IRIS Spezial

Eine Publikation der
Europäischen Audiovisuellen Informationsstelle

# Smart TV und Datenschutz

EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

**IRIS *Spezial***
**Smart TV und Datenschutz**

Europäische Audiovisuelle Informationsstelle, Straßburg 2016
ISBN 978-92-871-8240-1
EUR 49

**Verlagsleitung** – Susanne Nikoltchev
Geschäftsführende Direktorin der Europäischen Audiovisuellen Informationsstelle

**Redaktionelle Betreuung** – Maja Cappello
Leiterin der Abteilung für juristische Informationen, Europäische Audiovisuelle Informationsstelle

**Redaktionsteam** – Francisco Javier Cabrera Blázquez, Maja Cappello, Sophie Valais
Europäische Audiovisuelle Informationsstelle

**Autoren** – Britt van Breda, Nico van Eijk, Kristina Irion, Tarlach McGonagle, Sander van Voorst
Institut für Informationsrecht (IViR), Universität Amsterdam

**Verlagsassistent** – Olivier Mabilat, Snezana Jacevski, Europäische Audiovisuelle Informationsstelle

**Marketing** – Markus Booms, markus.booms@coe.int, Europäische Audiovisuelle Informationsstelle

**Press und PR** – Alison Hindhaugh, alison.hindhaugh@coe.int, Europäische Audiovisuelle Informationsstelle

**Übersetzung / Korrektur** – Aurélie Courtinat, Johanna Fell, Julie Mamou, Maco Polo Traductions, Stefan Pooth, Roland Schmid, Sonja Schmidt, Lucy Turner, Anne-Lise Weidmann

**Herausgeber**
Europäische Audiovisuelle Informationsstelle, 76, allée de la Robertsau, 67000 Straßburg, Frankreich
Tel. : +33 (0)3 90 21 60 00, Fax : +33 (0)3 90 21 60 19
E-Mail: info.obs@coe.int, www.obs.coe.int

**Beitragende Partnerorganisation**
Institut für Informationsrecht (IViR), Universität Amsterdam, Vendelstraat 7, 1012 XX Amsterdam, Niederlande
Tel: +31 (0) 20 525 3406, Fax: +31 (0) 20 525 3033
E-mail: ivir@ivir.nl, www.ivir.nl

**Umschlaggestaltung** – P O I N T I L L É S, Hoenheim, France

Bitte zitieren Sie diese Publikation wie folgt:
Cappello M. (Hrsg.), *Smart-TV und Datenschutz*, IRIS Spezial 2015-2, Europäische Audiovisuelle Informationsstelle, Straßburg, 2016



Eine Veröffentlichung der Europäischen Audiovisuellen Informationsstelle

# Smart TV
# und Datenschutz

Britt van Breda

Nico van Eijk

Kristina Irion

Tarlach McGonagle

Sander van Voorst

EUROPÄISCHE
AUDIOVISUELLE
INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# Vorwort

Ein Mann geht durch ein Einkaufszentrum. Seine Augen werden von Dutzenden von Kameras mit Netzhaut-Scannern abgetastet. Plötzlich flimmern über die Bildschirme des Einkaufszentrums Werbebotschaften, die auf ihn persönlich zugeschnitten sind …

Das ist ganz offensichtlich eine Szene aus einem Science Fiction-Film (aus „Minority Report“ von Steven Spielberg). Aber so weit von dem, was wir heute bereits erleben können, ist diese Szene keineswegs entfernt. Im Zeitalter des Internet, von Connected TV und „Second screens” („zweiten Bildschirmen“) sind die Möglichkeiten, persönliche Daten der Nutzer zu erhalten, exponentiell angestiegen, und zwar sowohl auf legale als auch auf illegale Weise. Solche Daten sind für die Werbebranche ungeheuer wichtig, denn sie ermöglichen personalisierte Werbung in Online-Diensten und auf vernetzten Geräten. Außerdem können persönliche Daten, die über Suchmaschinen, soziale Medien und vernetzte Geräte gewonnen werden, genutzt werden, um dem Nutzer eines Online-Dienstes bessere Erfahrungswerte zu bieten.

Es gibt jedoch auch eine Kehrseite: Wenn persönliche Daten von Nutzern in die Hände von Dritten gelangen, unabhängig davon, ob diese Daten vom Nutzer freiwillig übermittelt oder unbemerkt weitergegeben werden, kann dies erhebliche Eingriffe in die Privatsphäre der Nutzer bedeuten. Noch schlimmer – es gibt Situationen, in denen die Einblicke in das Leben eines Nutzers weit über das hinausgehen, was er zu akzeptieren bereit ist.

Das wird besonders deutlich beim Fernsehkonsum über Smart TVs, die langsam, aber sicher unsere Wohnzimmer erobern. Weltweit hat sich die Zahl der Smart TVs zwischen 2011 und 2015 verdoppelt, und es wird nicht mehr lange dauern, bis die Mehrzahl der europäischen Haushalte mit solchen Geräten ausgestattet ist.

Ein Smart TV ist ein Fernsehgerät, das über eine Vielzahl von Netzfunktionen verfügt, auf jeden Fall aber über eine Internetverbindung. Wenn diese Geräte mit dem Internet verbunden sind, können sie eine Vielzahl von Nutzerdaten sammeln, etwa über seinen sozialen Hintergrund und sein Finanzprofil. Und diese Daten können genutzt werden, um das Online-Verhalten der Nutzer für direkte Marketingzwecke oder für das Erstellen eines Nutzerprofils für Werbezwecke zu beeinflussen. Diese Geräte enthalten auch Funktionen zur Sprach- und Gesichtserkennung, Bewegungssensoren, für die Schaffung eines Account und viele weitere interaktive Fähigkeiten.

In einer Zeit, in der der traditionelle Fernsehkonsum zurückgeht und immer mehr durch nicht-linearen interaktiven (und „intelligenten“) Konsum ersetzt wird, brauchen wir neue Instrumente. Instrumente, die in der Lage sind, ein wirksames Gleichgewicht zu schaffen zwischen dem Wunsch des Anbieters, sein Angebot zu verbessern und stärker auf die persönlichen Vorlieben des Nutzers abzustimmen, und der Notwendigkeit, die Privatsphäre des Nutzers besser zu schützen. Außerdem wird es immer wichtiger, den Nutzer vor den Gefahren einer solchen Entwicklung zu schützen, um zu verhindern, dass seine Wahlfreiheit eingeschränkt wird, dass er nur begrenzte Informationen erhält und im schlimmsten Fall sogar manipuliert wird.

Es gibt derzeit in Europa keinen einheitlichen Regulierungsrahmen für diesen Bereich. Die Vorschriften zum Datenschutz sind über eine Vielzahl von Rechtsquellen verteilt: So enthält die Richtlinie über audiovisuelle Mediendienste besondere Vorschriften zur Medienregulierung; im Rechtsrahmen für die elektronische Kommunikation gibt es sektorspezifische Regeln, ebenso in der

Richtlinie über den elektronischen Geschäftsverkehr und der Richtlinie über den Schutz der Privatsphäre; ferner enthalten die Datenschutzrichtlinie und die allgemeine Datenschutzverordnung einen allgemeinen Rahmen für den Schutz der Privatsphäre, und schließlich gibt es noch eine Dachverordnung, die auch den Verbraucherschutzrahmen und die menschenrechtliche Dimension enthält.

Dieser zersplitterte Rechtsrahmen hat zur Folge, dass auf nationaler Ebene immer häufiger Fragen auftauchen, wie mit den personenbezogenen Nutzerdaten umgegangen werden soll, die von den Betreibern von Smart TVs gesammelt werden. Diese Ausgabe von IRIS *Spezial*, die vom Institut für Informationsrecht (IViR) der Universität Amsterdam erstellt wurde, gibt einen Überblick über die Besonderheiten von Smart TVs im Vergleich zu anderen Formen audiovisueller Medien. Sie untersucht den Rechtsrahmen für diese Fernsehgeräte, analysiert vier Fallstudien und berichtet über den laufenden Reformprozess.

Die Entwicklungen, die wir zurzeit erleben, etwa Smart Homes mit „Family Hub Refrigerators“ und intelligenten Geräten wie vernetzten „healthcare belts“, müssen zweifellos unter einer ganzheitlichen Perspektive gesehen werden, die alle Aspekte abdeckt. Dies ist auch wichtig unter institutionellen Gesichtspunkten, wo eine Koordinierung zwischen den unterschiedlichen öffentlichen Akteuren notwendiger denn je ist. Diese Fragen werden unter anderem im Rahmen der neuen Datenschutz-Grundverordnung behandelt, auf die sich der Rat, das Europäische Parlament und die Kommission am 15. Dezember 2015 geeinigt haben.[1]

Diese Veröffentlichung gibt erste Einblicke in das Ergebnis dieses langen Entscheidungsprozesses, der bereits 2012 begonnen hat. Der Entwurf war bereits Thema eines Workshops, der am 11. Dezember 2015 von der Informationsstelle in Straßburg durchgeführt wurde und den Titel trug: „The grey areas between media regulation and data protection“ („Grauzonen zwischen Medienregulierung und Datenschutz“). [2] Auf diesem Workshop wurde unter anderem über die Herausforderungen diskutiert, denen die Beteiligten in diesem Bereich gegenüberstehen – Medienregulierungsbehörden, Datenschützer, die Branche, Mediendiensteanbieter und Verbraucher. Die Beteiligung an der Diskussion über die Themen, um die es in diesem Zusammenhang geht, setzt detaillierte Information voraus, und die folgenden Kapitel sollen einen Überblick über die wichtigsten Fragen im Zusammenhang mit dem interaktiven Konsum audiovisueller Inhalte liefern. Dies kann jedoch nur ein Anfang sein.

Straßburg, Januar 2016
**Maja Cappello**
Leiterin der Abteilung für juristische Informationen
Europäische Audiovisuelle Informationsstelle

[1] Siehe http://www.consilium.europa.eu/de/press/press-releases/2015/12/18-data-protection/.

[2] Siehe http://www.obs.coe.int/workshops/-/asset_publisher/kNG5qM2wH8Kq/content/dli-workshop-obs-epra-the-grey-areas-between-media-regulation-and-data-protection.

# Inhaltsverzeichnis

Einführung ..... 7
Aufbau ..... 9
1. Definitionen und Merkmale ..... 11
1.1. Was ist ein Smart-TV-Gerät? ..... 11
1.2. Welche Daten kann ein Smart-TV-Gerät erfassen? ..... 14
1.2.1. Spracherkennung ..... 15
1.2.2. Bewegungssteuerung und Gesichtserkennung ..... 16
1.2.3. (Samsung) Konto ..... 16
2. Regulierungssysteme ..... 19
2.1. Die Richtlinie über audiovisuelle Mediendienste ..... 20
2.2. Regulierung für elektronische Kommunikation ..... 21
2.3. Regelungen zum Schutz der Privatsphäre und zum Datenschutz ..... 24
2.3.1. Anwendungsbereich ..... 25
2.3.2. Allgemeine Definitionen und Grundsätze ..... 25
2.3.2.1. Personenbezogene Daten ..... 25
2.3.2.2. Verarbeitung ..... 26
2.3.2.3. Der für die Verarbeitung Verantwortliche ..... 27
2.3.2.4. Einwilligung ..... 27
2.3.3. E-Privacy-Richtlinie ..... 27
2.3.4. Datenschutzrichtlinie ..... 28
2.3.4.1. Vertraulichkeit und Sicherheit der Verarbeitung ..... 30
2.3.4.2. Internationale Datenströme ..... 30
2.3.5. Neue Datenschutzverordnung ..... 31
2.4. E-Commerce-Richtlinie und EU-Verbraucherschutzgesetze ..... 31
2.5. Regelungsrahmen für Menschenrechte ..... 33
3. Länderspezifische Fallstudien ..... 35
3.1. Deutschland ..... 35
3.1.1. Die gemeinsame Position ..... 36
3.1.2. Die technische Prüfung ..... 37
3.1.3. Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste ..... 38
3.2. Niederlande ..... 40

3.2.1. Fallstudie 1 – *CBP / TP Vision* ..... 41
3.2.1.1. Sachverhalt ..... 41
3.2.1.2. Rechtsrahmen ..... 41
3.2.2. Fallstudie 2 – *CBP / Ziggo* ..... 44
3.2.2.1. Sachverhalt ..... 44
3.2.2.2. Rechtsrahmen ..... 45
3.2.2.3. Künftige Auswirkungen ..... 47
3.3. Ein Beispiel aus Amerika ..... 48
3.3.1. *Electronic Privacy Information Center / Samsung* ..... 49
3.3.1.1. Sachverhalt ..... 49
3.3.1.2. Rechtsrahmen ..... 50
3.3.1.3. Wahrscheinliche Folgen ..... 55
4. Die Datenschutzgrundverordnung ..... 57
4.1. Smart TV und die Datenschutzgrundverordnung ..... 57
4.1.1. Definitionen ..... 57
4.1.1.1. „Alle Informationen“ ..... 58
4.1.1.2. „Über“ ..... 59
4.1.1.3. „Eine bestimmte oder bestimmbare Person“ ..... 59
4.1.1.4. „Natürliche Person“ ..... 60
4.1.1.5. Besondere Kategorien personenbezogener Daten ..... 60
4.1.1.6. Räumlicher Anwendungsbereich ..... 60
4.1.2. Anwendung ..... 61
4.1.2.1. Spracherkennung ..... 61
4.1.2.2. Bewegungssteuerung und Gesichtserkennung ..... 62
4.1.2.3. Erstellen eines Kontos ..... 62
4.2. Das Schutzniveau der Verordnung ..... 64
4.2.1. Grundlegende Bestimmungen ..... 64
4.2.1.1. Vertragliche Pflichten ..... 65
4.2.1.2. Berechtigtes Interesse des für die Verarbeitung Verantwortlichen ..... 65
4.2.1.3. Einwilligung ..... 66
4.2.2. Sonstige wichtige Bestimmungen ..... 67
4.3. Was ist ein angemessenes Schutzniveau und bietet die Verordnung ein solches? ..... 70
4.3.1. Was muss geschützt werden und warum? ..... 70
4.3.2. Was ist angemessener Schutz? ..... 72
4.3.3. Bietet die Verordnung ein angemessenes Schutzniveau? ..... 74
4.3.3.1. Anonymität ..... 74

4.3.3.2. Einwilligung ..... 74
4.3.3.3. Sonstige Anforderungen ..... 76
Abschließende Analyse ..... 77

# Abkürzungen

| | |
|---|---|
| API | Application Programming Interface (Schnittstelle zur Anwenderprogrammierung) |
| AVMDR | Richtlinie über audiovisuelle Mediendienste |
| BCR | Binding Corporate Rules (verbindliche unternehmensinterne Vorschriften) |
| CBP | *College bescherming persoonsgegevens* (niederländische Datenschutzbehörde) |
| CCPA | (US) Cable Communications Policy Act |
| COPPA | (US) Children's Online Privacy Protection Act |
| DSR | Datenschutzrichtlinie (95/46/EG) |
| ECPA | (US) Electronic Communications Privacy Act |
| EPG | Electronic Programme Guide (elektronischer Programmführer) |
| EPIC | Electronic Privacy Information Center |
| FTC | (US) Federal Trade Commission |
| DSGV | Datenschutzgrundverordnung |
| HbbTV | Hybrid Broadcast Broadband TV |
| IoT | Internet of Things (Internet der Dinge) |
| WBP | *Wet bescherming persoonsgegevens* (niederländisches Datenschutzgesetz) |

# Einführung

Mit dem Aufkommen verschiedener Formen des interaktiven Fernsehens scheinen die dystopischen Vorhersagen von Autoren wie Aldous Huxley, Ray Bradbury und insbesondere George Orwell so nahe an der Wirklichkeit wie nie zuvor. Heute steht die Technologie, die den unheimlichen „Teleschirmen" im Roman *1984* zugrundeliegt, weitgehend zur Verfügung und ist weit verbreitet: Diese Schirme sind in der Lage, gleichzeitig zu empfangen und zu senden, sie können nur gedimmt, aber nie ganz ausgeschaltet werden, sie erfassen jedes Geräusch, „das lauter ist als ein sehr leises Flüstern", und jede Bewegung in ihrem Erfassungsbereich.[3]

Bestimmte Arten von Fernsehgeräten (sog. Smart-TV-Geräte) sind in der Lage, auf visuelle, Bewegungs- und akustische Reize wie Gesichtserkennung/Körperbewegungen bzw. Stimmen zu reagieren. Die Fähigkeit intelligenter Fernsehgeräte, von ihren Nutzern generierte personenbezogene Informationen zu erfassen, zu speichern und zu verarbeiten, wirft eine ganze Reihe von datenschutzrelevanten Fragen auf, die in den Regulierungssystemen für herkömmliche Arten audiovisueller Medien nicht thematisiert werden. Die vorliegende Studie[4] beschäftigt sich mit der Regulierung des Datenschutzes im Bereich audiovisueller Medien, wobei ein besonderer Schwerpunkt auf Smart-TV liegt.

In der Vergangenheit waren Fernsehgeräte sperrige Kisten, die in einer der Ecke des Wohnzimmers standen, und nicht viel mehr als „Lichter und Kabel in einem Kasten" - so das berühmte Zitat von Ed Murrow.[5] Später führte die Entwicklung im Bereich der Technik und in den Märkten zu tragbaren, leichteren Geräten mit Flachbildschirmen, doch am Grundsatz änderte sich nichts: Fernseher waren Geräte zum Empfang von Sendesignalen und zur Wiedergabe von Bildern auf einem Bildschirm. Verbreitet wurden die Signale dabei durch eine Punkt-zu-Mehrpunkt-Übertragung, und die Beziehung zwischen den Fernsehzuschauern und ihren Fernsehapparaten verlief immer nur in eine Richtung. Der Schutz der Privatsphäre der Fernsehzuschauer war deshalb weder medienrechtlich noch politisch ein Thema.

Erst in der jüngsten Zeit sind aufgrund der immer größer werdenden Verbreitung interaktiver Fernsehgeräte, die das Verhältnis zwischen Zuschauer und Fernsehgerät zu einer Zwei-Wege-Beziehung machten, datenschutzrelevante Aspekte für Medienrechtler und Politiker zunehmend in den Vordergrund gerückt. Dieser grundsätzliche Wandel ist zunächst und vor allem auf die interaktiven Merkmale von Fernsehgeräten zurückzuführen, aber auch auf eine langsame, aber stetige öffentliche Sensibilisierung für Aspekte des Datenschutzes allgemein.

---

[3] Orwell G., "Nineteen Eighty-Four", in Orwell G., *The Complete Novels*, London, Penguin, 2000, S. 743-744. (Im englischen Original: *telescreen*).

[4] Das Team dankt Natali Helberger für ihre Kommentare zum Entwurf der Studie und Patrick Leerssen für seine wertvolle Hilfe bei Übersetzungsarbeiten.

[5] Murrow E.R., "Wires and Lights in a Box" Speech, Radio Television News Directors Association Convention, Chicago, 15 October 1958, http://www.rtdna.org/content/edward_r_murrow_s_1958_wires_lights_in_a_box_speech.

„Connected-TV“, „Hybrid-TV“ und „Smart-TV“ sind im Wesentlichen synonyme Begriffe zur Beschreibung interaktiver Fernsehgeräte. Im Grunde bezeichnen sie alle Fernsehgeräte - oder die Kombination von Fernsehgeräten und ähnlicher Technologie in Set-Top-Boxen - mit denen lineares Fernsehen möglich ist, die aber auch die Möglichkeit bieten, über eine Internetverbindung Zusatzangebote zu nutzen. Der Begriff „Connected“ bezieht sich somit auf eine Internetverbindung, die es den Zuschauern (die man vielleicht jetzt besser als Nutzer bezeichnen sollte) ermöglicht, die Zusatzangebote zu nutzen. „Hybrid“ bezeichnet die konvergente Art der Technologie: ein Hybrid aus Fernsehgerät und Computer. „Smart“ (intelligent) ist ein Begriff aus dem Bereich Werbung/Marketing, mit dem diese Geräte von den weniger intelligenten Vorläuferprodukten abgegrenzt werden. In dieser Studie wird durchgängig der Begriff „Smart-TV-Gerät“ verwendet.

Wenn das Gerät nicht mit dem Internet verbunden ist oder die Zusatzfunktionen nicht aktiviert sind, bleibt ein Smart-TV-Gerät in jeder Hinsicht ein herkömmliches Fernsehgerät, mit dem eine lineare Fernsehnutzung möglich ist. Dies unterläuft jedoch die Zweckbestimmung der angebotenen zusätzlichen technischen Merkmalen und Fähigkeiten. Smart-TV-Geräte bieten Zugang zu einer Reihe von Internetdiensten wie Webbrowsern, Video-on-demand, Soziale Netzwerken und der Nutzung von Apps. Neben der Möglichkeit, sich Webseiten anzusehen, kann der Nutzer auch Transaktionen vornehmen.

Ian Walden und Lorna Woods haben eine nützliche Diagnose der datenschutzrechtlichen Aspekte im Zusammenhang mit den Fähigkeiten von Smart-TV-Geräten erstellt. Sie verweisen darauf, dass „in der derzeitigen Rundfunkumgebung in zwei Schlüsselbereichen zwei datenschutzrelevante Bedenken bestehen“:

> *„die verstärkten Möglichkeiten der Überwachung und Erfassung unserer Sehgewohnheiten insbesondere für Profiling- und Marketingzwecke; sowie die Möglichkeit, die Inhalte, die wir uns ansehen, zu überwachen oder abzufangen“.*[6]

Zu diesen Bedenken könnte man noch ähnliche Aspekte im Zusammenhang mit der Überwachung, Erfassung und Kontrolle unserer Gewohnheiten hinsichtlich der Nutzung von Informationen und von nicht über den Rundfunk verbreiteten Inhalten im Rahmen unserer sonstigen Online-Aktivitäten über das Smart-TV-Gerät hinzuzählen. Ein weiterer Aspekt hat mit der Fähigkeit der Smart-TV-Geräte zu tun, personenbezogene Daten durch verschiedene Funktionen wie Sprach- oder Gesichtserkennung zu erfassen und zu verarbeiten. Die Verarbeitung dieser Daten bedeutet in der Regel, dass die Daten mit verschiedenen Dritten geteilt werden, was aus der Perspektive des Datenschutzes betrachtet die Sache noch komplexer macht.

Zum Smart-TV-„Ökosystem“ gehört eine Reihe unterschiedlicher Akteure, die - auf die eine oder andere Art - Zugang zu Informationen über den Konsum von Rundfunkinhalten und über Online-Aktivitäten des Nutzers sowie Zugang zu personenbezogenen Daten des Nutzer erhalten. Zu diesem Ökosystem gehören der Hersteller der Smart-TV-Geräte, der Anbieter der sog. HbbTV-Dienste (Hybrid broadband broadcast TV), der Portalbetreiber, der Betreiber des App-Stores, der Anbieter der Apps und der Betreiber von Empfehlungsdiensten.[7] Insgesamt liegt bei der Verwendung von Smart-TV-Geräten aufgrund der verschiedenen Beteiligten, aber auch wegen der

[6] Walden I. and Woods L., “Broadcasting Privacy”, *Journal of Media Law,* 2011, 3(1), S. 117-141, hier 121.

[7] Düsseldorfer Kreis, *Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste*, 15-16 September 2015, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OH_Smart_TV_v1.0.pdf., S. 9.

komplexen Aspekte der Verbreitung, eine deutlich komplexere Wertschöpfungskette als bei traditionellen Fernsehdiensten vor.[8]

Die Tatsache, dass so viele unterschiedliche Beteiligte involviert sind, gibt zu der Befürchtung Anlass, dass dies zu einer Mehrfachüberwachung führen könnte: „einer Überwachung nicht einfach durch den Staat, sondern durch Firmen, Vermarkter und unsere sozialen Netzwerke".[9] Walden und Woods bringen es auf den Punkt: „Eine Reihe von Akteuren entlang der Dienstleistungskette ist in der Lage, die Nutzung von Rundfunkinhalten durch die Zuschauer zu überwachen, wobei weder die entsprechenden Verhältnisse transparent sein dürften, noch für die Parteien klar feststeht bzw. sie verstanden haben, welche Pflichten jeweils bestehen - nicht zuletzt aus der Sicht der Zuschauer".[10]

## Aufbau

Diese Studie befasst sich mit einer Reihe von Fragen:

- Was ist Smart-TV?
- Wie lässt sich Smart-TV mit anderen Formen audiovisueller Medien vergleichen?
- Welche Regulierungssyteme gelten für Smart-TV?
- Welche Erkenntnisse ergeben sich aus den ausgewählten länderspezifischen Fallstudien?
- Worin liegen die Gefahren im Zusammenhang mit der Erfassung, Speicherung und Verarbeitung von Informationen über private Nutzer durch Firmen?
- Wie werden sich die einschlägigen Regulierungssysteme wahrscheinlich weiterentwickeln?

In **Kapitel I** sind die verschiedenen terminologischen und definitorischen Ansätze zu „Smart-TV" dargestellt; dabei wird das smarte Fernsehen gegenüber anderen Formen von (interaktiven) audiovisuellen Medien abgegrenzt. Die wichtigsten Unterscheidungsmerkmale von Smart-TV-Geräten (die im Hinblick auf Datenschutz bzw. Schutz der Privatsphäre von Bedeutung sind) werden erläutert: Spracherkennung, Bewegungserkennung, Gesichtserkennung, interaktive Fähigkeiten (z.B. über Apps und soziale Medien) und integrierte Nutzerkonten (z.B. Samsung). Diese Funktionen von Smart-TV-Geräten erleichtern das Erfassen, Speichern und Verarbeiten personenbezogener Daten durch Unternehmen. Sie stehen im Mittelpunkt der Untersuchung von Regulierungssystemen sowie Fallstudien in den nachfolgenden Kapiteln.

In **Kapitel II** wird dargestellt, wie sich die Regulierung für audiovisuelle Medien und die Regulierung betr. den Datenschutz bzw. den Schutz der Privatsphäre traditionell unabhängig voneinander entwickelt haben. Konvergenzerscheinungen sowie das Aufkommen und die Verbreitung intelligenter Technologien zwingen die Regulierungsstellen in beiden Sektoren dazu, zusammenzuarbeiten und nach neuen Regelungsansätzen zu suchen, die diese Entwicklungen widerspiegeln und berücksichtigen. In diesem Kapitel wird auf die mangelnde Relevanz der AVMD-Richtlinie eingegangen, die begrenzte Relevanz der Rahmen- und Zugangsrichtlinien; die zunehmende Relevanz der Richtlinien für Datenschutz bzw. den Schutz der Privatsphäre; die

[8] Nooren P., Leurdijk A., van Eijk N., "Net neutrality and the value chain for video", *info*, 2012, Vol. 14 ss: 6, S. 45 – 58, http://www.ivir.nl/publicaties/download/511.

[9] Richards N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, New York, Oxford University Press, 2015, S. 5.

[10] Walden I. and Woods L., "Broadcasting Privacy", supra Fußnote 6, S. 140.

wahrscheinlichen Folgen der (vorgeschlagenen) Datenschutz-Grundverordnung. Weiter wird die Bedeutung von Verbraucherrechten und Menschenrechtsnormen dargestellt.

Ausgehend von der Analyse des komplexen Regulierungsrahmens bietet **Kapitel III** einen Überblick darüber, wie sich relevante Rechtsfragen ergeben und wie diese in der Praxis auf einzelstaatlicher Ebene beantwortet werden. Vier Fallstudien bilden den Kern des Kapitels und zeigen, welche Erfahrungen in Deutschland, den Niederlanden (zwei Fallstudien) und in den USA gemacht wurden:

1) Deutschland: Gemeinsame Position der deutschen Datenschutzbehörden, technische Prüfung von Smart-TV-Geräten und Orientierungshilfe;
2) die Untersuchungen der niederländischen Datenschutzbehörde über die Verarbeitung personenbezogener Daten auf Philips Smart-TV-Geräten durch TP Vision Netherlands B.V.;
3) die Untersuchungen der niederländischen Datenschutzbehörde über die Verarbeitung personenbezogener Daten durch Verwendung interaktiver Digitalfernsehdienste von Ziggo;
4) Electronic Privacy Information Center / Samsung: Beschwerde der Federal Trade Commission über routinemäßiges Abfangen und Aufzeichnen privater Gespräche in Wohnungen.

Die Fallstudien enthalten eine detaillierte Analyse der relevanten rechtlichen Aspekte und der allgemeinen Auswirkungen auf Regelungsansätze für Smart-TV-Geräte.

**Kapitel IV** baut auf dem vorausgehenden Kapitel auf. Es enthält Überlegungen zu möglichen regelungstechnischen Entwicklungen der Zukunft (insbesondere die möglichen Auswirkungen der vorgeschlagenen Datenschutz-Grundverordnung), wobei der Schwerpunkt auf den oben beschriebenen besonderen Funktionen von Smart-TV-Geräten sowie auf (potenziellen) Schäden liegt, die durch diese technologischen Funktionalitäten möglich Erfassung, Speicherung und Verarbeitung personenbezogener Daten möglich sind.

Ergänzt wird die Studie durch eine zusammenfassende Analyse.

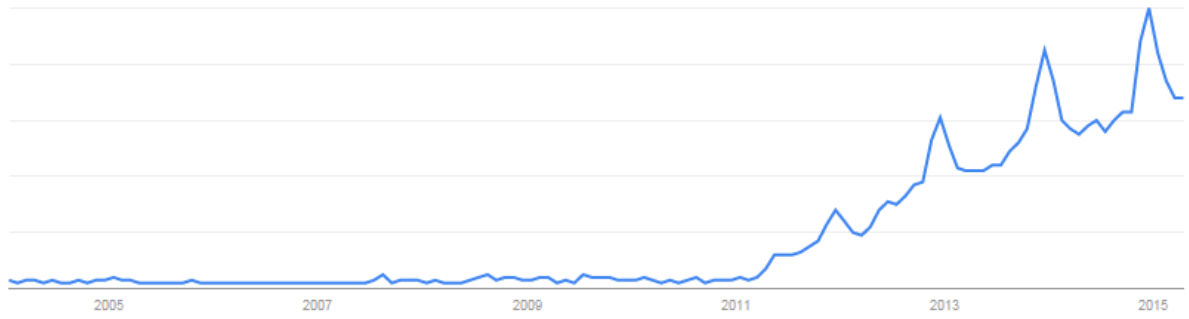
# 1. Definitionen und Merkmale

Smart-TV-Geräte erfreuen sich in europäischen Haushalten zunehmender Beliebtheit, was bedeutet, dass die Öffentlichkeit mit dem Konzept vertraut ist. Der Begriff „Smart-TV" erinnert zu Recht an den Begriff „Smartphone“, doch sind Smart-TV-Geräte noch nicht so weit verbreitet wie intelligente Telefone.

## 1.1. Was ist ein Smart-TV-Gerät?

Seit 2011 wird der Begriff „Smart-TV-Gerät“ zunehmend verwendet; dies lässt sich anhand von historischen Google-Suchdaten nachweisen (siehe Abb. 1).[11]

*Abb. 1: Historische Darstellung: Google-Suchanfragen nach dem Begriff „Smart-TV“*




*Quelle: Google trends*

Der Begriff wurde zwar noch nicht in das Oxford English Dictionary aufgenommen, wird aber im Allgemeinen als „ein internetfähiges Fernsehgerät“ definiert. Andere Definitionen verweisen auf die Möglichkeit der Verwendung bestimmter „Apps“, einschl. der Anwendungen Dritter.[12]

Eine einfache Definition könnte von einem Vergleich mit einem normalen (nicht intelligenten) Fernsehgerät ausgehen. Diese Apparate sind eigentlich kaum mehr als einen Bildschirm. Alle eingebauten Teile dienen dem Zweck, auf dem Bildschirm Inhalte wiederzugeben,

[11] Online via www.google.nl/trends.

[12] Kovach S., “What is a smart TV?”, *Business Insider*, 8. Dezember 2010, http://www.businessinsider.com/what-is-a-smart-tv-2010-12?IR=T.

die auf externe Quellen wie Antennen, Kabel, SCART- oder FBAS-Verbindungen zurückgehen. Entsprechendes kann man von Mobiltelefonen sagen. Ein herkömmliches Handy hat keine andere Funktion als die Übertragung von Sprache über ein Mobilfunknetz. Fortgeschrittenere Modelle waren in der Lage, eine einfache Internetverbindung über GPRS herzustellen. Doch sie zählten nicht zu der Kategorie von Smartphones.

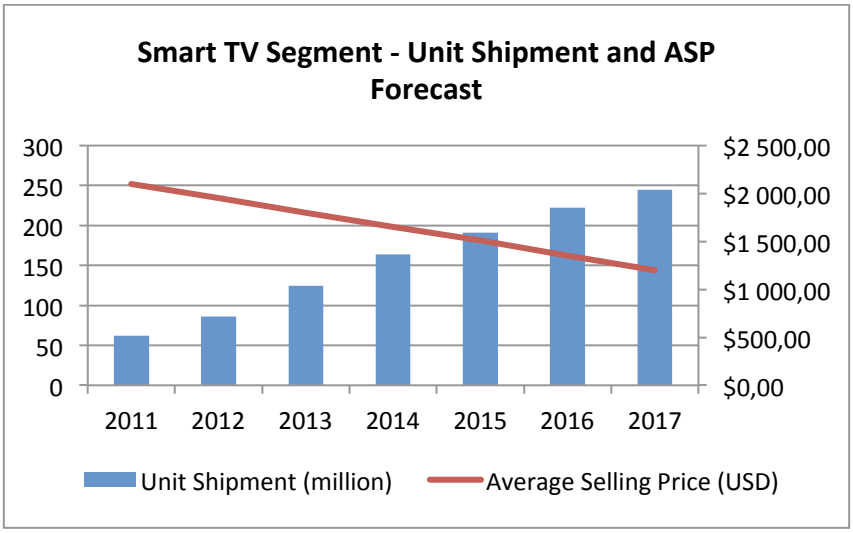
Ein Smart-TV kann wie ein ganz normales Fernsehgerät Inhalte über die oben genannten externen Quellen wiedergeben. Zusätzlich gibt es andere Methoden, Verbindungen zu einem solchen Fernsehgerät herzustellen. So sind die meisten Smart-TV-Geräte mit Ethernet, WLAN, USB und Bluetooth ausgestattet. Auch hier liegt wieder ein Vergleich mit dem Smartphone nahe. Diese Kommunikationskanäle bieten die Möglichkeit, sich nicht nur mit lokalen Quellen in der unmittelbaren Umgebung des Fernsehgeräts zu verbinden, sondern auch mit anderen Quellen im weiteren Umfeld, unabhängig von der physischen Entfernung. Auf diese Weise wird das Fernsehgerät zu einem wichtigen Element im Internet der Dinge (IoT).

