„Digitaler Kodex“

Zum Änderungsbedarf des Rechtsrahmens aufgrund der Konvergenz

Studie im Auftrag der

Aktionslinie Hessen-IT

des

Hessischen Ministeriums für Wirtschaft, Energie, Verkehr und Landesentwicklung

von

Prof. Dr. Joachim Scherer / Dr. Lukas Feiler / Caroline Heinickel / Dr. Holger Lutz

Baker & McKenzie

Frankfurt a.M., 22.4.2015

Inhalt

I. Einleitung: Zur Problemstellung und zum Gegenstandsbereich der Studie

Die zunehmende Konvergenz von Netzen, Plattformen, Diensten und Endgeräten der elektronischen Kommunikation, der Angebote und der Märkte scheint eine Konvergenz auch des Rechts zu erfordern.[1]

Ob und wie der geltende rechtliche Rahmen angesichts der Konvergenz angepasst werden sollte, ist Gegenstand dieser Studie.

Ihr Anspruch ist nicht der einer umfassenden Analyse der europarechtlichen, verfassungsrechtlichen, medien-, telekommunikations-, daten-, urheber- und verbraucherschutzrechtlichen Regelungen, die „zusammenwachsen" müssten,[2] damit man von einer „Konvergenz des Rechts" der elektronischen Kommunikation sprechen könnte.

Ziel dieser Studie ist es vielmehr, mit Blick auf ausgewählte Regelungsgegenstände und -materien (insbesondere des TKG und des TMG) sowie neuere Regelungsvorhaben (insbesondere den Entwurf eines IT-Sicherheitsgesetzes[3] und die geplante EU-Datenschutzgrundverordnung[4]) zu klären, ob es angesichts der im Folgenden (keineswegs abschließend) identifizierten, spezifischen Herausforderungen der Konvergenzentwicklung (dazu unten, 2.) Anpassungs- und Optimierungsbedarf gibt.

1. Konvergenz: Begriff und rechtliche Rahmenbedingungen

Der Begriff „Konvergenz" ist sprachlich „vielschichtig"[5]; *Latzer* stellt zutreffend fest:

> „Altogether, convergence is a fuzzy, multipurpose term that fulfils different functions … As an *analytical bracket*, it bridges and integrates both different disciplinary discourses on media change and conflicting detailed processes of convergence and divergence as two sides of the same trend. As a *metaphor*, it reduces the complexity of media change, and as a „*rhetorical tool*" … it might be used to convince stakeholders of certain reforms."[6]

Im Kontext der Telekommunikations- und Medienpolitik ist „Konvergenz" vor allem eine Metapher für komplexe technische und ökonomische Transformationsprozesse.

---

1 Siehe zu einer früheren Phase dieser Diskussion die Beiträge zum 64. Deutschen Juristentag und in dessen Vorfeld zum Thema „Konvergenz der Medien - Sollte das Recht der Medien harmonisiert werden?", u.a. G. Gounalakis, Gutachten zum 64. Deutschen Juristentag, Band I, Teil C, insbes. S. C 12 ff; G. Spindler, ebd., Bd. II/1, insbes. S. 85 ff; B. Holznagel, Konvergenz der Medien - Herausforderung an das Recht, NJW 2002, S. 2351 ff.

2 Zur Konvergenz als einem Prozess des „Zusammenwachsens" oder „Verschmelzens" s. B. Holznagel, Konvergenz der Medien - Herausforderung an das Recht, NJW 2002, 2351, 2352; G. Gounalakis, Gutachten zum 64. Deutschen Juristentag, Bd. I, Teil C, S. C 12; s. auch M. Latzer, Convergence, co-evolution and complexity in European communications policy, Working Paper - Media Change & Innovation Division, IPMZ, University of Zurich, May 2013, S. 1 („blurring lines between traditional communication modes … and blurring boundaries between their respective sub-sectors telecommunications and broadcasting").

3 S. https://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile, zuletzt abgerufen am 7.4.2015.

4 http://www.bundesrat.de/SharedDocs/drucksachen/2014/0501-0600/550-14(B).pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 7.4.2015.

5 So zutr. G. Gounalakis, Gutachten zum 64. Deutschen Juristentag, Bd. I, Teil C, S. C 12.

6 M. Latzer, Convergence, co-evolution and complexity in European communications policy, Working Paper - Media Change & Innovation Division, IPMZ, University of Zurich, May 2013, S. 2.

a. Konvergenz als Metapher

In der telekommunikations- und medienpolitischen Debatte der letzten 25 Jahre in Europa hat „Konvergenz“ unterschiedliche technische und ökonomische Transformationsprozesse bezeichnet: Die Verknüpfung von Computern und Telekommunikation, für die *Simon Nora* und *Alain Minc* 1978 den Begriff „Telematik“ prägten[7], war ein erster Konvergenzprozess; das 1997 veröffentlichte Grünbuch der Europäischen Kommission mit dem programmatischen Titel „Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologien und ihre ordnungspolitischen Auswirkungen: Ein Schritt in Richtung Informationsgesellschaft“[8] stand am Anfang eines tiefgreifenden Reformprozesses, der den Telekommunikationssektor und den Mediensektor erfasste.[9]

Für den Telekommunikationssektor wurde mit dem EU-Richtlinienpaket 2002[10] der Grundsatz der Technologieneutralität eingeführt (Art. 8 Abs. 1 UAbs. 1 Rahmen-RL), wonach die Mitgliedstaaten dafür zu sorgen haben, „dass die nationalen Regulierungsbehörden bei der Wahrnehmung [ihrer] regulatorischen Aufgaben, insbesondere der Aufgaben, die der Gewährleistung eines wirksamen Wettbewerbs dienen, weitestgehend berücksichtigen, dass die Regulierung technologieneutral sein sollte“. Damit wurden sämtliche elektronischen Telekommunikationsnetze[11], d.h. Übertragungssysteme, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen einer grundsätzlich einheitlichen, „technologieneutralen“ Telekommunikations-Regulierung unterworfen.

Für den Mediensektor wurde mit der Richtlinie über audiovisuelle Mediendienste vom 11.12.2007 („AMVD-Richtlinie“),[12] ein Konzept technologieneutraler, „abgestufter Regulierung“ umgesetzt,[13] wonach die konvergierenden audiovisuellen Mediendienste

---

7 S. Nora/A. Minc, L'informatisation de la société, 1978, Paris, S. 11: „Cette imbrication croissante des ordinateurs et des télécommunications - que nous appelerons la „télématique“ ... - ouvre un horizon radicalement neuf“.

8 KOM (97) 623.

9 S. zum Folgenden auch B. Holznagel, Grünbuch Konvergenz der Medien 2013, MMR 2014, S. 18, 19.

10 Richtlinie 2002/21/EG v. 7.3.2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, ABl. EU L 108/33 vom 24.4.2002 („Rahmen-RL“), Richtlinie 2002/20/EG v. 7.3.2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste, ABl. EU L 108/21 vom 24.4.2002 („Genehmigungs-RL“), Richtlinie 2002/22/EG v. 7.3.2002 über den Universaldienst und Nutzungsrechte bei elektronischen Kommunikationsnetzen und -diensten, ABl. EU L 108/33 vom 24.4.2002 („Universaldienst-RL“), Richtlinie 2002/19/EG v. 7.3.2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen und deren Zusammenschaltung („Zugangs-RL“), ABl. EU L 108/33 vom 24.4.2002 sowie Richtlinie 2002/58/EG v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EU L 201/37 vom 31.7.2002 („Datenschutz-RL“), s. dazu J. Scherer, Die Umgestaltung des europäischen und deutschen Telekommunikationsrechts durch das EU-Richtlinienpaket, K&R 2002, S. 273 ff., 329 ff., 385 ff.

11 Zum Folgenden s. die Legaldefinition in Art. 2 lit. a Rahmen-RL.

12 Richtlinie 2007/65/EG v. 11.12.2007, ABl. EU L 332/27 vom 18.12.2007; s. dazu krit. W. Schulz, Medienkonvergenz light - Zur neuen Europäischen Richtlinie über audiovisuelle Mediendienste, EuZW 2008, S. 107 ff.

13 Dazu im einzelnen W. Schulz, Medienkonvergenz light - Zur neuen Europäischen Richtlinie über audiovisuelle Mediendienste, EuZW 2008, 107, 108.

unabhängig davon, auf welchem Endgerät sie empfangen werden, abgestuft nach ihrer Wirkung auf den Empfänger reguliert werden.[14]

In ihrem 2013 vorgelegten „Grünbuch über die Vorbereitung auf die vollständige Konvergenz der audiovisuellen Welt“[15] betrachtet die Kommission Konvergenz „als fortschreitendes Zusammenwachsen herkömmlicher Rundfunkdienste mit dem Internet“:[16]

> „Dadurch werden ergänzende Inhalte nicht nur über Fernsehgeräte mit zusätzlicher Internetanbindung durch Set-Top-Boxen zur „OTT“-Übermittlung von Videoinhalten (Over The Top - OTT), sondern auch über audiovisuelle Mediendienste verfügbar, die auf PCs, Laptops oder Tablet-Computern und anderen mobilen Geräten bereitgestellt werden“.

Die Grenzen zwischen linearen und nicht-linearen audiovisuellen Mediendiensten[17] - eine regulierungsrechtliche Unterscheidung, die für die AVMD von 2007 noch grundlegend war - „verschwimmen“ - wie die Kommission sechs Jahre später feststellte - „rasch“.[18]

Das Grünbuch zur Konvergenz der Medien von 2013 hat sein Ziel, „eine breit angelegte öffentliche Debatte über die Auswirkungen des gegenwärtigen Wandels der audiovisuellen Medienlandschaft“ anzustoßen,[19] kaum erreicht und hat bislang nicht zu Rechtsetzungsmaßnahmen geführt.

Im Mai 2015 will die Juncker-Kommission eine „Strategie für den digitalen Binnenmarkt“ vorlegen, die sich auf drei Bereiche konzentrieren wird:[20]

- Besserer Zugang zu digitalen Gütern und Dienstleistungen für Verbraucher und Unternehmen, wozu eine „Modernisierung des Urheberrechts“ zählen soll.
- Gestaltung der Rahmenbedingungen für den Erfolg digitaler Netze und Dienstleistungen, darunter die Verabschiedung der Datenschutzgrundverordnung.
- Schaffung einer europäischen digitalen Wirtschaft mit langfristigem Wachstumspotential: Hierzu zählen u.a. die Unterstützung der Einführung neuer Technologien und der Umstellung auf ein intelligentes Industriesystem („Industry

---

14 Vgl. COM (2013) 231 final, S. 13 mit Hinweisen auf neuere Entwicklungen.

15 COM (2013) 231 final v. 24.4.2013, hierzu krit. B. Holznagel, Grünbuch Konvergenz der Medien 2013, MMR 2014, S. 18 ff.

16 COM (2013) 231 final, S. 3, auch zum Folgenden.

17 Audiovisuelle Mediendienste sind Dienstleistungen, für die ein Mediendiensteanbieter die redaktionelle Verantwortung trägt und deren Hauptzweck die Bereitstellung von Sendungen zur Information, Unterhaltung oder Bildung der allgemeinen Öffentlichkeit über elektronische Kommunikationsnetze ist. Bei diesen audiovisuellen Mediendiensten handelt es sich entweder um Fernsehprogramme oder um audiovisuelle Mediendienste auf Abruf (etwa Video-on-Demand-Angebote oder Beiträge in Mediatheken), siehe Art. 1 Abs. 1 lit.a i) AVMD-Richtlinie.

18 COM (2013) 231 final, S. 3, s. auch 13 f.

19 COM (2013) 231 final, S. 3, u.a. B. Holznagel, Grünbuch Konvergenz der Medien 2013, MMR 2014, S. 18 ff. Siehe die Zusammenfassung der im Rahmen der öffentlichen Konsultation zu dem Grünbuch eingegangenen Beiträge in: European Commission, Summaries of the replies to the public consultation launched by the Green Paper „Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values“, abrufbar unter: http://ec.europa.eu/information_society/newsroom/ cf/dae/document.cfm?action=display&doc_id=6761, zuletzt abgerufen am 7.4.2015.

