinen, nicht nur tatsächliche aktuelle, sondern auch gleich potentielle künftige Datenverarbeitungen zumindest formal zu legitimieren. Zudem kann ein Unternehmen den Erstellungs- und „Wartungs“-Aufwand für Datenschutzbestimmungen reduzieren, wenn für sämtliche aktuell – und idealerweise auch künftig – angebotenen Produkte und Dienstleistungen einheitliche Datenschutzbestimmungen verwendet werden (one fits all purposes-Ansatz). Pflegeleichte Allzweck-Datenschutzerklärungen folgen in der Praxis dem folgenden extrem vereinfachten Schema:



Struktur einer „one fits all purposes“-Datenschutzerklärung

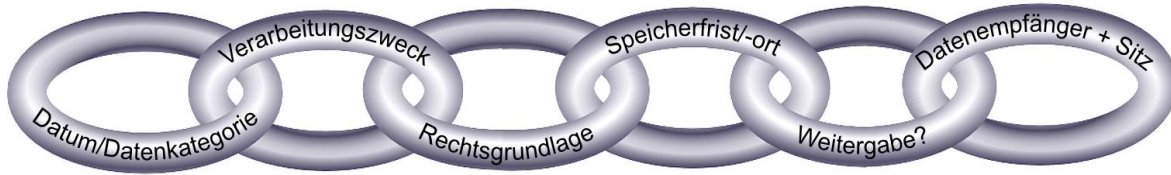
Vorteil dieses Schemas ist für Unternehmen, dass es jedenfalls auf den ersten Blick sämtliche erdenklichen Fallkonstellationen der Gegenwart und Zukunft abdeckt und so scheinbar eine nachhaltige Konformität mit der DSGVO herstellt. Mitunter lassen sich auf diese Weise auch besonders kritische Datenverarbeitungsvorgänge kaschieren.

Bei genauem Hinsehen steht ein solches Vorgehen jedoch in klarem Widerspruch zu den Anforderungen der DSGVO. Die DSGVO betont gleich an mehreren Stellen die Wichtigkeit der Transparenz sämtlicher Datenschutzbestimmungen. So statuiert die DSGVO nicht nur eine ganze Reihe konkreter Mitteilungspflichten, insbesondere in den Artikel 13 und 14. Sie sieht vielmehr in Art. 5 Abs. 1 lit. a) vor, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Art. 12 Abs. 1 DSGVO legt fest, dass die Mitteilungen zu Datenverarbeitungen nach Artikel 13 und 14 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln sind.

Um diesen Transparenzerfordernissen zu genügen, müssen Datenschutzbestimmungen stets für jedes personenbezogene Datum oder ggf. jede konkret umrissene, eng gefasste personenbezogene Datenkategorie erkennen lassen, ob¹¹ und wie diese genau verarbeitet werden. Gemäß der weiten Definition in Art. 4 Nr. 1 DSGVO umfasst der Begriff der Datenverarbeitung den gesamten Lebensweg eines Datums von der Wiege (Erfassung) bis zur Bahre (Löschung). Da Transparenz ausweislich Art. 5 Abs. 1 lit. a) DSGVO insbesondere

¹¹ Aufgrund von Formulierungen wie „möglicherweise“, „ggf.“, „je nach den Umständen“ ist für die betroffene Person oftmals schon gar nicht ersichtlich, ob ein Datum überhaupt erhoben wird.

auch die Nachvollziehbarkeit der Verarbeitung beinhaltet, muss ferner gewährleistet sein, dass die betroffene Person auch deren einzelne Elemente ohne Weiteres erkennen kann. Man kann in diesem Zusammenhang von einer Legitimationskette¹² sprechen, die in Datenschutzbestimmungen dargestellt werden muss:



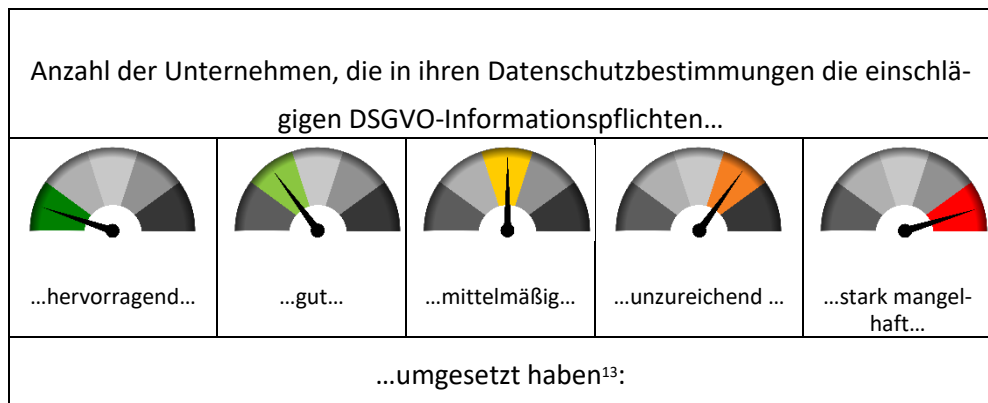
pixabay/Clker-Free-Vector-Images, verändert

Legitimationskette für Datenverarbeitungen

Mit dieser Maßgabe ist das Bundeskartellamt im Rahmen der Sektoruntersuchung der Frage nachgegangen, inwieweit im Hinblick auf Smart-TVs die wichtigsten Transparenzpflichten der DSGVO eingehalten werden. Zu diesem Zweck wurden die Datenschutzbestimmungen aller Fernseherhersteller mit wesentlichem Marktanteil in Deutschland analysiert. 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. Die Gerätenutzung setzt somit die Geltung (auch) der Datenschutzbestimmungen der vorgenannten Unternehmen voraus. Schätzungsweise dürften die insgesamt 14 ausgewerteten Datenschutztexte jedenfalls mehr als 90 Prozent der in Deutschland aktuell verkauften Smart-TVs betreffen.

Die wesentlichen Ergebnisse der Prüfung lassen sich der folgenden Übersichtstabelle entnehmen:

¹² Die Erkennbarkeit einer solchen Legitimationskette in Datenschutzbestimmungen ist freilich nicht automatisch mit der Rechtmäßigkeit der Datenverarbeitung an sich gleichzusetzen.



	...hervorragend...	...gut...	...mittelmäßig...	...unzureichendstark mangelhaft...
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	--	--	4	1	5
Erkennbarkeit der Datenempfänger	2	1	2	4	4
Erkennbarkeit von Datentransfers in Drittländer	--	--	1	--	9
Darstellung der Datenschutzgarantien und Auskunftsmöglichkeiten bzgl. Datentransfers in Drittländer	--	1	3	3	3
Erkennbarkeit der Speicherdauern	2	2	1	1	8

Überblick Umsetzung zentraler DSGVO-Informationspflichten

Nach Einschätzung des Bundeskartellamts sind jedenfalls die Einstufungen „unzureichend“ und „stark mangelhaft“ gleichbedeutend mit Verstößen gegen die entsprechenden Vorschriften der DSGVO.

¹³ Bei manchen Unternehmen waren nicht alle geprüften Aspekte einschlägig (z. B., weil eine bestimmte Rechtsgrundlage nicht in Anspruch genommen wurde oder ein Drittstaatentransfer nicht stattfand), so dass in Summe nicht immer 14 Unternehmen bewertet wurden.

2. Fehlende Rechtsgrundlagen für Datenverarbeitungen

Eng verbunden mit der Problematik intransparenter Datenschutzbestimmungen ist die Frage nach dem Vorliegen valider Rechtsgrundlagen für Datenverarbeitungen. Von den in Art. 6 DSGVO aufgeführten Rechtsgrundlagen für eine Datenverarbeitung spielen im Hinblick auf IoT-Geräte wie dem Smart-TV drei eine wesentliche Rolle:

- die Einwilligung der betroffenen Person (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO),
- die Notwendigkeit für die Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO) sowie
- die Wahrung berechtigter Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO).