Hinsichtlich der Definition, die auf die Möglichkeit der Nutzung von Applikationen abstellt, ist zu sagen, dass auch auf normalen Fernsehgeräten einfache Programme laufen können. Im Unterschied dazu verfügen Smart-TV-Geräte über ein Betriebssystem, das als Plattform für Applikationen verschiedener Entwickler dient. Ferner haben Smart-TV-Geräte im Allgemeinen eine Rechnerleistung, die es ermöglicht, sehr viel komplexere Programme als auf nichtintelligenten Geräten laufen zu lassen. Man könnte sagen, dass die gesamte Smart-TV-Architektur auf dieser Funktion beruht - neben der Wiedergabe von Bildern über externe Quellen.

Nach diesen Vorbemerkungen wird für Zwecke dieser Studie folgende Beschreibung bzw. Arbeitsdefinition vorgeschlagen: „Ein Smart-TV ist ein Fernsehgerät, das über eine Vielzahl von Verbindungsmöglichkeiten verfügt, wobei in jedem Fall eine Internetverbindung eingeschlossen ist. Darüber hinaus muss es über ein Betriebssystem verfügen, das über Apps Inhalte bereitstellt, wobei dies im Wesentlichen über das Internet erfolgt. Dadurch ist mit dem Smart-TV eine nichtlineare Fernsehnutzung möglich, und der Nutzer ist in der Lage, von ihm persönlich ausgewählte Inhalte zu einem Zeitpunkt seiner Wahl zu nutzen."

Weitere Erkenntnisse über die aktuelle Lage am Markt und das erwartete Marktwachstum vermitteln die folgenden Übersichten, die auf verschiedene Aspekte eingehen:

*Abb. 2: Weltweiter Absatz von Smart-TV-Geräten 2011-2017*

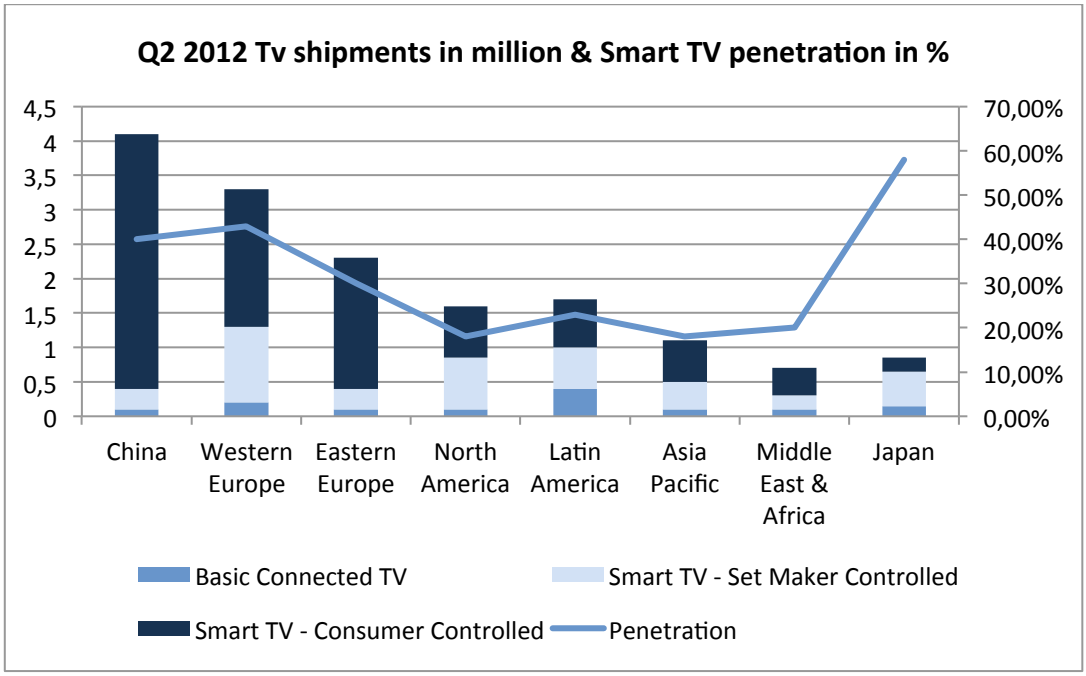



*Hinweis: Alle Zahlen gerundet. Basisjahr ist 2012*

*Quelle: Frost & Sullivan*

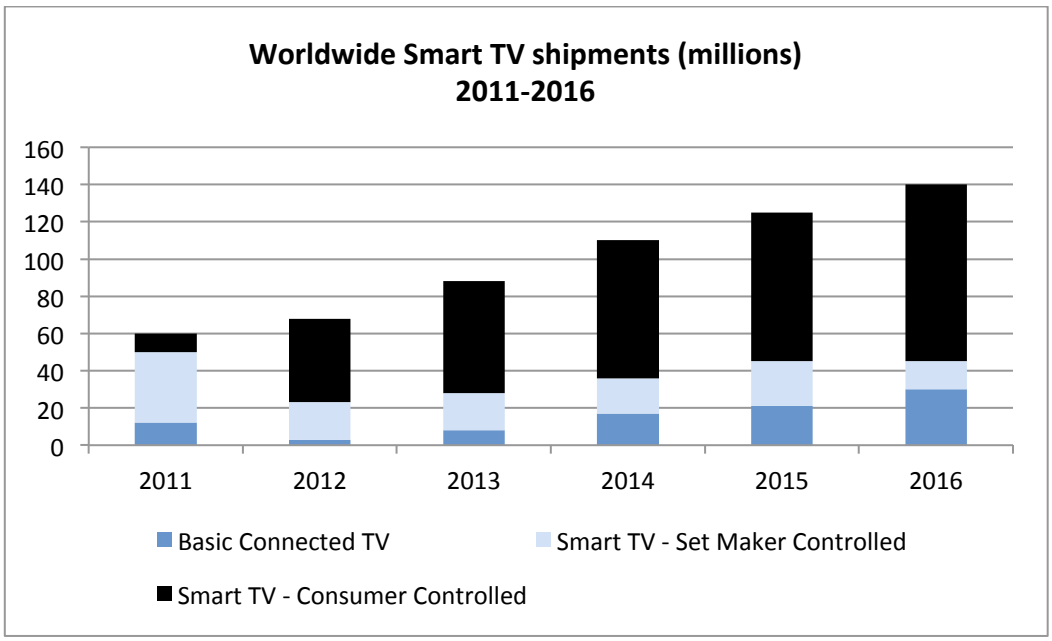
Abb. 2 zeigt anhand von Zahlen aus einer anderen Quelle (Frost&Sullivan), dass der Absatz von Smart-TV in den nächsten Jahren steigen und dass - wie bei „neuen“ Technologien üblich - der Durchschnittsverkaufspreis kontinuierlich sinken wird.

*Abb. 3: Absatz von Smart-TV im 2. Quartal 2012 nach Region (in Tsd.)*




*Quelle: NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report*

*Abb. 4: Absatz von Smart-TV-Geräten, Prognose 2011-2016*




*Quelle: NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report*

Abb. 3 und 4 geben eine Überblick über die Art der Steuerung der Internetverbindung. Der Trend geht eindeutig in Richtung von Smart-TV-Geräten mit nutzergesteuerten Browsern (Consumer Controlled). Denn die Nutzer möchten sich frei im Internet bewegen können und nach Inhalten (im Wesentlichen Video-Inhalten) suchen, die ihrem Geschmack entsprechen. Nutzergesteuerte Smart-TV-Geräte erlauben dies - im Gegensatz zu Geräten mit entsprechenden Voreinstellungen seitens der Hersteller (*Set-Maker-Control*), bei denen die Nutzer nur die vom Hersteller gestaltete Plattform verwenden können.

*Übersicht 1: Anzahl internetfähiger Fernsehgeräte (in Mio.)*

| 2. Q. 14 Rangfolge | Hersteller | 2. Q. 14 | 2. Q. 13 | 2. Q. 14 Anteil | 2. Q. 14 Veränderung gegenüber Vorjahr |
|---|---|---|---|---|---|
| 1 | Sony | 123,8 | 96,8 | 24,8% | 27,9% |
| 2 | Samsung | 62,3 | 34,4 | 12,5% | 80,9% |
| 3 | Nintendo | 56,8 | 67,5 | 11,4% | -15,8% |
| 4 | Microsoft | 55,4 | 53,8 | 11,1% | 2,9% |
| 5 | LG | 32,2 | 16,0 | 6,5% | 101,9% |
| 6 | Panasonic | 29,9 | 19,6 | 6,0% | 52,4% |
| 7 | Apple | 18,7 | 13,0 | 3,8% | 44,7% |
| 8 | Sharp | 15,0 | 9,8 | 3,0% | 52,7% |
| 9 | Toshiba | 10,2 | 5,1 | 2,0% | 98,8% |
| 10 | Philips | 9,7 | 5,7 | 1,9% | 70,0% |
| 11 | Roku | 8,3 | 5,5 | 1,7% | 51,9% |
| 12 | Google | 6,0 | 0,0 | 1,2% | keine Angaben |

Hinweis: Zu den internetfähigen Fernsehgeräten zählen Smart-TV-Geräte, Smart Blu-ray-Player, Spielkonsolen und digitale Media-Streamer.

*Quelle: Gartner, Global Connected TV Device Tracker: 2. Q. 2014*

## 1.2. Welche Daten kann ein Smart-TV-Gerät erfassen?

Nach der Entwicklung einer Arbeitsdefinition für Smart-TV erscheint es nunmehr sinnvoll, die technischen Funktionen (der meisten) Smart-TV-Geräte genauer zu beschreiben. Die Beschreibung basiert auf einem durchschnittlichen Fernsehgerät der Firma Samsung.[13] Mit einem globalen Marktanteil von 29% ist Samsung der führende Hersteller weltweit.[14] Das Gerät verfügt über einen

[13] Das Modell UE40F6320 von Samsung verfügt über die meisten am Markt verfügbaren Funktionen, siehe: http://www.samsung.com/uk/consumer/tv-audio-video/televisions/hd-tvs/UE40F6320AKXXU.

[14] Siehe https://technology.ihs.com/548718/tv-shipments-post-largest-annual-decline-in-five-years-ihs-says.

sog. SMART-Hub, das „Herz“ des Geräts, das Zugang zu vielen Arten von Apps und anderen intelligenten Funktionen ermöglicht.[15]

Die verschiedenen Funktionen des Geräts sind in der Gebrauchsanleitung dargestellt. Unter der Überschrift „Smart-Interaktion“ ist eine Reihe von Funktionen aufgelistet, u.a.

- Spracherkennung
- Bewegungssteuerung
- Gesichtserkennung
- Erstellung eines Samsung-Kontos

Offensichtlich gibt es mehrere Arten der Steuerung des Geräts sowie die Möglichkeit, ein Konto einzurichten. Obwohl diese Funktionen das Seherlebnis sicherlich verbessern, sind einige Vorbehalte zu machen. Wie oben ausgeführt, sind herkömmliche Fernsehgeräte kaum mehr als Bildschirme. Im Falle von Smart-TV-Geräten ergibt sich aufgrund der vorgesehenen zusätzlichen Funktionalitäten die Notwendigkeit, das Gerät mit einer Reihe von Sensoren - mit Augen und Ohren - auszustatten.

Im folgenden Abschnitt wird auf diese Sensoren und die Daten, die mit ihnen erfasst werden können, eingegangen. Der Schwerpunkt liegt dabei auf den technischen Möglichkeiten. Die Frage, ob die Datenerfassung in der Praxis tatsächlich erfolgt, wird nicht diskutiert, da dies einen ganz anderen Forschungsansatz erfordert. Gelegentlich wird jedoch auf Beispiele aus der Praxis verwiesen.

### 1.2.1. Spracherkennung

Für das Erkennen von Sprachbefehlen muss das Smart-TV mit einem Mikrofon ausgestattet sein, das die Geräusche aus der Umgebung des Geräts erfasst. Der Begriff „Spracherkennung“ deutet darauf hin, dass das Gerät nicht nur in der Lage ist, Geräusche zu erfassen, sondern diese Daten auch filtern und in Befehle umsetzen kann. Im Prinzip ist es somit möglich, dass das Smart-TV-Gerät alle in der Nähe des Geräts gesprochenen Worte aufzeichnet und diese nach möglichen Befehlen durchsucht. Dass es sich dabei um keine rein hypothetische Möglichkeit handelt, zeigt der Wirbel um einen Absatz in den Nutzungsbedingungen für Smart-TV-Geräte von Samsung:

> *„Bitte beachten Sie: Sollten die von Ihnen gesprochenen Worte persönliche oder andere sensible Informationen enthalten, gehören diese Informationen zu den erfassten und an Dritte weitergeleiteten Daten.“*[16]

Samsung hat als Reaktion auf diese negative Werbung den entsprechenden Absatz schnell geändert, doch zeigt der Vorfall, dass es durchaus realistisch ist, dass Smart-TV-Geräte mehr aufzeichnen als man zunächst annimmt. Aus der Perspektive der Werbewirtschaft betrachtet ermöglicht diese Funktion - im wörtlichen und übertragenen Sinne - den Zugang zu Privathaushalten, was völlig neue

[15] Siehe Gebrauchsanleitung für Samsung UE40F6320, 2013, http://org.downloadcenter.samsung.com/downloadfile/ContentsFile.aspx?CDSite=UNI_DE&CttFileID=5376929&CDCttType=UM&ModelType=N&ModelName=UE40F6320AW&VPath=UM/201303/20130316093517079/[DEU]X12DVBEUF-0313.pdf.

[16] Harris S., “Your Samsung SmartTV Is Spying on You, Basically”, *The Daily Beast*, 2. Mai 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html#.

Möglichkeiten der Vermarktung eröffnet. Diese Aspekte werden im Zusammenhang mit der Fallstudie über die Beschwerde des Electronic Privacy Information Centre bei der United States Federal Trade Commission in Kapitel III näher erläutert.

### 1.2.2. Bewegungssteuerung und Gesichtserkennung

Das Fernsehgerät kann Sprachbefehle erkennen und auf Gesten und Bewegungen reagieren. Zusätzlich besteht die Möglichkeit, dass sich Nutzer über die Funktion Gesichtserkennung in den SMART-Hub einloggen können.

Diese Funktionen setzen voraus, dass das Gerät über eine Kamera verfügt. Beim hier berücksichtigten Modell wurde eine externe Kamera verwendet, obwohl es viele Modelle mit eingebauter Kamera gibt. Mit dieser Kamera kann das Fernsehgerät Bilder aufzeichnen - z.B. um Voice-Chat zu ermöglichen. Wie bei der Spracherkennung ist ein nachgeschaltetes Filtern möglich, mit dem das Programm Gesichter einzelner Nutzer erkennen und voneinander unterscheiden kann. Dadurch könnten Rückschlüsse auf die Anzahl der Zuschauer bei bestimmten Angeboten gezogen werden; Entsprechendes gilt aber auch hinsichtlich der Identität der Beteiligten bzw. zumindest für Nutzerprofile auf der Grundlage von Sehgewohnheiten.

### 1.2.3. (Samsung) Konto

Diese Datenkategorie umfasst verschiedene Daten, deren Erfassung technisch möglich ist und die zur (freiwilligen oder unfreiwilligen) Erstellung von „Profilen“ führen könnten.

Die Nutzer von Smart-TV-Geräten haben die Option, ein Konto einzurichten, mit dem verschiedene Daten verknüpft werden können. Zu diesen Daten können gehören: inhaltliche Anregungen oder Empfehlungen ausgehend vom Sehverhalten, Werbung ausgehend vom Sehverhalten oder von Reaktionen auf frühere Werbung. Aus Sicht der Werbetreibenden ist die Einrichtung eines Kontos durch den Nutzer selbst wahrscheinlich die attraktivste Option. Die Gründe für diese Präferenz werden weiter unter dargestellt.

Hinzu kommt, dass Daten auch ohne ein vom Nutzer eingerichtetes Konto erfasst werden können. Wie bei anderen miteinander verbundenen Geräten ist es - sobald das Gerät mit dem Internet verbunden ist - einfach, ein Profil über das Sehverhalten zu erstellen und es mit der IP-Adresse des Geräts (die auch Aufschluss über seinen Standort gibt) zu verknüpfen. Das Sehverhalten an sich wird durch verschiedene Faktoren wie gesehene Inhalte, Identität des Zuschauers, Zeitpunkt und Dauer der Nutzung bestimmt (vgl. die deutsche Fallstudie in Kapitel III). Das Ganze lässt sich natürlich dadurch vermeiden, dass man das Smart-TV-Gerät nicht mit dem Internet verbindet. Das macht dann ein Smart-TV-Gerät zu einem ganz normalen Bildschirm. Aufgrund der verschiedenen attraktiven Merkmale, die die smarten Funktionen aufweisen, ist dieses Szenario eher unwahrscheinlich. Die Analogie mit dem Smartphone ist schnell hergestellt: Ohne Internet ist es nicht mehr als ein Telefon mit einer Reihe von funktionslos gewordenen Applikationen.

Aufgrund der vorstehenden Ausführungen kann man zu dem Schluss kommen, dass sich ein Smart-TV-Gerät hauptsächlich durch die Eigenschaft auszeichnet, die es zu einem Teil des Internets der Dinge macht: die Internetfähigkeit. Hinzu kommt, dass es ein leistungsfähiger Prozessor ermöglicht, verschiedene Apps laufen zu lassen. Zusätzlich zu den im Definitionsteil zu Beginn dieses Abschnitts beschriebenen Merkmalen ist das Smart-TV-Gerät mit einer Reihe von Sensoren ausgestattet, mit denen eine Beobachtung der Umgebung des Geräts möglich ist. Deshalb ist das

Gerät in der Lage, alle Arten von Daten zu erfassen und diese über das Internet weltweit zu verbreiten. Die Tatsache, dass dies auf undifferenzierte Weise erfolgen kann, bedeutet, dass auch Daten von Minderjährigen und Besuchern aufgezeichnet werden können.

Die Integration all dieser Funktionalitäten in ein einziges Gerät macht das Smart-TV im Zuge der Entwicklung des intelligenten und interaktiven Fernsehens zu einem bemerkenswerten Phänomen. Diese Funktionalitäten - sofern es sie vorher überhaupt gab - waren traditionell unterschiedlich und mit unterschiedlichen Technologien verknüpft, für die wiederum verschiedene Regulierungssysteme galten. Einer der historischen Gründe für eine Medienregulierung war die Fähigkeit der Medien, die öffentliche Meinung zu beeinflussen. In diesem Zusammenhang werden die Reichweite und Wirkung audiovisueller Medien oft genannt, und der US Supreme Court sprach bekanntermaßen von der „einzigartigen Allgegenwart " des Mediums Fernsehen, die sich u.a. daran zeige, dass es bis in die „Privatsphäre der Wohnung" vordringen könne, wo doch das „Recht, in Ruhe gelassen zu werden" einen Ehrenplatz habe.[17] Diese Feststellung wurde im Zusammenhang mit einer Rechtssache (*F.C.C. gegen Pacifica*) getroffen, in der es um die Frage ging, ob es zulässig ist, dass vom Rundfunk ausgestrahlte anstößige oder unanständige Bilder bis in die privatesten aller Räume - die Wohnung - vordringen können. Die dazu verwendete Technik, die ein solches Vordringen möglich machte - ein einfacher Fernseher aus den 1970er Jahren - war ein Verfahren, das eine Übertragung in nur einer Richtung zuließ. Smart-TV-Geräte sind jedoch von der Technologie her ganz anders geartet. Ihre Fähigkeit, bidirektionale Übertragungen zu ermöglichen, verleiht dem Begriff der „einzigartigen Allgegenwart" des Fernsehens eine völlig neue Bedeutung.

[17] *Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726, at 748, https://supreme.justia.com/cases/federal/us/438/726/case.html.

# 2. Regulierungssysteme

Smart-TV-Geräte gehören zu einer neuen Generation konvergenter Geräte für den Nutzer, und die Funktionen und Dienste, die damit genutzt werden können, sind in verschiedenen sektorspezifischen Bestimmungen auf EU-Ebene geregelt. Die fünf Regelungsbereiche, die für Smart-TV in Frage kommen, sind audiovisuelle Medien, elektronische Kommunikation, Datenschutz, Verbraucherschutz und Menschenrechte. Jedes Regelungsinstrument hat dabei seine speziellen Zielsetzungen und widmet sich unterschiedlichen Aspekten von Smart-TV-Geräten. Bei der Darstellung dieser Instrumente ist darauf zu achten, auf welche Weise Smart-TV-Geräte dem jeweiligen Anwendungsbereich zugeordnet werden können und für welchen Akteur im Smart-TV-Ökosystem die gesetzlichen Auflagen gelten.[18]

Auf EU-Ebene kann die Arbeitsteilung in Sachen Regulierung wie folgt dargestellt werden: die AVMD-Richtlinie sieht eine Mindestharmonisierung der Bestimmungen für lineare audiovisuelle Mediendienste bzw. audiovisuelle Mediendienste auf Abruf vor (sog. abgestufte Regelungsdichte).[19] Der Regelungsrahmen für elektronische Kommunikation umfasst fünf Richtlinien, die folgende Bereiche abdecken: elektronische Kommunikationsnetzwerke und -dienste, die für die Übertragung elektronischer Signale verwendet werden; zugehörige Einrichtungen und Dienste und bestimmte Aspekte von Endgeräten. Bezüglich Smart-TV sind bestimmte Regelungen der Rahmenrichtlinie [20] und der Zugangsrichtlinie [21] von Bedeutung, insbesondere im Hinblick auf technische Merkmale digitaler Fernsehdienste, so die Schnittstellen zur Anwendungsprogrammierung (API), die Zugangskontrollsysteme und der elektronische Programmführer (EPG) - die alle für den Zugang zu Inhalten und letztlich für die Auffindbarkeit der Inhalte von Bedeutung sind. Der Zugang zu Diensten fällt unter die Regelung über Netzneutralität (in der Universaldienstrichtlinie).[22] Die

[18] Zu einer ausführlicheren Darstellung dieser Aspekte siehe allgemein: Hans-Bredow-Institut für Medienforschung und Institut für Informationsrecht, „Hermes: Study on the Future of European Audiovisual Regulation“, Hamburg/Amsterdam, October 2015, http://www.ivir.nl/publicaties/download/1643.

[19] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rats vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32010L0013.

[20] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) in der durch Richtlinie 2009/140/EG und Verordnung 544/2009 abgeänderten Form,

https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf (inoffizielle konsolidierte Fassung).

[21] Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie) in der durch Richtlinie 2009/140/EG geänderten Fassung,

http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140access_1.pdf (inoffizielle konsolidierte Fassung).

[22] Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom Donnerstag, 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie) in der durch Richtlinie 2009/136/EG geänderten Fassung,

https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Directive%202002%2022%20EC_0.pdf (inoffizielle konsolidierte Fassung).

Datenschutzrichtlinie für elektronische Kommunikation (sog. E-Privacy-Richtlinie)[23], die auch Bestandteil der Rahmenregelungen für elektronische Kommunikation ist, führt harmonisierte Regelungen für das Recht auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikation ein. Diese Richtlinie spezifiziert und ergänzt die Datenschutzrichtlinie[24], die für die Verarbeitung personenbezogener Daten im Allgemeinen gilt. Auf bestimmte Aspekte der Richtlinie über den elektronischen Geschäftsverkehr[25] und der EU-Bestimmungen zum Verbraucherschutz sollte hingewiesen werden, so etwa die Bestimmungen zu Verbraucherverträgen über digitale Inhalte. Letztlich ist auch noch die Bedeutung der Menschenrechtsnormen zu betonen.

Trotz der hier praktizierten regelungstechnischen Arbeitsteilung ergeben sich auch Herausforderungen - wie sich noch in diesem Abschnitt zeigen wird, da sich diese Regelungssysteme traditionell unabhängig voneinander entwickelt haben. Die einzelnen Regelungen gelten zwar gemeinsam für Smart-TV-Geräte, doch sind die Ziele der jeweiligen anderen Regelungen nicht ausreichend berücksichtigt, und die Regelungen scheinen sich von der Wirkung her nicht in optimaler Weise zu ergänzen. Hinzu kommt, dass die Zuständigkeiten für die Aufsicht und die Durchsetzung in den EU-Mitgliedstaaten entsprechend auf unterschiedliche Stellen aufgeteilt sind, wobei jede Stelle für die Umsetzung ihrer jeweiligen sektorspezifischen Regelung zuständig ist. Von wenigen Ausnahmen abgesehen gibt es in der Praxis zwischen den nationalen Behörden wenig Informationsaustausch und Koordinierung über Sektorgrenzen hinweg, was wirksame Reaktionen auf übergreifende regulierungstechnische Herausforderungen durch Smart-TV-Geräte erschwert.

## 2.1. Die Richtlinie über audiovisuelle Mediendienste

Das Kernstück der EU-Regulierung im audiovisuellen Mediensektor ist zurzeit die AVMD-Richtlinie.[26] Die Richtlinie ist die Nachfolgerin der Richtlinie Fernsehen ohne Grenzen aus dem Jahr 1989 und stellt eine unmittelbare Reaktion auf die Konvergenz der Medien und die Veränderungen im Medienbereich hinsichtlich Produktion, Formate und Vertrieb dar. Der neu eingeführte Begriff „audiovisuelle Mediendienste“ [Artikel 1 (1) a)] umfasst bekannte Fernsehformate und Abrufdienste, die von Anbietern aus festgelegten Katalogen bereitgestellt werden. Obwohl Smart-TV-Geräte den Zugang zu audiovisuellen Mediendiensten - neben Online-Diensten im Allgemeinen - erleichtern können, hat die AVMD-Richtlinie nicht das Ziel, Verbrauchergeräte als solche zu regulieren.[27] Die Hersteller von Smart-TV-Geräten werden von der Definition nicht erfasst und fallen nicht in den Anwendungsbereich der Richtlinie. Digitale Plattformen, die über Smart-TV-Geräte laufen, sind *per se* nicht vom Anwendungsbereich ausgenommen, sofern sie audiovisuelle Mediendienste anbieten. Vertikal integrierte Anbieter, die neben der Hardware auch noch Zugang zu audiovisuellen Mediendiensten bieten, sind am Pay-TV-Markt häufig anzutreffen. Daher fallen sie in den

[23] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch Richtlinie 2006/24/EG und Richtlinie 2009/136/EG geänderten Fassung, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/24eprivacy_2.pdf (inoffizielle konsolidierte Fassung).

[24] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

http://eur-lex.europa.eu/legal-content/DN/TXT/?uri=URISERV:l14012.

[25] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rats vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32000L0031.

[26] AVMD-Richtlinie, supra Fußnote 19.

[27] Technische Normen und Aspekte der Interoperabilität sind nicht Gegenstand der AVMD-Richtlinie.

Anwendungsbereich der AVMD-Richtlinie. Solche Fälle vertikaler Integration sind jedoch im Smart-TV-Markt, wo die Gerätehersteller traditionsgemäß keine Inhalte produzieren, noch nicht die Norm.

Das Smart-TV-Ökosystem umfasst jedoch die Anbieter von audiovisuellen Mediendiensten wie Fernsehprogramme und Programmkataloge audiovisueller Abrufdienste, die entsprechend der AVMD-Richtlinie in den einzelnen Mitgliedstaaten gesetzlich reguliert sind. Im Falle von Smart-TV-Geräten kann es dazu kommen, dass die AVMD-Richtlinie zu unterschiedlichen Regelungsanforderungen für audiovisuelle Inhalte führt - je nachdem, ob sie linear oder nichtlinear sind -, die aber alle auf demselben Bildschirm wiedergegeben werden.[28] In der Entschließung des Europäischen Parlaments über „Connected TV“ heißt es diesbezüglich, dass „die abgestufte Regulierung, die zwischen Fernsehprogrammen [...] und audiovisuellen Mediendiensten auf Abruf differenziert, in der bestehenden Form an Bedeutung verlieren könnte, obwohl unterschiedlich regulierte Informations- und Kommunikationsdienste [...] auf ein und demselben Gerät verfügbar sind [...]“.[29]

In den meisten Fällen ist das Smart-TV-Gerät die Hardware einer digitalen Plattform, die Dritte - etwa Anbieter audiovisueller Mediendienste und Anbieter anderer Online-Inhalte und –Dienste, über die Schnittstelle zur Anwenderprogrammierung des Geräts und über den entsprechenden App-Store mit den Nutzern verbindet. Wie digitale Plattformen fallen deren Anbieter jedoch derzeit nicht unter die AVMD-Richtlinie. Sog. *Layover Ads*, bei denen die Anbieter digitaler Plattformen eigene Werbemittel auf das Smart-TV-Gerät legen, machen die derzeitigen Grenzen der AVMD-Richtlinie deutlich.[30] Da der Anbieter der Plattform selbst keine audiovisuellen Mediendienste anbietet, fällt diese neue Form der Werbung derzeit nicht unter die AVMD-Richtlinie - auch nicht, wenn die *Layover Ads* in Verbindung mit audiovisuellen Inhalten dritter Anbieter angezeigt werden. Die Schlussfolgerung der Entschließung des Europäischen Parlaments über „Connected TV“ lautet, dass die Regelungen der AVMD-Richtlinie „die voranschreitende technische Verschmelzung noch nicht abbilden“ und dass es im Zuge der anstehenden Revision der AVMD-Richtlinie und anderer einschlägiger Verordnungen - insbesondere des TK-Pakets - erforderlich sein kann, den „Plattformbegriff“ zu erweitern.[31]

## 2.2. Regulierung für elektronische Kommunikation

Bei der Regulierung der Aspekte der elektronischen Kommunikation stehen im Wesentlichen Aspekte der Infrastruktur und Übertragung im Vordergrund. Nicht erfasst sind die Bereitstellung von Inhalten, die Wahrnehmung redaktioneller Kontrolle von Inhalten oder Diensten der Informationsgesellschaft, die nicht vollständig oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen.[32] Seit der Revision im Jahr 2002 ist der Anwendungsbereich der Regulierung technologieneutral gehalten; Rundfunknetze und

[28] Vgl. Wagner C., “Connected TV: A challenge for market players and regulators”, Global Media & Communications Quarterly, Spring issue 2012,
http://www.hoganlovells.com/files/Publication/41c5d3e3-0a16-4784-80c0-09193994456c/Presentation/PublicationAttachment/5fc8d47d-18e7-499a-8231-3b61f5067100/GMC_Quarterly_Summer_2012_v2.pdf;
Europäische Kommission, Grünbuch über die Vorbereitung auf die vollständige Konvergenz der audiovisuellen Welt: Wachstum, Schöpfung und Werte, COM(2013) 231, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2013:0231:FIN.

[29] Entschließung des Europäischen Parlaments vom 4.Juli 2013 über Connected TV (2012/2300(INI)),
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2013-329.

[30] Europäische Kommission, supra Fußnote 28.

[31] Europäisches Parlament, supra Fußnote 29.

[32] Rahmenrichtlinie, supra Fußnote 20, Artikel 2 (c) und Erwägungsgründe (5) und (10).

Übertragungsdienste sowie Verbrauchergeräte, die für das Digitalfernsehen verwendet werden, sind explizit eingeschlossen.[33] Seither enthalten die Rahmenrichtlinie und die Zugangsrichtlinie neue Regelungen für digitale Fernsehdienste, die für Smart-TV-Geräte von herausragender Bedeutung sind. Diese Entwicklung unterstreicht die zunehmende Relevanz der Backend-Technologie im Bereich digitaler Fernsehdienste. In den folgenden Abschnitten liegt der Schwerpunkt auf der Regulierung digitaler Fernsehdienste und ihrer Zusatzdienste im Kontext von Smart-TV-Geräten.

Das zentrale Instrument zur Regulierung des Bereichs elektronische Kommunikation ist die Rahmenrichtlinie, die wichtige Begriffsbestimmungen enthält. Smart-TV-Geräte würden sicherlich die Definition „erweiterte digitale Fernsehgeräte“ in Artikel 2 o) der Rahmenrichtlinie erfüllen, die u.a. „integrierte digitale Fernsehgeräte zum Empfang digitaler interaktiver Fernsehdienste“ einschließt. Digitale Plattformen, die über Smart-TV-Geräte laufen, umfassen in der Regel neben einem Zugangsberechtigungssystem eine Schnittstelle zur Anwenderprogrammierung sowie elektronische Programmführer. Beide, Zugangsberechtigungssysteme und elektronische Programmführer (EPG), werden in Artikel 2 e) als „zugehörige Einrichtungen“ bezeichnet. Weiterhin enthält die Rahmenrichtlinie Definitionen für das Zugangsberechtigungssystem (Artikel 2 f)) und die Schnittstelle für Anwendungsprogramme (API) (Artikel 2 p)). Die Rahmenrichtlinie selbst enthält Bestimmungen für die Schnittstellen für Anwendungsprogramme (API); die Regelungen für Zugangssysteme und elektronische Programmführer finden sich jedoch in der Zugangsrichtlinie.

Die Schnittstelle für Anwendungsprogramme ist im Hinblick auf die Interoperabilität von Anwendungen von Rundfunkveranstaltern oder Diensteanbietern und den in den erweiterten digitalen Geräten - d.h. hier den Smart-TV-Geräten - eingesetzten Mitteln von ganz zentraler Bedeutung. Artikel 18 der Rahmenrichtlinie verlangt von den Mitgliedstaaten, dass sie sich bei digitalen interaktiven Fernsehdiensten und Geräten für offene API einsetzen, um eine Interoperabilität der digitalen interaktiven Fernsehdienste zu ermöglichen. Dies gilt insbesondere für „Anbieter aller erweiterter digitaler Fernsehgeräte, die für den Empfang digitaler interaktiver Fernsehdienste auf interaktiven digitalen Fernsehplattformen bestimmt sind“ (Rahmenrichtlinie Artikel 18 (1) b). Die API-Eigentümer sollen ermutigt werden, ihre Schnittstelle „auf faire, angemessene und nichtdiskriminierende Weise gegen angemessene Vergütung zur Verfügung [zu] stellen“ und „alle Informationen, die es den Anbietern von digitalen interaktiven Fernsehdiensten ermöglichen, ihre API-unterstützten Dienste voll funktionsfähig anzubieten“, bereitzustellen (Artikel 18 (2) Rahmenrichtlinie). Jedoch handelt es sich hier um Aufgaben, die die Mitgliedstaaten zu erfüllen haben, weshalb die regulatorischen Auswirkungen nicht so groß sind wie im Falle strenger Auflagen.