20 Europäische Kommission, Pressemitteilung IP-15-4653 vom 25. März 2015.

4.0“)[21] und die Adressierung von Fragen im Zusammenhang mit „Big Data“, insbesondere die Frage nach dem Eigentum an den Daten.[22]

Die Metapher „Konvergenz“ kommt in den bisher vorliegenden Vorentwürfen der „Strategie für den digitalen Binnenmarkt“ (noch) nicht vor.

b. Konvergenz aus technologischer Sicht

Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) hat in einem Bericht über Konvergente Dienste[23] Konvergenz als Prozess technologischer Veränderungen analysiert, die dazu führen, dass unterschiedliche Netze in die Lage versetzt werden, vielfältige (Kommunikations-)Dienste zu erbringen.[24]

Zu Zwecken der Systematisierung konvergenter Dienste kann unterschieden werden zwischen

- bestehenden Diensten der elektronischen Kommunikation, die über unterschiedliche Netze erbracht werden,
- (technisch und qualitativ) verbesserten Diensten und
- neuen Diensten.

Zur erstgenannten Gruppe von konvergenten Diensten zählen

- konvergente Dienste im Bereich der Festnetztelefonie (wie Sprachdienste auf Grundlage des Internet-Protokolls - VoIP -, Home-Zone-Dienste, WiFi Zugangsdienste),
- konvergente Dienste im Bereich der Mobilfunkkommunikation (wie z.B. Dienste auf der Grundlage von Femto-Zellen, die eine verbesserte Mobilkommunikation in geschlossenen Räumen ermöglichen),
- konvergente Dienste zur Ermöglichung des Zugangs zum Internet (z.B. über USB-Modems, 3G Dongles oder WiFi-Zugänge).

Zu der zweitgenannten Gruppe von technisch und qualitativ verbesserten (enhanced) Diensten zählen z.B. „HD Voice“ auf der Basis von 3 G-Netzen oder High Definition IPTV.[25]

Zu den neuen konvergenten Diensten zählt BEREC

- Cloud Computing, d.h. „a way to externalize services that have usually been provided internally by companies themselves. The cloud environment allows for

---

21 S. hierzu H. Kagemann et al., Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0, abrufbar unter http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf, zuletzt abgerufen am 20.3.2015 und noch unter II.1.b.(1).

22 Vgl. M. Dorner, Big Data und „Dateneigentum” – Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617.

23 BEREC, Report on convergent services, BoR (10) 65, 2010.

24 BEREC, BoR (10) 65, S. 2: „... [C]onvergence can be described as the technological improvements by which a number of networks arise with enhanced capabilities to provide multiple services“.

25 „Big data refers to large amounts of data produced very quickly by a high number of diverse sources“, s. https://ec.europa.eu/digital-agenda/en/content-and-media/data, zuletzt abgerufen am 7.4.2015; J.-P. Ohrtmann/S. Schwiering, Big Data und Datenschutz - Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984.

infrastructures, platforms, software etc. to be provided from an external network where the services are deployed as a kind of outsourcing“[26],

- Machine-to-Machine-(M2M-)Dienste, verstanden als „a generic concept that indicates the exchange of information in data format between two remote machines, through a mobile or fixed network, without human intervention“[27] sowie
- die elektronische Geldbörse („E-wallet“), d.h. „a service based on NFC (Near Field Communications) technology for mobile payments directly at the point of sale terminals (POS) which are installed in stores.“[28]

2. Digitaler Kodex: Begriff und rechtliche Gestaltungsoptionen

Einen „Digitalen Kodex“ im Sinne einer strukturierten Sammlung von Rechtsregeln gibt es bislang weder für das EU-Recht noch für das nationale Recht.[29] Die Europäische Kommission hat in einer - werbewirksam - als „Kodex der EU-Online-Rechte“ bezeichneten Veröffentlichung[30] bestehende „Rechte und Prinzipien“ zusammengefasst. Die Einleitung dieses „Kodex“ beschreibt das Dilemma der Verrechtlichung konvergenter Netze und Dienste im Mehrebenensystem von EU und Mitgliedstaaten recht präzise:

> „Die…Rechte und Prinzipien, [welche die Bürgerinnen und Bürger beim Zugang zu und der Nutzung von Online-Netzen und -Diensten schützen] sind nicht immer leicht verständlich, da sie sich nicht ausschließlich auf das digitale Umfeld beziehen und über verschiedene Richtlinien, Verordnungen und Übereinkommen in den Bereichen elektronische Kommunikation, E-Commerce und Verbraucherschutz verteilt sind. Darüber hinaus fallen diese Rechte und Prinzipien in vielen Fällen unter die Mindestharmonisierung, d.h. die Mitgliedstaaten haben die Möglichkeit, über die nach EU-Recht zu erfüllenden Mindestanforderungen hinauszugehen.“[31]

Die vorliegende Studie betrachtet einige der Regelungskategorien, Rechtsregeln und Gestaltungsprinzipien des bestehenden Kodex und stellt einige geplante Änderungen[32] auf den Prüfstand.

3. Zum Gang der Untersuchung

Ausgangspunkt der Studie ist eine Bestandsaufnahme einiger der Herausforderungen, vor denen der europäische und der nationale Gesetzgeber sowie Regulierungsbehörden angesichts der Konvergenz von elektronischen Diensten und Infrastrukturen stehen. Die Bestandsaufnahme erhebt keinen Anspruch auf Vollständigkeit, sondern konzentriert sich auf ausgewählte konvergente Dienste (dazu II.1. und 3.), die Sicherheit (telekommunikationsgestützter) IT-Systeme (dazu II.2.) und die Problematik der Rechtsdurchsetzung gegen ausländische Verletzer von Urheberrechten (dazu II.4.).

In einem zweiten Schritt wird untersucht, ob und inwieweit die geltenden Regeln des nationalen und EU-Rechts sowie aktuelle Gesetzgebungsvorhaben (insbesondere der Entwurf des IT-

---

[26] BEREC, BoR (10) 65, S. 6.

[27] BEREC, BoR (10) 65, S. 6: „These services are used as a means of payment (terminal point of sale), tele-management and tele-measurement in the distribution of utilities (water, power supply etc.), safety and management of alarms, management of fleets, tele-medicine, automotive and emergencies and tele-maintenance of vending machines“. S. dazu noch unten II.1.b.(1).

[28] BEREC, BoR (10) 65, S. 6.

[29] Zur Diskussion auf nationaler Ebene s. Deutsches Institut für Vertrauen und Sicherheit im Internet - DIVSI/iRightslab - (Hrsg.), Braucht Deutschland einen Digitalen Kodex? Verantwortung, Plattformen und soziale Normen im Internet, Hamburg 2014.

[30] Europäische Kommission, Kodex der EU-Online-Rechte, Luxemburg 2012, S. 2.

[31] Europäische Kommission, Kodex der EU-Online-Rechte, Luxemburg 2012, S. 2.

[32] S. dazu unten III.2. und III.3.d.

Sicherheitsgesetzes (dazu IV.2.) und die geplante EU-Datenschutzgrundverordnung, (dazu III.3.d.) geeignet sind, den zuvor identifizierten Regelungsproblemen gerecht zu werden.

Hieraus ergeben sich Empfehlungen für eine Optimierung des Rechtsrahmens (dazu IV.).

II. Herausforderungen der Digitalisierung von Wirtschaft und Gesellschaft - Eine Bestandsaufnahme

Die technisch bedingte Konvergenz von Infrastrukturen, Diensten und Endgeräten der elektronischen Information und Kommunikation wirft die Frage nach der Tauglichkeit der überkommenen rechtlichen Kategorien zur Erreichung der mit ihnen verfolgten Regelungsziele auf, zu denen der Schutz der öffentlichen Sicherheit, Verbraucher- und Datenschutz, Schutz des chancengleichen Wettbewerbs und - für konvergente Dienste mit „Meinungsrelevanz" - die Sicherung der Informations- und Kommunikationsfreiheiten sowie der Meinungsvielfalt zählen:

Dienste der Machine-to-Machine-(M2M-)Kommunikation erfordern es, die auf die Kommunikation von Menschen zugeschnittenen Rechtsregeln für „traditionelle" Kommunikationsdienste anzupassen, um den spezifischen Charakteristika dieser neuartigen Dienste angemessen Rechnung zu tragen (dazu 1.a.).

Die Verbreitung von Internetzugängen und Geräten mit der Möglichkeit zur Standortbestimmung führt zu einem wachsenden Interesse der Wirtschaft an standortbezogenen Diensten („Location Based Services") und einer schnell wachsenden Vielfalt standortbezogener Dienste, die den Schutz der Privatsphäre der Nutzer vor neue Herausforderungen, insbesondere an Information und Einwilligung, stellt (dazu 1.b.).

Ähnliches gilt für Unified Communications Services, in ihrer Ausprägung als sog. Messenger-Dienste, die zunehmend als Ersatz für SMS und auch Telefonie genutzt werden und bei denen daher insbesondere der Inhalt der Kommunikation der Nutzer vertraulich bleiben sollte (dazu 1.c.).

Die zunehmende Vernetzung sämtlicher Bereiche von Wirtschaft und Gesellschaft, die durch die Konvergenz der Netze und Dienste ermöglicht und getrieben wird, hat zur Folge, dass Infrastrukturen, von denen das Funktionieren des Gemeinwesens abhängt (sog. „Kritische Infrastrukturen"), in hohem Maße auf eine verfügbare und sichere IT-Infrastruktur angewiesen sind. Damit wird die Gewährleistung von IT-Sicherheit zu einer dringend zu bewältigenden gesetzgeberischen Aufgabe auf nationaler wie auf supranationaler Ebene (dazu 2.).

Die Konvergenzentwicklung hat vielfältige „Over the top" (OTT)-Angebote[33] im Internet ermöglicht, deren Geschäftsmodelle grundsätzliche Fragen des Umgangs mit personenbezogenen Daten, aber auch Fragen nach der Durchsetzung insbesondere daten- und verbraucherschutzrechtlicher Regelungen aufwerfen (dazu 3. und 4.).

---

[33] Hiermit wird die Bereitstellung von Audio-, Video- oder sonstigen Inhalten sowie von Kommunikationsfunktionen (wie z.B. Textnachrichten) ohne die unmittelbare Beteiligung von Internet-Access-Providern bezeichnet; die Dienste des Internet-Access-Providers werden zwar verwendet, um ein OTT-Angebot in Anspruch zu nehmen, der Internet-Access-Provider hat allerdings weder die Möglichkeit, das OTT-Angebot zu kontrollieren, noch ist er für dieses verantwortlich. Vgl. M. Schneider, WhatsApp & Co. - Dilemma um anwendbare Datenschutzregeln - Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZR 2014, 231, 232; vgl. BEREC, Work Programme 2013, BEREC Board of Regulators, 7.12.2012, BoR (12) 142, 23, verfügbar unter http://berec.europa.eu/files/document_register_store/2013/1/BoR_%2812%29_142_BEREC_WP-2013_f.pdf, zuletzt abgerufen am 30.3.2015, wonach „OTT player" vorläufig als Marktteilnehmer definiert werden, welche sich auf die Steuerung und den Vertrieb von Inhalten fokussieren, ohne eine Beziehung mit einem bestimmten Netzwerk bzw. Telekommunikationsanbieter einzugehen. Eine exakte Definition des Begriffs „OTT-Anbieter" wird BEREC in einem noch im Jahre 2015 vorzulegenden Bericht über OTT-Anbieter vornehmen, vgl. BEREC, Work Programme 2015, BEREC Board of Regulators, 4.12.2014, BoR (14) 185, 16, verfügbar unter http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/4779-work-programme-2015-berec-board-of-regul_0.pdf.

1. Konvergenz der rechtlichen Steuerungskategorien?

a. Telemediendienste und Telekommunikationsdienste

Der geltende Rechtsrahmen unterscheidet sowohl auf nationaler[34] als auch auf EU-Ebene[35] strikt zwischen dem Transport von Kommunikationsdaten einerseits (d.h. dem Bereich der Telekommunikationsdienste bzw. der elektronischen Kommunikationsdienste) und dem Inhalt der Kommunikation (d.h. dem Bereich der Telemediendienste bzw. Dienste der Informationsgesellschaft).

Bislang wird die Zuordnung von Diensten zu den Kategorien „Telekommunikationsdienst" oder „Telemediendienst" regelmäßig nicht bezogen auf den Dienst in seiner Gesamtheit vorgenommen,[36] sondern Diensteangebote werden in Elemente unterteilt, die „ganz oder überwiegend in der Übertragung von Signalen" bestehen (d.h. Telekommunikationsdienste darstellen) und Elemente, deren Schwerpunkt die „Bereitstellung von Inhalten"[37] ist (und die damit den Telemediendiensten zugeordnet werden).