Von diesen Rechtsgrundlagen machten die befragten Unternehmen in unterschiedlichem Ausmaß Gebrauch. Es kam auch durchaus vor, dass Unternehmen für vergleichbare Daten(kategorien) unterschiedliche Rechtfertigungsgründe nannten.

Wurden Nutzern Einwilligungsersuchen vorgelegt, so fehlte es diesen praktisch durchgängig an einer Darstellung aller wesentlichen Angaben, die die Nutzer für eine informierte Einwilligung benötigen würden. Informiertheit ist jedoch bereits nach der Begriffsdefinition in Art. 4 Nr. 11 DSGVO zwingende Voraussetzung für eine freiwillige Einwilligung. Erteilte Einwilligungen wären demnach in den meisten Fällen als unwirksam anzusehen.

Soweit Datenverarbeitungen auf die Notwendigkeit für die Vertragserfüllung gestützt wurden, bot sich ein uneinheitliches Bild. Einige Anbieter legten die Notwendigkeit nachvollziehbar dar, z. B. die Übermittlung bestimmter Gerätedaten zur Durchführung von Software-Updates. Überwiegend bestand jedoch das Problem, dass gar nicht klar war, welche Daten genau als für die Vertragserfüllung notwendig angesehen und verarbeitet wurden. In diesen Fällen scheidet eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO aus, da eine generelle Erforderlichkeit der Verarbeitung sämtlicher verarbeiteter personenbezogener Daten praktisch nie gegeben ist.

Erhebliche Zweifel bestanden zumeist auch im Hinblick auf die berechtigten Interessen, die die Unternehmen in ihren Datenschutzbestimmungen angaben. Ganz überwiegend wurden berechnete Interessen – z. T. extrem – weit und abstrakt formuliert. Es war auch nicht möglich, diese weit formulierten Interessen durch anschauliche Verwendungszwecke, welche man den Interessen erkennbar hätte zuordnen können, hinreichend zu konkretisieren. Wiederum bestand zudem das generelle Problem, dass häufig unklar war, welche Datenverarbeitungen genau von dem Rechtfertigungsgrund der berechtigten Interessen abgedeckt sein sollten. Die gebotene Abwägung mit den Interessen der jeweils betroffenen Personen scheidet so bereits im Ansatz. So wurde in vielen Fällen als ein berechtigtes Interesse die Verbesserung des eigenen Produkts bzw. der eigenen Dienstleistung ins Feld geführt. Dabei wurde jedoch nicht erkennbar, worin diese Verbesserung bestehen könnte und welche der verarbeiteten Daten für diese Verbesserung überhaupt herangezogen werden sollten. Anhand solcher vager Angaben kann auch nicht nachvollzogen werden, ob die angestrebten Verbesserungen nicht im Wesentlichen ebenso gut mit anonymisierten Daten erreicht werden könnten.

Vor diesem Hintergrund ist im Hinblick auf die meisten Smart-TV-Hersteller bzw. TV-Portal-Betreiber anzunehmen, dass ein wesentlicher Teil der Datenverarbeitungen ohne Rechtsgrundlage und damit rechtswidrig erfolgt.