Artikel 2 f) der Rahmenrichtlinie definiert „Zugangsberechtigungssystem“ als „jede technische Maßnahme und/oder Vorrichtung, die den Zugang zu einem geschützten Hörfunk- oder Fernsehdienst in unverschlüsselter Form von einem Abonnement oder einer vorherigen individuellen Erlaubnis abhängig macht“. Die Definition würde Smart-TV-Geräte einschließen, die bedingten Zugang zu geschützten Fernsehdiensten wie Pay-TV gewähren, aber nicht erfassen, wenn es sich um andere geschützte Inhalte wie etwa nichtlineare audiovisuelle Mediendienste oder andere Online-Dienste handelt. Im Zusammenhang mit den kombinierten Funktionalitäten von Smart-TV-Geräten „kann die Unterscheidung [...] schwierig und untauglich sein“.[34] Damit gelten die in Artikel 6 (1) der Zugangsrichtlinie genannten und in Anhang I Teil I aufgelisteten Bedingungen für Zugangsberechtigungssysteme nur in Verbindung mit geschützten Fernsehdiensten. Die Bestimmungen sehen u.a. vor, dass Betreiber von Zugangsberechtigungssystemen dazu verpflichtet sind, den Sendeanstalten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen Zugang

[33] Ibid. Erwägungsgrund (8).

[34] Helberger N., “Access to Technical Facilities in Digital Broadcasting”, in: Castendyk O., Dommering E. and Scheuer A., *European media law,* Alphen aan den Rijn: Wolters Kluwer), 2008, S. 1129-1150, 1135.

zu gewähren. Dies gilt entsprechend für die Inhaber von Rechten an Zugangsberechtigungssystemen bei der Gewährung von Lizenzen an Hersteller von Geräten für den Verbraucher.

Die nationalen Regulierungsbehörden sind befugt, ähnliche Zugangsbedingungen für Anbieter von API und EPG festzulegen, um den Zugang zu digitalen Hörfunk- und Fernsehdiensten für Endnutzer zu gewährleisten (Artikel 5 (1) b) in Verbindung mit Anhang 1 Teil II Zugangsrichtlinie). Ferner können die nationalen Regulierungsbehörden „Verpflichtungen in Bezug auf die Darstellungsaspekte elektronischer Programmführer und ähnlicher Anzeige- und Orientierungshilfen festlegen“ (Artikel 6 (4) Zugangsrichtlinie). Allerdings bestehen für die Hersteller von Smart-TV-Geräten und den zugehörigen Plattformen keine Must-Carry-Auflagen (Übertragungspflichten) für die frei empfangbare Ausstrahlung bestimmter Hörfunk- und Fernsehkanäle und -dienste (Artikel 31(1) der Universaldienstrichtlinie). Die Bestimmung betr. Übertragungspflichten richtet sich speziell an Unternehmen, die elektronische Kommunikationsnetze betreiben, die für den freien Empfang von Hörfunk- oder Fernsehsendern verwendet werden.

Abgesehen von den begrenzten Anforderungen für Zugangsberechtigungsdienste, API und EPG in Verbindung mit digitalen Hörfunk- und Fernsehdiensten enthalten die Rahmenregelungen für elektronische Kommunikation keine allgemeine Verpflichtung hinsichtlich Neutralität und Zugang zu fairen, angemessenen und nichtdiskriminierenden Bedingungen [35], die für Smart-TV-Geräte und deren digitale Plattformen gelten würde. In ihrem Grünbuch über Medienkonvergenz hat die Europäische Kommission darauf hingewiesen, dass es angesichts des großen Angebots an Online-Inhalten aus verschiedenen Gründen - etwa exzessive Filter- und Personalisierungsmechanismen, Entscheidungen der Gerätehersteller usw. - für die Nutzer zu einer Herausforderung werden kann, Inhalte von allgemeinem Interesse zu finden.[36] Die Entschließung des Europäischen Parlaments zu „Connected TV“ spricht sich für die Einführung von „Regelungen zur Auffindbarkeit und des diskriminierungsfreien Zugangs zu Plattformen für Inhalteanbieter und Inhalteentwickler sowie für Nutzer“ aus.[37]

Für den Internet-Rückkanal, der interaktive Smart-TV-Dienste ermöglicht, gelten auch die Bestimmungen zur Netzneutralität der Rahmenregelung für elektronische Kommunikation. In Artikel 8 (4) der Rahmenrichtlinie ist festgelegt, dass die Mitgliedstaaten aufgefordert sind, „die Endnutzer in die Lage zu versetzen, Informationen abzurufen und zu verbreiten oder Anwendungen und Dienste ihrer Wahl zu nutzen“. Dazu enthält die Universaldienstrichtlinie weitere Ausführungen, in denen Transparenz gefordert wird und Eingriffsmöglichkeiten für Regulierer vorsehen sind. Transparenz bedeutet dabei, dass die Nutzer über sämtliche von Unternehmen eingerichtete Verfahren zur Messung und Gestaltung des Datenverkehrs zur Vermeidung der Überlastung von Netzwerkverbindungen und darüber, wie diese Verfahren sich auf die Qualität der Dienste auswirken können, informiert werden müssen. Die Regulierer sind befugt, Unternehmen, die öffentliche Kommunikationsnetze betreiben, Mindestanforderungen hinsichtlich der Qualität der Dienste vorzuschreiben, um eine Verschlechterung des Angebots an Diensten und Verzögerungen oder Blockaden in Netzwerken zu verhindern. Diese Rahmenregelungen zur Netzneutralität werden zurzeit überarbeitet. Es ist davon auszugehen, dass dies zu einer weiteren Priorisierung sog. spezialisierter Dienste führen wird. Auch die Bereitstellung kostenloser Dienste (zero rating / Nullsatz) kann sich vereinfachen.[38]

---

[35] „fair, angemessen und diskriminierungsfrei“; FRND (englisch) steht für ‘Fair, Reasonable and Non Discriminatory’. Dabei handelt es sich um einen bei der Regulierung im Bereich Telekommunikation verwendeten wichtigen Begriff.

[36] Europäische Kommission, supra Fußnote 28.

[37] Europäisches Parlament, supra Fußnote 29.

[38] Europäische Kommission, Pressemitteilung, „Kommission begrüßt Vereinbarung zur Abschaffung der Roaminggebühren und zur Sicherstellung des offenen Internets”, Brüssel, IP/15/5265, 30. Juni 2015, http://europa.eu/rapid/press-release_IP-15-5265_de.htm.

## 2.3. Regelungen zum Schutz der Privatsphäre und zum Datenschutz

In diesem Abschnitt wird die wachsende Bedeutung des EU-Datenschutzrahmens für das Smart-TV-Ökosystem dargestellt. Es sei hier daran erinnert, dass die EU-Institutionen im Jahr 2000 die Charta der Grundrechte der Europäischen Union offiziell proklamiert haben, die 2009 mit Inkrafttreten des Vertrags von Lissabon rechtsverbindlich wurde.[39] In der Grundrechtecharta sind die Grundrechte der EU-Bürger auf Achtung des Privat- und Familienlebens (Artikel 7) und auf Schutz personenbezogener Daten (Artikel 8) kodifiziert.

In ihrem Grünbuch über die „Vorbereitung auf die vollständige Konvergenz der audiovisuellen Welt: Wachstum, Schöpfung und Werte“ vertritt die Europäische Kommission die Auffassung, dass „die Verarbeitung personenbezogener Daten oftmals Voraussetzung für ein ordnungsgemäßes Funktionieren neuer Dienste ist, selbst wenn die Betroffenen sich häufig nicht in vollem Umfang der Tatsache bewusst sind, dass personenbezogene Daten erhoben und verarbeitet werden“.[40] Eine Personalisierung von Inhalten, z.B. im EPG und anderen Portaldiensten, „kann Verbrauchern und Werbetreibenden zugutekommen; dies gilt allerdings nur, wenn die dafür verwendeten Mittel den Schutz personenbezogener Daten nicht beeinträchtigen“.[41] Im Ökosystem des Smart-TV fließen die persönlichen Daten der Nutzer nicht nur zu dem jeweiligen Gerätehersteller, dem Anbieter der digitalen Plattform und dem Anbieter der audiovisuellen Mediendienste wie Fernsehsender und Anbieter von Programmkatalogen, sondern auch zu den Anbietern von Online-Diensten. Bei der Verarbeitung personenbezogener Daten sind jedoch die Gesetze der Mitgliedstaaten, die auf die Bestimmungen des EU-Datenschutzrahmens zurückgehen, einzuhalten.

Die gemeinsame Behandlung der E-Privacy-Richtlinie,[42] die eigentlich ein Instrument der oben beschriebenen Rahmenregelung für elektronische Kommunikation ist, und der Datenschutzrichtlinie[43] lässt sich damit rechtfertigen, dass das erstgenannte sektorspezifische Instrument das letztgenannte detailliert und ergänzt (Artikel 1 (2) E-Privacy-Richtlinie). Beide Instrumente haben den Schutz „der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“ zum Ziel (Artikel 1 (1) Datenschutzrichtlinie und Artikel 1 (1) E-Privacy-Richtlinie, allerdings begrenzt auf den Sektor elektronische Kommunikation). Gleichzeitig sind beide auch Binnenmarktinstrumente, mit denen der freie Fluss personenbezogener Daten zwischen Mitgliedstaaten sichergestellt werden soll.

In der nächsten Zeit wird die Datenschutzrichtlinie, die aus dem Jahr 1995 stammt, durch ein modernisiertes Instrument ersetzt werden. Der EU-Gesetzgeber ist gerade dabei, eine neue Datenschutz-Grundverordnung (DSGV) vorzubereiten, die noch dieses Jahr angenommen werden soll und die eine vollständige Harmonisierung der Regelungen zum Schutz personenbezogener Daten in der ganzen EU vorsieht.[44] Am Ende dieses Abschnitts wird ein Überblick über die regulatorischen Auswirkungen auf die Verarbeitung personenbezogener Daten in Verbindung mit Smart-TV gegeben, der in Kapitel IV als Bezugsrahmen verwendet wird.

---

[39] Charta der Grundrechte der Europäischen Union, in Verbindung mit Artikel 6(1) des Vertrags über die Europäische Union (konsolidierte Fassung, Lissabohttp://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT.

[40] Europäische Kommission, supra Fußnote 28, S. 11f.

[41] Ibid.

[42] Supra Fußnote 23.

[43] Supra Fußnote 24.

[44] Entwürfe, die derzeit im Trilog zwischen Rat, Europäischen Parlament und Europäischer Kommission diskutiert werden, sind abrufbar unter:http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.

## 2.3.1. Anwendungsbereich

Die Datenschutzrichtlinie gilt für die Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen im Hoheitsgebiet eines Mitgliedstaats, oder, wenn dies nicht der Fall ist, für den für die Verarbeitung Verantwortlichen, der zum Zweck der Verarbeitung personenbezogener Daten auf Mittel zurückgreift, die im Hoheitsgebiet eines Mitgliedstaats gelegen sind ( Artikel 4 (1) a) und c) Datenschutzrichtlinie). Obwohl eine ganze Reihe von Herstellern von Smart-TV-Geräten ihren Hauptsitz außerhalb der EU hat, operieren die meisten über lokale Tochtergesellschaften, was hinsichtlich des territorialen Anwendungsbereichs der Datenschutzrichtlinie unproblematisch ist.

Im Falle von Anbietern von Online-Diensten, die nicht in der EU ansässig sind und deren Angebote für Nutzer über internetfähige Smart-TV-Geräte potenziell zugänglich sind, gibt es zwei Möglichkeiten, einen Bezug zum territorialen Anwendungsbereich herzustellen: Zum einen hat der EuGH Artikel 4 (1) a) der Datenschutzrichtlinie so ausgelegt, dass er für den für die Verarbeitung Verantwortlichen mit einer Niederlassung in einem Mitgliedstaat Anwendung findet, dessen Tätigkeiten untrennbar mit der Datenverarbeitung durch den für die Verarbeitung Verantwortlichen verbunden sind.[45] Zum anderen betrachtet die Artikel-29-Datenschutzgruppe das Einrichten von Cookies auf Endgeräten von Endnutzern als Nutzung von Mitteln, die im Hoheitsgebiet der EU belegen sind.[46] Entsprechend dieser weiten Auslegungen würden die meisten Anbieter, die Online-Dienste über Smart-TV-Geräte bereitstellen und personenbezogene Daten von EU-Bürgern verarbeiten, in den territorialen Anwendungsbereich des EU-Datenschutzrechts fallen.

## 2.3.2. Allgemeine Definitionen und Grundsätze

Die Datenschutzrichtlinie enthält Definitionen für die Begriffe „personenbezogene Daten“ und „Verarbeitung“, die zur Festlegung des materiellen Umfangs des Anwendungsbereichs in Artikel 3 (1) verwendet werden. Ferner wichtig sind die Einführung des Begriffs „für die Verarbeitung Verantwortlicher“, der verpflichtet ist, sich an die Datenschutzgesetze des Mitgliedstaats zu halten, die auf den Richtlinien basieren, sowie die Definition von „Einwilligung“. Die E-Privacy-Richtlinie (Datenschutzrichtlinie für elektronische Kommunikation) übernimmt diese Begriffsbestimmungen aus der Datenschutzrichtlinie (Artikel 2 E-Privacy-Richtlinie).

### 2.3.2.1. Personenbezogene Daten

Nach Artikel 2 a) der Datenschutzrichtline sind „personenbezogene Daten“ „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (“betroffene Person“)“. Die Artikel-29-Datenschutzgruppe, in der die zuständigen Datenschutzbehörden der Mitgliedstaaten und der EU vertreten sind, hat in einer Stellungnahme Leitlinien zur exakten Auslegung der einzelnen Elemente der Begriffsbestimmung von „personenbezogenen Daten“ herausgegeben.[47] Im Zusammenhang mit

[45] EuGH, *Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos (AEPD),* Urteil vom 13. Mai 2014, Rechtssache C-131/12, Randnr. 56, 60, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

[46] Artikel-29-Datenschutzgruppe, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, angenommen am 30. Mai 2002 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf, p. 11.

[47] Artickel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", angenommen am 20. Juni 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf, S. 6f.

Smart-TV sind folgende Arten personenbezogener Daten sehr wahrscheinlich von Bedeutung: Informationen des Nutzerkontos (sofern vorhanden), Identifikationsnummer des Geräts oder andere eindeutige Kennungen (einschl. Cookies), statische oder dynamische IP-Adressen, Seh- und Surfgewohnheiten (z.B. Verfolgung von Umschaltvorgängen), individuelle Nutzerprofile, Standortdaten und Bewegungssteuerung (sofern aktiviert).[48] Gesichts- und Spracherkennungssysteme, die Smart-TV-Gerätehersteller teilweise einbauen und die sie für ihre Plattformen nutzen, verarbeiten biometrische Daten, die ebenfalls als personenbezogene Daten zu bewerten sind.[49]

Solange diese Daten mit einer bestimmten oder bestimmbaren natürlichen Person in Zusammenhang stehen, handelt es sich um personenbezogene Daten im Sinne der Definition der Datenschutzrichtlinie. Natürliche Personen sind z.B. über eindeutige Kenngrößen bestimmbar, und durch die Verwendung von Pseudonymen wird der Bezug zu einer betroffenen Person nicht aufgehoben. Deshalb fallen auch Geräteidentifikationsnummern oder andere eindeutige Kennungen im EU-Datenschutzrecht unter die Definition von „personenbezogenen Daten“. Im Gegensatz dazu sind anonymisierte oder anonyme Daten keine personenbezogenen Daten, und damit fällt deren Verarbeitung nicht unter die EU-Datenschutzregelungen, es sei denn, die Daten beziehen sich auf eine natürliche Person. Die Anonymisierung personenbezogener Daten muss nach bewährten Praktiken erfolgen, um das Restrisiko einer Identifizierung auszuschließen.[50]

### 2.3.2.2. Verarbeitung

Die „Verarbeitung personenbezogener Daten“ umfasst „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten“ (Artikel 2 b) Datenschutzrichtlinie). Es handelt sich hier somit um einen recht weit gefassten Begriff, und jeder interne Verarbeitungsschritt, der von einem für die Verarbeitung Verantwortlichen durchgeführt wird, dürfte unter diese Definition fallen. Bei Beeinträchtigungen des Rechts auf Schutz der Privatsphäre und Datenschutz und somit auch bei der Definition von Verarbeitung kommt es nicht darauf an, ob die Informationen über die Privatsphäre von Betroffenen sensibel sind oder ob durch die Verarbeitung personenbezogener Daten der betroffenen Person Unannehmlichkeiten oder Schaden entstanden sind.[51]

---

[48] Diese Aufzählung berücksichtigt die in Kapitel III genannten Fälle.

[49] Artikel-29-Datenschutzgruppe, Arbeitspapier über Biometrie, angenommen am 1. August 2003, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_de.pdf; Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, angenommen am 27. April 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_de.pdf.

[50] Das wird oftmals nicht beachtet; vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 05/2014 zu Anonymisierungstechniken, angenommen am 10. April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

[51] Vgl. EuGH, *Österreichischer Rundfunk und andere* (Rechtssachen C 465/00, C 138/01 und C 139/01), Randnr. 75, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62000CJ0465; *Digital Rights Ireland and Seitlinger gegen Minister for Communications, Marine and Natural Resources* (C-293/12 und C-594/12) [2014] E.C.R. I-238, Randnr. 33, http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1446899221432&uri=CELEX:62012CJ0293.

#### 2.3.2.3. Der für die Verarbeitung Verantwortliche

„Für die Verarbeitung Verantwortlicher“ bedeutet „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Artikel 2 d) Datenschutzrichtlinie). Im Smart-TV-Ökosystem gibt es potenziell mehrere für die Verarbeitung der personenbezogenen Daten von Nutzern Verantwortliche: den Gerätehersteller, den Anbieter der Plattform und der Anwendungen, den Anbieter audiovisueller Mediendienste und den Anbieter von Online-Inhalten und -diensten. In einigen Fällen sind sie aufgrund ihres Zusammenwirkens als gemeinsame Verantwortliche zu betrachten, und in anderen müssen sie als alleinige für die Verarbeitung Verantwortliche gesehen werden. Andere Diensteanbieter können bei bestimmten Backend-Diensten im Zusammenhang etwa mit Cloud-Speicherdiensten oder Spracherkennungsdiensten eingebunden werden, die dann bestimmte Aufgaben erfüllen und „personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeit[en]“ (Artikel 2 e) Datenschutzrichtlinie). Diese Akteure werden in der Datenschutzterminologie als „Auftragsverarbeiter“ bezeichnet, sofern sie eine untergeordnete Funktion erfüllen und nicht selbst neue Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen.

#### 2.3.2.4. Einwilligung

Die Einwilligung der betroffenen Person ist im Hinblick auf die Legitimierung der Verarbeitung personenbezogener Daten durch den Verantwortlichen von zentraler Bedeutung. „Einwilligung“ ist definiert als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden“ (Artikel 2 h) Datenschutzrichtlinie). Die Verarbeitung personenbezogener Daten kann auf der Grundlage einer „ohne jeden Zweifel“ gegebenen Einwilligung der betroffenen Person (Artikel 7 a) Datenschutzrichtlinie) erfolgen, und in einigen Fällen ist eine ausdrückliche Einwilligung erforderlich, so für die Verarbeitung besonderer Kategorien personenbezogener Daten, aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht sowie für die Verarbeitung von Daten über Gesundheit und Sexualleben (Artikel 8 (1), (2) a) Datenschutzrichtlinie). Voraussetzung für eine Einwilligung zur Erhebung personenbezogener Daten betroffener Personen ist, dass der für die Verarbeitung Verantwortliche die betroffene Person, wie in Artikel 10 der Datenschutzrichtlinie vorgesehen, klar und umfassend informiert.

### 2.3.3. E-Privacy-Richtlinie

Als sektorspezifisches Instrument regelt die E-Privacy-Richtlinie die Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikation. Die sich aus der Richtlinie ergebenden Pflichten gelten für Anbieter öffentlich verfügbarer elektronischer Kommunikationsnetze und öffentlicher elektronischer Kommunikationsdienste, wie diese in der oben genannten Rahmenrichtlinie definiert sind; damit fallen Inhalteanbieter, die Ausübung redaktioneller Kontrolle von Inhalten sowie Dienste der Informationsgesellschaft nicht unter die Richtlinie. Die Richtlinie regelt im Wesentlichen die Rechte von Nutzern und Abonnenten elektronischer Kommunikationsdienste (einschl. juristischer Personen), schützt die Vertraulichkeit der Kommunikation und legt Regeln für die Verwendung von Verkehrs- und Standortdaten. Somit berücksichtigt die E-Privacy-Richtlinie nur einen Teil der beteiligten Akteure - und dies zu einer Zeit, in der die wirtschaftliche Bedeutung der Verarbeitung personenbezogener Daten durch digitale Dienste ständig zunimmt.

Die meisten Bestimmungen der E-Privacy-Richtlinie gelten nicht für Hersteller von Smart-TV-Geräten und Anbieter digitaler Plattformen; ebenso wenig gelten sie für Fernsehkanäle und Anbieter von Diensten der Informationsgesellschaft, die über Smart-TV-Geräte erbracht werden. Im Gegensatz dazu sind Betreiber von Rundfunknetzen als Betreiber öffentlicher elektronischer Kommunikationsnetze, HbbTV-Anbieter[52] (d.h. der Rückkanal) und Kabelbetreiber an die E-Privacy-Richtlinie gebunden. Anbieter von öffentlichen elektronischen Kommunikationsdiensten über Smart-TV wie IP-Telefonie oder Video Chats fallen ebenso unter die Richtlinie. Es gibt nur zwei Ausnahmen von dieser Regel, die horizontal für alle Wirtschaftsbeteiligten gelten: zum einen die Bestimmungen in Artikel 5 (3) über die Speicherung von Informationen und den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind (besser bekannt als sog. Cookie-Regel), und zum anderen die Bestimmungen hinsichtlich unerbetener Werbenachrichten (Artikel 13 E-Privacy-Richtlinie). Entsprechend Erwägungsgrund 8 der Rahmenrichtlinie fallen Smart-TV-Geräte als Endgeräte für Verbraucher, die für das Digitalfernsehen genutzt werden, unter die Regelungen für elektronische Kommunikation, und damit findet Artikel 5 3) der E-Privacy-Richtlinie Anwendung:

> *Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf im Endgerät eines Teilnehmers oder Nutzers bereits gespeicherte Informationen nur unter der Bedingung erlaubt ist, dass der betreffende Teilnehmer oder Nutzer seine Einwilligung gegeben hat, nachdem er gem. der Richtlinie 95/46/EG klare und umfassende Informationen u.a. über den Zweck der Verarbeitung erhalten hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft bereitzustellen.*

Beim Setzen von Cookies oder Beacons in Smart-TV-Geräten oder beim Zugriff auf bereits im Smart-TV-Gerät gespeicherte Informationen müssen die verschiedenen Akteure des Smart-TV-Ökosystems die Einwilligung des Nutzers einholen und die Informationspflichten nach der Datenschutzrichtlinie erfüllen. In anderen Worten: Die Gerätehersteller und Diensteanbieter müssen einen Datenschutzhinweis vorsehen, bevor sie Cookies setzen oder auf Informationen zugreifen, die auf dem Smart-TV-Gerät gespeichert sind.[53] Auf jeden Fall müssen die Nutzer über das Recht verfügen, der Verarbeitung durch den verarbeitenden Verantwortlichen nicht zuzustimmen. Das Speichern von Informationen oder das Zugreifen auf bereits im Endgerät gespeicherte Informationen ist insofern zulässig, als dies unbedingt notwendig ist, um einen Dienst der Informationsgesellschaft bereitstellen zu können, den der Teilnehmer oder Nutzer ausdrücklich angefordert hat.

## 2.3.4. Datenschutzrichtlinie

Die für die Verarbeitung Verantwortlichen sind grundsätzlich verpflichtet, die personenbezogenen Daten nach Treu und Glauben und auf rechtmäßige Weise entsprechend den Grundsätzen von Artikel 6 der Datenschutzrichtlinie zu verarbeiten. Diese Grundsätze lassen Aspekte des zulässigen

[52] Hybrid broadcast broadband TV (HbbTV) ist eine weltweite Initiative, die das Ziel verfolgt, die Übertragung von Unterhaltungsinhalten über Rundfunk und Breitband mittels Connected TV, Set-Top-Boxen und Mehrbildschirmgeräten zum Verbraucher zu harmonisieren. Näheres dazu unter: https://www.hbbtv.org/.

[53] So gab es früher den Vorwurf, dass ein Smart-TV-Gerät Dateien von einem USB-Stick ausgelesen und diese an den Hersteller weitergeleitet hat; vgl. Arthur C., "Information commissioner investigates LG snooping smart TV data collection" The Guardian, 21 November 2013, http://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection.

Anwendungsbereichs, des Umfangs, des Zwecks und der Dauer der Verarbeitung von personenbezogenen Daten unberücksichtigt und setzen auf die Wirkung der Prinzipien von Rechtmäßigkeit, Zweckbindung und Datenminimierung. Darüber hinaus darf die Verarbeitung nur erfolgen, wenn eine der in Artikel 7 der Datenschutzrichtlinie genannten rechtlichen Voraussetzungen erfüllt ist; dazu gehört u.a. die zweifelsfreie Einwilligung der betroffenen Person zur Verarbeitung der Daten wie oben definiert. Bezüglich ihrer personenbezogenen Daten haben natürliche Personen ein Auskunftsrecht über die Verarbeitungstätigkeiten des für die Verarbeitung Verantwortlichen und der vom Verantwortlichen gehaltenen personenbezogenen Daten; dazu zählt auch das Recht auf Berichtigungen, Löschungen oder Sperrung personenbezogener Daten (Artikel 12 a) und b) Datenschutzrichtlinie). Ferner ist in Artikel 14 der Datenschutzrichtlinie unter bestimmten Bedingungen ein Widerspruchsrecht der betroffenen Personen vorgesehen, das auch bei ansonsten rechtlich zulässiger Datenverarbeitung wahrgenommen werden kann - so etwa im Fall von Werbung gem. Artikel 13 (2) der E-Privacy-Richtlinie.

Die Datenschutzgesetze müssen speziell auf jeden Verarbeitungsschritt und bezogen auf den jeweiligen Zweck der Operation angewandt werden, wodurch es hinsichtlich der Auslegung der Grundsätze und der Rechtsgrundlage von Fall zu Fall Unterschiede geben kann. Aus argumentativen Gründen wird gemeinhin zwischen primären und sekundären Zwecken unterschieden, wobei sich der primäre Zweck der Datenverarbeitung mit dem Merkmal des Dienstes deckt, den der Nutzer in Anspruch nehmen möchte. Ein Nebenzweck liegt im Gegensatz dazu eher im Interesse des für die Verarbeitung Verantwortlichen - etwa das Einstellen von kontext- oder verhaltensbezogener Werbung. Ein Beispiel:

- Der Kauf eines Smart-TV-Geräts basiert im Wesentlichen auf einem Kaufvertrag; dabei besteht kein bzw. kaum ein Zusammenhang mit der Verarbeitung personenbezogener Daten - abgesehen von technischen und vielleicht Softwareupdates. Eine weitergehende Verarbeitung personenbezogener Daten würde eine andere Rechtsgrundlage erfordern und kann nicht damit begründet werden, dass die Verarbeitung für die Erfüllung eines Vertrags notwendig ist.

- Personenbezogene Dienste über elektronische Programmführer implizieren eine Rückverfolgung und Verarbeitung individueller Seh- und Verhaltensmuster. Für Nutzer, die personalisierte Dienste abonniert haben und die über den Umfang und Zweck der Verarbeitung unterrichtet sind, kann die Verarbeitung für die Erfüllung eines Vertrags erforderlich bzw. der Hauptzweck sein (Artikel 7 b) Datenschutzrichtlinie). Jedoch ist das ie Erfordernis eines Vertrages eng auszulegen, und es darf sich nur um Fälle handeln, in denen „Bestimmung eng auszulegen; sie gilt nicht für Situationen, in denen die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern der betroffenen Person von dem für die Verarbeitung Verantwortlichen einseitig auferlegt wird“.[54]

- Wenn dieser Verantwortliche zusätzliche Zwecke (Nebenzwecke) einführen möchte, für die dieselben personenbezogenen Daten zur Verwendung kämen - z.B. Erstellen individueller Profile für kontext- oder verhaltensbezogene Werbung -, würde dies die zweifelsfreie Einwilligung der betroffenen Person voraussetzen.

- Ein anderer Anbieter, etwa ein frei empfangbarer Fernsehsender (linearer audiovisueller Mediendienst) konnte nicht überzeugend darlegen, dass die Rückverfolgung individueller Seh- und Verhaltensmuster für die Erfüllung eines Vertrags notwendig ist; da es sich hier lediglich um ein lineare, im Programm vorgesehene Sendung handelte und die Situation

[54] Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, angenommen am 9. April 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.

einer One-to-many-Kommunikation vorlag. Um die Verarbeitung der personenbezogenen Daten zu legitimieren, muss der Verantwortliche die zweifelsfreie Einwilligung der betroffenen Person einholen.

Vor allem müssen die Grundeinstellungen die Situation wiedergeben, die besteht, bevor der Nutzer eines Smart-TV-Geräts oder eines Online-Dienstes über Smart-TV eine Einwilligung zur Verarbeitung seiner personenbezogenen Daten gibt. Die einzelnen Nutzer sollten in der Lage sein, die Erfassung und Verwendung ihrer personenbezogenen Daten in den Einstellungen des Smart-TV-Geräts zu kontrollieren.

Aus dem Gesagten wird deutlich, dass die Anwendung und die Beachtung von EU-Datenschutzbestimmungen keine statische Angelegenheit ist, sondern immer vom jeweiligen Fall und den besonderen Umständen der Verarbeitung abhängen. Damit ist schon der Versuch, alle möglichen Zwecke aufzulisten, für die personenbezogene Daten von allen Beteiligten des Smart-TV-Ökosystems verarbeitet werden dürfen, und zu erklären, wie die Datenschutzregelungen *in concreto* anzuwenden sind, zum Scheitern verurteilt.

### 2.3.4.1. Vertraulichkeit und Sicherheit der Verarbeitung

Die Datenschutzrichtlinie legt auch Anforderungen hinsichtlich der Vertraulichkeit und Sicherheit der Verarbeitung fest. Nach Artikel 16 der Datenschutzrichtlinie sind Personen, die Mitarbeiter des für die Verarbeitung Verantwortlichen sind oder die beauftragt sind, personenbezogene Daten zu verarbeiten, und die Zugang zu diesen Daten haben, verpflichtet, sich an die Weisungen des für die Verarbeitung Verantwortlichen zu halten. Gem. Artikel 17 der Datenschutzrichtlinie muss „der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen [...], die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind“. Im Zusammenhang mit den Strömen personenbezogener Daten in Verbindung mit Smart-TV-Geräten dürfte dies auf die Anforderung hinauslaufen, die Datenströme zu verschlüsseln und Maßnahmen im Sinne der Triade der Informationssicherheit - Vertraulichkeit, Integrität und Verfügbarkeit der Daten - zu ergreifen.

### 2.3.4.2. Internationale Datenströme

Schließlich ist nach EU-Datenschutzrecht die Übermittlung personenbezogener Daten von der EU in ein Drittland nur zulässig, wenn dort ein angemessenes Schutzniveau hinsichtlich personenbezogener Daten besteht oder wenn eine der Ausnahmen von Artikel 26 der Datenschutzrichtlinie Anwendung findet. Wenn ein Smart-TV-Gerät z.B. personenbezogene Daten von betroffenen Personen in der EU erfasst und diese an einen Gerätehersteller mit Hauptsitz außerhalb der EU übermittelt, stellt dies eine internationale Übermittlung personenbezogener Daten dar.[55] Derartige internationale Übermittlungen personenbezogener Daten sind nur zulässig, wenn feststeht, dass das Drittland über ein angemessenes Schutzniveau in Bezug auf personenbezogene

[55] Ibid.

Daten verfügt.[56] Liegt eine entsprechende Feststellung seitens der Europäischen Kommission nicht vor, können diese internationalen Übermittlungen auf der Grundlage verbindlicher unternehmensinterner Vorschriften (BCR), Standardklauseln in Verträgen oder durch zweifelsfreie Einwilligung der betreffenden Person erfolgen (Artikel 26 (1), (4) Datenschutzrichtlinie).

### 2.3.5. Neue Datenschutzverordnung

Die vorliegenden Gesetzesvorschläge für eine Datenschutzgrundverordnung (DGVO) sehen vor, den territorialen Anwendungsbereich auszuweiten und - zusätzlich - Fälle zu berücksichtigen, in denen der für die Verarbeitung Verantwortliche nicht in der EU ansässig ist und die Verarbeitungstätigkeiten sich beziehen auf a) ein Angebot von Gütern oder Dienstleistungen - unabhängig davon, ob dies Zahlungen seitens der betroffenen Person voraussetzt - an betroffene Personen in der EU; oder b) die Überwachung dieser betroffenen Personen. Wenn die vorgelegten Vorschläge angenommen werden, würde dies zur Klärung gewisser Punkte und zu bestimmten gesetzlichen Neuerungen führen, die zum Teil für Smart-TV-Geräte von Bedeutung sind. Wenn der Trennungsgrundsatz vom EU-Gesetzgeber bestätigt wird, liegt eine Einwilligung „ohne Zwang“ der betroffenen Person nur dann vor, wenn die betroffene Person die Möglichkeit hat, ihre Einwilligung nicht zu geben. Weiter müssen Diensteanbieter auch ein Umfeld schaffen, in dem die betreffende Person von einer Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für Nebenzwecke absehen kann.

Im Entwurf der DGVO sind auch neue Bestimmungen für das Profiling und die Grundsätze des Datenschutzes durch Design (*data protection by design*) und durch die Datenschutz-Grundeinstellungen (*data protection by default*) vorgesehen.

Das Verfolgen und Verarbeiten von Sehmustern betroffener Personen durch unterschiedliche Akteure des Smart-TV-Umfelds würde wahrscheinlich dieser Definition genügen und damit zusätzliche Schutzmaßnahmen sowie das Recht der betroffenen Person, einem Profiling widersprechen zu können, erforderlich machen.

Aus den Grundsätzen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen ergibt sich für die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter die Pflicht, geeignete und angemessene organisatorische Maßnahmen durchzuführen, die den Stand der Technik, das aktuelle technische Know-how und international bewährte Praktiken sowie die Risiken der Datenverarbeitungsverfahren berücksichtigen.