Die rechtlichen Steuerungskategorien „Telekommunikation" und „Telemedium" sowie die Praxis der Klassifizierung von Diensten nach Maßgabe dieser Kategorien (mit der Konsequenz, dass je unterschiedliche Regelungsregimes anwendbar sind) sollte mit Blick auf die durch die Konvergenz der Netze und Dienste ermöglichten neuartigen Diensteangebote angesichts vielfältiger Abgrenzungsprobleme einer kritischen Überprüfung unterzogen werden.

b. Grenzverwischungen und neue rechtliche Abgrenzungen

Im Folgenden werden die rechtlichen Herausforderungen, die sich mit fortschreitender Konvergenz für die konsistente (telekommunikations- und medien-)rechtliche Behandlung von Telekommunikationsdiensten und Inhaltediensten stellen, anhand dreier Beispiele illustriert: ***Erstens*** wird beschrieben, welche neuen rechtlichen Abgrenzungen sich ergeben, wenn nicht länger Menschen mit Menschen mittels „klassischer" Telekommunikationsmedien (wie z.B. das Telefon), sondern Maschinen mit Maschinen mithilfe des „Internet der Dinge" kommunizieren. ***Zweitens*** setzt sich die Studie mit den Herausforderungen auseinander, die sich aufgrund technologischer Entwicklungen für die Regulierung sog. „Location Based" Services ergeben. ***Drittens*** wird am Beispiel von Messenger-Diensten illustriert, welche Herausforderungen im Grenzbereich zwischen Telekommunikation und Inhaltediensten für die Gewährleistung eines einheitlichen Datenschutzes bestehen.

(1) Internet of Things - die Machine-to-Machine-Kommunikation

Die zunehmende Digitalisierung[38] führt zu einer *„Vernetzung aller Systeme und Dinge"*[39] durch das Internet, es entsteht ein „Internet der Dinge" (*Internet of Things*, IoT)[40]. Die EU-Kommission beschreibt dieses Internet der Dinge wie folgt:

---

34 § 1 TMG, § 3 Nr. 24 TKG.

35 Art. 2 lit. c und Erwägungsgrund 5 Rahmen-RL.

36 Vgl. u.a. F.J. Säcker, in: F.J. Säcker (Hrsg.), TKG-Kommentar, 3. Aufl. 2013, § 3 Rn. 62; R. Schütz, in: M. Geppert/R. Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 3 Rn. 79.

37 Vgl. Erwägungsgrund 10 S. 4 Rahmen-RL.

38 S. zu der damit einhergehenden Bedeutung der IT-Infrastruktur noch unten, 2.

39 Bundesamt für Sicherheit in der Informationstechnologie (BSI), „Die Lage der IT-Sicherheit in Deutschland 2014", Stand November 2014 („BSI Sicherheitsbericht 2014"), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, zuletzt abgerufen am 17.3.2015.

„IoT is a long term technology and market development based on the connection of everyday objects to the Internet. Connected objects exchange, aggregate and process information on their physical environment to provide value added services to end-users, from individuals to companies to society as a whole. IoT has the potential to considerably improve the life of EU citizens by addressing many of today's societal challenges in health, transport, environment, energy etc. It will create tremendous opportunities for innovation-based growth and jobs creation in Europe …".[41]

Im IoT kommunizieren nicht Menschen mit Menschen, sondern vernetzte Objekte untereinander.[42] Die Kommunikation von Maschinen mit Maschinen wird als „Machine-to-Machine-" (oder auch „M2M"-) Kommunikation bezeichnet. Beispiele für die Machine-to-Machine-Kommunikation sind sog. „Smart Grids" und „Smart Meters"[43] im Energiebereich,[44] tragbare Geräte, die unterschiedliche Körperfunktionen ihres Trägers messen,[45] aber auch die „intelligente Fabrik", die Gegenstand des Zukunftsprojekts Industrie 4.0[46] unter der Schirmherrschaft des Bundesministeriums für Bildung und Forschung ist.

Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) definiert die Machine-to-Machine-Kommunikation als

„Austausch von Informationen in einem Datenformat zwischen zwei voneinander entfernten Maschinen ohne menschliche Intervention über Mobile Netzwerke oder Festnetze".[47]

Charakterisierend für die Machine-to-Machine-Kommunikation ist somit, dass Menschen in dem Kommunikationsvorgang entweder keine oder allenfalls eine untergeordnete Rolle spielen. Der Umstand, dass nicht länger Menschen miteinander kommunizieren, führt zu einer Vielzahl regulatorischer Herausforderungen,[48] die wir im weiteren Verlauf der Studie

---

40 S. zum Begriff bereits ITU, Internet Reports 2005, „The Internet of Things", Executive Summary, S. 3, abrufbar unter http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf, zuletzt abgerufen am 20.3.2015.

41 EU-Kommission, Report on the Public Consulation on IoT Governance, S. 2, abrufbar unter http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746, zuletzt abgerufen am 17.3.2015. Übersetzung: „IoT ist eine langfristige Technologie und Marktentwicklung, die auf der Verknüpfung von Gegenständen des täglichen Lebens mit dem Internet beruht. Verbundene Objekte tauschen sich aus, sammeln und bearbeiten Informationen über ihre physische Umgebung, um den Endnutzern, angefangen von Einzelpersonen über Firmen bis hin zur Gesellschaft als Ganzes, Mehrwertdienstleistungen zu bieten. Indem IoT eine Vielzahl von gesellschaftlichen Herausforderungen in den Bereichen Gesundheit, Transport, Umwelt, Energie etc. adressiert, hat es das Potential das Leben der EU-Bürger deutlich zu verbessern. IoT wird enorme Möglichkeiten für innovationsbasiertes Wachstum sowie für die Schaffung von Arbeitsplätzen in Europa bieten …"

42 Vgl. zu den unterschiedlichen Kommunikationsformen im IoT EU Kommission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet of Things - An action plan for Europe, 18.6.2009, COM (2009) 278 final, S. 2.

43 Sog. „Intelligente Zähler" i.S.d. §§ 21c ff. Energiewirtschaftsgesetz, EnWG.

44 S. dazu P. Gabriel/K. Gaßner/S. Lange, Das Internet der Dinge – Basis für die IKT-Infrastruktur von morgen, 2010, Berlin, S. 10.

45 Für weitere Beispiele s. EU Kommission, Commission Staff Working Document SEC (2008) 2416 v. 29.9.2008.

46 S. H. Kagemann et al., Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0, abrufbar unter http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf, zuletzt abgerufen am 20.3.2015.

47 The „exchange of information in data format between two remote machines, through a mobile or fixed network, without human intervention"; s. BEREC report on convergent services, BoR (10) 65, 2010, S. 6.

48 S. dazu EU Kommission, Report on the public consultation on IoT governance, 16.1.2013, die Berichte der Expertengruppen sind abrufbar unter http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514, zuletzt abgerufen am 20.3.2015. Ausführlich zur Regulierung von Machine-to-Machine-Anwendungen und -Diensten J.

mit Blick auf das steigende Erfordernis der Gewährleistung von IT-Sicherheit[49] sowie das mögliche Erfordernis einer Anpassung der telekommunikationsrechtlichen Regelungen,[50] die bislang im Wesentlichen auf die Kommunikation von Menschen zugeschnitten sind, weitergehend beleuchten werden.

Dienste der Machine-to-Machine-Kommunikation unterscheiden sich auch unter einem weiteren Aspekt grundlegend von „klassischen" Telekommunikationsdiensten. Während bei klassischen Telefonie- und Internetzugangsdiensten die Bereitstellung der Möglichkeit zur Kommunikation (d.h. das Zur-Verfügung-Stellen von Konnektivität) den Kern des Geschäftsmodells ausmacht, hat die Verfügbarkeit von Konnektivität bei Geschäftsmodellen der Machine-to-Machine-Kommunikation nur eine untergeordnete, dienende Funktion. So ist beispielsweise Zweck eines „Smart Meters", dem Kunden und dem Energieversorger Aufschluss über den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit seines Anschlusses zu geben.[51] Über eine Telekommunikationsverbindung übermittelt die „in ein Kommunikationsnetz eingebundene Messeinrichtung" (§ 21d Abs. 1 EnwG) diese Daten an die IT-Systeme des Energieversorgers des Kunden. Im Vordergrund der Dienstleistung steht die „Erfassung der elektrischen Energie" in einer Weise, „die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt", und nicht die telekommunikationsgestützte Übermittlung der diesbezüglichen Daten.

Ein weiteres Beispiel für die lediglich „dienende" Funktion der Konnektivität sind sog. „vernetzte Automobile" (oder „Connected Cars"). Connected Cars sind dadurch gekennzeichnet, dass sie (typischerweise) mit fest verbauten SIM-Karten ausgestattet sind (sog. „embedded SIM-cards"), über die eine mobile Datenverbindung[52] zu den IT-Systemen des Fahrzeugherstellers etabliert wird. Mittels dieser Verbindung können Fahrzeugdaten automatisiert an die Systeme des Fahrzeugherstellers übermittelt werden, die zur Bereitstellung u.a. von Diagnostik- und Sicherheitsdienstleistungen genutzt werden können. Dem Kunden wird die Bereitstellung der Datenverbindung regelmäßig nicht gesondert in Rechnung gestellt, diese Verbindung ist vielmehr ein untergeordneter Bestandteil der von dem Kunden in Anspruch genommenen Diagnostik- und Sicherheitsdienstleistungen. Für die rechtliche Einordnung[53] der Machine-to-Machine-Dienste ist entscheidend, ob der dem Kunden angebotene Dienst insgesamt oder die einzelnen Elemente der Dienstleistung jeweils gesondert betrachtet werden müssen (dazu unten, III.1.a.).

Scherer/C. Heinickel, Regulating Machine-to-Machine Applications and Services in the Internet of Things, ENLR 2014, S. 141 ff.

49 III.2.

50 III.1.a.

51 § 21d Abs. 1 EnWG.

52 Connected Car-Angebote beinhalten zum Teil auch Sprachverbindungen, die es dem Kunden ermöglichen, „point-to-point" eine Verbindung beispielsweise zu einem Call- oder Service-Center des Anbieters aufzubauen. Diese durch einen Menschen initiierte Kommunikationsverbindung wird im Rahmen dieser Studie nicht als Machine-to-Machine-Kommunikation i.S.d. oben dargestellten Definition behandelt, sondern der Mensch-zu-Mensch-Kommunikation zugeordnet.

53 Im Rahmen dieser Studie gehen wir nicht auf die weiteren rechtlichen Fragestellungen ein, die sich insbesondere mit Blick auf die globale Bereitstellung von M2M-Diensten und die extra-territoriale Nutzung von Nummern ergeben; s. dazu J. Scherer/C. Heinickel, Regulating Machine-to-Machine Applications and Services in the Internet of Things, ENLR 2014, 141, 143 ff.

(2) Location Based Services

Standortdaten[54] wurden bis vor wenigen Jahren noch vorwiegend von speziellen Dienst- und Gerätekategorien verarbeitet. Beispielsweise dienten Navigationsgeräte vor allem einem Zweck - der Navigation - und Ortungsdienste wurden vor allem von Mobilfunkanbietern bereitgestellt (zum Beispiel für die Verbindung mit der nächsten Taxi-Zentrale).

Die technologische Entwicklung hat zu einer Verschiebung der Art und Weise der Erhebung von Standortdaten geführt: Der Standort eines Mobiltelefons lässt sich seit jeher durch den Netzbetreiber ermitteln, indem er auswertet, in welchen Funkzellen das Mobiltelefon eingebucht ist. Heute wird der Standort aber meist anders bestimmt. Programme auf Mobiltelefonen („Apps“) bedienen sich zur Standortbestimmung beispielweise der GPS-Sensoren oder auch des WLAN-Empfängers. Nach der Standortermittlung werden die Standortdaten häufig zur weiteren Verarbeitung über das Internet an Server des Anbieters der App übertragen.[55] Neben Mobiltelefonen verfügen inzwischen auch zahlreiche andere Geräte über GPS-Sensor und Internetzugang (zum Beispiel Navigationsgeräte, Digitalkameras, etc.), so dass auch auf diesen Location Based Services angeboten werden können. Technisch wird dabei meist so vorgegangen wie bei Smartphone-Apps.