3. Lückenhafte Information des Verbrauchers vor dem Kauf

Im Einzelhandel werden Smart-TVs und andere IoT-Geräte typischerweise ohne jegliche Hinweise angeboten, welche Allgemeinen Geschäftsbedingungen oder Datenschutzbestimmungen dem späteren Nutzungsverhältnis zwischen dem Käufer und dem TV-Portal-Betreiber zugrunde gelegt werden. Die vollumfängliche Nutzung des Geräts ist jedoch möglicherweise von der Erteilung von Einwilligungen abhängig, um die die betroffene Person erst nach erfolgtem Kauf im Rahmen der Erstinstallation ersucht wird. Ebenso enthalten Produktbeschreibungen von Smart-TVs in der Regel keine Angaben über einen ggf. vom Hersteller abweichenden Betreiber des auf dem Fernsehgerät vorinstallierten TV-Portals. Angaben über die Notwendigkeit eines Nutzerkontos zur vollumfänglichen Verwendung des Smart-TVs werden nur teilweise gemacht. Solche Informationsdefizite gelten gleichermaßen für den Internethandel wie den Kauf im Ladenlokal.

Gemäß § 5a Abs. 2 UWG dürfen dem Verbraucher entscheidungserhebliche wesentliche Informationen nicht vorenthalten werden. Soweit ersichtlich, gibt es bislang für die Frage der Information vor dem Kauf im Bereich der IoT-Geräte keine einschlägige Rechtsprechung. Das Bundeskartellamt geht indessen von der Erwartung des Verbrauchers aus, dass ihm vorab beispielsweise mitgeteilt wird, wenn essentielle Funktionen des Smart-TVs (etwa die Vornahme von Firmware-Updates oder das Streamen von Filmen über populäre Plattformen) ohne Anlegen eines Nutzerkontos nicht zur Verfügung stehen. Hingegen wäre nach Auffassung des Bundeskartellamts die Nennung eines vom Hersteller abweichenden TV-Portal-Betreibers oder ein Hinweis auf die für den späteren Betrieb des Geräts relevanten Nutzungsbedingungen und Datenschutzbestimmungen zwar wünschenswert, aber in Ansehung der Verbrauchererwartung beim Erwerb von Smart-TVs eher nicht als wesentliche Information i. S. d. § 5a Abs. 2 UWG einzustufen.

4. Ausbleiben von Software-Updates

Die im Rahmen der Sektoruntersuchung befragten Unternehmen nannten sehr unterschiedliche Zeiträume, während derer sie für Sicherheitsupdates der Software ihrer Geräte sorgen. Die Angaben reichten von 0 bis 60 Monate. Die meisten Unternehmen stellen für zwei bis drei Jahre nach dem ersten Inverkehrbringen einer bestimmten Smart-TV-Modellreihe Aktualisierungen zu Sicherheitszwecken bereit. Der Durchschnitt lag bei 27 Monaten. Der Käufer muss daher – vor allem bei Modellen der Vorjahre – damit rechnen, nur noch für relativ kurze Zeit nach dem Kauf Sicherheitsupdates zu erhalten. Da kein Hersteller in Produktbeschreibungen konkrete Mindestzeiträume für Sicherheitsupdates angibt, kann der Verbraucher diesen Aspekt auch nicht in seine Kaufentscheidung einbeziehen.

Nach aktueller Rechtslage hat der Käufer nur dann Gewährleistungsansprüche gegen den Verkäufer, wenn eine Software-Sicherheitslücke bereits bei Gefahrübergang¹⁴ bestand und (jedenfalls fachkundigen Kreisen) bekannt war. Erst nach dem Gefahrübergang offenbar werdende Sicherheitslücken begründen keinen Anspruch auf Mangelabhilfe, etwa durch Zurverfügungstellung eines Software-Updates.¹⁵ Im Lauterkeits- wie im Deliktsrecht besteht in Ansehung der bislang ergangenen Rechtsprechung die Schwierigkeit, eine Pflicht des Herstellers zur Gefahrabwendung durch Bereitstellung von Software-Updates zu begründen.