## 2.4. E-Commerce-Richtlinie und EU-Verbraucherschutzgesetze

Mit der E-Commerce-Richtlinie[57] kommen Online-Dienste hinzu, die zum einen nichtöffentliche elektronische Kommunikationsdienste sind, die ganz oder überwiegend in der Übertragung von Signalen bestehen, und zum anderen nicht-lineare audiovisuelle Mediendienste, d.h. Fernsehdienste.[58] Nach der Terminologie der E-Commerce-Richtlinie sind diese Dienste als Dienste der Informationsgesellschaft zu betrachten, die unter Bezugnahme auf eine weitere Richtlinie

[56] Vgl. EuGH, Urteil vom 6. Oktober 2015 (Maximillian Schrems gegen Data Protection Commissioner), Rechtssache C-362/14,http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0362.

[57] Supra Fußnote 25.

[58] Supra Fußnote 25, Erwägungsgrund (18).

definiert sind.[59] Dienste der Informationsgesellschaft sind „alle Dienstleistungen, die in der Regel gegen Entgelt im Fernabsatz mittels Geräten für die elektronische Verarbeitung [...] auf individuellen Abruf eines Empfängers erbracht werden“ (Artikel 2 (a) E-Commerce-Richtlinie in Verbindung mit Artikel 1 (2) der Richtlinie 98/34/EG in der durch Richtlinie 98/48/EG abgeänderten Form).[60] Im Smart-TV-Umfeld sind zahlreiche Dienste der Informationsgesellschaft wie u.a. Video-on-Demand-Dienste, elektronische Programmführer, App-Stores und Anwendungen möglich.

Die E-Commerce-Richtlinie sieht für diese Dienste keine umfassenden Regelungen vor, beschäftigt sich jedoch im Wesentlichen mit Aspekten der Schaffung eines Binnenmarkts für solche Dienste, wobei die Möglichkeit gewährleistet ist, Verträge auf elektronischem Weg abzuschließen. Sie sieht aber für die Diensteanbieter eine recht umfassende Reihe von Informationspflichten bezüglich kommerzieller Kommunikationen vor (Artikel 5, 6 der E-Commerce-Richtlinie).

Zusätzlich enthält die E-Commerce-Richtlinie eine Reihe von Haftungsausnahmen für bestimmte Vermittler, die eine „reine Durchleitung“, „Caching“ und „Hosting“ betreiben (Artikel 12 bis 14 der E-Commerce-Richtlinie). Im Smart-TV-Ökosystem sind diese Funktionalitäten alle vorhanden; um aber in den Genuss der Haftungsfreistellung zu kommen, muss der angebotene Dienst genau der jeweiligen Definition in der Richtlinie entsprechen. Eine digitale Plattform, die das Caching und/oder Hosting von audiovisuellen Mediendiensten und Online-Inhalten einer dritten Partei vornimmt, kann die Haftungsfreistellung in Anspruch nehmen, wenn diese „Tätigkeit [...] rein technischer, automatischer und passiver Art [ist], was bedeutet, dass der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt.“ (Erwägungsgrund 42 der E-Commerce-Richtlinie).

Wichtig hier ist, dass die E-Commerce-Richtlinie den Bestimmungen der EU-Datenschutzverordnung nicht vorgreift. In Erwägungsgrund 14 der E-Commerce-Richtlinie wird deutlich darauf hingewiesen, dass die „Grundsätze des Schutzes personenbezogener Daten [...] bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten“ sind.

Die Richtlinie über Verbraucherrechte[61], die zum Besitzstand der EU-Verbraucherrechte gehört, sieht eine Angleichung der Gesetze der Mitgliedstaaten für Verträge zwischen Verbrauchern und Unternehmen über den Verkauf von Waren und Dienstleistungen einschl. des Fernabsatzvertrags und des außerhalb von Geschäftsräumen geschlossenen Vertrags vor. Im Besonderen reguliert die Richtlinie Verträge über die Bereitstellung digitaler Inhalte.[62] Erwägungsgrund (19) definiert digitale Inhalte wie folgt: „Daten, die in digitaler Form hergestellt und bereitgestellt werden, wie etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte, unabhängig davon, ob auf sie durch Herunterladen oder Herunterladen in Echtzeit (Streaming), von einem körperlichen Datenträger oder in sonstiger Weise zugegriffen wird“. Abgesehen von den allgemeinen Verbraucherschutzregelungen wie dem Widerrufsrecht ist bemerkenswert, dass die allgemeinen Informationspflichten gelten und der Verbraucher aber auch über die Funktionsweise bzw. Interoperabilität digitaler Inhalte informiert werden muss - und dies bevor der Verbraucher an den Vertrag gebunden ist.[63] Der Begriff „Funktionsweise“ deckt jedoch auch den Aspekt ab, wie digitale Inhalte u.a. für die Nachverfolgung des Verhaltens von Verbrauchern genutzt werden können. Dies gilt für Verkaufsverträge über digitale Inhalte, die in oder außerhalb von Geschäftsräumen

[59] Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften in der durch Richtlinie 98/48/EG abgeänderten Fassung und durch Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 kodifizierten Fassung, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L1535&from=EN.

[60] Ibid.

[61] Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32011L0083.

[62] Ibid., Erwägungsgrund (19).

[63] Ibid.

geschlossen werden, und für Fernabsatzverträge (Artikel 5 und 6 der Richtlinie über Verbraucherrechte). Neben den Informationspflichten aufgrund des EU-Datenschutzrechts ist die Richtlinie eine weitere Rechtsquelle, nach der die Verfolgung von Verbraucherverhalten im Voraus offenzulegen ist.

## 2.5. Regelungsrahmen für Menschenrechte

Wie bereits erwähnt, liegen die Schwerpunkte der europäischen Rahmenregelungen für Menschenrechte auf dem Recht auf Schutz der Privatsphäre und Datenschutz. Die wichtigsten Bestimmungen finden sich in Artikel 8 der Europäischen Konvention der Menschenrechte (Recht auf Achtung des Privat- und Familienlebens) und in den Artikeln 7 (Achtung des Privat- und Familienlebens) und 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Europäischen Union. Die in diesen Bestimmungen dargelegten Grundsätze, die in der ständigen Rechtsprechung weiterentwickelt wurden, bieten im Hinblick auf Inhalt und Umfang der Grund- oder Menschenrechte auf Schutz der Privatsphäre und Datenschutz eine wertvolle Hilfe. Der Anwendungsbereich von Artikel 8 EMRK schließt den Schutz personenbezogener Daten ein - auch wenn nicht ausdrücklich darauf verwiesen wird. In der Charta der Grundrechte sind die Rechte auf Privatsphäre bzw. auf den Schutz personenbezogener Daten separat behandelt; diese Trennung spiegelt die Entwicklung des Datenschutzrechts zu einem eigenständigen Bereich mit sektorspezifischen gesetzlichen Regelungen wider. Dennoch ist es sinnvoll, im Zusammenhang mit Smart-TV-Geräten an die zugrundeliegende Verbindung zwischen Privatsphäre und personenbezogenen Daten zu erinnern. Die Spracherkennungsfunktion von Smart-TV-Geräten und ihre Fähigkeit, in der Wohnung geführte private Gespräche zu erfassen, führen zu berechtigten Fragestellungen hinsichtlich der Achtung des Privat- und Familienlebens.

Unbeschadet der Bedeutung dieser Menschenrechte ist ihre Anwendung auf die Anbieter von Diensten, die über Smart-TV-Geräte erbracht werden, komplex. Die EMRK schafft - wie bei internationalen Abkommen üblich - lediglich Verpflichtungen für staatliche Stellen und in der Regel nicht für private Parteien. Wie von führenden Kommentatoren dargestellt, gibt es in Bezug auf die EMRK keine *Drittwirkung*; nach dieser Doktrin kann sich eine natürliche Person auf eine nationale Grundrechtecharta berufen, um gegen eine private Partei gerichtlich vorzugehen, die seine Rechte, über die er gem. diesem Instrument verfügt, verletzt hat.[64] Das soll aber nicht heißen, dass die EMRK keine unmittelbare Wirkung auf das Verhalten privater Parteien haben kann - etwa durch die positiven Verpflichtungen, die sie Staaten auferlegt.[65] Ferner ist darauf hinzuweisen, dass sich die nationalen Gesetzgeber auch dieser Fragen annehmen könnten.

Artikel 1 EMRK verpflichtet die Vertragsstaaten dazu, „allen ihrer Hoheitsgewalt unterstehenden Personen die in [der Konvention] bestimmten Rechte und Freiheiten zu[zusichern]". Die Verpflichtung, diese Rechte „zuzusichern", ist eindeutig und beinhaltet notwendigerweise die Garantie, dass die fraglichen Rechte nicht „theoretisch oder illusorisch", sondern „praktisch und wirksam" sind.[66] Zur Sicherung dieser Rechte ist es nicht immer ausreichend, wenn ein Staat davon absieht, nicht in individuelle Menschenrechte einzugreifen - positive oder affirmative Maßnahmen sind zumeist ebenfalls notwendig. Zum Teil sind positive Pflichten ausdrücklich in der EMRK

[64] Harris D.J., O'Boyle M., Bates E.P. & Buckley C., *Law of the European Convention on Human Rights* (3rd ed.) (Oxford, Oxford University Press, 2014), S. 23.

[65] Ibid.

[66] *Airey gegen Irland*, Urteil vom 9. Oktober 1979, Series A Nr. 32, Randnr. 24, http://hudoc.echr.coe.int/eng?i=001-57420#{"itemid":["001-57420"]}.

vorgesehen, wie in Artikel 6 (Recht auf ein faires Verfahren) und Artikel 13 (Recht auf wirksame Beschwerde). Beide Rechte setzen eindeutig affirmative Maßnahmen seitens des Staates voraus, wenn die garantierten Rechte in der Praxis verwirklicht werden sollen. Neben derartigen positiven, im Text der EMRK verankerten Pflichten hat der Gerichtshof im Laufe der Jahre verschiedene positive Pflichten identifiziert, die implizit im Text angelegt sind.[67]

In seinem *Airey*-Urteil stellt der Gerichtshof fest: „Wenn auch der wesentliche Zweck von Artikel 8 darin liegt, den Einzelnen gegen willkürliche Eingriffe staatlicher Stellen zu schützen, so verpflichtet diese Bestimmung den Staat jedoch nicht nur dazu, sich solcher Eingriffe zu enthalten; zusätzlich zu dieser primären negativen Pflicht können sich aus dem Gebot effektiver Achtung des Privat- und Familienlebens positive Pflichten ergeben [...]."[68] In der Rechtssache *X.und Y. gegen Niederlande* wurde diese Feststellung ergänzt und zugestanden, dass diese „Pflichten die Annahme von Maßnahmen zur Gewährleistung der Achtung des Privatlebens auch im Bereich der Beziehungen zwischen Einzelpersonen selbst beinhalten können".[69] Dies stellt eine wichtige Erweiterung des in vorausgegangenen Entscheidungen artikulierten Grundsatzes dar; darin zeigt sich eine gewisse horizontale Anwendbarkeit der relevanten Rechte. Das Übereinkommen des Europarats über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten stellt einen Rechtsrahmen dar, der von den Mitgliedstaaten umzusetzen ist.[70] Der Gerichtshof beruft sich in Rechtssachen mit Bezug zu automatischer Verarbeitung personenbezogener Daten häufig auf dieses Übereinkommen.[71]

Ähnlich wichtig ist, sich an die spezifische Anwendbarkeit der Charta der Grundrechte der Europäischen Union zu erinnern. Die Bestimmungen der Charta gelten „für die Organe, Einrichtungen und sonstige Stellen der Union unter Wahrung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union" (Artikel 51 (1). „Dementsprechend achten sie die Rechte, halten sie sich an die Grundsätze und fördern sie deren Anwendung entsprechend ihren jeweiligen Zuständigkeiten und unter Achtung der Grenzen der Zuständigkeiten, die der Union in den Verträgen übertragen werden" (*ibid.*). „Die Bestimmungen dieser Charta, in denen Grundsätze festgelegt sind, können durch Akte der Gesetzgebung und der Ausführung der Organe, Einrichtungen und sonstigen Stellen der Union in Ausübung ihrer jeweiligen Zuständigkeiten umgesetzt werden" (Artikel 52 5)). Jedoch können sie „vor Gericht nur bei Auslegung dieser Akte und bei Entscheidungen über deren Rechtmäßigkeit herangezogen werden" (*ibid.).*

[67] Ausführlichere Angaben hierzu, vgl. allgemein, Mowbray A., *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*, Oxford, Hart Publishing Ltd., 2004.

[68] *Airey gegen Irland*, op.cit., Fußnote 66, Randnr. 32.

[69] *X. und Y. gegen Niederlande*, Urteil vom 26. März 1985, Series A Nr. 91, Randnr. 23, http://hudoc.echr.coe.int/eng?i=001-57603#{"itemid":["001-57603"]}.

[70] Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) und das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV 181),

http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

[71] Z.B. *Amann gegen die Schweiz* [2000] ECtHR 27798/95 [65], http://hudoc.echr.coe.int/eng?i=001-58497#{"itemid":["001-58497"]}.

# 3. Länderspezifische Fallstudien

Die gemeinsame Position der deutschen Datenschutzbehörden und die technische Prüfung von Smart-TV-Geräten betreffen grundsätzlich alle vier genannten Funktionen von Smart-TV-Geräten: Spracherkennung, Bewegungssteuerung, Gesichtserkennung und Kontoerstellung. Bei den niederländischen Fällen TP Vision und Ziggo geht es speziell um die Kontoerstellung, und die Beschwerde von EPIC bei der amerikanischen FTC betrifft die Spracherkennung.

Diese länderspezifischen Fallstudien illustrieren zunächst umfassend, wie Leitlinien angelegt werden könnten oder wie (Datenschutz-) Behörden die zahlreichen rechtlichen Implikationen von Smart-TV-Geräten angehen könnten, indem sie ähnliche Leitlinien erstellen, wie sie die gemeinsame Position in Deutschland enthält. Im Anschluss verdeutlichen die niederländischen Fallstudien konkret, welche Rechtsfragen im Zusammenhang mit Datenschutz und Privatsphäre berührt sind. Das amerikanische Beispiel zeigt die allgemeineren Konsequenzen für regulatorische Ansätze gegenüber Smart-TV-Geräten, u. a. das Telekommunikations-, Kinderschutz- und Verbraucherschutzrecht.

## 3.1. Deutschland

Vor dem Hintergrund von Untersuchungen der deutschen Stiftung Warentest im Frühjahr 2014[72] machte die Frage nach der Privatsphäre und dem Schutz der personenbezogenen Daten der Zuschauer und Nutzer der interaktiven Funktionen von Smart-TV-Geräten Schlagzeilen. Die Stiftung Warentest kritisierte besonders die HbbTV-Funktion von Smart-TV-Geräten, bei der sich herausstellte, dass sie den Medienkonsum der Nutzer an die Fernsehsender und verschiedene Drittparteien, darunter Google, meldet. Auch ein Smart-TV-Gerät, das die Gesichtserkennung nutzt, um personalisierte Empfehlungen für Fernseh- und Online-Inhalte zu geben, greift den Ergebnissen der Stiftung Warentest zufolge in die Privatsphäre der Nutzer ein, vor allem weil sich der Hersteller in seinen Datenschutzrichtlinien das Recht vorbehielt, personenbezogene Daten an Dritte zu übertragen. Andere Funktionen wie integrierte Kameras und Mikrofone wurden damals als unproblematisch betrachtet. Allerdings warnte die Stiftung Warentest vor der Verwendung der Spracherkennung, da es sich bei der Stimme um ein individuelles biometrisches Merkmal handele.

Danach räumten die deutschen Datenschutzbehörden dem Thema Smart TV im Hinblick auf die Einhaltung lokaler Datenschutzgesetze Priorität ein. Die zuständigen Länderbehörden gaben gemeinsam ein Positionspapier[73] heraus und leiteten eine technische Untersuchung der

[72] Stiftung Warentest, „Ausgespäht: Datenschutz beim Fernsehen“, test 5(2014), https://www.test.de/filestore/4697612_t201405040.pdf?path=/protected/46/21/2b850438-9820-4bc1-bcfb-12f9cb905c2f-protectedfile.pdf.

[73] Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, „Smartes Fernsehen nur mit smartem Datenschutz“, Mai 2014, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Beschluss_SmartTV.html.

personenbezogenen Datenflüsse bei Smart-TV-Geräten ein.[74] Im September 2015 gipfelten diese Aktivitäten darin, dass die zuständigen deutschen Datenschutzbehörden eine Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste verabschiedeten.[75]

### 3.1.1. Die gemeinsame Position

Die gemeinsame Position mit dem Titel „Smartes Fernsehen nur mit smartem Datenschutz“[76] beschreibt die gemeinsame Linie der für die Durchsetzung der Datenschutzgesetze im privaten Bereich zuständigen Datenschutzbehörden (des sogenannten Düsseldorfer Kreises) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten und wird vor allem von der Direktorenkonferenz der Landesmedienanstalten (DLM) unterstützt.

Die gemeinsame Position erläutert zunächst, dass Zuschauer und Nutzer von Smart TV nicht ohne Weiteres zwischen linearem Fernsehen und dem Zugriff auf Inhalte im Internet unterscheiden könnten, weil der Empfang audiovisueller Signale und die Interaktivität mit dem Internet jetzt über einen Rückkanal integriert seien. Oft sei für die Nutzer nicht erkennbar, welchen Dienst sie gerade nutzen. Im Gegensatz zum traditionellen Fernsehen stelle die Internetverbindung einen Rückkanal von den Nutzern zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten her. Über diesen Rückkanal könne das individuelle Nutzungsverhalten erfasst und ausgewertet werden.

Anschließend verknüpft die gemeinsame Position das Recht auf freien Informationszugang mit der Erfassung und Nutzung von Daten zum Nutzungsverhalten. Die Wahrnehmung des Rechts auf freien Informationszugang, das als fester Bestandteil des Rechts auf freie Meinungsäußerung unter dem Schutz des Grundgesetzes stehe und eine Grundbedingung der freiheitlich demokratischen Grundordnung darstellt, werde dadurch beeinträchtigt.

Im Anschluss werden die Anforderungen aufgezählt, die aus Sicht des deutschen Datenschutzrechts, d. h. des Telemediengesetzes,[77] zu beachten sind: Im deutschen Recht sind Telemediendienste ähnlich definiert wie Dienste der Informationsgesellschaft in der Richtlinie über den elektronischen Geschäftsverkehr. Sie umfassen somit elektronische Informations- und Kommunikationsdienste, die weder Rundfunk noch eine bloße Übertragung von Signalen über Telekommunikationsnetze darstellen (§ 1 Abs. 1 Telemediengesetz). Die gemeinsame Position gibt eine Orientierungshilfe zu der Frage, wie die gesetzlichen Bestimmungen auf Smart-TV-Geräte anzuwenden sind.

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei der Nutzung von Smart-TV-Geräten gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Telemedienanbieter müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:
    a. Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

---

[74] Bayrisches Landesamt für Datenschutzaufsicht, „Datenschutz und Smart TV“, Pressemitteilung vom 27. Februar 2015, https://www.datenschutz-mv.de/presse/2015/pm-SmartTV.pdf.

[75] Supra Fußnote 7.

[76] Supra Fußnote 73.

[77] Telemediengesetz vom 26. Februar 2007, zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2015, http://www.gesetze-im-Internet.de/tmg/BJNR017910007.html.

b. Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.
c. Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere sind im Gerät hinterlegte Merkmale (z.B. Cookies) dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
d. Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „Privacy by Default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.
4. Smart-TV-Geräte, die HbbTV- Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

### 3.1.2. Die technische Prüfung

Anfang 2015 wurden unter der Leitung des Bayerischen Landesamts für Datenschutzaufsicht im Rahmen einer koordinierten bundesweiten technischen Prüfaktion Smart-TV-Geräte von 13 Herstellern untersucht, die etwa 90 % des Marktes in Deutschland abdecken.[78] Ziel der technischen Prüfung war nicht, die Konformität oder Nichtkonformität spezifischer Geräte oder Hersteller mit den einschlägigen deutschen Datenschutzgesetzen festzustellen. Vielmehr ging es in der Prüfung darum, aus technischer Sicht zu erkennen, welche Daten die Geräte verlassen, und eine differenzierte Vorstellung davon zu gewinnen, welche Akteure beteiligt sind. Konkret fokussierte sich die technische Prüfung auf die Informationspflichten der Gerätehersteller und auf die Analyse der Datenflüsse im Zusammenhang mit HbbTV, App-Stores und personalisierten Empfehlungsdiensten. Die Verschlüsselung von Datenflüssen aus Smart-TV-Geräten ist unter dem Aspekt der Informationssicherheit wichtig, stellte für die technische Prüfung jedoch auch einen limitierenden Faktor dar, da nicht genau festgestellt werden konnte, welche Informationen genau übermittelt wurden.

[78] Supra Fußnote 74.

Die folgende Passage gibt anhand der Präsentation in der Pressekonferenz am 27. Februar 2015 einen kurzen Überblick über die Prüfungsergebnisse:[79]

- Von den 13 geprüften Smart-TV-Geräten zeigten sechs Informationen zum Datenschutz an, bevor das Gerät mit dem Internet verbunden wurde.
- Sieben von zehn Sendern verfolgten über die HbbTV-Funktion („Red Button“), wann der Nutzer den Sender wechselt.
- Acht von zehn Sendern informierten die Nutzer der HbbTV-Funktion über die Verarbeitung personenbezogener Daten und verlangten deren Zustimmung.
- Sechs von 13 Smart-TV-Geräten verschlüsselten Daten bei der Nutzung der App-Stores, die vom Gerätehersteller vorinstalliert wurden; von den sieben Smart-TV-Geräten, die unverschlüsselt mit dem App-Store kommunizierten, übermittelten fünf den Namen der App, die der Nutzer gestartet hatte.
- Wenn die Nutzer personalisierte Empfehlungen über den elektronischen Programmführer (EPG)[80] empfingen, schickten sieben der 13 Smart-TV-Geräte verschlüsselte Daten an den EPG-Server. Bei den anderen sechs Smart-TV-Geräten wurde keinerlei Datenverkehr festgestellt.
- Beim Anschluss eines externen Speichermediums, in diesem Fall eines USB-Sticks, an das Smart-TV-Gerät verschickten vier der 13 Geräte verschlüsselte Daten.[81]
- Von den zwölf Smart-TV-Geräten mit Aufnahmefunktion meldete eines die Aufnahme über den Rückkanal, und fünf verschickten verschlüsselte Daten.
- Im linearen Fernsehbetrieb empfingen alle zehn geprüften Sender Daten über den Rückkanal, ebenso wie vier der 13 Gerätehersteller.

Als Ergebnis der technischen Prüfaktion haben die zuständigen Datenschutzbehörden der Länder eine Orientierungshilfe zum Thema Smart-TV erstellt, die der Stärkung von Um- und Durchsetzungsmaßnahmen dienen soll. Parallel dazu werden die zuständigen Datenschutzbehörden mit den Geräteherstellern in Kontakt bleiben, um näher zu klären und festzulegen, was zu tun ist, um die Datenschutzkonformität ihrer Smart-TV-Geräte zu erreichen.

### 3.1.3. Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste

Bei ihrer Sitzung vom 15.–16. September 2015 stimmten die im Düsseldorfer Kreis organisierten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich einer neuen Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste[82] zu. Die Orientierungshilfe richtet sich an die Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und Anbieter von HbbTV-

[79] Bayerisches Landesamt für Datenschutzaufsicht, „Technische Prüfung SmartTV“, Pressekonferenz vom 27. Februar 2015 https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

[80] Sofern jeglicher Verarbeitung personenbezogener Daten zugestimmt wurde.

[81] Im Zusammenhang mit früheren Behauptungen, dass ein Smart-TV-Gerät Dateien von USB-Sticks gelesen und dies dem Hersteller mitgeteilt habe, vgl. Arthur C., „Information commissioner investigates LG snooping smart TV data collection“, op. cit.

[82] Düsseldorfer Kreis, supra Fußnote 73.

Angeboten. Die Orientierungshilfe gibt einen umfangreichen Überblick darüber, wie die zuständigen Aufsichtsbehörden deren Aktivitäten im Rahmen des deutschen Datenschutzrechts (Bundesdatenschutzgesetz) beurteilen.

Die Orientierungshilfe erläutert genau, welche der von Smart-TV-Geräten bereitgestellten Dienste zu personenbezogenen Datenflüssen führen, und enthält auch Definitionen und Erklärungen von Schlüsselbegriffen des deutschen Datenschutzrechts. Ebenfalls vorbildlich ist an der Orientierungshilfe der ganzheitliche Ansatz gegenüber Datenschutzfragen im Smart-TV-Ökosystem, der verschiedene Akteure und Dienste umfasst, sich aber auch der vertikalen Integration in der Wertkette bewusst ist.[83] Einem modularen Ansatz folgend wird daher ausführlich auf die Anforderungen des deutschen Datenschutzes für eine Reihe von Diensten über Smart-TV-Geräte eingegangen, bei denen personenbezogene Daten fließen.

Die Beurteilung basiert auf dem deutschen Datenschutzrecht, das in einigen wenigen wichtigen Aspekten von dem in Kapitel 2 beschriebenen EU-Datenschutzrecht abweicht. Grundsätzlich beschreibt die Orientierungshilfe, unter welchen Umständen die deutsche Rechtslage eine rechtliche Basis für die Verarbeitung personenbezogener Daten bietet und wann ein einzelner Nutzer der Verarbeitung personenbezogener Daten explizit zustimmen muss. Das einschlägige deutsche Telemediengesetz unterscheide zwischen dem Umgang mit Bestandsdaten und mit Nutzungsdaten einzelner Nutzer, für die verschiedene rechtliche Anforderungen gelten. Insbesondere hätten Nutzer nach dem Telemediengesetz das Recht, als Telemediendienste geltende Dienste anonym zu nutzen, soweit dies technisch möglich ist. Daher müsse den Nutzern diesbezüglich eine Wahlmöglichkeit geboten werden. Diese Anforderung beispielsweise gebe es im EU-Datenschutzrecht nicht.

Eine weitere Besonderheit des Telemediengesetzes sei, dass Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen dürfen, sofern der Nutzer dem nicht widerspricht (d. h. eine Opt-out-Anforderung).[84] Die Pseudonymisierung erfordere jedoch eine Trennung zwischen dem pseudonymen Nutzungsprofil und dem einzelnen Nutzer, und diese sei nicht gegeben, wenn Nutzungsprofile mit Gerätekennungen oder IP-Adressen verknüpft werden.

Großer Wert wird auf die Informationspflichten gelegt, die nach dem deutschen Datenschutzrecht zu erfüllen sind, wobei die Informationen angezeigt werden müssen, bevor personenbezogene Daten verarbeitet werden dürfen.[85] Zudem müssten die Nutzer die Möglichkeit haben, jederzeit auf die Informationen über den Umgang mit ihren personenbezogenen Daten zuzugreifen. Die Orientierungshilfe stellt klar, dass eine Information, die in den Allgemeinen Geschäftsbedingungen des Dienstes erfolgt, den Transparenzanforderungen des deutschen Datenschutzrechts nicht genügen würde. Darüber hinaus enthalte das deutsche Datenschutzrecht die Datenschutzprinzipien, die auch im EU-Recht bekannt sind.

Eine weitere Gruppe wichtiger Anforderungen betreffe die Möglichkeit der Nutzer, die Einstellungen und Präferenzen, z. B. für Cookies, an ihrem Gerät zu verwalten, sowie eingebauten Datenschutz und datenschutzfreundliche Voreinstellungen im Zusammenhang mit HbbTV-fähigen Onlinediensten und eingebauten Mikrofonen und Kameras.[86]

Abschließend ist darauf hinzuweisen, dass die Orientierungshilfe die technischen und organisatorischen Maßnahmen nennt, die zum Schutz der Sicherheit der personenbezogenen Daten notwendig sind. So müssen insbesondere die Gerätehersteller regelmäßige Sicherheitsupdates

[83] Ibid.

[84] Ibid.

[85] Ibid.

[86] Ibid.

gewährleisten, und alle personenbezogenen Datenflüsse zwischen dem Smart-TV-Gerät und den Dienstanbietern müssen während der Übertragung verschlüsselt sein.

Die vorstehend beschriebene gemeinsame Position ist ein Grundsatzpapier, während die später herausgegebene Orientierungshilfe genauer angibt, wie die zuständigen deutschen Datenschutzbehörden das Recht in Bezug auf die Verarbeitung personenbezogener Daten durch die verschiedenen Anbieter im Smart-TV-Ökosystem auslegen und anwenden werden. Die Orientierungshilfe wendet die einschlägigen deutschen Datenschutzbestimmungen aus dem Telemediengesetz und dem Bundesdatenschutzgesetz streng an. Sie geht nicht programmatisch über die Anforderungen der Gesetze hinaus, doch sind diese in jedem Fall recht streng. Die Hauptleistung der Orientierungshilfe besteht darin, dass die rechtliche Beurteilung entsprechend den spezifischen Aktivitäten, bei denen personenbezogene Daten verarbeitet werden, modular erfolgt, unabhängig von der Rolle des Anbieters im Smart-TV-Ökosystem.

## 3.2. Niederlande

Die niederländische Datenschutzbehörde (*College bescherming persoonsgegevens* – CBP) hat zwei Unternehmen untersucht, die an der Verarbeitung personenbezogener Daten im Zusammenhang mit interaktiven Digitalfernseh- und Onlinediensten über Smart-TV-Geräte beteiligt waren. Die CBP überwacht die Einhaltung des niederländischen Datenschutzgesetzes[87] (*Wet bescherming persoonsgegevens* – WBP), das die EU-Datenschutzrichtlinie umsetzt, die in Kapitel 2 zum europäischen Rechtsrahmen näher erörtert wird.[88] Bei einem Verstoß gegen niederländisches Recht kann die CBP Durchsetzungsbefugnisse ausüben und etwa Geldbußen verhängen.[89]

Die CBP erkannte in der Verarbeitung personenbezogener Daten zum Sehverhalten – angesichts des größeren Themas „Verfolgung und Ortung“ – eine Thematik, die besondere Aufmerksamkeit verdient.[90] Die erste Untersuchung betraf die Firma TP Vision, die Smart-TV-Dienste über Philips-Geräte anbietet. Die zweite Untersuchung galt dem Kabelfernsehbetreiber Ziggo, der seinen Abonnenten audiovisuelle Medien anbietet. Aufgrund der detaillierten Analyse des niederländisches Datenschutzgesetzes zeigen diese Beispiele nicht nur niederländische Rechtsfolgen auf, sondern werfen auch Fragen zum europäischen Datenschutzrahmen für die Regulierung von Smart-TV-Geräten auf.

Sachverhalt und Rechtsrahmen der beiden Fälle werden nachstehend gesondert analysiert, und danach werden in einer Schlussbemerkung zu den niederländischen Beispielen künftige Auswirkungen auf die Regulierung von Smart-TV-Geräten beschrieben.

---

[87] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_26-10-2015.

[88] Kapitel 2, unter „Regelungen zum Schutz der Privatsphäre und Datenschutz in der elektronischen Kommunikation“

[89] https://www.cbpweb.nl/en/node/1930.

[90] Niederländische Datenschutzbehörde, Untersuchung der Verarbeitung personenbezogener Daten durch Verwendung interaktiver Digitalfernsehdienste von Ziggo, Bericht vom 28. April 2015, S. 4, https://cbpweb.nl/sites/default/files/atoms/files/onderzoek_ziggo.pdf. Niederländische Datenschutzbehörde, Jahresbericht 2014, S. 3, https://cbpweb.nl/sites/default/files/atoms/files/annual_report_2014.pdf.

### 3.2.1. Fallstudie 1 – *CBP / TP Vision*

Am 2. Juli 2013 veröffentlichte die niederländische Datenschutzbehörde ihre Ergebnisse zu der niederländischen Firma TP Vision, dem Hersteller der Smart-TV-Geräte von Philips.[91] Die CBP untersuchte die Verarbeitung personenbezogener Daten der Nutzer von Philips Smart-TV-Geräten in den Niederlanden. Die Behörde erklärt, durch den Mangel an klaren, zugänglichen und umfassenden Informationen über die Verarbeitung personenbezogener Daten, das Fehlen einer informierten Einwilligung zum Setzen von Tracking-Cookies und die Abwesenheit eines Vertrags mit Dritten habe TP Vision gegen das niederländische Datenschutzgesetz (WBP) verstoßen. Die von TP Vision verarbeiteten Daten betreffen die Möglichkeiten zur Kontoerstellung sowie interaktive Funktionen von Smart-TV-Geräten, wie sie oben näher beschrieben wurden.[92]

Diese Fallstudie analysiert zunächst den Sachverhalt, der zur Untersuchung der Smart-TV-Geräte von TP Vision durch die CBP führte. Im Anschluss wird auf den Rechtsrahmen eingegangen, der dem Bericht der CBP über die Smart-TV-Geräte von TP Vision zugrunde liegt.

#### 3.2.1.1. Sachverhalt

Auslöser der Untersuchung von Smart-TV-Geräten und insbesondere von TP Vision durch die CBP waren die steigenden Verkaufszahlen von Fernsehgeräten mit interaktiven Fähigkeiten und Video-on-Demand-Diensten, die Nutzerinformationen sammeln. TP Vision entwickelt und produziert Smart-TV-Geräte für Philips, von denen in den Niederlanden seit 2009 schätzungsweise 1,2 Millionen verkauft wurden. TP Vision sammelt und speichert Daten zum Online-Zuschauerverhalten, zur App-Nutzung und zum Website-Verlauf – z. B. mit (Tracking-) Cookies. Außerdem sammeln Smart-TV-Geräte von TP Vision Daten über Nutzergewohnheiten wie Lieblingsprogramme und -Apps, aufgezeichnete Programme, entliehene Videos und auf Abruf gesehene Sendungen. Anhand dieser Daten bietet TP Vision Nutzern personalisierte Empfehlungen an und will künftig auch personalisierte Werbung anbieten.

#### 3.2.1.2. Rechtsrahmen

Nach einem umfassenden Überblick über die Praktiken von TP Vision und andere Umstände des Falls untersucht die CBP diese Handlungen und Praktiken aus Sicht des WBP. Von den verschiedenen Verpflichtungen im WBP konzentriert sich diese Untersuchung der CBP auf die primären Anforderungen des Begriffs „personenbezogene Daten“, die Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die Informationspflichten und die Verträge mit Dritten.