Standortbezogene Dienste, wie z.B. Navigationsdienste, Taxiruf-Dienste, Stadt- und Hotelführer, aber auch Spiele[56], verzeichnen ein hohes Wachstum, das sich voraussichtlich fortsetzen wird.[57]

Auch die Wirtschaft zeigt ein stetig wachsendes Interesse an Standortdaten. Sie dienen zum einen der Optimierung betrieblicher Abläufe, etwa beim Flottenmanagement und in der Logistik- oder in der Sicherheitsbranche. Darüber hinaus kann die Auswertung von Standortdaten zur Verbesserung von Dienstleistungen dienen, etwa der Optimierung von Verkehrsprognosen oder der Erkennung von Straßensperrungen bei Navigationsdiensten. Schließlich spielen Standortdaten eine zunehmende Rolle bei der Ansprache (potentieller) Kunden. So lassen sich Standortdaten nutzen, um zielgerichtet Werbung auf dem Smartphone einzublenden oder auch Konsumwünsche des Kunden zu prognostizieren.[58]

Das zunehmende wirtschaftliche Interesse an der Verwertung von Standortdaten hat zur Folge, dass die Methoden zur Standortbestimmung immer vielfältiger werden: Relativ ungenau ist noch das IP-Geo-Tagging, bei dem aus der einem Endgerät zugewiesenen IP-Adresse auf den geographischen Standort geschlossen wird. Dies funktioniert vor allem bei ortsfesten Einrichtungen, die selbst einen IP-Adressraum verwalten, beispielsweise

---

54 Eine Legaldefinition des Begriffs „Standortdaten“ findet sich in § 3 Nr. 19 TKG (vgl. unten, III.1.b.). Der im Text verwandte Begriff ist breiter, um auch das TMG in den Blick nehmen zu können. Unter Standortdaten werden daher, wenn nicht anders vermerkt, alle Daten verstanden, die sich auf den Standort einer individuellen natürlichen Person beziehen oder beziehen lassen.

55 Zu den technischen Aspekten vgl. A. Sachs/M. Meder, Datenschutzrechtliche Anforderungen an App-Anbieter, ZD 2013, 303, 306 f.

56 Die Kategorie der „Augmented Reality“-Spiele, die Elemente der realen Welt mit der Spielwelt verweben, hat mit dem Spiel „Ingress“ der Google-Tochter Niantic Labs auch eine zunehmende öffentliche Wahrnehmung erfahren. Bei Ingress besuchen Spieler zweier Teams mit ihren Smartphones Orte der realen Welt, um sie - im Spiel - für ihre Gruppe zu erobern. Voraussetzung dafür ist, dass das Spiel erkennt, an welchem Ort sie sich befinden.

57 Goldmedia GmbH Strategy Consulting im Auftrag der Bayerischen Landeszentrale für neue Medien, Location-based Services Monitor 2014, abrufbar unter http://www.blm.de/files/pdf1/140512_Location-based_Services_Monitor_2014.pdf, zuletzt abgerufen am 30.3.2015, S. 13 u. 52 f.

58 Zum Beispiel könnte einem Kunden, der sich häufig auf einem Tennisplatz aufhält, Sportbekleidung angeboten werden, wenn die Standortdaten des Kunden mit den Adressdaten des Tennisvereins und den Produktdaten des Anbieters verbunden werden.

Universitäten. Andere Methoden verwenden Sendeeinrichtungen unterschiedlicher Netzinfrastrukturen (beispielsweise das Mobilfunknetz oder in der Nähe befindliche WLAN-Stationen) um die Position zu bestimmen; umgekehrt können auch diese Netzinfrastrukturen unter Umständen erkennen, welche Endgeräte sich bei ihnen anmelden, was einen Rückschluss auf die Nutzer in der Nähe bestimmter Sendeeinrichtungen ermöglicht. Schließlich gibt es mit GPS oder Techniken der In-House-Ortung Methoden, die sehr präzise Standortbestimmungen zulassen. Absehbar ist, dass sich auch indirekte Methoden der Standortbestimmung etablieren werden, beispielsweise indem eine Anwendung Bilder von der Umgebung macht und markante Gebäude identifiziert.[59]

Die Erhebung, Verarbeitung und Nutzung von Standortdaten stellt eine besondere Herausforderung für den Schutz der informationellen Selbstbestimmung des Einzelnen dar. Die Analyse von Standortdaten ermöglicht es, vielfältige Informationen über den Betroffenen zu gewinnen. Zum Beispiel kann über den regelmäßigen Aufenthalt nachts und tagsüber auf die Wohnung und die Arbeitsstätte geschlossen werden. Sucht der Betroffene bestimmte Arztpraxen auf, ermöglicht dies evtl. einen Rückschluss auf bestimmte Krankheiten.[60] Auch Hobbies lassen sich ermitteln, zum Beispiel indem die Standortdaten mit den Standorten von Vereinen und Sportstätten abgeglichen werden. Schließlich lassen Standortdaten auch Rückschlüsse auf Freundschaften und Bekanntschaften zu, indem die Standortdaten des Nutzers mit denen anderer Personen abgeglichen werden.[61]

(3) Unified Communications Services, insbesondere Messenger-Dienste

Ein illustratives Beispiel für konvergente Dienste, bei denen die Grenzlinien zwischen Telekommunikations- und Telemediendienst oftmals verschwimmen, sind sog. Messenger-Dienste. Dies sind Dienste, die den Sofort-Austausch von Nachrichten zwischen einem im Voraus festgelegten und zahlenmäßig begrenzten Kreis von Empfängern ermöglichen. Die Nachrichten können dabei neben Text auch jede andere Art von Daten (Bilder, Ton, Videos, Computer-Dateien, etc.) beinhalten. Sofort-Austausch bedeutet, dass die Nachrichten unmittelbar beim Empfänger ankommen und anders als üblicherweise beim E-Mail-Versand kein Abruf notwendig ist (sog. Push-Verfahren).

Messenger-Dienste sind am Markt entweder als eigenständige Anwendungen (wie z.B. WhatsApp) oder als Bestandteil von sog. „Unified Communications Services“[62] verfügbar.

Messenger-Dienste erfreuen sich nach wie vor wachsender Beliebtheit.[63] Dies hängt mit mehreren Faktoren zusammen: Das Bedürfnis zum Austausch kurzer Nachrichten besteht

---

59 Apps mit derartigen Funktionen gibt es bereits seit einigen Jahren, vgl. M. Schubert, Google Goggles: Bilderkennung mit dem Android-Handy, netzwelt.de, 10.12.2009, abrufbar unter http://www.netzwelt.de/news/81352-google-goggles-bilderkennung-android-handy-update.html, zuletzt abgerufen am 2.4.2015.

60 Ausführlich Artikel-29-Datenschutzgruppe, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, WP 185, S. 7 f.; vgl. auch S. Hellmich, Location Based Services - Datenschutzrechtliche Anforderungen, MMR 2002, 152.

61 Vgl. Artikel-29-Datenschutzgruppe, a.a.O. (Fn. 60). So konnte der Fahrdienstvermittler Uber identifizieren, welche seiner Nutzer sich für einen One-Night-Stand trafen; dies allein aus den Daten über Fahrtbuchungen, nicht über eine langfristige Aufzeichnung der Standortdaten; dazu J. Klofta/J. Rest, Uber sammelt Daten über One-Night-Stands der Kunden, 07.01.2015, abrufbar unter: http://www.berliner-zeitung.de/wirtschaft/taxidienst-uber-sammelt-daten-ueber-one-night-stands-der-kunden,10808230,29506654.html, zuletzt abgerufen am 7.4.2015.

62 Der Begriff beschreibt auf der Diensteebene die Verbindung von Echtzeit- und Nicht-Echtzeitkommunikationsdiensten und auf der Infrastrukturebene die Integration von - zuvor getrennter - IT- und Telekommunikationsinfrastruktur; s. dazu H. Lutz/M. Weigl, Unified Communications as a Service, CR 2014, S. 85 f.

offenbar vor allem vom Mobilgerät aus, so dass sich Messenger-Dienste (die es zuvor schon als Desktop-PC-Anwendungen gab) mit der Verbreitung des mobilen Internets und der Smartphones als (kostengünstige) Alternative zum Short-Message-Service der Mobilfunkanbieter durchsetzen konnten.[64] Messenger-Dienste ermöglichen darüber hinaus Zusatznutzen, etwa durch Verschlüsselung, Übertragung kurzer Sprachnachrichten, Priorisierung und Blockierung bestimmter Kontakte usw. Und schließlich sind Messenger-Dienste durch ihre Einbettung in bestehende Soziale Netzwerke Teil eines „Ökosystems" persönlicher Kontakte und Kommunikation.[65] Gegenüber der E-Mail zeichnen sich die Systeme durch die schnelle Zustellung der Nachrichten und die Unmittelbarkeit des Nachrichtenaustauschs aus. Sie dienen inzwischen vielen Nutzern als Ersatz für SMS[66] und wohl auch für Telefonate[67].

Der Markterfolg der Messenger-Dienste hängt mit ihrer mobilen Verfügbarkeit zusammen; es gibt sie in einer kaum überblickbaren Vielfalt und - wie erwähnt - auch für Desktop-PCs. Bei einigen handelt es sich um Teil-Systeme, zum Beispiel um eine Anwendung, die auf einem Smartphone oder einem Desktop-PC ausgeführt werden kann und die standardisierte Protokolle nutzt,[68] während andere Dienste ein geschlossenes System aus Kommunikations-Protokoll, Server-Infrastruktur und Anwendungen für Smartphone und PC bilden.[69]

Messenger-Dienste lassen sich auf verschiedene Art und Weise technisch implementieren. Wie im Einzelnen zu zeigen sein wird (siehe unten, III.1.c.), hat die Art und Weise der technischen Umsetzung Auswirkungen auf den jeweils anwendbaren Rechtsrahmen. Unterschieden wird zwischen Systemen, bei denen die Nachrichten vom Nutzer an einen Server gesendet werden und von diesem weiter an die Empfänger (Server-basierte Messenger), und Systemen, bei denen die Nachrichten direkt zwischen den Nutzern ausgetauscht werden und der Dienstanbieter lediglich anfangs über sein Nutzerverzeichnis[70] die Verbindung zwischen den Nutzern herstellt (peer-to-peer Messenger). An der Kommunikation selbst ist die Infrastruktur des Anbieters dann nicht mehr beteiligt, diese findet unmittelbar zwischen den Kommunikationspartnern über das Internet statt. Der Nutzer bekommt von dieser technischen Implementierung in der Regel nichts mit: Bei allen Diensten kann er nach anderen Nutzern suchen und Nachrichten mit diesen austauschen.

---

63 M. Kroker, Erste Prognose für 2015: Messenger überholen in diesem Jahr soziale Netzwerke, 6.1.2015, abrufbar unter: http://blog.wiwo.de/look-at-it/2015/01/06/erste-prognose-fur-2015-messenger-uberholen-in-diesem-jahr-soziale-netzwerke/, zuletzt abgerufen am 3.4.2015.

64 Vgl. BITKOM, Presseinformation - Gezeitenwechsel bei Kurznachrichten, abrufbar unter http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Zahl_der_SMS_gesunken_30_05_2014.pdf, zuletzt abgerufen am 30.3.2015.

65 Beispielsweise kann der Nutzer bei Facebook entscheiden, ob er (teil-)öffentlich auf der Pinnwand eines Bekannten eine Nachricht veröffentlicht oder diese per Messenger versendet.

66 BNetzA, Jahresbericht 2013, S. 77.

67 BNetzA, Jahresbericht 2013, S. 78.

68 Vgl. beispielsweise zum XMPP-Protokoll T. Kleinz, Jabber: Der Chat für alle bleibt eine Utopie, abrufbar unter http://blog.zdf.de/hyperland/2013/06/jabber-der-chat-fuer-alle-bleibt-eine-utopie/, zuletzt abgerufen am 3.4.2015.

69 Dazu gehört beispielsweise Skype, das neben Internettelefonie auch Messaging anbietet, vgl. T. Messerer/B. Eickhoff, Einsatz von Skype im Unternehmen, abrufbar unter http://www.esk.fraunhofer.de/content/dam/esk/de/documents/Skype_im-Unternehmen.pdf, zuletzt abgerufen am 3.4.2015, S. 9 f.