Eine Informationspflicht über die künftige Versorgung eines Smartphones mit Sicherheits-Updates hat das Oberlandesgericht (OLG) Köln zuletzt sowohl nach Verbrauchervertragsrecht als auch nach Lauterkeitsrecht abgelehnt.¹⁶ Es verwies dabei im Wesentlichen darauf, dass dem Verkäufer (offenbar auch hinsichtlich öffentlich bekannter Sicherheitslücken) die Beschaffung der entsprechenden Informationen nicht zuzumuten sei. Dieses Argument verfängt indessen nicht bezüglich einer möglichen Informationspflicht des hier im Fokus stehenden Geräteherstellers (die nicht Gegenstand des Rechtsstreits vor dem OLG Köln war). In seinem Urteil spricht das Gericht zwar auch davon, dass dem Hersteller nicht bekannt sei, wann etwa ein neues Sicherheitsupdate des Betriebssystems veröffentlicht würde.¹⁷ Allerdings hindert dies den Hersteller nicht daran, darüber zu informieren, innerhalb welchen Zeitraums neu erscheinende Sicherheitsupdates des Betriebssystemherstellers (ggf. in angepasster Form) für das Gerät des Käufers in jedem Fall bereitgestellt („weitergegeben“) werden sollen. Für eigene Erweiterungen und Änderungen des Betriebssystems kann der Hersteller ohnehin selbstständig Sicherheitspatches entwickeln. Es erscheint daher durchaus nicht unplausibel, es als Vorenthalten einer wesentlichen Information (§ 5a Abs. 2 UWG) anzusehen, potentielle Käufer nicht über Mindestzeiträume für Sicherheits-Software-Updates in Kenntnis zu setzen.

C. Handlungsbedarf und Lösungsansätze

Wie oben dargestellt, ist die rechtliche Situation des Verbrauchers beim Umgang mit Smart-TVs in vielerlei Hinsicht nicht zufriedenstellend. Zum einen ist davon auszugehen, dass derzeit in vielen Fällen personenbezogene Verbraucherdaten unrechtmäßig verarbeitet werden, ohne dass sich betroffene Personen hiergegen effektiv zur Wehr setzen könnten. Zum anderen ist die Informationslage aus Sicht des Verbrauchers unvollständig. Dies gilt im Hinblick auf wichtige produktbezogene Informationen vor dem Kauf ebenso wie für spätere Verarbeitungen personenbezogener Daten.

¹⁴ Gefahrübergang ist der Zeitpunkt, in dem die Gefahr von Verlust oder Beschädigung der Sache auf den Käufer übergeht. Beim Versandungskauf findet der Gefahrübergang erst dann statt, wenn der Verbraucher die Sache erhalten hat (§ 475 Abs. 2 BGB als Ausnahme zu § 447 Abs. 1 BGB).

¹⁵ Vgl. *Raue*, Haftung für unsichere Software, NJW 2017, 1841, 1843; OLG Koblenz, Urteil vom 30.04.2009, Az. 6 U 268/08. Mit Anwendbarkeit der auf der Warenkaufrichtlinie (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) beruhenden nationalen Umsetzungsvorschriften zum 01.01.2022 muss der Verkäufer für eine aus Käufersicht erwartbare Zeitspanne auch Updates zur Verfügung stellen. Art. 7 Abs. 5 der Warenkaufrichtlinie lässt hiervon wiederum eine Ausnahme zu, sofern der Käufer gesondert zustimmt.

¹⁶ OLG Köln, Urteil vom 30.10.2019, Az. I-6 U 100/19.

¹⁷ OLG Köln, a. a. O., juris Rn. 73.