##### 3.2.1.2.1. Personenbezogene Daten

Personenbezogene Daten sind im WBP definiert als *„Informationen über eine bestimmte oder bestimmbare natürliche Person“*.[93] Da die Definition dieselben Merkmale aufweist wie die in der EU-

[91] Niederländische Datenschutzbehörde, Untersuchung der Verarbeitung personenbezogener Daten auf Philips Smart-TV-Geräten durch TP Vision Netherlands B.V., Bericht vom 2. Juli 2013,

https://www.cbpweb.nl/sites/default/files/downloads/pb/pb_20130822-persoonsgegevens-smart-tv.pdf.

[92] Kapitel 1.

[93] Artikel 1 (a) WBP; Artikel 1 (a) Datenschutzrichtlinie. Für weitere Informationen siehe: Artikel-29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20. Juni 2007.

Datenschutzrichtlinie verwendete und von der Artikel-29-Datenschutzgruppe erläuterte Definition, reicht die genaue Untersuchung „personenbezogener Daten“ in Kapitel 2 für einen umfassenden Überblick über diesen Bericht der CBP aus. Der CBP zufolge sind die gesammelten Daten als personenbezogene Daten einzustufen, weil die von TP Vision gesammelten Informationen – darunter IP-Adressen, gesehene Fernsehprogramme, benutzte Apps und besuchte Websites – tiefe Einblicke in die Fernsehgewohnheiten, das Verhalten und die Vorlieben der Nutzer erlaubten.[94] Darüber hinaus stuft die CBP die personenbezogenen Daten als sensibel ein, weil sie viel über einzelne Personen verrieten.[95] So könnten sie etwa auf einen spezifischen sozialen Hintergrund, ein finanzielles Profil und/oder eine familiäre Situation hinweisen. Daher könnten solche Daten verwendet werden, um das Verhalten von (Online-) Nutzern zu beeinflussen, und zu direkten Marketingzwecken oder zum Profiling von Smart-TV-Nutzern dienen. Dieser Aspekt der Ergebnisse ist beachtenswert, weil er sensible personenbezogene Daten als Kategorie einführt, die sich von den ansonsten geschützten Sonderkategorien personenbezogener Daten unterscheidet, die Auskunft über Gesundheit, religiöse Überzeugungen, politische Einstellungen usw. geben.

TP Vision legt die Zwecke und Mittel der Verarbeitung personenbezogener Daten fest. TP Vision gilt daher in Bezug auf die personenbezogenen Daten aus Smart-TV-Geräten als „für die Verarbeitung Verantwortlicher“.[96] Auch die Definition des „für die Verarbeitung Verantwortlichen“ entspricht der Definition im oben beschriebenen europäischen Rechtsrahmen.

#### 3.2.1.2.2. Information

Dem WBP zufolge müssen für die Verarbeitung Verantwortliche den betroffenen Personen spezifische Informationen mitteilen: die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung, die Empfänger der Daten und das Vorhandensein ihrer Auskunfts- und Berichtigungsrechte.[97] Diese Informationen müssen klar und verständlich bereitgestellt werden, um dem Nutzer mehr Kontrolle über die Verbreitung personenbezogener Daten zu geben.

Die CBP erklärte, TP Vision habe diese Informationspflichten nicht erfüllt. Die Verbraucher seien weder auf der Website von Philips noch in den Datenschutzrichtlinien, im Cookie-Banner oder in den Nutzungsbedingungen von TP Vision informiert worden. Insbesondere hätten die Nutzer keine Informationen über das Bestehen und die Verantwortlichkeiten von TP Vision, das Setzen von Cookies, die Art der gesammelten Daten oder die Speicherdauer dieser Daten erhalten.

Im Verlauf der Untersuchung passte TP Vision seine Datenschutzerklärung, seine Cookie-Richtlinien und seine Nutzungsbedingungen an, um die geltenden Vorschriften zu erfüllen. Dennoch sind die Informationen der CBP zufolge noch immer zu unklar, inkonsistent und für die Öffentlichkeit unzugänglich. So würden die Informationen erstens nicht auf Niederländisch, in kurzen und leicht lesbaren Texten, präsentiert, und zweitens würden sie nicht vorab bereitgestellt, sondern erst nachdem das Smart-TV-Gerät bereits mit dem Internet verbunden worden sei.

---

[94] Die vollständige Liste der gesammelten Daten findet sich in: Niederländische Datenschutzbehörde, Untersuchung der Verarbeitung personenbezogener Daten auf Philips Smart-TV-Geräten durch TP Vision Netherlands B.V., Bericht vom 2. Juli 2013, S. 53.

[95] Ibid.

[96] Artikel 1 (d) WBP; Artikel 2 (d) Datenschutzrichtlinie. Für weitere Informationen zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16. Februar 2010 (WP 169),

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

[97] Artikel 33 und 34 WBP; Artikel 10 und 11 Datenschutzrichtlinie.

#### 3.2.1.2.3. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die CBP stellt in ihrem Bericht fest, dass sich TP Vision durch das Setzen von Cookies Zugang zu Nutzerinformationen verschaffe. Aufgrund des Einsatzes von Cookies müsse die Firma auch das niederländische Telekommunikationsgesetz[98] einhalten.

Wenn ein für die Verarbeitung Verantwortlicher Informationen speichert oder sich Zugriff auf Informationen verschafft, die bereits auf einem Gerät gespeichert sind, muss der betroffene Nutzer in die Speicherung oder den Informationszugriff einwilligen, damit diese Handlungen rechtmäßig sind, – sofern sie nicht *„unbedingt erforderlich sind, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen“.*[99] In Übereinstimmung mit dem niederländischen Telekommunikationsgesetz sowie der erwähnten E-Privacy-Richtlinie der EU muss die Einwilligung des Nutzers auf klaren und umfassenden Informationen des für die Verarbeitung Verantwortlichen u. a. über die Zweckbestimmungen der Verarbeitung basieren.

Darüber hinaus verarbeiten die von TP Vision gesetzten Cookies personenbezogene Daten. Daher benötigt der für die Verarbeitung Verantwortliche eine Rechtsgrundlage, damit diese Verarbeitung personenbezogener Daten nach dem WBP[100] rechtmäßig ist.

Nach Auffassung der CBP muss TP Vision eine „zweifelsfreie Einwilligung“ einholen, bevor es mit Cookies personenbezogene Daten sammeln darf. Diese Einwilligung müsse auf einer freien, spezifischen und informierten Willenserklärung basieren. TP Vision habe zunächst überhaupt nicht um Erlaubnis gebeten, diese Politik später aber geändert. zudem werde die Einwilligung nicht frei erteilt, da sie bei der Installation des Smart-TV-Geräts verlangt werde. Daher müsse der Nutzer die Nutzungsbedingungen akzeptieren. Dasselbe gelte, wenn TP Vision „Pop-ups“ mit Opt-out-Möglichkeiten einsetze, um die Einwilligung einzuholen, da nur Opt-in-Möglichkeiten als freie Willenserklärung zu betrachten seien.

Weiterhin präsentiere TP Vision, wie oben bereits ausgeführt, keine klaren und zugänglichen Informationen zum Einsatz von Cookies und zu den Einzelheiten der stattfindenden Verarbeitung. Dieser Mangel an Transparenz sei nicht als gültige Einwilligung in die Verarbeitung von Daten zu betrachten, weil eine „spezifische“ und „informierte“ Einwilligung fehle.

#### 3.2.1.2.4. Verarbeitungsvertrag

Für die Verarbeitung personenbezogener Daten nutzt TP Vision die Dienste von fünf verschiedenen Unternehmen. Da diese Unternehmen nach dem niederländisches Datenschutzgesetz als „Auftragsverarbeiter“ betrachtet werden können, ist TP Vision verpflichtet, mit ihnen einen Verarbeitungsvertrag oder sonstigen Rechtsakt über die Verantwortlichkeiten beider Seiten abzuschließen, um die Verarbeitung personenbezogener Daten nach Treu und Glauben sicherzustellen.[101]

Die CBP erklärte, TP Vision verstoße gegen diese Anforderung, da mit Google kein Verarbeitungsvertrag über die Nutzung der Dienste von Google Analytics unterzeichnet worden sei. Google habe sich jedoch geweigert, den Vertrag zu unterzeichnen, sodass die Angelegenheit durch eine vollständige Beendigung der Zusammenarbeit mit Google gelöst worden sei. Mit anderen Auftagsverarbeitern habe TP Vision bereits Verträge unterzeichnet, die nach Auffassung der CBP lediglich leicht angepasst werden müssten, damit sie dem WBP entsprechen.

---

[98] Niederländisches Telekommunikationsgesetz vom 19. Oktober 1998 (*Telecommunicatiewet*), http://www.wetboek-online.nl/wet/Telecommunicatiewet.html.

[99] Artikel 11.7 a (3) (b) Tw.

[100] Artikel 8 WBP; Artikel 7 Datenschutzrichtlinie.

[101] Artikel 14 WBP; Artikel 17 (4) Datenschutzrichtlinie.

Als Reaktion auf die Untersuchung der CBP änderte TP Vision seine Datenschutzerklärung, seine Cookie-Politik und seine Nutzungsbedingungen, um seine Praktiken mit dem WBP in Übereinstimmung zu bringen. Informationen über die Sammlung von Cookies zur Überwachung des Zuschauerverhaltens werden bei der Installation des Smart-TV-Geräts deutlicher angezeigt; ferner stehen klare und umfassende Informationen über die Verarbeitung von Daten zu Werbezwecken zur Verfügung. Wie oben ausgeführt, ist die CBP der Auffassung, dass TP Vision noch immer gegen das niederländische Datenschutzrecht verstößt. Allerdings kündigte sie an, dass sie wegen der teilweisen Beendigung des Verstoßes nicht mit formalen Durchsetzungsmaßnahmen fortfahren werde.[102] Dennoch werde die CBP die Einhaltung des WBP durch TP Vision weiterhin beobachten.

## 3.2.2. Fallstudie 2 – *CBP / Ziggo*

Am 28. April 2015 veröffentlichte die niederländische Datenschutzbehörde den Bericht über ihre Untersuchung des Kabelfernsehbetreibers Ziggo. Der Bericht erläutert, wie Ziggo durch die Überwachung des Sehverhaltens von Nutzern interaktiver Digitalfernsehdienste gegen das niederländische Datenschutzgesetz verstoßen habe. Diese personenbezogenen Daten, entsprechend den Ergebnissen im Fall TP Vision, betreffen die Möglichkeiten zur Kontoerstellung sowie interaktive Funktionen von Smart-TV-Geräten, wie sie in Kapitel 1 näher beschrieben wurden. Der CBP zufolge verstieß Ziggo gegen das WBP, indem es den Nutzern keine ausreichenden Informationen über die Verarbeitung personenbezogener Daten bereitstellte. Zudem kam die Untersuchung zu dem Ergebnis, dass Ziggo für die Verarbeitung personenbezogener Daten nicht die erforderliche zweifelsfreie Einwilligung eingeholt habe.

Diese Fallstudie analysiert zunächst den Sachverhalt, der den Hintergrund des CBP-Berichts bildet. Im Anschluss wird auf den Rechtsrahmen eingegangen, der der CBP-Untersuchung der interaktiven Dienste von Ziggo zugrunde liegt.

### 3.2.2.1. Sachverhalt

Ziggo B.V. ist ein niederländischer Kabelfernsehbetreiber, der interaktive Digitalfernsehdienste bereitstellt. Ziggo fusionierte vor Kurzem mit der UPC Nederland, doch die CBP-Untersuchung fand vor dieser Fusion statt und berücksichtigt daher nur die Handlungen und Tätigkeiten von Ziggo. Anlass für die CBP-Untersuchung von Ziggo ist die Tatsache, dass Ziggo in den Niederlanden mit 2,3 Millionen Nutzern der größte Anbieter von Digitalfernsehdiensten war. Heute hat Ziggo 4,2 Millionen Kunden.

Die CBP diskutiert in ihrem Bericht drei verschiedene Formen der Überwachung des Zuschauerverhaltens, um festzustellen, wie Ziggo diese Daten zu Profiling- und Marketingzwecken nutzt. Die CBP konzentriert sich auf „regulären“ (d. h. linearen) Fernsehkonsum, (Video-) On-Demand-Konsum und Pay-per-Event-Konsum. In der ersten Kategorie, dem linearen Fernsehkonsum, konnte Ziggo das Sehverhalten konkreter Personen feststellen und daher Zuschauerquoten im größeren Maßstab ermitteln. Der CBP-Bericht erklärt, Ziggo habe diese personenbezogenen Daten mithilfe eines aktivierten interaktiven Fernsehdecoders verarbeitet.

Bei On-Demand-Diensten habe Ziggo, ebenfalls mithilfe interaktiver Decoder, den Sehverlauf der Nutzer überwachen können. Durch das Profiling des Verhaltens von Video-on-Demand-Nutzern

[102] Siehe https://www.cbpweb.nl/nl/nieuws/tp-vision-past-privacybeleid-aan-na-onderzoek-cbp.

habe Ziggo Sehempfehlungen für spezifische Nutzer personalisiert und könne zudem auch Sehempfehlungen im Allgemeinen geben.

Drittens unterschied die CBP zwischen „Pay-per-View"- und „Pay-per-Event"-Überwachung. Dabei sei Pay-per-View der interaktive Dienst, mit dem Nutzer bestimmte Programme oder Filme online kaufen können, primär in der Kategorie Sport und Erotik. Ziggo habe diese Zuschauerinformationen einmalig zu Direktmarketingzwecken genutzt.

### 3.2.2.2. Rechtsrahmen

Die CBP beginnt ihren Bericht mit einem umfassenden Überblick über Verfahrensaspekte und Sachverhalte der Verarbeitung personenbezogener Daten durch Ziggo. Im Anschluss untersucht sie die Handlungen und Praktiken von Ziggo aus Sicht des WBP. Ähnlich wie bei der Analyse der CBP im Fall TP Vision konzentriert sich diese CBP-Untersuchung gemäß den verschiedenen Anforderungen des WBP auf den Begriff „personenbezogene Daten", die Informationspflicht und die Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Diese Verpflichtungen werden vor dem Hintergrund der von der CBP getroffenen Unterscheidung zwischen linearem, On-Demand- und Pay-per-Event-Konsum diskutiert. Die CBP erkennt in jedem dieser Bereiche Verstöße gegen das Datenschutzrecht.

#### 3.2.2.2.1. Personenbezogene Daten

Der CBP zufolge sammelt Ziggo personenbezogene Daten durch Überwachung des Zuschauerverhaltens. Durch die spätere Analyse und/oder Kombination dieser Daten könne Ziggo Nutzer bestimmten Profilen zuordnen und sie anders behandeln oder gezielter ansprechen.

Insbesondere verwies die CBP auf die Sensibilität der personenbezogenen Daten, die in die Datenverarbeitungsaktivitäten von Ziggo involviert seien. Ihrer Bewertung im Fall TP Vision folgend sollten die personenbezogenen Daten als sensibel betrachtet werden, da die Überwachung des Digitalfernsehkonsums – insbesondere die Pay-per-View-Historie von Erotikinhalten – die Gewohnheiten und Vorlieben der Nutzer schonungslos aufdecke. Dies könne auf einen spezifischen sozialen Hintergrund, ein finanzielles Profil und/oder eine familiäre Situation hinweisen. Daher könnten diese Daten verwendet werden, um das Verhalten von (Online-) Nutzern zu beeinflussen, oder direkten Marketingzwecken und dem Profiling von Ziggo-Nutzern dienen.[103]

#### 3.2.2.2.2. Information

Dem WBP zufolge müssen für die Verarbeitung Verantwortliche den betroffenen Personen spezifische Informationen mitteilen, z. B. die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung, die Empfänger der Daten und das Bestehen ihrer Auskunftsrechte in Bezug auf ihre personenbezogenen Daten.[104] Diese Informationen müssen klar und verständlich bereitgestellt werden, um dem Nutzer mehr Kontrolle über die Verbreitung personenbezogener Daten zu geben.

Bei der ersten Kategorie, den linearen Fernsehdiensten, konnte Ziggo das Sehverhalten konkreter Personen feststellen, ohne dass die Betroffenen ausreichend informiert worden wären.

[103] Ibid.

[104] Artikel 33 und 34 WBP; Artikel 10 und 11 Datenschutzrichtlinie.

Nach Auffassung der CBP stellt Ziggo nicht ausreichend klar, welche personenbezogenen Daten zu welchen konkreten Zwecken gesammelt und verarbeitet werden.

Ziggo habe auf diesen Verstoß reagiert, indem es die Decoder so angepasst habe, dass Informationen zum Sehverhalten nicht mehr zu bestimmten Personen zurückverfolgt werden können. Durch die Umsetzung dieser Anonymisierungsmethoden seien die verarbeiteten Daten nicht mehr als personenbezogene Daten zu betrachten. Aufgrund dieser Anpassungen sei das niederländische Datenschutzrecht nicht mehr relevant, wodurch sich auch die früheren Gesetzesverstöße erledigt hätten, erklärte die CBP.

In der Kategorie des On-Demand-Fernsehens habe Ziggo zu mehreren Aspekten keine ausreichenden Informationen vorgelegt. Zum einen heiße es in den Datenschutzrichtlinien von Ziggo, alle Informationen würden anonym verarbeitet, was nach den Erkenntnissen der CBP jedoch nicht zutreffe. Auch sei den Nutzern nicht bewusst, welche Verhaltensdaten verarbeitet würden. Drittens verstoße Ziggo gegen die Informationspflicht, weil die Zweckbestimmungen der Verarbeitung nicht klargestellt würden. Die *„Anpassung von Diensten an Kunden“* sei als Zweckangabe nicht konkret genug. Darüber hinaus wüssten die Nutzer nicht, dass ihr Sehverhalten zur Erstellung von Nutzerprofilen verwendet werde. Überdies seien die Datenschutzrichtlinien von Ziggo für die meisten Kunden generell unzugänglich, da sie auf der Website von Ziggo schwer zu finden seien.

Auch in der letzten Kategorie, dem Pay-per-Event-Konsum, habe Ziggo seine Informationspflichten nicht erfüllt. Die Überwachung des (sensiblen) Digitalkonsums habe stattgefunden, ohne dass Ziggo seine Nutzer über irgendeinen Aspekt der Verarbeitung aufgeklärt hätte. Im Allgemeinen wüssten die Nutzer nicht, dass Ziggo zu Marketingzwecken ein Profil ihres persönlichen Sehverhaltens erstelle.

#### 3.2.2.2.3. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Laut WBP benötigt der für die Verarbeitung Verantwortliche eine Rechtsgrundlage, damit die Verarbeitung personenbezogener Daten rechtmäßig ist.[105] Die CBP erklärt, mit der Überwachung des linearen Fernsehkonsums, des On-Demand-Konsums und des Pay-per-Event-Konsums ohne gültige Einwilligung verstoße Ziggo gegen diese Anforderung. Als Rechtsgrundlage für Ziggo komme ausschließlich eine „zweifelsfreie Einwilligung“ in Frage, da die Verarbeitung sensible Daten betreffe.

Zur ersten Kategorie, dem linearen Fernsehen, stellt die CBP fest, Ziggo habe die erforderliche zweifelsfreie Einwilligung nicht eingeholt, bevor personenbezogene Daten der Nutzer verarbeitet worden seien. Ziggo habe den Nutzern seinerzeit keine Möglichkeit gegeben, zu irgendeinem Zeitpunkt während der Datensammlung ihre Einwilligung zu erklären. Der Verstoß gegen die Bestimmung des WBP sei, wie bereits ausgeführt, durch die Anonymisierung der verarbeiteten Daten behoben worden, da die Informationen über das Sehverhalten nicht mehr zu bestimmten Personen zurückverfolgt werden könnten.

Nach Auffassung der CBP stellte die Nutzung personenbezogener Daten zum On-Demand-Konsum einen Verstoß gegen das WBP dar. Ziggo habe keine gültige informierte Einwilligung eingeholt; die Nutzer hätten keine wirksame Möglichkeit gehabt, die Erlaubnis für diese Verarbeitungshandlung zu verweigern.

Anfangs habe Ziggo überhaupt keine Einwilligung verlangt. Später habe Ziggo dann die Schaltfläche „Ich stimme nicht zu“ eingeführt. Es sei versucht worden, die Einwilligungsaufforderung konkreter zu formulieren, doch habe dies nichts daran ändern können, dass nur unzureichend darüber informiert wurde, welche personenbezogenen Daten gesammelt wurden. Ziggo informiere

[105] Artikel 8 WBP; Artikel 7 Datenschutzrichtlinie.

die Nutzer nicht über die spezifischen Kategorien personenbezogener Daten, die zur Personalisierung von Inhalten genutzt würden. Außerdem informiere Ziggo die Nutzer, wie bereits ausgeführt, nicht über die Erstellung von Profilen. Darüber hinaus sei diese Aufforderung nur Neukunden gezeigt wurden, nicht aber bestehenden Ziggo-Nutzern. Da eine Einwilligung unbedingt erforderlich gewesen sei, seien die Aktivitäten durch deren Fehlen rechtswidrig gewesen. Ziggo habe seine On-Demand-Aktivitäten nochmals angepasst, und die Verbraucher würden nun aufgefordert, eine gültige Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zu erteilen oder eben nicht.[106]

Bei der letzten Kategorie, dem Pay-per-Event-Konsum, seien Zuschauerinformationen einmalig zu Direktmarketingzwecken verwendet worden. Die Feststellungen zum linearen Fernsehen und zum On-Demand-Fernsehen seien auch für diese Kategorie gültig. Vor allem weil es sich bei den Informationen nach den Erkenntnissen der CBP um sensible personenbezogene Daten handele, habe Ziggo das WBP nicht eingehalten, weil es keine gültige Einwilligung verlangt habe.

Als Reaktion auf den CBP-Bericht beendete Ziggo die Verstöße gegen das WBP durch mehrere Anpassungen seiner Datenschutzrichtlinien. Die CBP erklärt, Ziggo erfülle die Anforderungen des WBP nun, indem es die Abonnenten korrekt informiere und ihre zweifelsfreie Einwilligung in die Verarbeitung ihrer personenbezogenen Daten verlange.[107]

### 3.2.2.3. Künftige Auswirkungen

Grundsätzlich räumt die CBP ein, dass es bei den Konsumenten bislang kaum ein Bewusstsein für die Risiken bei der Nutzung von Smart-TV-Geräten gebe, da diese auf dem Fernsehmarkt noch relativ neu seien. Daher werde sich die CBP wohl weiterhin auf dieses neue Phänomen konzentrieren, um die Rechte der Abonnenten und Nutzer von interaktiven und Smart-TV-Diensten zu wahren. Die Durchsetzungsorientierung der CBP unterstreicht, dass sich die Behörde der Auswirkungen von interaktiven Diensten wie Smart-TV, die ohne Weiteres verschiedene Aspekte des Privatlebens verknüpfen, auf Privatsphäre und Datenschutz bewusst ist.[108] In den Niederlanden kam ein Bündnis zwischen Datenschutzbeauftragten und öffentlich-rechtlichen Rundfunkanstalten – oder eine andere bereichsübergreifende Koordination – wie das deutsche Bündnis bisher (noch) nicht zustande.

#### 3.2.2.3.1. Interaktive Fernsehgeräte

Beide Untersuchungen sind repräsentativ für den Ansatz der niederländischen Datenschutzbehörde, selektive Durchsetzungsmaßnahmen zu ergreifen, die für die Verarbeitung personenbezogener Daten im Kontext interaktiver Smart-TV-Dienste exemplarisch sind. Die Ziggo-Untersuchung verdeutlicht interessante Merkmale der Überwachung und des Profilings von Nutzern interaktiver Fernsehgeräte. Die weit verbreiteten Möglichkeiten von Smart-TV-Geräten werden diskutiert, indem speziell auf die Unterschiede zwischen linearem Fernsehkonsum, On-Demand-Konsum und Pay-per-Event-Konsum eingegangen wird. Im Fall TP Vision dagegen ging es um andere Dienste im Zusammenhang mit Smart-TV-Geräten, z. B. die Überwachung des Online-Zuschauerverhaltens, die

[106] CBP Persbericht, *Ziggo beëindigt privacy overtredingen digitale tv na onderzoek CBP*, 9. Juni 2015, https://cbpweb.nl/nl/nieuws/ziggo-beeindigt-privacyovertredingen-digitale-tv-na-onderzoek-cbp.

[107] Ibid.

[108] Die Artikel-29-Datenschutzgruppe hat einen Bericht über die Bedeutung der Transparenz im Bereich vernetzter Geräte veröffentlicht, siehe: Artikel-29-Datenschutzgruppe, „Stellungnahme 8/2014 über die neuesten Entwicklungen beim Internet der Dinge“ (WP 223) 16. September 2014.

Nutzung von Apps und, allgemeiner betrachtet, den Website-Verlauf[109]. Darüber hinaus bestätigt die CBP, dass Informationen zum Sehverlauf der Nutzer, sei es beim On-Demand- oder beim Pay-per-Event-Konsum, als sensible personenbezogene Daten einzustufen sind. Dies könnte implizit auch auf andere interaktive Verbrauchergeräte anwendbar sein, die Profile des individuellen Nutzerverhaltens erstellen.

#### 3.2.2.3.2. Die Rolle von Information und Transparenz

In den beiden niederländischen Beispielen wird deutlich, dass der Hauptaspekt der Rechtsverletzung im Fehlen ausreichender Informationen für die betroffenen Personen liegt. Die Informationspflicht ist eine spezifische Anforderung im niederländischen (und EU-) Datenschutzrecht. Sie beeinflusst auch die Gültigkeit einer Einwilligung, da diese auf einer „informierten" Willenserklärung basieren muss. Man könnte den Schluss ziehen, dass dieser Informationsaspekt des Datenschutzes eine wichtige Rolle spielt.

Beide Berichte der niederländischen CBP zeigen die Bedeutung der Transparenz im Bereich vernetzter Verbrauchergeräte. Die Erhöhung der Transparenz in Bezug auf die Einzelheiten der Verarbeitung personenbezogener Daten und die Verträge mit Auftragsverarbeitern wird wahrscheinlich die Entscheidungsfindung verbessern und den Nutzern bessere Möglichkeiten geben, ihre personenbezogenen Daten wirksam zu kontrollieren.

In Verbindung mit einer Medienregulierung, deren Ziel es ist, den Einzelnen zu ermächtigen (Stichwort Medienkompetenz), zielt auch die Datenschutzregulierung auf Ermächtigung und Transparenz. Andere Anforderungen im WBP, z. B. das Auskunftsrecht der betroffenen Person, sollen den Einzelnen gegenüber den mit der Verarbeitung personenbezogener Daten Verantwortlichen ermächtigen.

Bei den von der CBP in den beiden Fallstudien angesprochenen Verstößen geht es also primär um die Ermächtigung des Einzelnen. In den niederländischen Fällen werden keine Verbraucherschutzgesetze erwähnt. Die Ermächtigung des Einzelnen hat aber wohl dasselbe Ziel wie die Verbraucherschutzvorschriften, wie weiter unten gezeigt.

Zudem verdeutlicht auch die gemeinsame Position der deutschen Behörden den Informationsmangel, vor allem weil der Empfang audiovisueller Signale und die Interaktivität mit dem Internet über einen Rückkanal jetzt integriert sind. Die technische Prüfung von Smart-TV-Geräten ergab, dass sechs von 13 geprüften Geräten Informationen zum Datenschutz anzeigten, bevor sie mit dem Internet verbunden wurden.[110]

## 3.3. Ein Beispiel aus Amerika

An der folgenden Fallstudie aus den USA ist interessant, dass EPIC verschiedene regulatorische Möglichkeiten beschreibt, wie die Federal Trade Commission gegen Samsung vorgehen kann. Wie in Kapitel 2 erläutert, sind auf Smart-TV-Geräte (mindestens) fünf Regelwerke anwendbar. Anders als die Beispiele aus den Niederlanden zeigt diese Fallstudie die Möglichkeit, mit dem Verbraucherschutz- – und insbesondere Jugendschutz- – sowie dem Datenschutz- und dem Telekommunikationsrecht gegen die mutmaßlich unzulässige Verarbeitung von (Sprachaufnahme-)

[109] Niederländische Datenschutzbehörde, Untersuchung über die Verarbeitung personenbezogener Daten bei Philips Smart TVs durch TP Vision Netherlands B.V., Bericht vom 2. Juli 2013.

[110] Bayerisches Landesamt für Datenschutzaufsicht, „Technische Prüfung SmartTV", Pressekonferenz vom 27. Februar 2015 https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

Daten vorzugehen. Ob die FTC hiergegen Klage erheben wird, steht nicht fest, doch es ist interessant, die verschiedenen Möglichkeiten zur Regulierung von Smart-TV-Geräten in den USA zu sehen.

## 3.3.1. *Electronic Privacy Information Center / Samsung*

Am 24. Februar 2015 reichte das Electronic Privacy Information Center (EPIC)[111] bei der US-amerikanischen Federal Trade Commission (FTC) eine Beschwerde gegen die Smart-TV-Geräte von Samsung ein.[112] Darin erklärt EPIC, die Geschäftspraktiken von Samsung hätten negative Auswirkungen auf die Privatsphäre der Verbraucher in den USA, da Samsung routinemäßig deren private Kommunikation in der Wohnung mithilfe der Sprachaufnahmefunktionen von Smart-TV-Geräten abfange und aufzeichne. Daher bittet EPIC die FTC, diesbezüglich tätig zu werden.

Diese Fallstudie analysiert zunächst den Sachverhalt, der den Hintergrund der Beschwerde von EPIC bildet. Im Anschluss daran wird auf den Rechtsrahmen eingegangen, der dieser Beschwerde gegen die mutmaßlich in die Privatsphäre eingreifenden Smart-TV-Geräte von Samsung zugrunde liegt. Der letzte Abschnitt untersucht mögliche Auswirkungen des Ersuchens von EPIC an die FTC.

### 3.3.1.1. Sachverhalt

Die Beschwerde von EPIC betrifft die Spracherkennungsmöglichkeiten der Smart-TV-Geräte von Samsung. Die „Smart Touch"-Fernbedienung von Samsung verfügt über ein eingebautes Mikrofon für Sprachaufnahmen. Wie bereits erläutert,[113] gehen die Fähigkeiten der Smart-TV-Geräte von Samsung über die von EPIC untersuchte Spracherkennungsfunktion hinaus. Die Funktionen Bewegungssteuerung, Gesichtserkennung und Kontoerstellung werden daher in dieser Fallstudie nicht behandelt.

Die Grundlage für die Aussage von EPIC, Samsung würde Privatgespräche in der Wohnung abfangen und aufzeichnen, findet sich in den früheren[114] wie auch in den aktuellen[115] Datenschutzrichtlinien von Samsung. EPIC nennt drei Abschnitte dieser Datenschutzrichtlinien, um auf die mutmaßlichen Verletzungen der Privatsphäre von Verbrauchern hinzuweisen.

Der erste und primäre Abschnitt, den EPIC anführt, ist der Text nach der Überschrift „Spracherkennung" in der früheren Datenschutzrichtlinie: *„Bitte beachten Sie: Sollten die von Ihnen gesprochenen Worte persönliche oder andere sensible Informationen enthalten, gehören diese Informationen zu den Daten, die durch Ihre Nutzung der Spracherkennung erfasst und an eine Drittpartei weitergeleitet werden."*[116] Sobald diese Spracherkennungsfunktion des Smart-TV-Geräts aktiviert wird, wird nach Angaben von EPIC alles, was ein Nutzer vor dem Gerät sagt, aufgezeichnet und über das Internet an eine Drittpartei weitergeleitet – unabhängig davon, ob es einen Bezug zur Erbringung des Dienstes hat. Die in der Datenschutzrichtlinie erwähnte „Drittpartei" wurde in der

[111] EPIC ist ein gemeinnütziges Forschungszentrum in Washington DC.

[112] EPIC, *In the matter of Samsung Electronics Co., Ltd., EPIC Complaint, Request for Investigation, Injunction and Other Relief*, 24. Februar 2015, https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

[113] Abschnitt 1.2.

[114] Siehe http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[115] Siehe http://www.samsung.com/uk/info/privacy-SmartTV.html.

[116] Supra Fußnote 114.

früheren Fassung dieser Richtlinie noch nicht genannt.[117] Später – nach negativen Medienberichten – erklärte Samsung, bei der „Drittpartei" handle es sich um die Spracherkennungsfirma Nuance Communications, Inc.[118]

Außerdem zitiert EPIC einen Abschnitt der aktuellen Datenschutzrichtlinien von Samsung: *„Bitte beachten Sie: Wenn Sie ein Video ansehen oder auf von einer Drittpartei bereitgestellte Applikationen oder Inhalte zugreifen, kann der betreffende Anbieter Informationen über Ihr Smart-TV-Gerät (z. B. dessen IP-Adresse und Gerätekennungen), die angeforderte Transaktion (z. B. Ihre Anforderung zum Kaufen oder Leihen des Videos) und Ihre Nutzung der Applikation oder des Dienstes sammeln oder empfangen. Samsung ist für die Datenschutz- oder Sicherheitspraktiken dieser Anbieter nicht verantwortlich. Sie sollten daher Vorsicht walten lassen und sich die Datenschutzerklärungen ansehen, die für die von Ihnen genutzten Websites und Dienste von Drittanbietern gelten."*[119] Aufgrund dieses Abschnitts erklärt EPIC, Samsung versuche, die Haftung für alle Datenschutz- oder Sicherheitspraktiken von Drittparteien auszuschließen, einschließlich der Datenschutz- oder Sicherheitspraktiken von Nuance.[120]

Drittens erwähnte EPIC, Samsung habe erklärt, dass es die Sprachkommunikation verschlüssele, die es an Nuance übertrage.[121] Die Informatiker Ken Munro und David Lodge hätten jedoch herausgefunden, dass Samsung nicht alle Sprachaufnahmen verschlüssele, die es aufzeichne und an Nuance übertrage.[122] Als Reaktion auf seine Recherchen habe Samsung später eingeräumt, dass das Unternehmen nicht alle Gespräche verschlüssele und die zur Verschlüsselung von Klartextübertragungen notwendige Software nicht eingesetzt habe.[123]

EPIC untermauert seine Beschwerde, indem es Zitate von Datenschutzexperten zitiert und Verbrauchererfahrungen sammelt. EPIC zufolge warnen Datenschutzexperten, die „Always-on"-Spracherkennungspraxis von Samsung sei für die Verbraucher irreführend, und wer von dieser Praxis erfahren habe, bezeichne sie als unlauter und irreführend.[124]

### 3.3.1.2. Rechtsrahmen

EPIC demonstriert die mutmaßliche Rechtswidrigkeit der Smart-TV-Geräte von Samsung – das oben erwähnte verbreitete Abfangen und Aufzeichnen privater Gespräche, das (teilweise) Fehlen einer Verschlüsselung und den Versuch, die Haftung auszuschließen, – durch Verweis auf mehrere US-Gesetze (Cable Act, Electronic Communications Privacy Act, Children's Online Privacy Protection Act und FTC Act). Der Kern der Beschwerde stützt sich auf den FTC Act und die entsprechenden Grundsatzerklärungen der FTC (Policy Statement on Deception und Policy Statement on Unfairness).