70 Das heißt, die Registrierung der Nutzer und die Suche nach einem bestimmten Nutzer („Lookup") wird über Server des Anbieters abgewickelt, vgl. H. Lundgren et al., „A Distributed Instant Messaging Architecture based on the Pastry PeerToPeer Routing Substrate", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.9133&rep=rep1&type=pdf, zuletzt abgerufen am 27. 3.2015, S. 1.

Die rasche Verbreitung von Messenger-Diensten und ihre Nutzung als Ersatz für herkömmliche Telekommunikationsdienste führt zu der Frage, ob der geltende Rechtsrahmen die Vertraulichkeit dieser Kommunikationsform ausreichend schützt. Im Folgenden (siehe unten, III.1.b. und IV.7.) wird zu zeigen sein, dass dies für einige Formen von Messenger-Diensten nicht der Fall ist und es werden Empfehlungen gegeben, um diese Lücke zu schließen.

2. IT-Sicherheit

Mit zunehmender Konvergenz der Netze und Dienste und der damit einhergehenden Vernetzung und Komplexität von IT-Systemen und -Infrastrukturen[71] wächst die Abhängigkeit von Wirtschaft und Gesellschaft von einer zuverlässig verfügbaren und sicheren Informationstechnologie.[72] IT-Infrastrukturen, -Systeme und -Dienste, deren Ausfall schwerwiegende Folgen für das Gemeinwesen hätte, sog. „Kritische Infrastrukturen" („KI"),[73] und die für das Funktionieren dieser Infrastrukturen erforderlichen Telekommunikationsinfrastrukturen bedürfen eines besonderen Schutzes.[74] Fehlt ein ausreichendes Schutzniveau für IT-Infrastrukturen, -Systeme und -Dienste, so behindert dies zudem die Entwicklung neuartiger Dienste und wirkt so innovationshemmend.[75] Es ist somit - auch und gerade angesichts einer vom Bundesamt für Sicherheit in der Informationstechnologie („BSI") „nach wie vor als „kritisch" eingestuften Gefährdungslage",[76] unabdingbar, ein ausreichendes Maß an IT-Sicherheit zu schaffen.[77]

Die Gewährleistung eines ausreichenden Maßes an IT-Sicherheit hängt entscheidend davon ab, dass bestehende Informationsasymmetrien behoben werden und so die Transparenz der IT-Sicherheit erhöht sowie eine Fragmentierung von Sicherheitsvorgaben vermieden und so ein einheitliches Mindestschutzniveau geschaffen wird.

a. Intransparenz der IT-Sicherheit und ihre Auswirkungen

Bislang bestehen nur für einige wenige Branchen verbindliche Vorgaben zur Gewährleistung von IT-Sicherheit für Kritische Infrastrukturen[78] und zur Meldung sicherheitsrelevanter

---

71 S. Bundesamt für Sicherheit in der Informationstechnologie (BSI), „Die Lage der IT-Sicherheit in Deutschland 2014", Stand November 2014 („BSI Sicherheitsbericht 2014"), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, zuletzt abgerufen am 17.3.2015, S. 7; vgl. u.a. auch B. Freund, IT-Sicherheitsgesetz - zum neuen Entwurf eines Gesetzes gegen Cyber-Attacken, ITRB 2014, 256, 257; P. Bräutigam/S. Wilmer, Big brother is watching you? - Meldepflichten im geplanten IT-Sicherheitsgesetz, ZPR 2015, 38; D. Klett/T. Ammann, Gesetzliche Initiativen zur Cyber-Sicherheit, CR 2014, 93 f.

72 S. EU Kommission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection („Communication on Critical Information Infrastructure Protection"), 30.3.2009, COM (2009) 149 final, S. 1; s. auch Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme v. 25.2.2015, BR-Drs. 18/4096, S. 1.

73 EU Kommission, Communication on Critical Information Infrastructure Protection, S. 1; diesen Begriff greift auch der Entwurf für ein IT-Sicherheitsgesetz auf, s. unten, III.2.

74 Experten sagten im Jahr 2008 voraus, dass es in den nächsten zehn Jahren mit einer Wahrscheinlichkeit von 10% - 20% zu einem signifikanten Ausfall Kritischer Infrastrukturen kommen wird, der weltweit zu gesamtwirtschaftlichen Schäden in einer Höhe von bis zu 250 Mrd. USD führen kann (vgl. EU Kommission, Communication on Critical Information Infrastructure Protection, S. 1 m.w.N.).

75 Vgl. R. Anderson/R. Böhme/R. Clayton/T. Moore, Security Economics and the Internal Market, 2007, S. 3.

76 S. BSI Sicherheitsbericht 2014, S. 4.

77 Vgl. Koalitionsvertrag zwischen CDU, CSU und SPD, Deutschlands Zukunft gestalten, S. 97, 103 f.

78 U.a. Energiesektor (§ 11 Abs. 1a EnWG), Finanzwesen (insbesondere § 25a KWG i.V.m BaFin, Rundschreiben 10/2012 (BA), Mindestanforderungen an ein Riskomanagement (MaRisk), AT 7.2), Telekommunikationssektor (§ 109 TKG).

Vorfälle.[79] Dies bewirkt, dass IT-Sicherheit oft nur unzureichend gewährleistet ist und dass es eine erhebliche Dunkelziffer nicht gemeldeter IT-Sicherheitsvorfälle gibt.[80]

Eine unzureichende Meldung von Sicherheitsvorfällen an eine zentrale Stelle führt dazu, dass zwischen betroffenen Betreibern, staatlichen Stellen und den von den Sicherheitsvorfällen betroffenen Bürgerinnen und Bürgern erhebliche Informationsasymmetrien bestehen. Nur durch den Abbau solcher Informationsasymmetrien kann gewährleistet werden, dass aufeinander abgestimmte und schnelle Reaktionen im Hinblick auf Sicherheitslücken und die möglichen Folgen von Sicherheitsvorfällen erfolgen können.[81]

b. Verstärkte Interdependenzen zwischen IT-Dienstleistern

Die Verletzlichkeit Kritischer Infrastrukturen wird verstärkt durch die wechselseitige Abhängigkeit dieser Infrastrukturen untereinander,[82] die nicht durch Ländergrenzen beschränkt wird.[83]

Die EU Kommission beschreibt diese Abhängigkeit wie folgt: „Given that networks and information systems are interconnected and the global nature of the Internet, many NIS incidents transcend national borders and undermine the functioning of the Internal market.“[84]

Diese globalen Interdependenzen verbieten es, den Schutz Kritischer Infrastrukturen als nationalstaatliche Aufgabe zu begreifen.[85] Es ist vielmehr erforderlich, auch auf europäischer und globaler Ebene sicherzustellen, dass ein ausreichendes Maß an IT-Sicherheit auf Grundlage gemeinsamer Mindeststandards geschaffen wird (dazu noch unten, IV.2.).[86]

3. OTT – Over The Top-Angebote im Internet

Mit dem Begriff „Over The Top (OTT)-Angebot“ wird die Bereitstellung von Audio-, Video- oder sonstigen Inhalten sowie von Kommunikationsfunktionen (wie z.B. Textnachrichten) ohne die unmittelbare Beteiligung des Internet-Access-Providers bezeichnet.[87] Die Dienste des Internet-Access-Providers werden zwar verwendet, um ein OTT-Angebot in Anspruch zu nehmen, der

---

79 §§ 109, 109a TKG, Verordnung (EU) Nr. 611/2013 der Kommission vom 24. Juni 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation); ABl. EU L 173/2 v. 26.6.2013.

80 BKA, Bundeslagebericht Cybercrime 2013 v. 27.8.2014, S. 10, abrufbar unter http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2013.pdf, zuletzt abgerufen am 17.3.2015.

81 Vgl. R. Anderson/R. Böhme/R. Clayton/T. Moore, Security Economics and the Internal Market, 2007, S. 18, 40 ff.

82 Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BR-Drs. 643/14 v. 29.12.2014, S. 2.

83 S. EU Kommission, Communication on Critical Information Infrastructure Protection, S. 4; vgl. auch Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union COM (2013) 48 final, S. 2 f.

84 Übersetzung: „Weil Netze und Dienste miteinander verbunden sind und wegen der globalen Natur des Internets überschreiten viele IT-Sicherheitsvorfälle nationale Grenzen und untergraben die Funktionsfähigkeit des Binnenmarktes“; EU Kommission, SWD (2013) 31 final, 7.2.2013, S. 3.

85 S. EU Kommission, Communication on Critical Information Infrastructure Protection, S. 5.

86 Vgl. R. Anderson/R. Böhme/R. Clayton/T. Moore, Security Economics and the Internal Market, 2007.

87 Vgl. M. Schneider, WhatsApp & Co. – Dilemma um anwendbare Datenschutzregeln – Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZR 2014, 231, 232.

Internet-Access-Provider hat allerdings weder die Möglichkeit, das OTT-Angebot zu kontrollieren, noch ist er für dieses verantwortlich.[88]

Zur Proliferation von OTT-Angeboten und zur Konzentration auf einige wenige Anbieter tragen u.a. zwei ökonomische Faktoren bei:

Erstens wird der Wert vieler OTT-Angebote für Nutzer dadurch maßgeblich gesteigert, dass viele andere Nutzer dasselbe OTT-Angebot verwenden. Dies trifft beispielsweise auf Instant-Messaging-Dienste wie WhatsApp zu: Je mehr Bekannte einer Person WhatsApp verwenden, desto wertvoller wird WhatsApp für die betreffende Person. Umgekehrt ist ein Konkurrenzdienst mit wenigen Nutzern kaum von Interesse, da der Kreis der potentiellen Kommunikationspartner wesentlich geringer ist. Derartige Netzwerkeffekte[89] treten bei allen geschlossenen Kommunikationsplattformen, insbesondere bei allen Networking-Diensten auf. Anbieter von Telekommunikationsdiensten profitieren demgegenüber grundsätzlich nicht von derartigen Netzwerkeffekten, da ihre bzw. die von ihnen genutzten Netze interoperabel mit den Netzen anderer Anbieter sind und daher z.B. ein Kunde eines kleinen Internet-Access-Providers auch mit den Kunden anderer Internet-Access-Provider kommunizieren kann.

Zweitens sind OTT-Angebote typischerweise dadurch gekennzeichnet, dass die Bereitstellung des Angebots mit hohen Fixkosten, jedoch mit sehr geringen variablen (mengenabhängigen) Kosten verbunden ist, was zu Massenproduktionsvorteilen führt. Die Fixkosten bestehen meist aus Kosten für die Programmierung des Angebotes und die etwaige Lizenzierung von Inhalten. An variablen Kosten fallen hingegen meist nur die Kosten zusätzlicher Rechen-, Speicher- und Übertragungskapazitäten an, die aufgrund der raschen technischen Entwicklung verhältnismäßig gering sind.[90] OTT-Anbieter mit einer großen Anzahl an Nutzern können daher den Nutzern einen wesentlich geringeren Preis anbieten, als dies OTT-Anbieter mit einer kleinen Anzahl an Nutzern möglich ist.

Herausforderungen für das Recht ergeben sich aus dem spezifischen Umgang vieler OTT-Anbieter mit personenbezogenen Daten (dazu a.), aus den Vermarktungsbedingungen für digitale Inhalte (dazu b.) und aus den Rahmenbedingungen für die Rechtsdurchsetzung gegenüber globalen OTT-Anbietern (dazu c.).

a. Die Behandlung personenbezogener Daten als Vermögenswert

Der Vermögenswert, der personenbezogenen Daten aus Unternehmenssicht zukommt, ist insbesondere darauf zurückzuführen, dass sie die potentiell sehr profitablen Geschäftspraktiken der personenbezogenen Werbung sowie der Preisdifferenzierung ermöglichen.[91] Um den ökonomischen Wert personenbezogener Daten besser zu erfassen, werden diese beiden Geschäftspraktiken zunächst näher beleuchtet:

Personenbezogene Werbung basiert darauf, einem Nutzer jene Werbeinhalte zu präsentieren, die seinen Bedürfnissen, seinen Interessen und seiner ökonomischen Leistungsfähigkeit entsprechen. Je vollständiger die über einen Nutzer vorhandenen Informationen sind, desto

---

88 Vgl. BEREC, Work Programme 2013, BEREC Board of Regulators, 7.12.2012, BoR (12) 142, 23, verfügbar unter http://berec.europa.eu/files/document_register_store/2013/1/BoR_%2812%29_142_BEREC_WP-2013_f.pdf, zuletzt aufgerufen am 30.3.2015; s. dazu bereits oben, Fußnote 33.