I. Handlungsbedarf trotz (oder wegen?) des Privacy Paradox

Es ist einerseits unbestreitbar und empirisch hinreichend belegt, dass Verbraucher ihrer Privatsphäre eine hohe Bedeutung beimessen, gleichzeitig aber in Alltagssituationen den Schutz ihrer personenbezogenen Daten häufig vernachlässigen. Andererseits gibt es für dieses scheinbar widersprüchliche Verhalten (sog. Privacy Paradox) mittlerweile eine ganze Reihe plausibler Erklärungsansätze. So handelt die betroffene Person im Moment der Datenpreisgabe in der Regel schon nicht in Kenntnis aller entscheidungsrelevanten Informationen. Dies kann etwa daran liegen, dass diese nicht verfügbar, nicht verständlich oder (z. B. aufgrund der Informationsfülle¹⁸) nicht erkennbar sind. Besonders schwierig ist es auch, sich ein konkretes Bild von den Risiken zu machen, die mit der Datenpreisgabe in ggf. ferner Zukunft verbunden sein könnten. Hier kommt erschwerend hinzu, dass der Durchschnittsverbraucher ohnehin nachweislich dazu neigt, sofortige Gewinne stärker zu gewichten als künftige Nachteile. Von zentraler Bedeutung ist zudem, dass der Verbraucher – sei es objektiv oder zumindest nach seinem Dafürhalten – in vielen Fällen schlicht über keine niedrighschwellige Ausweichoption verfügt. Das Umsteigen auf ein anderes Produkt bzw. eine andere Dienstleistung kann aufgrund von Netzwerkeffekten, qualitativen Gründen oder schlicht deshalb ausscheiden, weil die Alternativen nicht erkennbar datenschutzfreundlicher sind als das fragliche Angebot.

Bei allen Lösungsansätzen muss es daher zum einen darum gehen, den Verbraucher ungeachtet seiner womöglich kurzen Aufmerksamkeitsspanne besser zu informieren. Es muss zudem darauf hingewirkt werden, dass dem Verbraucher erkennbare realistische Auswahlalternativen zur Verfügung stehen. Dies kann einerseits durch bessere Angebotstransparenz sowie andererseits durch rechtliches Vorgehen gegen unzulässige Datenverarbeitungsbestimmungen und -praktiken von Unternehmen erreicht werden.

II. Datenschutz als Wettbewerbsfaktor etablieren

Die Sektoruntersuchung hat gezeigt, dass Unternehmen einer effektiven Information von Verbrauchern in Datenschutzfragen keine hohe Priorität beimessen. Datenschutz stellt derzeit für die Hersteller von Smart-TVs keinen maßgeblichen Wettbewerbsfaktor dar. Um dies zu ändern, kann an mehreren Stellschrauben angesetzt werden.

1. Mehr Transparenz schaffen

Bislang ist der Verbraucher bei IoT-Geräten kaum in der Lage, unterschiedliche Angebote im Hinblick auf ihre Datenschutzqualität zu vergleichen. Eine spürbare und marktverändernde Nachfrage nach datenschutzfreundlichen Produkten kann sich unter diesen Bedingungen nicht herausbilden.

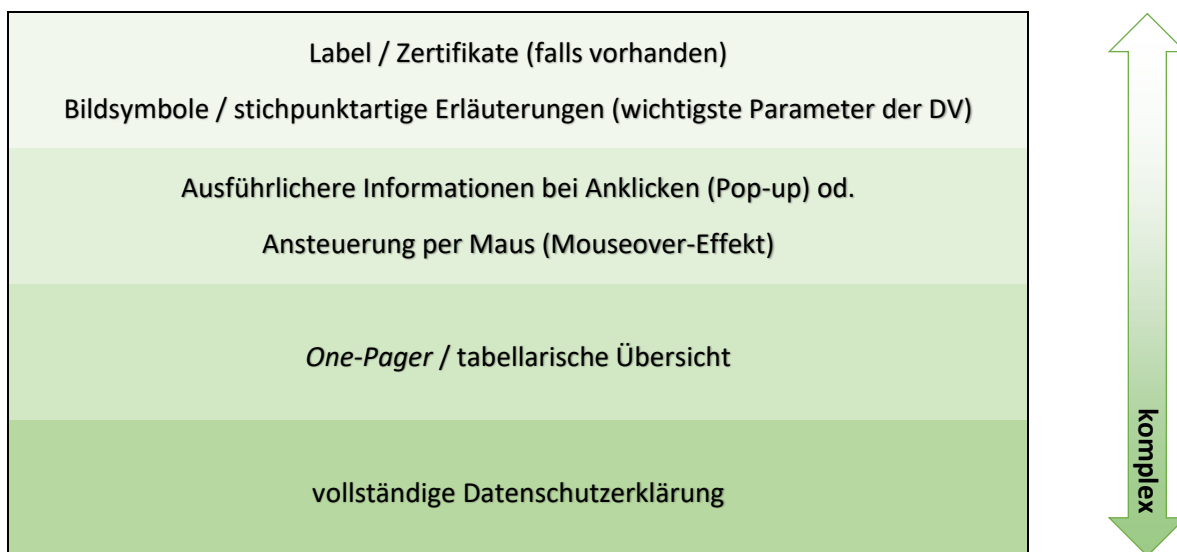
Mehr Transparenz erfordert zum einen ein Nachbessern aufseiten der Verwender von Datenschutzbestimmungen. Diese sollten für jedes – konkret zu bezeichnende – verarbeitete personenbezogene Datum