---

[117] Ibid.

[118] Ibid.

[119] Supra Fußnote 112, Abs. 24; Samsung Global Privacy Policy http://www.samsung.com/us/common/privacy.html.

[120] Supra Fußnote 112, Abs. 23.

[121] Ibid., Abs. 25; *„Samsung nimmt die Privatsphäre der Verbraucher sehr ernst, und der Datenschutz wird bei der Gestaltung unserer Produkte berücksichtigt. Wir nutzen dem Branchenstandard entsprechende Sicherheitsvorkehrungen und -praktiken, einschließlich Datenverschlüsselung, um die personenbezogenen Informationen der Verbraucher zu sichern und deren unbefugte Sammlung oder Nutzung zu verhindern."* http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[122] Supra Fußnote 112, Abs. 27; https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/.

[123] Ibid., Abs. 28 und 29; http://www.bbc.com/news/technology-31523497.

[124] Ibid., Abs. 30-57.

#### 3.3.1.2.1. Cable Communications Policy Act

Als erstes führt EPIC den Cable Communications Policy Act (CCPA) an,[125] der dem Schutz personenbezogener Informationen der Kunden von Kabelfernsehanbietern dient.

Die Bestimmung 47 U.S.C. 551 §631(b) CCPA verbiete die Sammlung personenbeziehbarer Informationen über einen Abonnenten ohne dessen vorherige schriftliche oder elektronische Einwilligung. 47 U.S.C. 551 § 631(c) untersagt darüber hinaus die Weitergabe personenbeziehbarer Informationen über einen Abonnenten[126] und verlange, dass Kabelanbieter alle erforderlichen Maßnahmen treffen, um den unbefugten Zugriff von Personen außer dem Abonnenten oder Kabelbetreiber zu verhindern – also auch den Zugriff der Spracherkennungsfirma Nuance.

Als Reaktion auf diese Anforderungen erklärt EPIC: *„Samsung holt keine schriftliche oder elektronische Einwilligung in die Aufzeichnung der privaten Gespräche von Menschen in ihrer Wohnung und in die Übertragung dieser Sprachaufnahmen an Nuance ein.“*[127] Darüber hinaus erklärt EPIC, Samsung treffe *„keine erforderlichen Maßnahmen, um den unbefugten Zugriff auf Abonnenteninformationen zu verhindern,“* und sammle *„bewusst zu viele Informationen, die von Kabelkunden bereitgestellt werden“*.[128] EPIC geht nicht konkret darauf ein, in welcher Weise das Sammeln von zu vielen Informationen stattfindet.

#### 3.3.1.2.2. Electronic Communications Privacy Act

Das zweite von EPIC angeführte Gesetz ist der Electronic Communications Privacy Act (ECPA).[129] Der ECPA schütze die kabelgebundene, mündliche und elektronische Kommunikation und gilt für E-Mails, Telefongespräche und elektronisch gespeicherte Daten.

18 U.S.C. § 2511(1) EPCA bestimme, dass jede Person,[130] die *„eine kabelgebundene, mündliche oder elektronische Kommunikation vorsätzlich abfängt, abzufangen versucht oder von einer anderen Person abfangen lässt“*[131] oder *„den Inhalt einer kabelgebundenen, mündlichen oder elektronischen Kommunikation vorsätzlich an eine andere Person weitergibt oder weiterzugeben versucht, wenn sie weiß oder wissen müsste, dass die Information durch das Abfangen einer kabelgebundenen, mündlichen oder elektronischen Kommunikation unter Verstoß gegen die vorliegende Ziffer erlangt wurde“*[132], gegen den EPCA verstößt.

EPIC erklärt, Samsung verstoße gegen den ECPA, indem es die private Kommunikation in der Wohnung abfange und aufzeichne,[133] da Samsung vorsätzlich Gespräche abfange und diese Sprachaufnahmen an Nuance weitergebe, wobei *es „keine Ausnahme einem Unternehmen erlaubt, heimlich die private Kommunikation in der Wohnung aufzuzeichnen“.*[134]

---

[125] Cable Communications Policy Act of 1984 (CCPA), 47 U.S.C. §521-573.

[126] Ausnahmen von dem Weitergabeverbot gemäß 47 U.S.C. 551 § 631(2), staatliche Ersuchen aufgrund eines Gerichtsbeschlusses oder zur Erbringung von Kabeldiensten notwendige Weitergaben, seien in dem zugrunde liegenden Fall nicht anwendbar.

[127] Supra Fußnote 112, Abs. 60.

[128] Ibid., Abs. 61.

[129] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-2522.

[130] Die Definition des Begriffs „Person“ schließe auch Körperschaften ein; 18 U.S.C. § 2510(6).

[131] 18 U.S.C. § 2511(1)(a).

[132] 18 U.S.C. § 2511(1)(c).

[133] Supra Fußnote 112, Abs. 71.

[134] Ibid., Abs. 70.

#### 3.3.1.2.3. Children's Online Privacy Protection Act

EPIC verweist weiterhin auf den Children's Online Privacy Protection Act (COPPA)[135], um die Rechtmäßigkeit von FTC-Maßnahmen zu belegen. Ähnlich wie beim FTC Act sei die FTC auch zur Durchsetzung des COPPA befugt.

Dieses Gesetz solle die Privatsphäre von Kindern unter 13 Jahren schützen, indem es die Sammlung personenbezogener Informationen von Kindern durch die Betreiber von Websites und Onlinediensten regelt.

Die Anforderungen des COPPA gälten für Betreiber von Onlinediensten, Websites und Apps, die sich an Kinder unter 13 Jahren richten,[136] – und für Betreiber von Onlinediensten, Websites und Apps, die eine allgemeine Zielgruppe bedienen, die weiß, dass sie personenbezogene Informationen von einem Kind sammeln oder speichern.[137] Damit Betreiber, die zu diesem Kreis gehören, nicht gegen das Gesetz verstoßen, müssten sie:

a) auf der Website oder in dem Onlinedienst darauf hinweisen, welche Informationen sie über Kinder sammeln, wie sie diese Informationen nutzen und welche Weitergabepraktiken für diese Informationen gelten;[138]
b) eine überprüfbare elterliche Einwilligung einholen, bevor sie personenbezogene Informationen von Kindern sammeln, nutzen und/oder weitergeben;[139]
c) angemessene Mittel bereitstellen, mit denen Eltern die zu einem Kind gesammelten personenbezogenen Informationen prüfen und die Erlaubnis zu deren weiterer Nutzung oder Aufbewahrung verweigern können;[140]
d) die Teilnahme eines Kindes an einem Spiel, das Angebot eines Preises oder eine andere Aktivität nicht von der Preisgabe von Informationen abhängig machen;[141]
e) angemessene Verfahren einführen und aufrechterhalten, um die Vertraulichkeit, Sicherheit und Integrität der über Kinder gesammelten personenbezogenen Informationen zu schützen.[142]

EPIC versucht zunächst zu beweisen, dass Samsung als Anbieter von Onlinediensten zu betrachten sei, der die obigen Anforderungen erfüllen müsse. Dazu verweist EPIC auf die ergänzende Smart-TV-Datenschutzrichtlinie – die Datenschutzrichtlinie speziell für die Smart-TV-Geräte von Samsung. In dieser ergänzenden Datenschutzrichtlinie heißt es: *„Smart-TV-Dienste können Bildungsvideos und andere für Kinder geeignete Inhalte zur Verfügung stellen, aber wir sammeln personenbezogene Informationen von Kindern unter 13 Jahren nicht wissentlich ohne elterliche Einwilligung, außer wenn dies gesetzlich zulässig ist."*[143] Nach Auffassung von EPIC stellt sich Samsung daher als Onlinedienstebetreiber mit allgemeiner Zielgruppe vor, der den COPPA einhält.

Allerdings, so EPIC, zielt Samsung mit einigen Funktionen von Smart-TV-Geräten speziell auf junge Kinder; Samsung ermutige Eltern, ihre Kinder mit dem Smart-TV-Gerät von Samsung interagieren zu lassen, und das Unternehmen habe bestätigt, dass Smart-TV-Geräte häufig von

---

[135] Children's Online Privacy Act of 1998 (COPPA), 15 U.S.C. § 6501-6505.

[136] Title 16 of the Code of Federal Regulation (16 C.F.R.) §312.3.

[137] 16 C.F.R. §312.3.

[138] 16 C.F.R. §312.4(b).

[139] 16 C.F.R. §312.5.

[140] 16 C.F.R. §312.6.

[141] 16 C.F.R. §312.7.

[142] 16 C.F.R. §312.8.

[143] Supra Fußnote 112, Abs. 87; Samsung Global Privacy Policy SmartTV Supplement, https://www.samsung.com/uk/info/privacy-SmartTV.html?CID=AFL-hq-mul-0813-11000170.

Familien mit Kindern unter 13 Jahren gekauft würden.[144] Aufgrund dieser Informationen kommt EPIC zu dem Schluss, dass Samsung gegen den COPPA verstoße, indem es nicht, wie gemäß 16 C.F.R. §312.3 erforderlich, die Eltern um die Erlaubnis bitte, bevor es die Stimmen von Kindern aufzeichne, speichere und an eine Drittpartei übertrage.

#### 3.3.1.2.4. Federal Trade Commission Act

Gemäß Abschnitt 5 des Federal Trade Commission Act ist die FTC berechtigt, unlautere und irreführende Handlungen und Praktiken zu verhindern.[145] Dieses Gesetz vermittelt der FTC keine spezifische Befugnis zum Schutz der Privatsphäre, doch wird es so ausgelegt, dass sie bestimmte Eingriffe in die Privatsphäre auf der Basis unlauterer und irreführender Handlungen und Praktiken verhindern darf.[146]

EPIC beschreibt sowohl die Täuschung durch die Smart-TV-Geräte als auch deren Unlauterkeit und analysiert den FTC Act in Verbindung mit den Policy Statements der FTC zu Täuschung[147] und Unlauterkeit.[148]

Unlauterkeit

Handelspraktiken gälten als unlauter, wenn sie *„dem Verbraucher einen erheblichen Schaden zufügen oder zufügen können, der von ihm selbst nicht mit vertretbarem Aufwand zu vermeiden ist und nicht durch entsprechende Vorteile für den Verbraucher oder den Wettbewerb aufgewogen wird.“*[149]

Zum einen sei ein „erheblicher“ Schaden in diesem Zusammenhang zumeist ein finanzieller Schaden, er könne aber auch unvertretbare Gesundheits- und Sicherheitsrisiken einschließen. Emotionale Schäden und andere „subjektivere Arten von Schäden“ begründeten im Allgemeinen keine Unlauterkeit der betreffenden Praktiken.[150]

Hinsichtlich des zweiten Elements, nämlich dass der Schaden nicht durch entsprechende Vorteile für den Verbraucher oder den Wettbewerb aufgewogen werden dürfe, untersucht die FTC, ob eine Praxis „in ihren Nettoauswirkungen schädlich“ sei.[151]

Drittens werde die FTC prüfen, ob es sich um einen Schaden handele, der nicht mit vertretbarem Aufwand zu vermeiden gewesen wäre.

EPIC erklärt, das Element des „erheblichen Schadens“ sei gegeben, weil Samsung keine Verantwortung für die Privatsphäre und Sicherheit der aufgezeichneten Gespräche der Nutzer übernehme und damit *„in unvertretbarer Weise ein Hindernis für die Entscheidungsfreiheit der Verbraucher schafft oder ausnutzt.“*[152] Um diesen Schaden festzustellen, rekapituliert EPIC die Versuche von Samsung, die Haftung für die Datenschutz- und Sicherheitspraktiken von Unternehmen auszuschließen, an die es die von Verbrauchern gesammelten Nutzerdaten übertrage,

---

[144] Supra Fußnote 112, Abs. 89-91.

[145] 15 U.S.C. § 45(a)(2).

[146] Electronic Privacy Information Center, *„Federal Trade Commission: Overview of Statutory Authority to Remedy Privacy Infringements“*, https://epic.org/privacy/internet/ftc/Authority.html.

[147] Federal Trade Commission, FTC Policy Statement on Deception, 1983, https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[148] Federal Trade Commission, FTC Policy Statement on Unfairness, 1980, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[149] 15 U.S.C. § 45 (n).

[150] Supra Fußnote 148.

[151] Ibid.

[152] Supra Fußnote 112, Abs. 107.

und die Tatsache, dass Samsung die privaten Gespräche von Smart-TV-Nutzern an das Drittunternehmen Nuance übermittle.[153] Zudem verweist EPIC auf die Datenschutzrichtlinie von Samsung, die den Verbrauchern nicht den Namen des Drittunternehmens genannt habe. Samsung habe die Verbraucher über den Einsatz von Verschlüsselung zur Übermittlung aufgezeichneter Gespräche weiterhin irregeführt, so EPIC.

Zweitens würden die unzureichenden Schutzmaßnahmen nicht durch entsprechende Vorteile für den Verbraucher oder den Wettbewerb aufgewogen.[154]

Abschließend erklärt EPIC, Nutzer der Smart-TV-Geräte von Samsung hätten nicht vernünftigerweise damit rechnen können, dass durch die Nutzung des Geräts ihre privaten Gespräche, manchmal unverschlüsselt, an Nuance übermittelt würden.[155] Daher, so EPIC, stellten die unzureichenden Angaben von Samsung unlautere Handlungen oder Praktiken dar.[156]

Täuschung

Gemäß der FTC Deception Policy ist eine Handlung irreführend, wenn sie *„mit einer Darstellung, Unterlassung oder Praxis verbunden ist, die den unter den gegebenen Umständen vernünftig handelnden Verbraucher zu dessen Nachteil irreführen kann.“*[157] Die Täuschung bestehe somit aus drei Elementen.

Als erstes müsse die Darstellung, Unterlassung oder Praxis den Verbraucher irreführen können. Zu den als irreführend eingestuften Praktiken zählten falsche schriftliche Darstellungen, irreführende Preisangaben und die Nichterbringung zugesagter Dienste.[158] Dabei sei eine Handlung oder Praxis nicht nur dann irreführend, wenn sie den Verbraucher tatsächlich irregeführt habe, sondern bereits dann, wenn eine Irreführung wahrscheinlich sei.[159]

Zweitens müsse die Handlung oder Praxis aus der Sicht des unter den gegebenen Umständen vernünftig handelnden Verbrauchers als irreführend betrachtet werden. Die FTC prüfe die betreffende Handlung oder Praxis in ihrer Gesamtheit.[160]

Drittens müsse die Handlung oder Praxis „wesentlich“ sein, d. h. die Handlung oder Praxis müsse geeignet sein, das Verhalten oder die Entscheidung des Verbrauchers in Bezug auf ein Produkt oder eine Dienstleistung zu beeinflussen.[161] Die FTC werde daher prüfen, ob Verbraucher ohne die Täuschung ein anderes Produkt gewählt hätten.

EPIC erklärte, Samsung habe getäuscht, indem es nicht offengelegt habe, dass es mit seinen Smart-TV-Geräten private Gespräche aufzeichne und übermittle. Die Verbraucher seien irregeführt worden, weil sie nicht gewusst hätten, dass ihre privaten Gespräche aufgezeichnet und an eine Drittpartei übermittelt würden. Außerdem habe Samsung ihnen versichert, dass alle aufgezeichneten Übertragungen verschlüsselt würden, obwohl einige Sprachaufzeichnungen in Wirklichkeit unverschlüsselt übermittelt worden seien. Als Nutzer die Wahrheit über diese Datensammlung und -übertragung herausgefunden hätten, hätten sie Einwände erhoben und sie als rechtswidrige Praxis eingestuft. Dies deute darauf hin, dass diese falsche Darstellung für die Verbraucher „wesentlich“ gewesen sei. EPIC gelangt zu dem Schluss, dass die unzureichenden

[153] Ibid., Abs. 103.

[154] Ibid., Abs. 109.

[155] Ibid., Abs. 108.

[156] Ibid., Abs. 110.

[157] Supra Fußnote 147.

[158] Ibid.

[159] Ibid.

[160] Ibid.

[161] Ibid.

Angaben von Samsung trügerische Handlungen oder Praktiken darstellten, die nach 15 U.S.C. § 45(a) unzulässig seien.[162]

### 3.3.1.3. Wahrscheinliche Folgen

Die FTC ist bis heute nicht formal gegen Samsung vorgegangen. Die Reaktion der FTC in diesem Fall könnte weitreichende Folgen haben, weil interaktive Verbrauchergeräte generell stark auf dem Vormarsch sind und eine einschlägige Rechtsprechung sowohl in den USA als auch in Europa fehlt. Wie auch immer die Sache ausgehen mag – diese Fallstudie zeigt interessante Wahlmöglichkeiten auf, die bei der Regulierung der Auswirkungen von Smart-TV-Geräten auf den Datenschutz zur Verfügung stehen. Die rechtlichen Bestimmungen, auf die sich die Beschwerde von EPIC stützt, zeigen mögliche Reaktionen auf die Ausbreitung von Smart-TV-Geräten: die Stärkung des Verbraucherschutzes durch Verbesserung der Transparenz in den Datenschutzrichtlinien oder die Durchsetzung spezifischer staatlicher Gesetze wie CCPA und ECPA, die konkreter auf rechtswidrige Übertragungen personenbezogener Daten eingehen.

Der Ausgang lässt sich kaum vorhersagen, doch die FTC-Vorsitzende Edith Ramirez sprach vor Kurzem das spezifische Problem an, dass Endgeräte Verbraucher ausspionieren, und verwies dabei konkret auf Smart-TV-Geräte. Ramirez erklärte: *„Vernünftige Grenzen für Datensammlung und Datenspeicherung sind die erste Verteidigungslinie für die Privatsphäre der Verbraucher."*[163] Aufgrund dieser Aussage könnte man vermuten, dass sich die FTC mit den Auswirkungen von Smart-TV-Geräten auf die Privatsphäre befassen wird.

EPIC rief die FTC und das Justizministerium vor Kurzem auf, eine umfassende Untersuchung durchzuführen, um festzustellen, ob „Always-on"-Verbrauchergeräte gegen den Wiretap Act, einzelstaatliche Datenschutzgesetze oder den FTC Act verstoßen.[164] EPIC wandte sich nochmals mit dem Ziel an die FTC, angesichts interaktiver Verbrauchergeräte die Privatsphäre der Verbraucher zu schützen.

[162] Supra Fußnote 112, Abs. 102.

[163] Privacy and the Internet of Things: Navigating Policy Issues – *Opening Remarks of FTC Chairwoman Edith Ramirez,* International Consumer Electronics Show, Las Vegas, 6. Januar 2015.

[164] Siehe https://epic.org/2015/07/epic-urges-investigation-of-al.html.

# 4. Die Datenschutzgrundverordnung

Dieses Kapitel gibt im Wesentlichen eine Vorschau auf die kommende Datenschutzgrundverordnung (DSGV oder „die Verordnung“). Das Gesetzgebungsverfahren für die neue DSGV ist noch nicht abgeschlossen, befindet sich aber in der Endphase. Am 24. Juni 2015 haben das Europäische Parlament, der Rat und die Europäische Kommission Verhandlungen im Rahmen des Mitentscheidungsverfahrens über die vorgeschlagene DSGV aufgenommen. Grundlage dieser Verhandlungen sind der Vorschlag der Kommission vom Januar 2012, die legislative Entschließung des Parlaments vom 12. März 2014 sowie die am 15. Juni 2015 angenommen Allgemeine Ausrichtung des Rates. [165] In diesem Teil der Studie werden die wichtigsten Unterschiede zwischen der derzeitigen DSR und der DSGV im Hinblick auf die Anwendbarkeit auf Smart-TV-Geräte dargestellt.[166] Die endgültige Fassung der DSGV wird voraussichtlich im Dezember 2015 vorliegen; die offizielle Annahme könnte dann Anfang 2016 erfolgen.[167]

## 4.1. Smart TV und die Datenschutzgrundverordnung

Nachdem in Kapitel I beschrieben wurde, was unter Smart-TV-Geräten zu verstehen ist und welche Daten diese Geräte erfassen können, widmet sich dieses Kapitel der Frage, ob diese Daten im Sinne der DSGV als personenbezogene Daten zu bewerten sind.

### 4.1.1. Definitionen

Hinsichtlich Definitionen und Anwendungsbereich der Verordnung bestehen enge Verbindungen zur DSR. Der Anwendungsbereich ist in Artikel 2 (*Räumlicher Anwendungsbereich*) beschrieben, in dem festgelegt ist, dass die Verordnung ausschließlich für die Verarbeitung personenbezogener Daten Anwendung findet. Damit werden gleichzeitig die beiden Schlüsselkonzepte des Datenschutzes

[165] Vorschlag für Verordnung des Europaïschen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM(2012)11 endgültig, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf; Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//de; Vorbereitung einer allgemeinen Ausrichtung, Dokuments des Rates 9565/15, 11. Juni 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

[166] Verweis auf Dokument des Rates 10391/15 vom 8. Juli 2015: http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.

[167] Der Europäische Datenschutzbeauftragte, Empfehlungen des EDSB zu den Optionen der EU für die Datenschutzreform, 2015/C301/01, 12. September 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_summary_DE.pdf.

eingeführt: *Verarbeitung* und *personenbezogene Daten*. In Artikel 4 der Verordnung (*Begriffsbestimmungen*) werden diese Begriffe erläutert.

Der erste Begriff *Verarbeitung* ist breit definiert, so dass fast jeder Vorgang eine Form der Verarbeitung darstellen kann. Trotz der Änderungsvorschläge des Europäischen Parlaments zur Definition dieses Begriffs[168] wird Artikel 2 DSGV nicht so weit gefasst, dass auch „jede Art der Verarbeitung" mit eingeschlossen wäre; und deshalb gilt die Verordnung nach wie vor für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten.[169]

Der weit gefasste Anwendungsbereich der DSR und der Verordnung zeigt sich u.a. im *Bodil Lindqvist*-Urteil,[170] bei dem das Konzept der Verarbeitung für Zwecke der Richtlinie 95/46 geprüft wurde. Die für diese Bestimmung angewandte Begründung kann auf die Verordnung übertragen werden, weil die jeweiligen Definitionen identisch sind. In diesem Fall kam der EuGH zu dem Ergebnis, dass die Veröffentlichung der Telefonnummern und der Freizeitbeschäftigung verschiedener Personen im Internet einen Verarbeitungsvorgang darstellt. Weiter von Bedeutung ist die Tatsache, dass diese Verarbeitung nicht voll automatisch erfolgte. Damit ist anerkannt worden, dass teilweise automatisierte Verarbeitung in den Anwendungsbereich der Verordnung fällt.

Auch der Begriff „personenbezogene Daten" hat sich im Verhältnis zur DSR nicht verändert. Personenbezogene Daten sind definiert als sämtliche Informationen über eine bestimmte oder bestimmbare natürliche Person.[171] Damit sind vier Aspekte für die Anwendung dieses Konzepts von Bedeutung. Laut der Artikel-29-Datenschutzgruppe sind diese Aspekte bzw. „Bausteine": 1) alle Informationen; 2) über; 3) eine bestimmte oder bestimmbare; 4) natürliche Person.[172]

#### 4.1.1.1. „Alle Informationen"

Die Verwendung der Worte „alle Informationen" spiegelt die Absicht des EU-Gesetzgebers wider, den Begriff personenbezogene Daten weit zu fassen. In den Stellungnahmen der Artikel-29-Datenschutzgruppe wird davon ausgegangen, dass sowohl objektive aber auch subjektive Informationen unter „alle Informationen" fallen. Dabei brauchen die Informationen nicht unbedingt wahr zu sein.[173] Ebenso wenig kommt es darauf an, ob sich die Informationen auf das Privat- oder Arbeitsleben einer Person beziehen. In der Rechtssache *Volker und Markus Schecke GbR und Hartmut Eifert gegen das Land Hessen*[174] hat der EuGH erkannt, dass berufliche Tätigkeiten auch in den Bereich der Privatsphäre fallen können. Diese Position spiegelt sich in der ständigen Rechtsprechung des EGMR, der in seinem Urteil in der Rechtssache *Amann* zu einer ähnlichen Bewertung kommt.[175] Auch die Art, wie die Daten gespeichert werden, kann ein Unterscheidungsmerkmal sein. Digitale Dateien, gedruckte Unterlagen und Tonbänder können alle personenbezogene Daten enthalten.

---

[168] Artikel 2 DSGV, siehe Dokument des Rates 10391/15 unter „EP Position/First Reading", supra Fußnote 166.

[169] „Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen" Artikel 2 (1) DSGV.

[170] CJEU 06-09-2003 C-101/01, (Bodil Lindqvist),

http://curia.europa.eu/juris/celex.jsf?celex=62001CJ0101&lang1=en&type=TXT&ancre=.

[171] Artikel 4 (1) DSGV: Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[172] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", supra Fußnote 47.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.

[173] Ibid.

[174] EuGH 09-11-2010, C-92/09 und C-93/09, (Volker und Markus Schecke GbR und Hartmut Eifert gegen das Land Hessen), http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62009CJ0092.

[175] EGMR 16-02-2000, Nr. 27798/95, (Amann gegen die Schweiz), supra Fußnote 71.

### 4.1.1.2. „Über“

Dieser Baustein scheint vielleicht auf den ersten Blick unproblematisch. Denn die Daten müssen sich auf die eine oder andere Art auf eine bestimmte Person „beziehen“, um als personenbezogene Daten betrachtet werden zu können. Doch die Wirklichkeit ist etwas nuancierter. Die Artikel-29-Datenschutzgruppe macht die Worte „beziehen“ bzw. „Beziehung“ an drei weiteren Größen fest: einem „Inhaltselement“, einem „Zweckelement“ oder einem „Ergebniselement“. Diese Elemente sind nicht kumulierbar.

Kurze Erläuterung: Daten deren *Inhalte* Auswirkungen auf die betroffene Person haben, *beziehen* sich auf diese Person. Und Daten beziehen sich auf eine Person, wenn sie für einen *Zweck* verwendet werden können, der z.B. darin besteht, das Verhalten einer Person zu beeinflussen. Schließlich können Daten, die verwendet werden können, um ein bestimmtes *Ergebnis* zu erreichen, das sich auf die Rechte und Interessen einer bestimmten Person auswirkt, als Daten bezeichnet werden, die sich auf diese Person beziehen.

### 4.1.1.3. „Eine bestimmte oder bestimmbare Person“

Der grundlegende Unterschied zwischen „bestimmt“ und „bestimmbar“ liegt darin, dass eine bestimmbare Person *noch nicht* identifiziert worden ist.[176] In Artikel 4 (1) der Verordnung wird auf die Möglichkeit verwiesen, eine Person direkt oder indirekt zu identifizieren.[177] Eine direkte Identifizierung kann z.B. durch den Erwerb des Namens einer Person erfolgen. Eine Identifizierung über persönliche Nummern wie die Reisepassnummer oder die Sozialversicherungsnummer ist eine Form der indirekten Identifizierung, da zusätzliche Daten oder Mittel notwendig sind, um die Identität der Person zu bestimmen. Ob eine Identifizierung unter Verwendung verschiedener „Identifizierungsmerkmale“ eine Möglichkeit ist, hängt von den jeweiligen Umständen ab. Eine indirekte Identifizierung kann als ein Identifizierungsprozess mittels einer Reihe von Elementen betrachtet werden, die es ermöglichen, eine Person in einer größeren Personengruppe zu unterscheiden. Dies führt zu der Frage, ab wann eine indirekte Identifizierung vorliegt. In anderen Worten handelt es sich hier um eine Situation, in der eine Partei ausreichend Gründe oder Möglichkeiten hat, die Person zu identifizieren. Die Verordnung geht in Erwägungsgrund 23 auf diese Frage ein und sieht dort vor, dass bei der Feststellung, ob eine Person bestimmbar ist, alle Mittel zu berücksichtigen sind, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung oder Unterscheidung der Person genutzt werden.[178] Bei der Prüfung der Vertretbarkeit sind alle relevanten Faktoren zu berücksichtigen wie der für die Identifizierung notwendige Aufwand an Zeit und Arbeit. Ferner sollten die neuesten technischen Entwicklungen und Fortschritte berücksichtigt werden.

Der Erwägungsgrund unterscheidet zwischen personenbezogenen und nichtpersonenbezogenen Daten.[179] Anonyme Daten und Daten, die nicht bis zu einer bestimmten Person zurückverfolgt werden können (z.B. nach Aggregation der Daten), gelten als anonyme Daten und werden nicht mehr als personenbezogen bewertet. Denn eine Verbindung der Daten mit einzelnen Personen ist nicht mehr möglich.

---

[176] Supra Fußnote 47.

[177] Artikel 4(1) DSGV, siehe Dokument des Rates 10391/15 unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[178] Ibid.

[179] Ibid.

#### 4.1.1.4. „Natürliche Person“

Der letzte Baustein beinhaltet, dass die Bestimmungen des Datenschutzes grundsätzlich für alle lebenden Personen gelten.[180] Es gibt einige wenige Ausnahmen, doch die sind für Zwecke dieser Studie von geringer Bedeutung.

#### 4.1.1.5. Besondere Kategorien personenbezogener Daten

Die vorgenannten Bausteine ergeben in Verbindung miteinander einen Bezugsrahmen, der für die Bestimmung, ob bestimmte Informationen als personenbezogene Daten zu betrachten sind, herangezogen werden kann. Wie die DSR unterscheidet die Verordnung weiter zwischen „normalen“ und besonderen Kategorien von Daten. Artikel 9 (Verarbeitung besonderer Datenkategorien) sieht vor, dass folgende Daten in eine besondere Kategorie fallen: Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft hervorgehen sowie die Verarbeitung genetischer Daten oder Daten über die Gesundheit oder das Sexualleben.[181] Im Text des Europäischen Parlaments zur ersten Lesung sind auch biometrische Daten, Daten über Verwaltungssanktionen, strafrechtliche Verurteilungen, mutmaßliche Straftaten und sonstige Verurteilungen enthalten.[182] Auch diese Unterkategorie ist eindeutig weit gefasst. Für diese besonderen Kategorien von Daten gelten strengere Regeln, auf die unten noch eingegangen wird. Hier soll der Hinweis genügen, dass es diese besondere Kategorie gibt.

#### 4.1.1.6. Räumlicher Anwendungsbereich

Neben dem oben beschriebenen sachlichen Anwendungsbereich der Verordnung ist in Artikel 3 (*Räumlicher Anwendungsbereich*) eine (extra-) territoriale Anwendbarkeit vorgesehen.[183] Im ersten Absatz wird darauf verwiesen, dass die Verordnung für die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union gilt, unabhängig davon, ob die Verarbeitung in oder außerhalb der Union stattfindet. Neu hinzugekommen ist Absatz 2 der Verordnung, der besagt, dass die Verordnung auch dann gilt, wenn der Auftragsverarbeiter nicht in der EU ansässig ist und die Verarbeitungstätigkeiten sich beziehen auf a) ein Angebot von Gütern oder Dienstleistungen - unabhängig davon, ob dies Zahlungen seitens der betroffenen Person voraussetzt - an betroffene Personen in der EU; oder b) die Überwachung dieser betroffenen Personen, soweit sich dies auf ihr Verhalten in der EU bezieht. Darin spiegelt sich die Absicht des Gesetzgebers wider, den Anwendungsbereich der Verordnung im Vergleich zur Richtlinie zu vergrößern.

[180] Supra Fußnote 47.

[181] Dokument des Rates 10319/15, supra Fußnote 166.

[182] Der genaue Wortlaut dieses Artikels ist noch umstritten. Siehe Dokument des Rates 10391/15 unter EP Postion/First Reading, supra Fußnote 166.

[183] Dokument des Rates 10391/15, supra Fußnote 166.

## 4.1.2. Anwendung

Der oben beschriebene Anwendungsbereich der Verordnung kann auf Smart-TV-Geräte - wie in Kapitel I definiert - bezogen werden. Soweit die Daten keine personenbezogenen Daten im Sinne der Verordnung sind, verlieren sämtliche weiteren Bestimmungen der Richtlinie ihre Bedeutung. Die verschiedenen in Kapitel I beschriebenen Funktionalitäten von Smart-TV-Geräten werden nun hinsichtlich ihrer rechtlichen Auswirkungen untersucht.

### 4.1.2.1. Spracherkennung

Oben wurde festgestellt, dass Smart-TV-Geräte in der Lage sind, Geräusche in der Nähe des Geräts aufzuzeichnen und Sprachmuster zu erkennen, die Befehle an das Gerät darstellen können. Hier stellt sich die Frage, ob bei dieser Funktion personenbezogene Daten verarbeitet werden. Die Antwort kann je nach Szenario unterschiedlich ausfallen.

Zunächst ist zu prüfen, welche Gespräche bzw. Gesprächsinhalte möglicherweise aufgezeichnet werden können. Da das Gerät in der Regel an einer zentralen Stelle im Haushalt steht, ist es wahrscheinlich, dass ein beträchtlicher Umfang der Gespräche erfasst wird. Der Inhalt dieser Gespräche ist natürlich immer unterschiedlich, und die Gespräche dürften eine unbegrenzte Anzahl von Wortkombinationen aufweisen. Unter diesen Worten sind zweifellos Namen, Ortsnamen und andere Angaben, die zu einer Identifizierung herangezogen werden können. Dazu gehört auch ein gewisser Anteil von „Schnee“, d.h. Informationen, die nicht von Belang sind oder keine Angaben enthalten, die eine Identifizierung ermöglichen.

Mit Blick auf die in der Verordnung genannten Kriterien ist zu beachten, dass der Begriff „personenbezogene Daten“ als „alle Informationen“ bezüglich einer natürlichen Person definiert ist. Analog dazu hat der niederländische Oberste Gerichtshof in der Rechtssache *Dexia*[184] festgestellt, dass aufgezeichnete Telefongespräche unter bestimmten Umständen als personenbezogene Daten bewertet werden können. Ferner wurde oben dargestellt, dass es relativ einfach ist, eine Person unmittelbar zu identifizieren, sofern ausreichend Identifikationsmerkmale erfasst werden können. Da Smart-TV-Geräte nicht unterscheiden, welche Geräusche erfasst werden und welche nicht - letztlich müssen alle Geräusche gefiltert werden, um Sprachbefehle zu erkennen -, ist die Schlussfolgerung zulässig, dass die in bewohnten Räumen erfassten Geräusche als personenbezogene Daten zu betrachten sind. Es bleibt die Frage, ob die Aufzeichnung auch einen Vorgang der Verarbeitung darstellt. Nach Artikel 4 (3) der Verordnung zählen das Erheben, das Erfassen, das Speichern, die Verwendung und die Übermittlung von Informationen zur Verarbeitung personenbezogener Daten. Dabei ist unerheblich, ob diese Vorgänge automatisch ablaufen oder nicht. Zusammenfassend lässt sich feststellen, dass die Erfassung von Inhalten von Gesprächen für die Zwecke der Verordnung eine Form der Verarbeitung personenbezogener Daten darstellt. Zu dieser Art der Verarbeitung können auch die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten gehören.