89 C. Shapiro/H.R. Varian, Information Rules, 1999, Boston, S. 13.

90 So hat sich das Mooresches Gesetz von 1965, wonach sich die Rechenkapazität von integrierten Schaltkreisen ca. alle zwei bis drei Jahre verdoppelt, bis heute als zutreffend erwiesen. Vgl. M. Kanellos, FAQ: Forty years of Moore's Law, CNET News, 1.4.2005, http://news.cnet.com/FAQ-Forty-years-of-Moores-Law/2100-1006_3-5647824.html, zuletzt abgerufen am 20.3.2015.

91 Vgl. L. Feiler, Information Security Law in the EU and the U.S., 2011, Wien, S. 35 f.

treffsicherer kann die Werbung gestaltet werden. Die Erhöhung der Effektivität personenbezogener Werbung stellt daher einen starken ökonomischen Anreiz für die Erhebung von personenbezogener Daten dar.[92]

Preisdifferenzierung (auch „Preisdiskriminierung“) besteht darin, dass ein Unternehmen für dieselben Waren oder Dienstleistungen unterschiedlichen Kunden unterschiedliche Preise berechnet. Starke Anreize, dies zu tun, bestehen für ein Unternehmen, wenn unterschiedliche Kundenkreise bereit sind, unterschiedliche Preise für dieselbe Leistung zu bezahlen. Sind beispielsweise von 100 Kunden 50 bereit, maximal EUR 10 für die Leistung des Unternehmens zu bezahlen, während die anderen 50 Kunden maximal EUR 5 bezahlen wollen, so stellt sich die Frage, zu welchem Preis die Leistung angeboten werden soll. Wenn der Verkaufspreis mit EUR 5 festgesetzt wird, liegt der Umsatz bei EUR 500 (beide Kundengruppen würden kaufen). Wird der Preis mit EUR 10 festgesetzt, liegt der Umsatz ebenso bei EUR 500 (nur die erste Kundengruppe würde kaufen). Wenn es dem Unternehmen allerdings gelingt, die Leistung für EUR 10 an die erste und für EUR 5 an die zweite Kundengruppe zu verkaufen, beträgt der Umsatz EUR 750. Dies setzt allerdings voraus, dass das Unternehmen detaillierte Kenntnis über die Vorlieben und die wirtschaftliche Leistungsfähigkeit seiner Kunden hat, was wiederum die Erhebung und Auswertung großer Mengen an Kundendaten erfordert.[93]

Gerade bei OTT-Angeboten, die digitale Inhalte anbieten, verstärken die sich Null annähernden variablen Kosten die wirtschaftlichen Anreize zur Preisdifferenzierung. Kostet es z.B. nur 5 Cent, einem weiteren Nutzer eine digitale Kopie eines Inhalts zum Download anzubieten, so ist es aus Sicht des Anbieters noch immer wirtschaftlich, die Kopie für 10 Cent einem Nutzer anzubieten, der sie für einen höheren Preis (z.B. EUR 10) gar nicht gekauft hätte.

Im Folgenden wird untersucht, inwieweit personenbezogene Daten, die aus Unternehmenssicht einen ökonomischen Wert haben, in der Praxis als Entgelt behandelt werden (dazu (1)). Sodann wird der Frage nachgegangen, welchen mittelbaren Wert personenbezogene Daten für OTT-Anbieter dadurch haben, dass die Schwierigkeiten einer Portierung der Daten zu einem anderen Anbieter zu einer stärkeren Kundenbindung führt (dazu (2)).

(1) Daten als Entgelt für „kostenlose“ Online-Dienste?

Zahlreiche OTT-Angebote sind für Nutzer ohne Zahlung eines Geldbetrages verfügbar. Dies bedeutet allerdings nicht, dass diese Angebote aus Freigiebigkeit erfolgen würden. Vielmehr sehen die Nutzungsbedingungen derartiger OTT-Angebote vor, dass eine Inanspruchnahme des Angebots nur dann gestattet ist, wenn der Nutzer in die Erhebung und Verarbeitung seiner Daten zu Zwecken der personalisierten Werbung einwilligt. Die auf Grundlage der Nutzungsbedingungen vom Anbieter verarbeiteten personenbezogenen Daten des Nutzers nehmen daher in ökonomischer Hinsicht die Funktion eines Entgelts ein.[94] Ob es sich auch in

---

92 Vgl. S. Garfinkel, Database Nation: The Death of Privacy in the 21st Century, 2000, S. 155 ff; P. Schaar, Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft, 2007, S. 186 ff.

93 A. Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, in: L. J. Camp/S. Lewis (Hrsg), Economics of Information Security, 2004, Boston, S. 187, 203, welche Preisdifferenzierung als eine der stärksten Anreize der Privatwirtschaft für Eingriff in die Privatsphäre nennen. Zur Preisdifferenzierung vgl. allgemein L. Philips, The Economics of Price Discrimination, 1983, Cambridge; H. R. Varian, Differential Pricing and Efficiency, First Monday, 5.8.1996, http://firstmonday.org/ojs/index.php/fm/article/view/473/394, zuletzt abgerufen am 20.3.2015.

94 Vgl. M. Dorner, Big Data und „Dateneigentum” – Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617, 618.

rechtlicher Hinsicht bei den personenbezogenen Daten bzw. der Zustimmung zu deren Verarbeitung um eine vom Nutzer zu erbringende (entgeltliche) Gegenleistung handelt, wird unten untersucht (dazu III.3.a).

(2) Datenportabilität und wirtschaftliche Lock-in-Effekte

Wenn es für Kunden mit erheblichen Kosten verbunden ist, von einem Anbieter zu einem anderen Anbieter zu wechseln, kann es zu einem „Lock-in-Effekt" kommen. Je höher die mit einem Anbieterwechsel verbundenen Kosten („switching costs") sind, desto stärker ist der Lock-in-Effekt.[95] Aus Sicht eines Anbieters stellt das Lock-in seiner Kunden einen unmittelbaren Wert dar, weil die Kunden trotz einer geringfügigen (den Lock-in-Effekt nicht übersteigenden) Preiserhöhung nicht zu einem anderen Anbieter wechseln werden.

Ist ein Markt von starken Lock-in-Effekten gekennzeichnet, so hat dies grundsätzlich zweierlei Auswirkungen auf den Wettbewerb. Einerseits wird der Wettbewerb um Neukunden verschärft, da jeder neu gewonnene Kunde für verhältnismäßig lange Zeit bzw. zu für den Anbieter verhältnismäßig vorteilhaften Bedingungen gehalten werden kann.[96]

Andererseits führen Lock-in-Effekte dazu, dass der Wettbewerb um bestehende Kunden geschwächt wird. Kostet beispielsweise ein bestimmtes OTT-Angebot bei allen Anbietern EUR 10 pro Monat und betragen die switching costs EUR 120, so wäre es für den Nutzer bei einer Preiserhöhung durch seinen Anbieter auf EUR 11 in wirtschaftlicher Hinsicht noch immer vorteilhaft, bei seinem bestehenden Anbieter zu verbleiben, da sich die Kostenersparnis von EUR 1 pro Monat beim Wechsel zu einem konkurrierenden Anbieter (ohne Berücksichtigung von Opportunitätskosten) erst nach ca. 10 Jahren realisieren würde.

In einem stark durchdrungenen Markt, in dem die meisten potentiellen Kunden bereits mit einem Anbieter einen Vertrag geschlossen haben, wird der Wettbewerb zwischen den Anbietern daher wesentlich beeinträchtigt. Darüber hinaus bestehen für neue Anbieter erhebliche Markteintrittsschwellen, da sie das Lock-in der Kunden ihrer Konkurrenten durch ein deutlich besseres Angebot überwinden müssen.

Bei zahlreichen OTT-Angeboten resultieren die Lock-in-Effekte nicht aus langen Kündigungsfristen oder sonstigen rechtlichen Hindernissen, sondern ergeben sich daraus, dass eine Migration der personenbezogenen Daten eines Nutzers von einem Anbieter zu einem anderen Anbieter entweder nur mit sehr hohem Aufwand oder gar nicht möglich ist.[97] Wer beispielsweise bei einem Anbieterwechsel seine bestehenden Daten aus technischen Gründen gar nicht migrieren kann, wird sich fragen, ob die Kosten, die darin bestehen, die beim bisherigen Anbieter gespeicherten Daten nicht mehr verwenden zu können, schwerer wiegen als die Vorteile, die der Anbieterwechsel mit sich bringt.

In diesem Zusammenhang kommt daher der Frage, ob ein Kunde gegenüber einem Anbieter das Recht hat, seine Daten zu portieren, d.h. die Daten in einem wiederverwendbaren Datenformat zu erhalten, entscheidende Bedeutung zu. Die Schaffung eines Rechts auf Datenportabilität dürfte geeignet sein, den Wettbewerb um bestehende Kunden zu fördern, neuen Anbietern den Markteintritt zu erleichtern und dadurch den Wettbewerb und damit die Innovationsanreize im Markt zu erhöhen.

---

95 Vgl. H. R. Varian/J. Farrel/C. Shapiro, The Economics of Information Technology, 2004, Cambridge, S. 21 ff.
96 H. R. Varian/J. Farrel/C. Shapiro, aaO, S. 22 f.
97 Vgl. C. Shapiro/H. R. Varian, Information Rules, 1999, Boston, S. 122 ff.

b. Digitale Vertriebsmodelle im Konflikt mit traditioneller Wertschöpfungskette

In vielen Fällen sind die Fixkosten eines einzelnen von einem OTT-Dienst angebotenen digitalen Inhalts (z.B. eines Songs) relativ gering, so dass es für einen OTT-Anbieter wirtschaftlich ist, einen Inhalt auch dann verfügbar zu machen, wenn er nur wenige Dutzend Abnehmer findet. Dies führt zu einem als „Long Tail“[98] beschriebenen Marktpotential für Anbieter digitaler Inhalte:

Klassische Vertriebsmodelle leiden daran, dass die für den Vertrieb notwendigen Ressourcen notwendiger Weise beschränkt sind. Dies trifft auf den Regalplatz im Plattenladen ebenso zu wie auf die Kinosäle in einem Kino oder die Sendezeit im Fernsehen oder Radio. Die Beschränktheit der Ressourcen führt dazu, dass sich die angebotenen Inhalte auf den „Mainstream“ beschränken, obwohl ein erheblicher Kundenkreis nur ein geringes Interesse am Mainstream hat.[99]

Das Geschäft mit digitalen Inhalten ist demgegenüber dadurch gekennzeichnet, dass es praktisch keine derartigen Ressourcenbeschränkungen gibt und dass es (geringe Fixkosten für einzelne digitale Inhalte vorausgesetzt) daher wirtschaftlich ist, auch Inhalte für Nischenmärkte anzubieten. Diese Nischenmärkte ermöglichen allerdings in Summe erhebliche Umsätze - auch im Verhältnis zu den Umsätzen in Mainstream-Märkten.

Die Möglichkeit, das Markpotentials des „Long Tail“ auszuschöpfen, in Verbindung mit der Möglichkeit der Preisdifferenzierung beschert Anbietern digitaler Inhalte entscheidende Wettbewerbsvorteile gegenüber Anbietern von Inhalten auf physischen Informationsträgern, wie z.B. Büchern oder CDs.

Bei Waren, die über traditionelle Vertriebswege auf den Markt gebracht werden, kommt dem Großhandel sowie dem Einzelhandel eine große Bedeutung zu. Insbesondere der Einzelhandel ist jedoch durch relativ hohe Kosten (z.B. Personalkosten und Kosten für Raummiete) gekennzeichnet.

Digitale Vertriebsmodelle ermöglichen es hingegen, auf ganze Absatzstufen zu verzichten und gewähren damit beträchtliche Wettbewerbsvorteile. Dies erzeugt einen überaus starken Preisdruck für Unternehmen, die am unteren Ende einer traditionellen Vertriebskette tätig sind.

Aber auch am oberen Ende traditioneller Vertriebsketten hat sich bereits in der Vergangenheit vieles geändert. So hat der von der Musikindustrie stark forcierte Schutz technischer Maßnahmen[100] („Digital Rights Management“ oder „DRM“) erheblich dazu beigetragen, dass die Hersteller derartiger DRM-Software einen bedeutenden Einfluss am Musikmarkt gewannen. Denn aufgrund der Inkompatibilitäten zwischen unterschiedlichen DRM-Systemen entstanden Lock-in-Effekte, von denen die Hersteller der DRM-Software und nicht die Musikverlage profitierten.[101]

---

98 Vgl. C. Anderson, The Long Tail: Why the Future of Business Is Selling Less or More, 2. Aufl. 2008, New York, S. 253.

99 Y. Benkler, The Wealth of Networks, 2006, Yale, S. 204 ff.

100 § 108b UrhG; vgl. auch Art. 6 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EU L 167/10, 22.6.2001.