¹⁸ Hierbei spielt auch eine Rolle, dass Verbraucher aufgrund der zunehmenden Verrechtlichung vieler Lebensbereiche häufig mit komplexen Rechtstexten wie Datenschutzbestimmungen oder Nutzungsbedingungen konfrontiert werden. Bei realistischer Betrachtung sind Verbraucher nicht ansatzweise in der Lage, diese Texte allesamt durchzulesen geschweige denn zu verstehen.

- den Nutzungsprozess nennen, bei dem das Datum erhoben wird,
- einen aussagekräftigen Verwendungszweck nennen,
- eine eindeutige DSGVO-Rechtsgrundlage nennen,
- konzerninterne und -externe Datenweiterleitungen und Drittlandtransfers erkennbar machen,
- wann immer möglich eine maximale Speicherdauer nennen.

Um den Überblick zu erleichtern, können diese Informationen auch in tabellarischer Form angegeben werden.

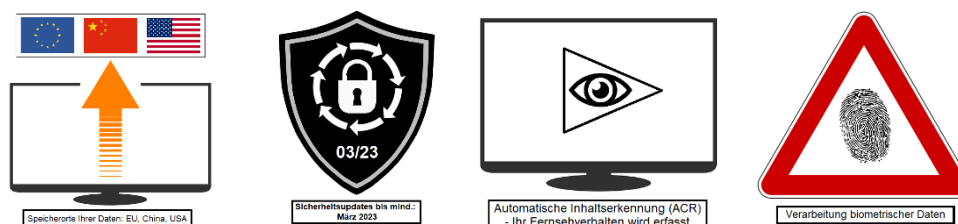
Zum anderen sollten Datenschutzbestimmungen nicht nur präzisiert werden. Vielmehr ist es notwendig, wesentliche Informationen deutlich schneller erfassbar zu machen. Dieser Ansatz wird in der nachfolgenden Abbildung modellhaft dargestellt:



Datenschutzinformationen im Schichtenmodell

Die oben dargestellten Schichten können dabei 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.

Unbeschadet der sinnvollen Möglichkeiten zur Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegeln und -prüfzeichen durch die Datenschutzbehörden nach Art. 42 DSGVO schlägt das Bundeskartellamt beispielhaft einige Bildsymbole vor, die das Verbraucherverständnis für Datenverarbeitungen verbessern können:



Beispielhafte Symbolik zu vier Datenschutzaspekten¹⁹

Jedenfalls die beiden links stehenden Symbole könnten bereits auf der Verkaufsverpackung angebracht oder bei Internetverkäufen im unmittelbaren Umfeld der Preisangabe angezeigt werden. Die beiden rechts stehenden Symbole könnten als Warnhinweis unmittelbar vor einer bevorstehenden Datenverarbeitung angezeigt werden. Des Weiteren wäre es sinnvoll, dem Verbraucher bereits vor dem Kauf den Zugriff auf sämtliche verbraucherrelevanten Informationen über einen Mausklick oder das Einlesen eines QR-Codes zu ermöglichen:



Symbol mit Internetlink zu allen verbraucherrelevanten Informationen²⁰

Auf der Zielseite könnte der Verbraucher dann nicht nur die wesentlichen Datenschutzbestimmungen (möglichst in Form eines geschichteten Modells, s. o.) abrufen, sondern ggf. auch die jeweiligen aktuellen Empfänger personenbezogener Nutzerdaten u. Ä.