[184] HR 29-06-2007, ECLI:NL:HR:2007:AZ4664 (Dexia), para. 3.8 ff., http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2007:AZ4664.

### 4.1.2.2. Bewegungssteuerung und Gesichtserkennung

In Kapitel I wurde erläutert, dass Smart-TV-Geräte Bilder erfassen sowie Gesichter erkennen können. Nach der Feststellung, dass das Erfassen von Geräuschen unter den Anwendungsbereich der Verordnung fällt, stellt sich dieselbe Frage im Hinblick auf die Erfassung von Bildern.

Im Falle von Bildern muss nuancierter vorgegangen werden als bei der Analyse von Geräuschen. Anhand von Fotografien ist eine unmittelbare Identifizierung von Personen möglich. Portraitfotos gelten im Allgemeinen als sensible Daten, da sie Merkmale enthalten, die z.B. auf die ethnische Zugehörigkeit schließen lassen.

Die Verordnung kommt zu keinem anderen Ergebnis. Bilder von Personen sind letztlich Informationen über eine bestimmte oder bestimmbare natürliche Person. In den vorausgegangenen Ausführungen über die Erfassung von Geräuschen wurde die Tatsache nicht berücksichtigt, dass dabei *jeder* in der Nähe des Geräts erfasst werden kann. Hinzu kommt die Möglichkeit, dass die erfassten Bilder und Töne sich auf Minderjährige oder Besucher des Haushalts beziehen und nicht auf die normalen/registrierten Nutzer. In diesen Fällen würden sich aufgrund der besonderen Stellung von Minderjährigen und Besuchern besondere Rechtssituationen ergeben.

Wie bei Geräuschen stellt die Erfassung dieser Informationen einen Vorgang der Verarbeitung dar. Daraus lässt sich schließen, dass Bewegungssteuerung und Gesichtserkennung in den Anwendungsbereich der Verordnung fallen.

### 4.1.2.3. Erstellen eines Kontos

Diese Datenkategorie stellt eine Restgröße dar, zu der sämtliche Daten zählen, die nicht im Zuge einer Erfassung von Bildern oder Geräuschen/Tönen anfallen. Das sollte jedoch nicht den Eindruck erwecken, dass diese Kategorie weniger wichtig ist. Ganz im Gegenteil: Für Zwecke dieser Studie sind folgende Aspekte von großer Bedeutung.

Als erstes wird auf die Informationen, die mit einem Nutzerkonto in Zusammenhang stehen, eingegangen, auch wenn zugestanden werden muss, dass viele Nutzer ein solches Konto nicht verwenden werden. Dasselbe dürfte in geringerem Umfang auch für Spracherkennung und Bewegungsteuerung zutreffen. Doch in diese Restkategorie fallen auch Daten, die für jeden Nutzer wichtig sind - und deshalb für diese Studie von großer Bedeutung.

Das Anlegen eines Kontos erfordert die Eingabe von Informationen wie Name, E-Mail-Adresse, Geburtsdatum und Postleitzahl. Der eigene Name ist selbstverständlich als personenbezogene Information zu betrachten. Obwohl die anderen Daten an sich nicht unbedingt als personenbezogene Daten zu bewerten sind, können sie in Verbindung miteinander zur Identifizierung von Personen verwendet werden. Die Informationen über ein Konto sind deshalb ohne Frage eine Art personenbezogener Daten.

Im Folgenden wird der Fall erörtert, in dem sich die Nutzer entscheiden, kein Konto einzurichten. Auch nach dem Wirbel um die Nutzungsbedingungen von Smart-TV-Geräten von Samsung ist der High-Tech-Riese nicht zur Ruhe gekommen. Kurz danach gab es einen Bericht, in dem Samsung vorgeworfen wurde, Werbung in Inhalte zu platzieren, auf die die Nutzer über ihr Heimnetzwerk zugreifen.[185] Dabei handelte es sich um Inhalte, die weder heruntergeladen noch gestreamt wurden, sondern um Inhalte, die von den Nutzern selbständig erworben worden waren. Samsung reagierte bald mit einer offiziellen Entschuldigung und ließ verlauten, dass es sich bei diesem Vorfall um einen Fehler handle. Auf jeden Fall wird hier deutlich, dass das Einblenden von

[185] Roettgers J., *Samsung TVs start inserting ads into your movies*, 10. Februar 2015, https://gigaom.com/2015/02/10/samsung-tvs-start-inserting-ads-into-your-movies/.

Werbung in lokal gespeicherte Inhalte zumindest technisch möglich ist. Ferner gehört es zu den Eigenschaften von Smart-TV-Geräten, Inhalte anzeigen zu können, die auf die Sehgewohnheiten der Nutzer zurückgehen. In diesem Zusammenhang ist es durchaus denkbar, dass die Sehgewohnheiten und der Nutzungsverlauf auch dazu verwendet werden, um zielgerichtete Werbung und personalisierte Inhalte anzubieten - wie das bei vielen Webseiten der Fall ist.[186]

Eine Analyse des Sehverhaltens anhand der erfassten Daten ist eine naheliegende Anwendung. Dies wird durch die Entwicklung im Bereich Online-Marketing in den letzten zehn Jahren veranschaulicht. Dass zunehmend auf Tracking-Cookies, Browser-Fingerprinting und das auf Verhaltensanalysen basierende Behavioural-Targeting zurückgegriffen wird, zeigt die enorme Nachfrage nach Informationen über Interessen und Vorlieben von Internet-Nutzern.[187] Deshalb dürfte es nicht überraschen, wenn nun mit Smart-TV-Geräten dasselbe versucht wird.

Bevor die Erläuterungen zur Definition personenbezogener Daten fortgesetzt werden, soll im Folgenden darauf eingegangen werden, welche Daten tatsächlich erfasst werden. Um zusätzliche inhaltliche Vorschläge machen zu können, müssen Smart-TV-Geräte in der Lage sein, das Verhalten der Nutzer zu registrieren. Technisch gesehen ist es denkbar, dass auch die Dauer und der Zeitpunkt der Nutzung sowie die Identität der Nutzer erfasst werden - und ob das jeweilige Programm über Rundfunk empfangen wird, über Online-Streaming läuft oder von Quellen im lokalen Netzwerk stammt. Anhand der IP-Adresse des Fernsehgeräts lassen sich Rückschlüsse auf den ungefähren Standort des Geräts ziehen. Man kann sich aber auch vorstellen, dass der Fernseher die Anwendung registriert, die verwendet wird, um Zugriff auf Inhalte zu bekommen, so etwa die Netflix-App. In diesem Fall dürften Samsung *und* Netflix ein Interesse an der Registrierung dieser Information haben. Am Rande sei auf die interessante Frage hingewiesen, wie diese Apps am Bildschirm dargestellt werden und wonach sich deren Rangfolge richtet. Doch auf Aspekte der Herausstellung und Auffindbarkeit kann im Rahmen dieser Studie nicht eingegangen werden.

Enthalten all diese Kategorien Informationen über eine bestimmte oder bestimmbare natürliche Person? Da kein Konto eingerichtet worden ist, gibt es keinen Grund zur Annahme, dass ein Zusammenhang mit einer identifizierten Person besteht. Somit geht es um die Frage der Identifizierbarkeit. Wie oben ausgeführt hängt dieses Kriterium von den Mitteln ab, mit denen man nach allgemeinem Ermessen erwarten kann, die fragliche Person zu identifizieren. Der betreffende Auftragsverarbeiter verfügt auf jeden Fall über die Informationen über den Inhalt, den Zeitpunkt und die Dauer der Nutzung sowie über die dabei verwendete Anwendung. Der Standort des Nutzers kann über die verwendete IP-Adresse annähernd bestimmt werden.[188] Die Antwort wird natürlich von Fall zu Fall unterschiedlich ausfallen, doch aufgrund der Vielfalt der verfügbaren Fernsehprogramme, Streamingangebote und anderer Inhalte bestünden relativ schnell ausreichend Informationen, um den Nutzer identifizieren zu können. Damit sind Schlussfolgerungen hinsichtlich der sozialen, psychischen und kulturellen Identität - so der Wortlaut der Verordnung - dieser Person möglich. Damit kann der Schluss gezogen werden, dass auch im Falle von Smart-TV-Geräten ohne Kamera und Mikrofon und auch ohne Einrichtung eines Kontos durch den Nutzer personenbezogene Daten verarbeitet werden können. Wie in Kapitel III dargestellt, haben Ermittlungen der niederländischen

---

[186] Titlow J.P., *How Yahoo's homepage delivers personalized news to 700 million people*, 2012, http://readwrite.com/2012/02/10/how_yahoos_homepage_delivers_personalized_news_to.

[187] Zuiderveen Borgesius, "Behavioural Sciences And The Regulation Of Privacy On The Internet", ALSLS 2014/54, S. 3 ff., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771.

[188] Ob eine IP-Addresse an sich ein personenbezogenes Datum darstellt, ist derzeit Gegenstand einer Vorlagefrage an den EuGH in der Rechtssache C-582/14 Breyer gegen Bundesrepublik Deutschland, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CN0582. Die Artikel-29-Datenschutzgruppe betrachtet IP-Adressen bereits als Daten, die sich auf eine bestimmbare Person beziehen, siehe: Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes. Die Verordnung selbst enthält in Erwägungsgrund 24 einen etwas zweideutigen Hinweis auf IP-Adressen, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_de.pdf.

Datenschutzbehörde ergeben, dass Informationen über Sehgewohnheiten von wesentlicher Bedeutung im Hinblick auf das Recht auf Achtung des Privatlebens sind: Sie könnten als sensible Daten betrachtet werden. [189] Da die Nutzer immer mehr Möglichkeiten haben, über Fernsehen auf Abruf eigene Inhalte auszuwählen, wird es interessanter und einfacher, persönliche Präferenzen auf der Grundlage des Sehverhaltens zu bestimmen

## 4.2. Das Schutzniveau der Verordnung

Nachdem in den vorausgehenden Abschnitten die Frage erörtert wurde, ob Smart-TV-Geräte in den meisten Fällen in den Anwendungsbereich der Verordnung fallen, und nachdem diese Frage bejaht wurde, soll im folgenden Abschnitt auf die in der Verordnung vorgesehenen Schutzmaßnahmen eingegangen werden. Dabei besteht nicht die Absicht, einen umfassenden Überblick über die Bestimmungen der Verordnung zu geben. Vielmehr liegt der Schwerpunkt dabei auf den Bestimmungen, die einen Bezug zu den in Kapitel III gestellten Rechtsfragen aufweisen; gleichzeitig werden Aufschlüsse über das in der Verordnung vorgesehene Schutzniveau vermittelt, das es dann in der Folge zu bewerten gilt.

### 4.2.1. Grundlegende Bestimmungen

Im zweiten Teil der Verordnung sind in Artikel 5 dieselben Grundsätze wie in Artikel 6 der Richtlinie 95/46/EG festgelegt - allerdings in einer etwas spezifischeren Form und mit gewissen Zusätzen.[190] Wie unten näher ausgeführt, wird das Konzept der Einwilligung in der Verordnung im Detail festgelegt. Wie in Kapitel II diskutiert, weisen diese Grundsätze auf die Grenzen einer rechtmäßigen Verarbeitung hin. Die Grundsätze als solche stellen einen allgemeinen Rahmen für die sonstigen Bestimmungen dar und sind für das Verständnis des Aufbaus der Verordnung wesentlich.

Bezogen auf das inzwischen vertraute Szenario geben diese Grundsätze vor, wie Samsung mit den erfassten personenbezogenen Daten umgehen sollte. Eine weitergehende Analyse ist nicht möglich, da nähere Angaben zum genauen Verlauf der Verarbeitung fehlen. Die Darstellung hier dient der Veranschaulichung und soll auf die Diskussion in den nachfolgenden Abschnitten vorbereiten.

Artikel 6 der Verordnung nennt die Grundlagen für eine rechtmäßige Verarbeitung. Dieses Verfahren, das auch von der Richtlinie bekannt ist, sieht vor, dass jeder einzelne Verarbeitungsschritt eine der nachstehenden Bedingungen erfüllen muss:

> *„a) Die betroffene Person hat ihre unmissverständliche Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.*
>
> *b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.*
>
> *c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.*

[189] Niederländische Datenschutzbehörde, supra Fußnote 109.

[190] Dokument des Rates 10391/15, supra Fußnote 166.

*d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen oder einer anderen Person zu schützen.*

*e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.*

*f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. […].“*[191]

Wie sich aus dem TP Vision-Urteil ergibt, sind von den vorgenannten Gründen drei für das hier betrachtete Szenario von besonderer Bedeutung:[192] a) Einwilligung, b) vertragliche Pflichten und f) berechtigtes Interesse des für die Verarbeitung Verantwortlichen.[193] Jetzt ist zu prüfen, ob diese Bedingungen eine Grundlage für die in Kapitel III beschriebenen Verarbeitungsvorgänge bilden.

### 4.2.1.1. Vertragliche Pflichten

Auf den ersten Blick scheint dieser Grund ein naheliegendes Verfahren zur Legitimierung der Datenverarbeitung zu sein. Samsung könnte in den Verkaufsverträgen einfach die Einwilligung zur Verarbeitung gem. Artikel 7 b) DSR einholen. Doch die Auslegung dieser Bestimmung durch die Artikel-29-Datenschutzgruppe ist sehr restriktiv:

> *„Die Bestimmung ist eng auszulegen; sie gilt nicht für Situationen, in denen die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern der betroffenen Person von dem für die Verarbeitung Verantwortlichen einseitig auferlegt wird.“*[194]

Die Verarbeitung muss somit für die Vertragserfüllung *wesentlich* sein. Darüber hinaus hat die niederländische Datenschutzbehörde im Fall TP Vision festgestellt, dass „eine Rechtfertigung für die Verarbeitung in Bezug auf die spezifische, betroffene Einzelperson vorliegen muss“.[195] Der Kauf eines Smart-TV-Geräts basiert im Wesentlichen auf einem Kaufvertrag; dabei besteht kein bzw. kaum ein Zusammenhang mit der Verarbeitung personenbezogener Bild- oder Tondaten. Diese Bestimmung ist deshalb weniger geeignet als zunächst erwartet.

### 4.2.1.2. Berechtigtes Interesse des für die Verarbeitung Verantwortlichen

Wenn dieser Grund angeführt wird, müssen die Interessen des für die Verarbeitung Verantwortlichen mit den Grundrechten der betroffenen Person abgewogen werden. Nach

[191] Artikel 6 (1) DSGV: Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[192] Niederländische Datenschutzbehörde, supra Fußnote 109. Artikel 29 Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.

[193] Eine Einwilligung ist die in der Praxis am meisten geforderte Bedingung. Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014, supra Fußnote 54.

[194] Ibid.

[195] Niederländische Datenschutzbehörde, supra Fußnote 109.

Auffassung der Artikel-29-Datenschutzgruppe können die „berechtigten Interessen des für die Verarbeitung Verantwortlichen“ eine ganze Reihe unterschiedlicher Interessen umfassen.[196] Letzten Endes entscheidet eine Abwägung der Interessen des für die Verarbeitung Verantwortlichen und derjenigen der betroffenen Person darüber, wessen Interessen überwiegen. Erwägungsgrund 38 der Verordnung enthält dazu weitere Ausführungen. Darin ist vorgesehen, dass neben den Grundrechten und Grundfreiheiten der betroffenen Person auch deren berechtigte Erwartungen zu berücksichtigen sind. Jedoch gab es - wie oben dargestellt – bei Artikel 7 f) DSR wesentliche Änderungen in Bezug auf den Schutz Minderjähriger. Wenn es sich bei der betroffenen Person um ein Kind handelt, ist es unwahrscheinlich, dass die berechtigten Interessen des für die Verarbeitung Verantwortlichen höher bewertet werden als die Interessen des Kindes[197].

Diese Bestimmung wurde in der DSR häufig kritisiert, weil sie unterschiedlich ausgelegt werden kann. Auch hier ist das wieder der Fall. Ein Aspekt der Kritik war der Einwand, dass ein Abwägen von Interessen erst nach erfolgter Verarbeitung möglich sei, d.h. wenn unangemessene Verarbeitungspraktiken festgestellt werden, dagegen geklagt wird und ein Gericht eine entsprechende Prüfung durchführt.[198]

Im Falle von Smart-TV-Geräten besteht das Interesse von Samsung im Wesentlichen darin, eine Werbeplattform für Dienste und Inhalte (einschl. Inhalte Dritter) zur Verfügung zu stellen. Das ist insbesondere der Fall, wenn es darum geht, Sehverhalten zu analysieren. Die berechtigten Erwartungen des Käufers werden sich zu einem großen Teil auf die technischen Spezifikationen des Smart-TV-Geräts selbst beziehen. Natürlich können intelligente Funktionen auch Erwartungen beeinflussen, obwohl es unwahrscheinlich ist, dass Nutzer Werbung, die auf Sehverhalten basiert, erwarten oder wünschen.

Das Abwägen der Grundrechte und Grundfreiheiten der betroffenen Person gegenüber den Interessen von Samsung ist nicht einfach. Ein wichtiger Aspekt dabei ist die Tatsache, dass ein Smart-TV-Gerät im Haushalt meist an einer zentralen Stelle steht, was einen besonderen Grund darstellt, sich gegen Überwachung und Eingriffe in das Privatleben zu wenden. Die Nutzung des Fernsehgeräts und die Auswahl von Inhalten sind in dem Zusammenhang ebenfalls relevant. Bei der Abwägung der Interessen im Falle TP Vision hat die niederländische Datenschutzbehörde (CBP) zugunsten des Schutzes der betroffenen Person entschieden.

#### 4.2.1.3. Einwilligung

Wie oben dargestellt ist die Einwilligung die am meisten verwendete Rechtsgrundlage, und nach Meinung der CBP die einzige angemessene Rechtfertigung für Datenverarbeitung durch Smart-TV-Geräte.[199] Dies erklärt vielleicht auch, warum der europäische Gesetzgeber beschlossen hat, zusätzliche Schutzmaßnahmen in die Verordnung aufzunehmen. Einwilligung ist in Artikel 4 (8) wie folgt definiert:

> *Einwilligung der betroffenen Person: „jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite **Willensbekundung** in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass*

[196] Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014, supra Fußnote 54.

[197] Artikel 6 (f) DSGV: Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[198] Bits of Freedom*, A loophole in data processing,* 2012, S. 10, https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf.

[199] Ibid.; Niederländische Datenschutzbehörde, supra Fußnote 109.

*sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"*[200] (Hervorhebung durch die Verfasser)

Während vorher die ausdrückliche Einwilligung nur für die Verarbeitung besonderer Kategorien personenbezogener Daten erforderlich war, ist dies jetzt zu einer allgemeinen Anforderung für das Erteilen der Einwilligung geworden[201]. Aus dem Wortlaut ergibt sich auch, dass eine Einwilligung nicht implizit gegeben werden kann, da hier Bezug auf eine „Erklärung" oder „eine eindeutige Handlung" genommen wird.

Zusätzlich zur Richtlinie enthält Artikel 7 DSGV detailliert ausgeführte Bedingungen für eine Einwilligung. Darin ist festgelegt, dass der für die Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die betroffene Person ihre Einwilligung erteilt hat.[202] Ferner gilt für den Fall, dass die Einwilligung durch eine schriftliche Erklärung erfolgen soll, die noch einen anderen Sachverhalt betrifft, das Erfordernis, die Einwilligung äußerlich erkennbar von dem anderen Sachverhalt zu trennen.[203] Weiter haben die betroffenen Personen die Möglichkeit, ihre Einwilligung jederzeit zu widerrufen, wobei der Widerruf so einfach sein sollte wie die Erteilung der Einwilligung. In diesen Fällen müssen die betroffenen Personen auch darüber unterrichtet werden, ob der Widerruf zur Beendigung der vom für die Verarbeitung Verantwortlichen angebotenen Dienste führt.[204] Schließlich ist in Artikel 7 - wie in Kapitel II beschrieben - festgelegt, dass sich die Einwilligung auf einen bestimmten Zweck beziehen muss und nicht mehr wirksam ist, wenn der Zweck nicht mehr gegeben ist oder sobald die Verarbeitung personenbezogener Daten für den Zweck, für den sie ursprünglich erfasst worden sind, nicht mehr erforderlich ist[205]. Der letzte Satz dieses Absatzes sieht vor, dass die Erfüllung eines Vertrags oder die Erbringung einer Dienstleistung nicht von der Einwilligung zur Verarbeitung von Daten abhängig gemacht wird, die für die Erfüllung des Vertrags oder der Bereitstellung nicht erforderlich sind.

Samsung muss diese Bedingungen erfüllen, wenn die Firma beabsichtigt, personenbezogene Daten auf der Grundlage einer Einwilligung zu verarbeiten. Das Ersuchen um Einwilligung der betroffenen Personen muss dabei so erfolgen, dass klar ist, wozu die Einwilligung erteilt wird. Samsung muss ferner angeben, welche Daten verarbeitet werden. Eine Studie aus dem Jahr 2014 zeigt, dass dies nicht immer der Fall ist;[206] sie kommt zu dem Ergebnis, dass im Hinblick auf Datenschutz bei verschiedenen Smart-TV-Geräten nicht alle Zwecke der Verarbeitung angegeben sind und das Ersuchen um Einwilligung äußerst zweideutig formuliert ist.

### 4.2.2. Sonstige wichtige Bestimmungen

In diesem Teil der Studie wird auf weitere Bestimmungen eingegangen, die für das Schutzniveau des Nutzers von Bedeutung sein können. In Artikel 8 (Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) sind für Daten, die sich auf Kinder unter 13 Jahren

[200] Siehe Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[201] Ibid.

[202] Artikel 7 (1) DSGV, Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[203] Artikel 7 (2) DSGV, Ibid.

[204] Artikel 7 (3) DSGV, Ibid.

[205] Artikel 7 (4) DSGV, Dokument des Rates 10391/15 unter „EP Position/First Reading", Ibid.

[206] Schermer B.V. und Falot N., *Analyse privacy voorwaarden Smart TV*, 2014, S. 29, http://www.considerati.com/wp-content/uploads/2014/09/201400820Onderzoek_privacyvoorwaarden_smarttv.pdf.

beziehen, zusätzliche Schutzmaßnahmen vorgesehen.[207] Eine Verarbeitung dieser Daten ist nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes bzw. mit deren Zustimmung erteilt wird. Ferner hat der für die Verarbeitung Verantwortliche unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen zu unternehmen, um nachzuweisen, dass in diesen Fällen die Einwilligung tatsächlich vom Träger der elterlichen Verantwortung gegeben bzw. genehmigt wurde.[208] Für Samsung bedeutet dies, dass ein Ersuchen um Einwilligung im Zuge der Installation zu erfolgen hat, weil (wie in Teil II dargestellt) die Möglichkeit besteht, dass personenbezogene Daten von Kindern verarbeitet werden können. Das war auch eindeutig ein Beschwerdepunkt, den EPIC bei der amerikanischen FTC vorgebracht hatte.[209]

Angesichts der Tatsache, dass personenbezogene Daten, die zu den „besonderen Kategorien“ gehören, auch im Zuge der Funktion Gesichtserkennung verarbeitet werden können, ist ein Hinweis auf Artikel 9 (Verarbeitung besonderer Kategorien von personenbezogenen Daten) sinnvoll.[210] Für diese Kategorien gelten - wie in Artikel 8 DSR - zusätzliche Schutzmaßnahmen. Gem. Absatz 2 können sie nur mit der Einwilligung der betroffenen Person verarbeitet werden. Die Einwilligung muss die oben genannten Bedingungen erfüllen. Es gibt Ausnahmen - bestimmte zusätzliche Gründe sind aufgelistet -, doch sind diese im Zusammenhang mit dieser Studie nur von begrenzter Bedeutung. In Bezug auf die hier durchgeführte Fallstudie könnte dies bedeuten, dass für die Aktivierung der Anwendung zur Gesichtserkennung eine Einwilligung erforderlich ist.

Artikel 14 (Informationspflicht bei Erhebung der Daten bei der betroffenen Person) sieht für den für die Verarbeitung Verantwortlichen verschiedene Informationspflichten vor.[211] Er enthält eine Auflistung der Informationen, die der betroffenen Person mitzuteilen sind, und er kann als Anforderungskatalog für den Datenschutz der Zukunft betrachtet werden. Von großer Bedeutung ist dabei, dass neben dem Zweck der Verarbeitung, der Dauer der Speicherung und dem Hinweis auf die Rechte der betroffenen Person auch die Identität des für die Verarbeitung Verantwortlichen mitgeteilt werden muss. Das ist nicht unbedingt neu, obwohl die Ausführungen im zweiten Teil zeigen, dass das in der Praxis nicht immer eingehalten wird.

Auch das „Recht auf Vergessenwerden“, das auf die Rechtssache Google/Spain[212] zurückgeht, hat den Weg in die Verordnung gefunden. Es sei hier erwähnt, weil es eng mit der Erteilung einer Einwilligung und dem Recht auf Widerruf derselben zusammenhängt. Das Recht ist in Artikel 17 (Recht auf Löschung und auf "Vergessenwerden") verankert und gibt der betroffenen Person das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung der sie betreffenden personenbezogener Daten zu verlangen.[213] Dieses Recht kann auch u.a. in Anspruch genommen werden, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, oder wenn die betroffene Person ihre Einwilligung widerruft.

Die Besitzer der Smart-TV-Geräte können die Löschung erfasster Daten verlangen, wenn sie beschließen, das Gerät nicht weiter zu benutzen. Dadurch haben sie eine gewisse Kontrolle über die sie betreffenden Informationen.

Bezüglich des hier betrachteten Szenarios sind zwei Artikel von besonderer Bedeutung: Artikel 19 (Widerspruchsrecht) und Artikel 20 (Profiling).[214] Nach diesen Bestimmungen haben

---

[207] Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[208] Artikel 8 DSGV, Ibid.

[209] EPIC, supra Fußnote 112.

[210] Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[211] Ibid.

[212] EuGH, C-131/12, supra Fußnote 45.

[213] Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[214] Ibid.

Nutzer die Möglichkeit, Profiling-Praktiken zu widersprechen. Profiling ist in Artikel 4 (3) bis definiert:

> *jeder mit automatisierten Verfahren ausgeführte Vorgang der Verarbeitung personenbezogener Daten mit dem Ziel, bestimmte persönliche Aspekte natürlicher Personen zu bewerten, oder im Besonderen die Leistung dieser Person bei der Arbeit, ihre wirtschaftliche Situation, ihren Standort, ihre Gesundheit, ihre persönlichen Vorlieben, ihre Zuverlässigkeit oder ihr Verhalten zu analysieren und vorherzusagen.*

Die Analyse der Sehgewohnheiten durch Smart-TV-Anbieter scheint unter diese Definition zu fallen, da es hier um die Bewertung von persönlichen Vorlieben und persönlichem Verhalten geht. Die Ergebnisse der Untersuchungen der CBP im Fall *Ziggo* bestätigen dies. Diese Bestimmung bezieht sich auf sog. Behavioural-Targeting-Verfahren, die von einigen Marktteilnehmern angewandt werden. Nach Artikel 19 können betroffene Personen gegen diese Art von Profiling-Praktiken Widerspruch einlegen. Weiter gilt nach Artikel 20 (2), dass diese Verfahren nur im Zusammenhang mit der Erfüllung eines Vertrages nach EU- oder dem Recht eines Mitgliedstaats oder auf der Grundlage einer Einwilligung der betroffenen Person eingesetzt werden dürfen. Wenn also Samsung oder Netflix das Sehverhalten analysieren wollen, müssen sie sich an eine dieser Rechtsgrundlagen halten. Die zwei Möglichkeiten, die sich bieten, sind - erstens - das Einholen einer Einwilligung und - zweitens - die Verwendung von Verträgen, in denen sich Samsung bzw. Netflix verpflichten, inhaltliche Vorschläge auf der Grundlage des Sehverhaltens der Nutzer zu machen.

Eine andere bemerkenswerte Bestimmung findet sich in Artikel 23 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen).[215] Er verpflichtet die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter dazu, geeignete und angemessene organisatorische Maßnahmen durchzuführen, die den Stand der Technik, das aktuelle technische Know-how und international bewährte Praktiken sowie die Risiken der Datenverarbeitungsverfahren berücksichtigen. In Bezug zu den in Kapitel II gemachten Feststellungen bedeutet dies, dass die für die Verarbeitung Verantwortlichen zusätzliche Maßnahmen ergreifen müssen, um sicherzustellen, dass ihre Produkte die einschlägigen Spezifikationen erfüllen und dass sie entsprechend optisch gestaltet sind. Denn die Nichteinhaltung dieser Vorschriften kann zu Geldstrafen bis zu EUR 1.000.000 oder 2% des weltweiten Umsatzes führen - eine Maßnahme, die zu verstärkten Anstrengungen bei der Durchsetzung führen dürfte.[216] Die Anhebung der Höchstbeträge der Geldbußen könnte für multinationale Unternehmen einen großen Anreiz darstellen, sich an die Vorschriften zu halten.

Ein letzter Aspekt, auf den hier eingegangen werden soll, ist die Rechtmäßigkeit internationaler Datentransfers. Im Falle TP Vision wurden die Daten lokal in den Niederlanden gespeichert, doch ist es natürlich möglich, dass andere Anbieter die Daten an andere Orte übermitteln. Diesbezügliche Regelungen finden sich in den Artikeln 41 bis 45 bis).[217] Nach Artikel 41 sind Datenübermittlungen an Drittländer zulässig, sofern ein entsprechender offizieller „Angemessenheitsbeschluss " vorliegt. Gem. Artikel 42 sind solche Übermittlungen auch gestattet, wenn feststeht, dass das Bestimmungsland geeignete Garantien bietet. In Artikel 43 schließlich ist vorgesehen, dass die für die Verarbeitung Verantwortlichen eine Datenübermittlung an Drittländer auf der Grundlage verbindlicher unternehmensinterner Vorschriften (binding corporate rules, BCR) vornehmen können.

---

[215] Ibid.

[216] Artikel 79(3)a), Dokument des Rates 10391/15, unter Allgemeine Ausrichtung des Rates (15.06.2015), supra Fußnote 166.

[217] Ibid., supra Fußnote 166.

Es hat sich gezeigt, dass die in der Richtlinie vorgesehene Regelung von Übermittlungen an Drittländer zu restriktiv war und zu hohe Anforderungen stellte, da Datentransfers im großen Stil oftmals innerhalb der Unternehmen selbst vorgenommen wurden. In einem Fachbeitrag wird der revidierte Ansatz der Verordnung wie folgt beschrieben: „Bezüglich des Problems des strukturellen Transfers personenbezogener Daten innerhalb von multinationalen Unternehmen bringt der Vorschlag zumindest durch die Kodifizierung spezifischer, in der Praxis entwickelter Regeln für verbindliche unternehmensinterne Vorschriften (BCR) Klärung. Der zentrale Aspekt, dass Auftragsverarbeiter auch verbindliche unternehmensinterne Vorschriften verwenden, macht eine Umsetzung in Drittländern für Zwecke des Offshoring und Cloud Computing möglich. Es ist jedoch nicht klar, wie die Auftragsverarbeiter verbindliche unternehmensinterne Vorschriften verwenden sollen.

Schließlich enthält der Vorschlag keine Lösung des Problems von Datenanfragen seitens Regierungsstellen in Drittländern. Angesichts der anhaltenden Globalisierung, der Intensivierung internationaler Datenströme und den damit zusammenhängenden Risiken hinsichtlich des Schutzes personenbezogener Daten kommt es nun darauf an, dass die neuen Vorschriften für den Datentransfer überprüft und verbessert werden, damit diese zu einem funktionsfähigen, zukunftssicheren Bezugsrahmen für die Datenverarbeitung auf internationaler Ebene und den Schutz der betroffenen Personen verwendet werden können.[218]

Zusammenfassend kann man sagen, dass die Bestimmungen für internationale Datentransfers in bestimmten Bereichen an Klarheit gewonnen haben. Die Verordnung dürfte zwar für mehr Rechtssicherheit beim grenzüberschreitenden Transfer personenbezogener Daten sorgen, doch könnte die jüngste Entscheidung des EuGH in der Rechtssache *Max Schrems* auch das Gegenteil bewirken.[219]

## 4.3. Was ist ein angemessenes Schutzniveau und bietet die Verordnung ein solches?

Bislang hat sich diese Studie mit der Definition von Smart-TV-Geräten und Daten, die mit diesen erfasst werden können, dem Anwendungsbereich der Verordnung und den darin enthaltenen Schutzmaßnahmen beschäftigt. In diesem Abschnitt werden zunächst die Anforderungen im Hinblick auf einen angemessenen Schutz der Nutzer von Smart-TV-Geräten dargestellt; anschließend erfolgt eine kritische Bewertung der Verordnung.

### 4.3.1. Was muss geschützt werden und warum?

Beim Konzept eines angemessenen Schutzniveaus wird implizit davon ausgegangen, dass es Personen gibt, die eines Schutzes bedürfen. Nur wenn feststeht, *was* geschützt werden soll, kann auf Gründe eingegangen werden, *warum* ein solcher Schutz notwendig ist. Ohne diesen Schritt bestünde für weitergehende Überlegungen keine Grundlage.

---

[218] Wisman N. ud de Vries H.H., *Doorgifte van persoonsgegevens onder de nieuwe Verordening*, P&I 2012, S. 117, http://www.recht.nl/vakliteratuur/staatsrecht/artikel/358929/doorgifte-van-persoonsgegevens-onder-de-nieuwe-verordening/.

[219] In dieser Rechtssache erklärte der Gerichtshof die sog. Safe-Harbor-Entscheidung für ungültig. Für weitere Informationen siehe: http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=; EuGH, C-362/14, supra Fußnote 56.