101 H. R. Varian, Keynote Address to the Third Digital Rights Management Conference, Berlin, 13.1.2005; vgl. N. Weinstock Netanel, Temptations of the Walled Garden: Digital Rights Management and Mobile Phone Carriers, Journal on Telecommunication and High Technology Law 2007, 77.

c. Rechtsdurchsetzung gegenüber globalen Diensteanbietern

Um einen fairen Wettbewerb am Markt der OTT-Anbieter zu gewährleisten, ist es grundsätzlich erforderlich, OTT-Anbieter nach dem Marktortprinzip dem Recht desjenigen Marktes zu unterwerfen, auf dem sie tätig sind. *De lege lata* ist dieses Marktortprinzip insbesondere für die Bereiche des Telekommunikationsrechts,[102] des Urheberrechts,[103] des Lauterkeitsrechts[104] sowie - nach Verabschiedung der EU-Datenschutzgrundverordnung - auch des Datenschutzrechts umgesetzt.[105]

In faktischer Hinsicht stehen der Durchsetzung des Rechts des Marktortes jedoch eine Reihe von Hindernissen entgegen, die in der EU auch und vor allem daraus resultieren, dass die Rechtsdurchsetzung gegenüber global agierenden OTT-Anbietern - mit Ausnahme des Anwendungsbereichs des Kartellrechts, für das die Europäische Kommission über eine Vollzugskompetenz verfügt[106] - ausschließlich durch nationale Behörden erfolgt:

Limitierte Ressourcen nationaler Behörden: Insbesondere dann, wenn die Zuständigkeit in einem Mitgliedstaat auf regionaler Ebene bzw. auf Landesebene angesiedelt ist, besteht das Risiko, dass einzelne Behörden nicht über die nötigen Ressourcen verfügen, um Rechtsdurchsetzungsmaßnahmen zu ergreifen und durchzusetzen.

Unwirtschaftlichkeit lokal rechtskonformer Dienste: Wenn jede in einem Mitgliedstaat oder einer Region zuständige Behörde für denselben OTT-Dienst unterschiedliche Auflagen erteilt, ist es für den OTT-Anbieter unter Umständen unwirtschaftlich, die für eine Region bzw. einen kleineren Mitgliedstaat speziell erforderlichen Modifikationen des OTT-Dienstes vorzunehmen. Dies kann dazu führen, dass der OTT-Dienst in den betroffenen Jurisdiktionen gar nicht angeboten wird. Beispielsweise gibt es nach zahlreichen von der österreichischen Datenschutzbehörde ausgesprochenen Auflagen nach wie vor kein Google Street View für österreichische Straßen.[107]

Rechtsdurchsetzung gegen OTT-Anbieter ohne Niederlassung in der EU: Hat der OTT-Anbieter keine Niederlassung in der EU, so steht eine kraft Marktortprinzip zuständige

---

[102] Vgl. § 3 Nr. 6 TKG, welcher bei der Definition des Begriffs des Diensteanbieters und damit des Anwendungsbereichs des TKG im Ergebnis auf die Diensteerbringung in der Bundesrepublik Deutschland abstellt.

[103] Vgl. Art. 8 Abs. 1 Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (im Folgenden Rom II-Verordnung), ABl. EU L 199, 31.7.2007, S. 40, wonach auf außervertragliche Schuldverhältnisse aus einer Verletzung von Rechten des geistigen Eigentums das Recht des Staates anzuwenden ist, für den der Schutz beansprucht wird.

[104] Vgl. Art. 6 Abs. 1 Rom II-Verordnung, wonach auf außervertragliche Schuldverhältnisse aus unlauterem Wettbewerbsverhalten das Recht des Staates anzuwenden ist, in dessen Gebiet die Wettbewerbsbeziehungen oder die kollektiven Interessen der Verbraucher beeinträchtigt worden sind oder wahrscheinlich beeinträchtigt werden.

[105] Vgl. Art. 3 Abs. 2 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014, wonach die DS-GVO auch auf durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter Anwendung findet, wenn personenbezogene Daten von in der Union ansässigen betroffenen Personen verarbeitet werden und die Datenverarbeitung (a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist oder (b) der Überwachung dieser betroffenen Personen dient.

[106] Art. 4 Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln (Text von Bedeutung für den EWR), ABl. EU L 1 vom 4.1.2003, S. 1.

[107] Vgl. Datenschutzbehörde, Neue Entwicklungen betreffend Google Street View, https://www.dsb.gv.at/site/6733/default.aspx, zuletzt abgerufen am 20.3.2015.

Behörde vor der meist nicht zu bewältigenden Herausforderung, Maßnahmen der Rechtsdurchsetzung außerhalb der EU zu vollstrecken.[108]

Die Effektivität der Durchsetzung des Rechts des Marktortes ist häufig dann gemindert, wenn und soweit die aus nicht rechtskonformen Verhalten resultierenden Gewinne die Kosten finanzieller Sanktionen deutlich übersteigen.

d. Lösungsansätze in der öffentlichen Diskussion

In der (rechts-)politischen Diskussion über die künftige Regelung von OTT-Angeboten steht das Wettbewerbsverhältnis zwischen OTT-Anbietern und Anbietern von Telekommunikationsdiensten im Vordergrund.

So wird unter dem Stichwort „Level Playing Field" diskutiert, dass für OTT-Anbieter und Anbieter von Telekommunikationsdiensten derzeit eine unterschiedliche Rechtslage (siehe hierzu II.1.a.) und damit unterschiedliche Wettbewerbsbedingungen bestehen und diese entsprechend angeglichen werden müssten.[109] Diese Angleichung sollte nach Ansicht mancher durch eine vollständige Deregulierung von Telekommunikationsdiensten erfolgen,[110] während andere eine Beschränkung des sachlichen Anwendungsbereichs der Telekommunikationsregulierung auf Dienste fordern, die den Zugang zu einem Kommunikationsnetz ermöglichen, womit alle sonstigen Dienste wie insbesondere Sprachtelefondienst, SMS und E-Mail aus der Regulierung entlassen wären.[111]

Ein weiterer öffentlich rege diskutierter Vorschlag zielt darauf, OTT-Anbieter, die über beträchtliche Marktmacht verfügen, zu entflechten.[112] So hat insbesondere das Europäische Parlament in einer nicht bindenden Entschließung vom November 2014 die Europäische Kommission aufgefordert, „Vorschläge in Betracht zu ziehen, die darauf abzielen,

---

[108] Wenn der OTT-Anbieter eine Niederlassung in der EU hat, kommt hingegen eine Vollstreckung nach der jeweiligen nationalen Umsetzung des Rahmenbeschlusses 2005/214/JI des Rates vom 24. Februar 2005 über die Anwendung des Grundsatzes der gegenseitigen Anerkennung von Geldstrafen und Geldbußen, ABl. EU L76/16, 22.3.2005, in Betracht.

[109] A.-M. Allouët/S. Le Franc/M.-N. Marques/L. Rossi, Achieving a Level Playing Field between the Players of the Internet Value Chain, Digiworld Economic Journal 2014, 99; F. Herrera-González, How to achieve a Level Playing Field in the Internet Value Chain: An Economic Analysis, 2014, http://www.telefonica.com/en/about_telefonica/pdf/Regulatory_Economics_brief_1.pdf, zuletzt abgerufen am 2.4.2015; Belgian operators call for level playing field, telecompaper, 12.1.2015, http://www.telecompaper.com/news/belgian-operators-call-for-level-playing-field--1059133, zuletzt abgerufen am 2.4.2015; A.D. Little, The Belgian Telecom Landscape, http://www.adlittle.com/downloads/tx_adlreports/ADL_StudyonBelgianTelecomsector_Economy_English.pdf, zuletzt abgerufen am 2.4.2015; T. Fairless, EU Considers New Telecom Rules to Level the Playing Field, Wall Street Journal, 25.3.2015, http://www.wsj.com/articles/eu-considers-new-telecom-rules-to-level-the-playing-field-1427295277, zuletzt abgerufen am 2.4.2015; K. Bhushan, Vodafone demands level-playing field with OTT players, digit, 15.10.2014, http://www.digit.in/telecom/vodafone-demands-level-playing-field-with-ott-players-24176.html, zuletzt abgerufen am 2.4.2015.

[110] F. Herrera-González, How to achieve a Level Playing Field in the Internet Value Chain: An Economic Analysis, 2014, S. 5, http://www.telefonica.com/en/about_telefonica/pdf/Regulatory_Economics_brief_1.pdf, zuletzt abgerufen am 2.4.2015.

[111] A.-M. Allouët/S. Le Franc/M.-N.Marques/L. Rossi, Achieving a Level Playing Field between the Players of the Internet Value Chain, Digiworld Economic Journal 2014, 99, 106 ff.

[112] Vgl. z.B. S. Gabriel, Unsere politischen Konsequenzen aus der Google-Debatte, Frankfurter Allgemeine Zeitung, 16.5.2014, verfügbar unter http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/sigmar-gabriel-konsequenzen-der-google-debatte-12941865.html?printPagedArticle=true, zuletzt abgerufen am 2.4.2015.

Suchmaschinen von anderen kommerziellen Dienstleistungen abzukoppeln“, da dies ein langfristiges Mittel sein könne, den Wettbewerb zu fördern.[113]

e. Wettbewerbsschutz vs. Wettbewerberschutz

Sowohl die Regeln des deutschen als auch des EU-Kartellrechts bezwecken primär den Schutz der Struktur des Marktes und damit des Wettbewerbs als solchem.[114] In ihrer Mitteilung zu Art. 102 AEUV hat die Europäische Kommission ausgesprochen, dass es ihr vor allem darum geht, „den Wettbewerbsprozess und nicht einfach die Wettbewerber zu schützen. Dies kann durchaus bedeuten, dass Wettbewerber, die den Verbrauchern in Bezug auf Preise, Auswahl, Qualität und Innovation weniger zu bieten haben, aus dem Markt ausscheiden.“[115]

Hierdurch wird deutlich zum Ausdruck gebracht, dass es nicht Funktion des Kartellrechts ist, einen Wettbewerber vor der höheren Konkurrenzfähigkeit eines anderen Wettbewerbers zu schützen. Auch vor diesem Hintergrund sind die vom Europäischen Parlament geäußerten Überlegungen hinsichtlich der Zerschlagung großer Suchmaschinenanbieter kritisch zu sehen.

4. Rechtsdurchsetzung gegen ausländische Rechtsverletzer

Eine besondere Herausforderung beim Geschäft mit digitalen Inhalten besteht darin, dass ausländische Rechtsverletzer unmittelbar mit inländischen Anbietern in Konkurrenz treten können. So bietet beispielsweise die Website kinox.to ihren Nutzern tausende Kinofilme unter Verstoß gegen § 19a UrhG per Streaming an. Dies ist möglich, weil sich der Server, von dem aus kinox.to betrieben wird, außerhalb der EU befindet[116] und die Inhaber der Domain bzw. die Betreiber der Website nicht ausfindig gemacht werden konnten.[117]

Allerdings gibt es in mehreren EU-Staaten Bestrebungen, gegen derartige ausländische Rechtsverletzer vorzugehen, indem Unterlassungsansprüche gegen inländische Intermediäre geltend gemacht werden.[118] Praktisch gesprochen bedeutet dies, dass Internet-Access-Provider gerichtlich

---

[113] Rn. 15 der Entschließung des Europäischen Parlaments vom 27. November 2014 zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt (2014/2973(RSP)), verfügbar unter http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2014-0071&language=DE&ring=B8-2014-0286.

[114] H.-J. Bunte, in: H.-J. Bunte (Hrsg.), Kartellrecht, Band 2, 12. Aufl. 2014, Köln, Einl. Rn. 36.

[115] Mitteilung der Kommission — Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen, ABl. EU C 45 vom 24.2.2009, S. 7, Rn. 6.