Auch während der Nutzungszeit eines IoT-Geräts sollte der Verbraucher jederzeit die Möglichkeit haben, seine datenschutzrechtlichen Entscheidungen zentral (z. B. im Einstellungsmenü oder über ein Datenschutz-Cockpit) 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.

Mittel- bis langfristig können auch digitale Helfer (z. B. Apps) hilfreich sein, mit denen der Verbraucher selbstständig Datenschutzregelungen analysieren kann. Erste Projekte hierzu gibt es bereits.

Als Begleitmaßnahme wäre zudem eine verstärkte Verbraucherbildung in Datenschutzfragen sinnvoll. Mutmaßlich ist vielen Verbrauchern häufig nicht bewusst, in welchen Situationen sie welche Daten preisgeben und wie sie ihre Privatsphäre besser schützen können.

¹⁹ Eigene Darstellungen auf Basis gemeinfreier Bilder.

²⁰ Eigene Darstellung auf Basis gemeinfreier Bilder.

2. Datenschutzregeln durchsetzen

Bei Smart-TVs und mutmaßlich auch anderen IoT-Geräten bietet die Befolgung von Datenschutzvorschriften im Wettbewerb derzeit keinen wirtschaftlichen Nutzen. Es kann im Vergleich zu Konkurrenten sogar einen Vorteil bedeuten, in größerem Umfang als diese personenbezogene Nutzungsdaten zu erheben. Zudem werden Datenschutzverletzungen momentan, soweit ersichtlich, allenfalls punktuell sanktioniert. Es besteht mithin für Unternehmen kein wirtschaftlicher Anreiz, Datenschutzvorschriften tatsächlich einzuhalten. Dies bedeutet umgekehrt, dass sich regeltreu verhaltende Unternehmen ggf. sogar einen Wettbewerbsnachteil hinnehmen müssen.

Nach der DSGVO ist ein behördliches Vorgehen gegen Datenschutzverletzungen grundsätzlich möglich, Anzahl und Umfang entsprechender Verfahren halten sich aktuell jedoch in einem überschaubaren Rahmen. Dies mag auch an der Notwendigkeit internationaler Koordination liegen, die ein einheitliches Vorgehen gegen Unternehmen mit Hauptsitzen in verschiedenen Staaten erschwert. Was Verstöße gegen das Lauterkeitsrecht und das bürgerliche Recht anbelangt, existiert überhaupt keine behördliche Rechtsdurchsetzung. Hier müssten private Verbände aktiv werden. Ein Mehr an behördlichen und gerichtlichen Leitentscheidungen würde jedenfalls eine effektivere Rechtsdurchsetzung in der Breite fördern und auch Compliance-Anstrengungen der Unternehmen erleichtern.

Punktuell könnte der Gesetzgeber zu mehr Rechtsklarheit beitragen. So wäre es etwa hilfreich, in klaren Verstößfällen auch den Betreiber einer „IoT-Plattform“ wie z. B. eines Smart-TVs zur Verantwortung ziehen zu können. Des Weiteren sollten unter Nachhaltigkeitsgesichtspunkten Hersteller von IoT-Geräten dazu verpflichtet werden, für einen bestimmten Zeitraum für Sicherheitsupdates zu sorgen oder zumindest anzugeben, bis zu welchem Zeitpunkt entsprechende Updates mindestens zur Verfügung gestellt werden.