Letztlich sind die Rechte auf Privat- und Familienleben (Artikel 7 der Charta der Grundrechte der EU) und auf Schutz personenbezogener Daten (Artikel 8 der Charta) Gegenstand des Schutzes. Die Prüfung, warum der physische Raum, den Smart-TV-Geräte einnehmen, schutzwürdig ist, erweist sich als aufschlussreich, da der Gegenstand des Schutzes der in den eigenen vier Wänden geschaffene Freiraum ist. Dieser Aspekt steht in Zusammenhang mit dem Anwendungsbereich von Artikel 7 der Charta, der die Bereiche Privat- und Familienleben, Wohnung und Kommunikation umfasst. Dieser Freiraum wird für die Verfolgung zahlreicher Aktivitäten genutzt. Die Tätigkeit des Fernsehens, die weltweit in großem Umfang stattfindet, gehört zu diesen Aktivitäten. Ferngesehen wird aus vielerlei Gründen, in den meisten Fällen zur Unterhaltung und zum Erwerb von Wissen. Traditionell geschah dies unter Nutzung nichtintelligenter Fernsehgeräte, die lediglich Bilder wiedergeben konnten. Wie oben ausgeführt, hat sich dies mit der Einführung von Smart-TV-Geräten dramatisch verändert. Plötzlich ist es möglich, den Zuschauer auch in seiner eigenen Wohnung zu überwachen. Als Reaktion darauf kann es dazu kommen, dass die Nutzer anfangen, ihr Verhalten - bewusst oder unbewusst - anzupassen. Das sollte aber in einem Raum, der frei sein sollte und in dem man Inhalte sehen und Informationen nutzen kann, die nach persönlichen Vorlieben ausgewählt wurden, nicht vorkommen. Der Gegenstand des Schutzes sollte der Raum sein, in dem man - sozusagen - ganz man selbst sein kann. Julie Cohen hat dieses Gefühl genauer beschrieben:

> *„Eine grundlegende Annahme unseres Diskurses über Tätigkeiten wie Lesen, Denken und Sprechen ist die, dass der Einzelne in unserer Gesellschaft die Garantie hat, seine Gedanken und Meinungen im privaten Umfeld frei äußern zu können - ohne dabei von staatlichen oder privaten Stellen überwacht zu werden.“*[220]

Was Julie Cohen zum Lesen sagt, lässt sich auch auf das „Fernsehen“ übertragen. Die beiden Arten, sich Informationen anzueignen, unterscheiden sich nicht grundsätzlich. Julie Cohen beantwortet gleichzeitig teilweise die Frage, *warum* ein Schutz notwendig ist, mit einem Hinweis auf den Ersten Zusatz zur Verfassung der Vereinigten Staaten, in dem das US-amerikanische Konzept der Meinungsfreiheit verankert ist. Auch Neil Richards spricht sich für den Schutz der Privatsphäre auf der Grundlage der Meinungsfreiheit aus:

> *„Wir meinen oft, dass Regeln zum Schutz der Privatsphäre nicht mit dem Ersten Zusatz zur Verfassung vereinbar sind, doch der Schutz der intellektuellen Privatsphäre ist etwas Anderes. Eine intellektuelle Privatsphäre ist für eine robuste Kultur der freien Meinungsäußerung von vitaler Bedeutung, da sie die Integrität unserer geistigen Aktivitäten sichert und sie vor unerwünschten Blicken oder der Einmischung anderer schützt. Wenn wir in der Öffentlichkeit etwas Interessantes zu sagen haben wollen, müssen wir auf die Freiheit, im Privaten neue Ideen entweder alleine oder mit Vertrauten entwickeln zu können, achten. Die Redefreiheit hängt also von einem angemessenen Maß an intellektueller Privatsphäre ab, die durch die weitverbreiteten elektronischen Aufzeichnungen unserer geistigen Tätigkeiten bedroht ist.“*

In seinem Werk mit dem Titel „Intellectual Privacy“ [221] argumentiert Richards, dass eine wirksame Nutzung des Rechts auf Meinungsfreiheit einen Raum voraussetzt, in dem man ungestört seinen Gedanken nachgehen und Ideen entwickeln kann. Ohne einen solchen Raum bestehe die Gefahr, dass der Schutz der Meinungsfreiheit bedeutungslos werde, da es sonst keine Gelegenheit gebe, Ideen zu entwickeln, die es wert wären, geschützt zu werden. Diese Logik gilt auch für die Nutzung

---

[220] Cohen J.E., *A Right to Read Anonymously*, CLR 1996, S. 2, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990.

[221] Richards N., *Intellectual Privacy*, TLR 2008, S. 387, http://ukcatalogue.oup.com/product/9780199946143.do. Siehe dazu auch Richards N., *Intellectual Privacy*, 2015, supra Fußnote 9.

des Fernsehgeräts in Privaträumen. Der von Richards genannte Raum umfasst sowohl physische Orte oder „räumliche Privatheit“[222] als auch „intellektuellen Raum“ - auch als „Freiheit der privaten intellektuellen Auseinandersetzung“ bezeichnet.[223] In Verbindung mit dem Grundprinzip „Freiheit des Denkens und Glaubens“ und „Freiheit der vertraulichen Kommunikationen“[224] sind diese Konzepte die Bausteine der „intellektuellen Privatheit“.

Der Europäische Gerichtshof für Menschenrechte geht in seiner Rechtsprechung von einen ähnlichen Ansatz aus und hat Bedenken geäußert, die denjenigen von Richards ähnlich sind. Der Gerichtshof hat z.B. festgestellt, dass „Gedanken und Meinungen zu öffentlichen Angelegenheit sensibler Natur“ sind, und:

> *„Deshalb stellt die schiere Möglichkeit von Eingriffen durch Behörden **oder private Parteien, die ohne angemessene Kontrolle** oder sogar mit Unterstützung der Behörden erfolgen, **eine ernsthafte Beeinträchtigung der freien Entstehung von Ideen** und der demokratischen Debatte dar und kann abschreckende Wirkung haben“*[225] (Hervorhebungen durch Verfasser)

Die hier angesprochene abschreckende Wirkung bezieht sich auf das Recht, ungestört nach Informationen zu suchen bzw. Zugang zu Informationen und Ideen zu haben. Diese abschreckende Wirkung beruht im Wesentlichen auf der „Mehrfachüberwachung“ sowohl der Fernsehnutzung als auch anderer über die Smart-TV-Geräte durchgeführter Online-Aktivitäten (weitere Einzelheiten dazu in der obenstehenden Einführung).

## 4.3.2. Was ist angemessener Schutz?

Nachdem nun Schutzgegenstand und -gründe feststehen, kann geprüft werden, wie dieser Raum in angemessener Weise geschützt werden kann. Das Konzept personenbezogener Daten lässt sich sehr gut für die Verwirklichung dieses Schutzes verwenden. In diesem Zusammenhang ist die Meinung von Fried zu Privatheit von Bedeutung: „Privatheit ist die Kontrolle, die wir über die Informationen über uns haben.“[226] Vielleicht noch bekannter ist die Definition des Begriffs „Privatheit“ von Westin: „der Anspruch einzelner Personen, Gruppen oder Institutionen selbst bestimmen zu können, wann, wie und in welchem Umfang Informationen über sie an andere kommuniziert werden.“[227]

Diese Aussagen haben zwei Aspekte gemeinsam: 1.) Kontrolle über Information und 2.) die Information bezieht sich auf uns. Der zweitgenannte Aspekt dürfte bekannt sein, da er bei der Definition personenbezogener Daten in Teil II thematisiert wird. Wie bereits im Zusammenhang mit den Artikeln 7 und 8 der Grundrechtecharta erläutert, kann man sagen, dass diese Rechte enge Verbindungen aufweisen. Ein Schutz des Privatlebens ist ohne individuelle Kontrolle über die eigenen persönlichen Daten nicht möglich.

Der Schlüsselbegriff für die Bewertung der Angemessenheit von Schutz ist *Kontrolle*. Kontrolle beschreibt die Autonomie Einzelner, auf Eingriffe in das Privatleben reagieren zu können. Beate Rössler hat dazu Folgendes formuliert:

---

[222] Ibid.

[223] Ibid.

[224] Ibid.

[225] *Altuğ Taner Akçam gegen Türkei*, Nr. 27520/07, § 81, 25. Oktober 2011, http://hudoc.echr.coe.int/eng?i=001-107206#{"itemid":["001-107206"]}.

[226] Fried, *Privacy*, YLJ 1968, S. 482.

[227] Westin A.F., *Privacy and Freedom*, W&L LR 1968, S. 7, http://www.jstor.org/stable/40708684?seq=1#page_scan_tab_contents.

> *„Der Grund nun, warum Personen diese Arten der Verletzung informationeller Privatheit als Beschädigungen, Entfremdungen begreifen, liegt nicht nur darin, dass sie sie einfachhin als unangenehm, beschämend, verletzend empfinden und deshalb ablehnen – dies auch; sondern auch und vor allem darin, dass mit jenen Verletzungen informationeller Privatheit immer auch zugleich Verletzungen der Bedingungen von Autonomie gegeben sind: individuelle Autonomie ist auf die informationelle Privatheit angewiesen.“*[228]

Die Notwendigkeit der Kontrolle über Informationen ist ein zentraler Punkt der Position der niederländischen und deutschen Aufsichtsbehörden für den Datenschutz, wenn es sich um das für Smart-TV-Geräte notwendige Schutzniveau handelt. Im Zusammenhang mit ihrer Untersuchung im Fall TP Vision[229]hat die niederländische Datenschutzbehörde eine Reihe von Anforderungen aufgelistet, die nach dem Datenschutzgesetz einzuhalten sind. Dies heißt nicht notwendigerweise, dass diese Gesetze angemessen sind, zeigt jedoch einen Schwerpunkt auf Bemühungen zur Stärkung der Autonomie von Einzelpersonen. Diese Anforderungen umfassen eine klare Beschreibung der Zwecke der Verarbeitung, um die betroffenen Person in die Lage zu versetzen, eine Einwilligung in Kenntnis der Sachlage zu erteilen. Somit sind aus Sicht der niederländischen Datenschutzbehörde Informationspflichten von großer Bedeutung. Eine der in Deutschland für Datenschutz zuständigen Stellen hat vier allgemeine Regeln formuliert, die bei der Nutzung von Smart-TV-Geräten zu beachten sind:[230]

1. „Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. [...] [P]ersonenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist. Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden. [...] Nutzungsprofile [dürfen nur dann erstellt werden], sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat.“
3. Beachtung des Prinzips „privacy by default“ bei den Grundeinstellungen der Smart-TV-Geräte. Dies könnte die Option für anonyme Nutzung und Cookie-Verwaltung einschließen.
4. „Smart-TV-Geräte [...] müssen über sicherheitstechnische Mechanismen verfügen“, die die Geräte so weit wie möglich „vor dem Zugriff unbefugter Dritter schützen.“

Interessant ist, dass in dieser Position auch die Möglichkeit der anonymen Nutzung des Fernsehgeräts gefordert wird - eine Haltung, die an das zu Beginn dieses Abschnitts der Studie angesprochene „Recht auf anonymes Lesen“ von Julie Cohen erinnert.

Man könnte somit bei der Bestimmung eines angemessenen Schutzniveaus von den folgenden Grundsätzen ausgehen: Ein angemessener Schutz bedeutet, dass der Nutzer eines Smart-TV-Geräts die Möglichkeit hat, das Gerät völlig anonym zu nutzen. Denn nur dann kann der sichere Raum entstehen, der für den wirksamen Genuss der „intellektuelle Privatheit“ notwendig ist. Das setzt erstens voraus, dass alle Informationen, die für die Verarbeitung personenbezogener Daten verwendet werden, eindeutig, in absteigender Reihenfolge ihrer „Wirkung“ angezeigt werden. Um es den Nutzern zu ermöglichen, ihre personenbezogenen Daten wirksam zu kontrollieren, setzt ein angemessenes Schutzniveau voraus, dass für die Verarbeitung eine Einwilligung des Nutzers

---

[228] Rössler B., *Der Wert des Privaten*, 2001, S 203, http://www.suhrkamp.de/buecher/der_wert_des_privaten-beate_roessler_29130.html.

[229] Niederländische Datenschutzbehörde, supra Fußnote 109.

[230] Ibid. supra Fußnote 73.

erforderlich ist. Daten sollten nur unter dieser Bedingung verarbeitet werden können, und andere Möglichkeiten dazu sollten nicht bestehen. Wenn die Verweigerung der Einwilligung dazu führt, dass der Nutzer bestimmte Dienste nicht mehr empfangen kann, sollte geprüft werden, ob diese Konsequenz angemessen ist. So ist es z.B. schwierig, ohne Nutzerprofile inhaltliche Vorschläge zu machen. Wenn der Nutzer keine Einwilligung zum Anlegen von Profilen erteilt, könnte dies bedeuten, dass dieser Dienst nicht zur Verfügung steht. Für viele Nutzer könnte diese eine vertretbare Option darstellen, sofern sie darüber im Voraus entsprechend klar unterrichtet werden.

Ein angemessenes Schutzniveau setzt weiter voraus, dass die Hersteller der Smart-TV-Geräte die Grundsätze „Datenschutz durch Design“ und/oder „durch Datenschutz-Grundeinstellungen“ beachten. Dadurch sind auch technisch weniger versierte Nutzer in der Lage, zu Beginn der Nutzung eine bewusste Entscheidung zu treffen.

Die Kontrollmöglichkeiten seitens der Nutzer sollten bezüglich des gesamten Verarbeitungszyklus' - von der für die Verarbeitung verantwortlichen Stelle über den Auftragsverarbeiter bis zum Sub-Auftragsverarbeiter - bestehen. Dies bedeutet, dass die Nutzer die Kontrolle über die Speicherung oder Löschung ihrer personenbezogenen Daten haben müssen.

## 4.3.3. Bietet die Verordnung ein angemessenes Schutzniveau?

Nach der Definition des Konzepts eines angemessenen Schutzes kann nun geprüft werden, ob die Verordnung diese Anforderung erfüllt. Dies soll anhand einer Diskussion über die einschlägigen Bestimmungen erfolgen.

### 4.3.3.1. Anonymität

Die Verordnung enthält nur an einer Stelle das Wort „anonym“: in Erwägungsgrund 23, wo anonymisierte Daten ausdrücklich nicht als personenbezogene Daten betrachtet werden, da eine Identifizierung nicht mehr möglich ist[231]. Auf Anonymität wird nicht weiter eingegangen, da dieser Aspekt nicht zu den Zielen der Verordnung gehört, deren Schwerpunkt im Übrigen auf den Grundsätzen und Bedingungen für eine Verarbeitung liegt. Bei diesem Ansatz wird davon ausgegangen und hingenommen, dass eine Verarbeitung personenbezogener Daten stattfindet, und es wird der Versuch unternommen, Schutzmaßnahmen bezüglich dieser Praktiken einzuführen. In der Anforderung der Einwilligung durch die Nutzer lässt sich im Kern vielleicht ein Aspekt von Anonymität erkennen.

### 4.3.3.2. Einwilligung

Wie bereits ausgeführt ist eine rechtmäßige Verarbeitung personenbezogener Daten nur auf der Grundlage der in Artikel 6 genannten Bedingungen möglich. Dazu gehört die Bedingung der Einwilligung. Wie oben dargestellt sollte eine Verarbeitung personenbezogener Daten von Smart-TV-Geräten *nur* auf der Grundlage einer Einwilligung erfolgen, weil die anderen Bedingungen den betroffenen Personen keine ausreichenden Kontrollmöglichkeiten geben. In der Verordnung sind jedoch neben der Einwilligung fünf weitere Rechtsgrundlagen aufgeführt, von denen zwei auf die Verarbeitung von Daten von Smart-TV-Geräten zutreffen dürften. Diesbezüglich scheint das

[231] Dokument des Rates 10391/15, supra Fußnote 166.

Schutzniveau nicht angemessen. Es gibt keine Klausel, die Samsung oder andere Anbieter dazu zwingen würde, die Einwilligung der betroffenen Personen einzuholen. Dies könnte dadurch erreicht werden, dass eine separate Kategorie „wesentliche Dienste" eingeführt wird, für die ähnliche Regelungen wie für die besonderen Kategorien personenbezogener Daten in der Richtlinie gelten, wobei die Einwilligung der einzig mögliche Rechtfertigungsgrund für eine Verarbeitung ist. Wesentliche Dienste (bzw. Einrichtungen) sollten Dienste sein, die in der Wirklichkeit des Alltags der Nutzer eine wichtige Rolle spielen und die für die Vermittlung von Wissen und das Sammeln von Informationen von entscheidender Bedeutung sind. Beispiele hierfür sind u.a. Fernsehen und Internet, aber auch Bibliotheken. Die niederländische Datenschutzbehörde hat bereits ähnliche Schritte unternommen und es den öffentlich-rechtlichen Rundfunkveranstalten untersagt, sog. Cookie-Walls einzurichten.[232] Die weiteren Auswirkungen eines solchen Ansatzes dürften schwer zu prognostizieren sein, doch wäre dies eine Möglichkeit, den notwendigen Schutz der „intellektuellen Privatheit" herzustellen.

Die in der Verordnung vorgesehene Anforderung der Einwilligung beruht auf einer Definition, die eine *explizite* Einwilligung voraussetzt, womit eine implizite oder standardmäßige Einwilligung ausscheidet. Diese Entwicklung ist als positiv zu bewerten, da die betroffenen Personen dadurch mehr Möglichkeiten der Kontrolle haben. Zwischen Einwilligung und Anonymität besteht ein gewisses Spannungsverhältnis dergestalt, dass eine Verweigerung der Zustimmung auch als Form und Ausdruck persönlicher Präferenzen registriert werden muss. Eine ähnlich gelagerte Diskussion findet derzeit zum Thema Cookies statt; ein Cookie ist dazu da, die Tatsache zu registrieren, dass ein Nutzer nicht wünscht, dass Cookies zum Einsatz kommen. Das muss jedoch nicht Anlass zu großer Sorge sein, da die Auswirkungen dieses einmaligen Verarbeitungsvorgangs begrenzt sind. Das Prinzip „privacy by default" könnte hier ebenfalls zu Ergebnissen führen, indem die anonyme Nutzung als Standardeinstellung vorgeschrieben wird. Ein gewisser Grad an Anonymität ist also dadurch zu erreichen, dass man die Einwilligung verweigert. Doch nach Borgesius - Verfasser eines Artikels mit dem Titel „Besserer Datenschutz: der Mythos der informierten Einwilligung" (*Privacybescherming online kan beter: De mythe van geïnformeerde toestemming*) - ist dies keine Patentlösung.[233] Dabei geht er von der Feststellung aus, dass viele Menschen dazu neigen, einfach auf „Ja" zu klicken, wenn das erforderlich ist; das macht den gesetzlich garantieren Datenschutz zur Illusion. Er schlägt vor, den Schwerpunkt auf *Empowerment* (was dem oben diskutierten Kontrollprinzip entspricht) und *Schutz* zu legen. Dieser Schutz muss durch Gesetze gewährleistet werden. Wie gezeigt wurde hat der EU-Gesetzgeber versucht, in der Verordnung die Anforderungen in Bezug auf Einwilligungen zu verbessern. Man kann sagen, dass Schwächen der entsprechenden Anforderungen in der Verordnung angemessen geändert worden sind und dass die Verordnung den betroffenen Personen ein ausreichendes Maß an Kontrollmöglichkeiten zugesteht. Ein Punkt, der noch verbessert werden könnte, bestünde darin, die Anforderung der Einwilligung für wesentliche Dienste und Einrichtungen verbindlich vorzusehen.

Erwähnenswert ist noch die Tatsache, dass bestimmte Dienste wie etwa Facebook z.B. ohne eine Zustimmung zur Verarbeitung von Daten nicht verfügbar sind. Die einzige Option besteht im Moment darin, diesen Dienst nicht zu nutzen. Doch diese Entscheidung ist wegen der starken Netzwerk-Effekte, die von vielen Online-Diensten angezeigt werden, kompliziert. Man könnte sich für ein Dienstangebot entscheiden, das nicht systematisch gegen Rechte verstößt, aber es ist unwahrscheinlich, dass auch Freunde und Bekannte dort registriert sind. Die derzeitige Einwilligungsanforderung ändert an dieser Situation nichts. Den Zugang zu Diensten gibt es nicht umsonst: Die Nutzer zahlen nicht mit Geld, sondern mit ihren persönlichen Daten. Eine Lösung

---

[232] CBP, *Brief aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap, inzake cookiebeleid NPO*, 2013, https://cbpweb.nl/sites/default/files/atoms/files/med_20130205-cookies-npo.pdf.

[233] Zuiderveen Borgesius, *Privacybescherming online kan beter*, NJB 2015/14, S. 878 ff., http://www.ivir.nl/publicaties/download/1536.

bestünde darin, eine zahlungspflichtige Option oder eine vereinfachte Version des Dienstes mit lediglich bestimmten Grundfunktionen anzubieten. Eine in dem Zusammenhang wichtige Bestimmung enthält Artikel 7 Absatz 4 der Verordnung; hier ist vorgesehen, dass die Erfüllung eines Vertrags oder die Bereitstellung eines Dienstes nicht von der Einwilligung zur Verarbeitung von Daten abhängig gemacht werden kann, die für die Erfüllung des Vertrags oder der Bereitstellung nicht notwendig sind.[234]

#### 4.3.3.3. Sonstige Anforderungen

Die sonstigen Anforderungen hinsichtlich eines angemessenen Schutzniveaus wie „privacy by design“, Kontrolle über die Entfernung personenbezogener Daten sowie klare Informationspflichten sind in der Verordnung berücksichtigt. Oben wurde ausgeführt, dass die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter aufgrund von Artikel 23 verpflichtet sind, den Grundsatz „privacy by design“ anzuwenden. Darüber hinaus sind enthalten: das „Recht auf Vergessenwerden“, die Informationspflichten und der Widerruf der Einwilligung. Zusätzliche Schutzmaßnahmen wie das Widerspruchsrecht, die Regelungen zum Profiling und zu internationalen Datentransfers stärken den Regelungsrahmen insgesamt und verbessern das Schutzniveau der betroffenen Personen.

Damit kann der Schluss gezogen werden, dass die Verordnung einem angemessenen Schutzniveau nahe kommt. Sofern sich die Anbieter von Smart-TV-Geräten und Dritte wie Netflix an diese Vorgaben halten, werden die Nutzer von Smart-TV-Geräten in der Lage sein, eine wirksame Kontrolle über ihre persönlichen Daten ausüben zu können. Von zentraler Bedeutung ist die Anforderung der Einwilligung, die im vorliegenden Szenario verbindlich gemacht werden sollte. Diesbezüglich kann die Verordnung noch verbessert werden. Nur wenn auf dieser Bedingung bestanden wird, ist gewährleistet, dass Nutzer die Möglichkeit haben, Inhalte anonym zu nutzen.

[234] Supra Fußnote 205.

# Abschließende Analyse

Es ist offensichtlich: Das Thema „Big Data“ ist im audiovisuellen Sektor angekommen. Die traditionellen Rundfunkdienste werden in rasantem Tempo durch nichtlineare Dienste ergänzt - und noch wichtiger - von diesen abgelöst. Doch bei beiden gibt es inzwischen Verbindungen zu den Nutzern. Über das Internet können Anbieter und Nutzer interagieren. Auf der Grundlage der ausgetauschten personenbezogenen Daten - der neuen Währung - können die Anbieter ihr Angebot optimieren, und die Nutzer erhalten Empfehlungen und Hinweise, die auf Grundlage ihrer persönlichen Profile zusammengestellt werden. Das ist die eine Seite der Medaille. Auf der anderen Seite gibt es Bedenken; es ist die Rede von Manipulation, „Rosinenpickerei“, Einschränkung der Wahlmöglichkeiten für die Zuschauer und Informationsisolation.

Eines der besten Beispiele für diese Entwicklungen ist das Smart-TV-Gerät. Diese Geräte sind mit dem Internet verbunden und bieten die vorgenannten Möglichkeiten. Das Wachstum von Smart-TV ist nicht mehr aufzuhalten. In den nächsten beiden Jahren wird in der Mehrheit der europäischen Haushalte ein solches Gerät stehen. Und wenn man noch andere Geräte mit ähnlichen Funktionen (Tablets, Smartphones und Set-Top-Boxen) mit in die Betrachtung einbezieht, kann man sagen, dass wir bereits jetzt den Punkt erreicht haben, wo es kein Zurück mehr gibt.

In diesem *IRIS Spezial* werden die Funktionalitäten von Smart-TV-Geräten im Detail beschrieben und die wichtigsten Aspekte des politischen und regelungstechnischen Kontexts diskutiert. Der Beitrag enthält aber auch Hintergrundinformationen zu den ersten Fällen, in denen die Nutzung von Smart-TV-Geräten zu datenschutzrechtlichen Bedenken führte. Daraus lassen sich mindestens die folgenden Schlussfolgerungen ziehen.

1. Die datenschutzrelevanten Aspekte in Verbindung mit Smart-TV-Geräten sind vielschichtig, weil das Smart-TV-Ökosystem viele Anbieter umfasst, die die personenbezogenen Daten der Nutzer auf unterschiedliche Weise verarbeiten. Informationen werden im Zuge von herkömmlichen Interaktionen erfasst - wie Fernbedienung und/oder in Verbindung mit Plattformen zur Auswahl von Inhalten (z.B. elektronische Programmführer). Doch die Geräte sind noch smarter; sie bieten Spracherkennung, Bewegungssteuerung sowie Gesichtserkennung und erfassen bzw. verwenden Daten ihrer Nutzer. Diese Aufzählung ist nicht vollständig, doch sollte man davon ausgehen, dass die technologische Entwicklung zu neuen Funktionen führen wird. Apps machen es möglich, physische und medizinische Daten mit der Nutzung audiovisueller Inhalte zu verbinden.
2. Die Analyse des bestehenden gesetzlichen und politischen Umfelds zeigt eine starke Fragmentierung, die sich durch spezielle Medienregulierungen - wie die Richtlinie über audiovisuelle Mediendienste, andere sektorspezifische Regulierungen (Telekomunikation, E-Commerce, E-Privacy) - und allgemeine Regelungen, die auf Smart-TV-Geräte Anwendung finden (allgemeiner Datenschutz), auszeichnet. Eingerahmt und ergänzt wird das Ganze durch Grundrechte, vor allem das Recht auf Meinungsfreiheit, Schutz der Privatsphäre und Datenschutz.
3. Die traditionelle Medienregulierung wie etwa die Richtlinie über audiovisuelle Mediendienste hat eine lange Geschichte und geht bis in die 1970er Jahre zurück. Interaktivität und Privatsphäre waren damals keine Themen, die hätten berücksichtigt

werden müssen. Auch bei den letzten Novellierungen konzentrierte man sich lediglich darauf, aus dieser traditionellen Perspektive neue Entwicklungen aufzunehmen: nichtlineare Dienste kamen hinzu, aber nur als Instrument zur Bereitstellung audiovisueller Inhalte auf andere Art. Die Schlüsselakteure - die Anbieter audiovisueller Dienste und die Nutzer - stehen im Mittelpunkt dieses traditionellen Rahmens. Möglichkeiten und Grenzen, z.B. Jugendschutzbestimmungen, wirken sich deshalb unmittelbar auf die Smart-TV-Umgebung aus.

4. Andere sektorspezifische Instrumente, die eher allgemeiner Natur sind und nicht spezifisch für den audiovisuellen Sektor vorgesehen sind, haben unmittelbare Auswirkungen auf die Funktionen und Verwendung von Smart-TV-Geräten. Das ist etwa bei Regulierung im Kommunikationsbereich der Fall, die für die zugrundeliegende Infrastruktur wie das Internet von Bedeutung ist und damit einen Schutz beim Informationsaustausch gewährleistet. In den EU-Richtlinien für den Kommunikationssektor liegt der Schwerpunkt auf Zugangsberechtigung, elektronischen Programmführern und Schnittstellen. Da diese Mechanismen immer mehr mit Entscheidungen der Nutzer und mit der Auffindbarkeit von Inhalten zusammenhängen, wächst ihre Bedeutung ständig. Die transaktionalen Aspekte in Verbindung mit Smart-TV-Geräten führen angesichts herkömmlicher Konzepte im Bereich der Rechtsprechung zu Komplikationen. Während im audiovisuellen Sektor die Zuständigkeit der Gerichte im Wesentlichen an das Herkunftsland geknüpft ist, können Verbraucher entsprechend den einschlägigen gesetzlichen Regelungen ihre Rechte in ihrem Heimatstaat geltend machen.
5. Die Aspekte im Zusammenhang mit neuen Erscheinungen wie Smart-TV machen die Bedeutung generischer Instrumente deutlich. Die Datenschutz-Grundverordnung hat direkte Auswirkungen auf die Erfassung, Verarbeitung und Speicherung personenbezogener Daten, die in Verbindung mit Smart-TV-Geräten erhoben werden. Im Hinblick auf den Anwendungsbereich von Gesetzen zum Datenschutz sind nicht die Definitionen der Kategorien regulierter Dienste relevant, sondern es geht darum, ob personenbezogene Daten verarbeitet werden und wer der für die Verarbeitung zuständige Verantwortliche ist. Gleichzeitig wird in den Datenschutzgesetzen nicht auf die besondere Rolle und Funktion audiovisueller Mediendienste für die Gesellschaft und die Demokratie eingegangen, und es sind auch keine besonderen Schutzmaßnahmen für Nutzer audiovisueller Dienste vorgesehen, die diese über Smart-TV-Geräte in Anspruch nehmen.
6. Auch Grundrechte haben Einfluss auf die Entwicklung des regelungstechnischen und politischen Umfelds; sie dienen der Orientierung, wenn es um die Frage geht, wie Staaten einen wirksamen Schutz der individuellen Rechte auf Meinungsfreiheit, Privatleben und Datenschutz gewährleisten können. Zu einem wirksamen Schutz dieser Rechte gehört notwendigerweise eine Reihe von negativen und positiven Pflichten für Staaten. Relevante positive Pflichten könnten Auswirkungen auf die Aktivitäten einer Reihe von Akteuren des Smart-TV-Ökosystems haben, soweit diese Aktivitäten Grundrechte beeinträchtigen.
7. In der nahen Zukunft werden Smart-TV-Geräte - *totum pro parte* - zu großen Herausforderungen. Dies gilt sowohl für die Industrie und die Nutzer bezüglich der Dienste als auch für die Regulierung und die Politik. Es gilt, die stark zersplitterte Regelungslandschaft aus einer ganzheitlichen Perspektive zu bewerten. Das wird bei der Prüfung, ob alle relevanten Aspekte konsequent berücksichtigt worden sind, helfen. Eine solche Analyse könnte ergeben, dass bestimmte Instrumente veraltetet sind und abgeschafft oder geändert werden müssen. Da Smart-TV-Geräte gezeigt haben, wie schnell sich die Landschaft verändern kann, könnte ein eher normativer Ansatz erforderlich sein, denn Regeln in Stein zu meißeln entspricht nicht der dynamischen Entwicklung des Sektors. Allgemeine Instrumente führen oftmals zu einem eher normativen Ansatz, setzen aber mehr Engagement im Hinblick auf die Anwendung und Umsetzung voraus. Dadurch ergeben sich

Herausforderungen an die Regulierer: Medien-, Datenschutz- und Verbraucherschutzbehörden müssen zusammenarbeiten und ihre Maßnahmen koordinieren. Koordinierung dürfte in vielerlei Hinsicht zu Fortschritten führen, denn der Aufbau eines Rahmens für Zwecke der Politik und Regulierung, bei dem sämtliche Aspekte berücksichtigt sind, wäre zu utopisch, zu zeitaufwendig und weder im Interesse der Diensteanbieter noch der Nutzer.

# EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

Im Dezember 1992 in Straßburg eingerichtet, hat die Europäische Audiovisuelle Informationsstelle zur Aufgabe, Informationen über den europäischen audiovisuellen Sektor zu sammeln, aufzubereiten und zu veröffentlichen.
Als öffentliche europäische Einrichtung umfasst sie derzeit 41 Staaten sowie die Europäische Union, die durch die Europäische Kommission vertreten wird. Die Informationsstelle ist ein Teil des Europarats und arbeitet mit diversen Partnern, Berufsverbänden und einem Korrespondentennetzwerk zusammen.

## Zu den Tätigkeitsschwerpunkten der Europäischen Audiovisuellen Informationsstelle gehören:

- der Jahrbuch-Online-Service,
  www.yearbook.obs.coe.int
- das Herausgeben von Publikationen wie Newslettern und Berichten
  www.obs.coe.int/publications
- ein umfassendes Informationsangebot über ihre Internetseite
  www.obs.coe.int
- Konferenzbeiträge
  www.obs.coe.int/events

## Die Informationsstelle bietet darüber hinaus einen kostenlosen Zugang zu Datenbanken an:

### IRIS Merlin
Datenbank für juristische Informationen von Relevanz für den audiovisuellen Sektor in Europa
www.merlin.obs.coe.int

### MAVISE
Datenbank zu Fernseh- und audiovisuellen Abrufdiensten und Unternehmen in Europa
www.mavise.obs.coe.int

### AVMSDatabase
Datenbank über die Umsetzung der Richtlinie in nationale Gesetzgebung
www.avmsd.obs.coe.int

### LUMIERE
Datenbank über Kinobesucherzahlen in Europa
www.lumiere.obs.coe.int

**Europäische Audiovisuelle Informationsstelle**
76 Allée de la Robertsau – 67000 Strasbourg – France
Tel.: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: info.obs@coe.int

IRIS Spezial

# Smart TV und Datenschutz

Samsung hat die Eigentümer ihrer Smart-TV-Geräte gewarnt, dass die Spracherkennung des Systems möglicherweise ihre privaten Unterhaltungen aufzeichnet und an Dritte weitergibt. Dieses „Bad Buzz" fällt in eine Zeit, in der Brüssel mit der Datenschutzgrundverordnung (DSGV) bevorstehende neue Gesetzgebung präzisiert, die uns vor Missbrauch und Zweckentfremdung unserer personenbezogenen Daten und Big Data zum Verbraucherverhalten, die von intelligenten Geräten wie Fernsehern gesammelt werden, schützen soll. Die Europäische Audiovisuelle Informationsstelle als Teil des Europarats in Straßburg verfolgt diese Entwicklungen und hat diesen IRIS *Spezial* Bericht mit dem Titel „Smart TV und Datenschutz" veröffentlicht.

Es ist eine Gemeinschaftspublikation der in Straßburg ansässigen Informationsstelle und ihrer Partnerinstitution, dem niederländischen Institut für Informationsrecht (IViR in Amsterdam). Der Bericht gab bereits den Anstoß für einen Fachworkshop in Dezember 2015 in Straßburg, der sich mit „den Grauzonen zwischen Medienregulierung und Datenschutz" befasste.

EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

EUR 49 - ISBN 978-92-871-8240-1