[116] Der Domainname kinox.to kann (z.B. mit dem unter Linux/Unix und Windows verfügbaren Befehl *nslookup*) in die IP-Adresse 91.202.61.170 aufgelöst werden, welche einem Betreiber auf den Britischen Jungferninseln zugewiesen ist.Vgl.https://apps.db.ripe.net/search/query.html?searchtext=91.202.61.170&search%3AdoSearch=Search#resultsAnchor, zuletzt abgerufen am 3.4.2015.

[117] Für die Top-Level-Domain .to (es handelt sich um die Country-Code Top Level Domain für das Königreich Tonga), wird im Unterschied zu den meisten anderen Top-Level-Domains keine vollständige WHOIS-Datenbank geführt, aus welcher die Identität des Domaininhabers ersichtlich wäre, vgl. https://www.tonic.to/faq.htm#16, zuletzt abgerufen am 3.4.2015; der wenig aussagende WHOIS-Eintrag für kinox.to ist unter https://www.tonic.to/whois?kinox.to verfügbar. Die Personen, von welchen vermutet wird, dass sie für den Betrieb von kinox.to verantwortlich sind, konnten bisher nicht gefasst werden, vgl. M. Böhm, Kinox.to-Gründer: Ermittlern fehlt noch immer heiße Spur, Spiegel Online, 3.4.2015, http://www.spiegel.de/netzwelt/netzpolitik/kinox-to-ermittler-suchen-noch-immer-betreiber-a-1027003.html, zuletzt abgerufen am 3.4.2015.

[118] Vgl. J. B. Nordemann, Anmerkung zu EuGH, Urteil vom 27. März 2014 – C-314/12 – UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH („Kino.to“), ZUM 2014, 499; L. Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?, Stanford-Vienna Transatlantic Technology Law Forum (TTLF)

verpflichtet werden, es zu unterlassen, ihren Nutzern ungehindert Zugang zu derartigen Websites zu gewähren. In technischer Hinsicht erfolgt die Umsetzung solcher Unterlassungsverfügungen durch Website-Sperren.[119] Ist eine solche Website-Sperre implementiert, so ist es den Kunden des Internet-Access-Providers nicht mehr möglich, ohne technische Umgehungsmaßnahmen eine Verbindung mit der blockierten Website herzustellen.

Bei der Diskussion über derartige Website-Sperren ist zu berücksichtigen, dass diese für Internet-Access-Provider mit erheblichen Kosten verbunden sein können. Darüber hinaus darf nicht vernachlässigt werden, dass es auch zur Sperrung von rechtmäßigen Websites kommen kann (sog. „Overblocking"). Dies kann beispielsweise dadurch geschehen, dass die IP-Adresse der rechtsverletzenden Website gesperrt wird, jedoch unter Verwendung derselben IP-Adresse auch andere - gänzlich rechtmäßige - Websites gehostet werden.[120]

Eine der zentralen Herausforderungen bei der Rechtsdurchsetzung gegen ausländische Rechtsverletzer besteht daher darin, eine effiziente Rechtsdurchsetzung auf eine Weise zu ermöglichen, die sowohl die Interessen der Intermediäre hinsichtlich der Kostentragung wahrt als auch geeignete Maßnahmen gegen Overblocking vorsieht.

Working Paper No. 13, S. 22, verfügbar unter http://www.law.stanford.edu/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf, zuletzt abgerufen am 2.4.2015.

[119] Zu den technischen Umsetzungsmöglichkeiten vgl. L. Feiler/A. Schnider, Webgesperrt: Europäischer Gerichtshof bejaht Website-Sperrungen bei Urheberrechtsverletzungen, c't 10/2014, 160.

[120] L. Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?, Stanford-Vienna Transatlantic Technology Law Forum (TTLF) Working Paper No. 13, S. 9 f, verfügbar unter http://www.law.stanford.edu/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf, zuletzt abgerufen am 2.4.2015); vgl. auch B. Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance, Berkman Center for Internet and Society, 2003, http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/, zuletzt abgerufen am 2.4.2015; CSMG, Study into Websites Sharing Internet Protocol Addresses, 2012, http://stakeholders.ofcom.org.uk/binaries/internet/websites-sharing.pdf, zuletzt abgerufen am 2.4.2015.

III. Der geltende Rechtsrahmen und seine europarechtlichen Grundlagen

Im Folgenden wird der Frage nachgegangen, ob der geltende Rechtsrahmen geeignet ist, die im vorangegangenen Kapitel dargestellten Herausforderungen zu bewältigen und aufgezeigt, an welchen Stellen Anpassungsbedarf besteht. Einzelne Vorschläge zur Anpassung des Rechtsrahmens finden sich im abschließenden Kapitel der Studie (unter IV.).

1. Telekommunikationsrecht und Recht der Telemedien

Unter II.1.b.(1) wurden die Charakteristika und Besonderheiten der Machine-to-Machine-Kommunikation, der Location Based Services sowie von Messenger-Diensten herausgearbeitet. Im Folgenden wird untersucht, ob der geltende telekommunikations- und medienrechtliche Rahmen zur Regulierung der genannten Dienstegruppen geeignet und ausreichend flexibel ist.

a. Die Regulierung der Machine-to-Machine Kommunikation im IoT

Die Machine-to-Machine-Kommunikation ist gesetzlich nicht spezifisch geregelt.[121] Wie unter II.1.b.(1) dargestellt, ist es charakteristisch für Machine-to-Machine-Dienste, dass die vernetzten Objekte über eine Telekommunikationsverbindung miteinander kommunizieren, wobei die Datenübermittlung jedoch lediglich eine untergeordnete Bedeutung für das Diensteangebot an sich hat. Kern des Diensteangebots sind vielmehr die über die Telekommunikationsverbindung erbrachten (Inhalte-)Dienstleistungen.

Ob Machine-to-Machine-Dienste der telekommunikationsrechtlichen Regulierung unterliegen, bestimmt sich maßgeblich danach, ob die Dienste als „Telekommunikationsdienste" i.S.d. § 3 Nr. 24 TKG anzusehen sind. Nach § 3 Nr. 24 TKG, der die relevanten europäischen Vorgaben der Rahmen-RL umsetzt,[122] sind dies „*in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze … bestehen.*" Wie bereits oben dargestellt, wird die Bewertung, ob ein Dienst „ganz oder überwiegend in der Übertragung von Signalen besteht" regelmäßig nicht bezogen auf den Dienst in seiner Gesamtheit, sondern im Hinblick auf einzelne Dienstebestandteile vorgenommen.[123]

Anbieter von öffentlich zugänglichen Telekommunikationsdiensten unterliegen - weitgehend in Umsetzung der relevanten europarechtlichen Vorgaben[124]- einer Vielzahl von telekommunikationsrechtlichen Verpflichtungen. In der Praxis der Bundesnetzagentur („BNetzA") ist „Anbieter" des Telekommunikationsdienstes derjenige, der aus Sicht des Kunden die Erbringung des Telekommunikationsdienstes vertraglich schuldet.

---

[121] Lediglich vereinzelt finden sich auf Ebene des Europarechts eng begrenzte Ausnahmeregelungen, wie beispielsweise in Art. 15 Abs. 4 der Verordnung (EU) 532/12 des Europäischen Parlaments und des Rates vom 13. Juni 2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, der eine Ausnahme von Transparenzpflichten bei regulierten Datenroamingdiensten für Geräte enthält, die eine mobile Machine-to-Machine-Kommunikation ermöglichen.

[122] Nach Art. 2 lit. c sind elektronische Kommunikationsdienste solche Dienste, die *„ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen".* Der einheitliche europäische Rechtsrahmen für Übertragungsnetze und -dienste findet dagegen keine Anwendung „auf die Inhalte", „die über elektronische Kommunikationsnetze und -dienste bereitgestellt werden, wie Rundfunkdienste und bestimmte Dienste der Informationsgesellschaft". Der europäische Gesetzgeber postuliert so eine grundsätzliche „Trennung der Regulierung von Übertragung und Inhalten", s. Erwägungsgrund 5 Rahmen-RL.

[123] Vgl. u.a. H. J. Säcker, in: H. J. Säcker (Hrsg.), TKG-Kommentar, 3. Aufl. 2013, § 3 Rn. 62; R. Schütz, in: M. Geppert/R.Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 3 Rn. 79.

[124] Vorgaben zur Notifizierung ergeben sich aus der Genehmigungsrichtlinie, Regelungen zum Kundenschutz aus der Universaldienstrichtlinie.

Da die Definition des „Telekommunikationsdienstes“ weit gefasst wurde, um eine technologie- und diensteneutrale Regulierung zu gewährleisten und Dienste nicht insgesamt, sondern regelmäßig hinsichtlich ihrer Bestandteile bewertet werden, sind Konstellationen denkbar, in denen Anbieter von Machine-to-Machine-Diensten dem Anwendungsbereich der telekommunikationsrechtlichen Vorschriften unterfallen.[125]

Entscheidend für den Umfang der regulatorischen Verpflichtungen ist ferner, ob es sich bei dem Telekommunikationsdienst um einen „öffentlich zugänglichen“ Telekommunikationsdienst handelt, d.h. um einen Dienst, welcher der Öffentlichkeit zur Verfügung steht (§ 3 Nr. 17a TKG). Dies ist bei Machine-to-Machine-Diensten, die ganz oder hinsichtlich einzelner Elemente als Telekommunikationsdienste klassifiziert werden, regelmäßig der Fall.

Ist der Anbieter des Machine-to-Machine-Dienstes als Anbieter eines öffentlich zugänglichen Telekommunikationsdienstes anzusehen, so unterliegt er unter anderem der Meldepflicht gegenüber der BNetzA (§ 6 TKG), Verpflichtungen aus dem Bereich des Kundenschutzes (u.a. im Hinblick auf Vertragsinhalt und -laufzeiten und im Zusammenhang mit dem Anbieterwechsel und der Nummernportierung, u.a. §§ 43a, 46 TKG) sowie Verpflichtungen im Hinblick auf die öffentliche Sicherheit (u.a. betreffend die Überwachung der Kommunikation und die Zusammenarbeit mit Sicherheitsbehörden, §§ 110 ff. TKG). Darüber hinaus finden die Vorgaben des Telekommunikationsdatenschutzes (dazu noch unten, c.) Anwendung.

Die oben genannten Verpflichtungen sind weitgehend auf eine Kommunikation zugeschnitten, bei der Menschen die Kommunikationsleistung aktiv nutzen. Sprechen Menschen miteinander, können sie die zugrundeliegende Kommunikationsverbindung beispielsweise dazu verwenden, Straftaten zu planen oder zu begehen. Daher ist es für die Strafverfolgungsbehörden notwendig, in den gesetzlich vorgesehenen Fällen auf den Inhalt der Kommunikation zugreifen zu können bzw. nachvollziehen zu können, wer eine bestimmte Kommunikationsverbindung zu einem bestimmten Zeitpunkt nutzt. Kommunizieren Maschinen mit Maschinen, so besteht ein entsprechendes Bedürfnis nicht in gleichem Maße. Zwar werden auch hier Daten über eine Kommunikationsverbindung automatisiert ausgetauscht. Wenn und soweit ein Zugriff des Menschen auf diesen Kommunikationsvorgang nicht besteht, wird aber der Inhalt des Kommunikationsvorgangs für die Strafverfolgungsbehörden in der Regel nicht von Interesse sein.

Auch im Bereich des Kundenschutzes zeigt sich, dass die geltenden Regelungen die Spezifika von Machine-to-Machine-Diensten nur unzureichend abbilden, wobei sich diese Anwendungsschwierigkeiten jedenfalls zum Teil durch eine zweckgerichtete Auslegung der entsprechenden Vorschriften abmildern lassen:

Die BNetzA knüpft im Hinblick auf die Vorschriften zur Nummernmitnahme (§ 46 Abs. 4 TKG) beispielsweise daran an, dass nach § 46 Abs. 4 TKG lediglich dem Teilnehmer „zugeteilte“ Rufnummern von den Vorgaben zur Portierung erfasst werden und versucht, durch eine restriktive Auslegung des Begriffs der Zuteilung den Anwendungsbereich der Portierungsregeln bei M2M-Diensten zu begrenzen. Nach Auffassung der BNetzA „spricht es dafür“, eine Nummer dann nicht als dem Teilnehmer zugeteilt anzusehen, wenn (i) dem Kunden der M2M-Anwendung bei Vertragsschluss die Nummer nicht benannt wird und eine Kenntnis der Nummer für den Dienst nicht erforderlich

[125] S. dazu BNetzA, Auswertung der Stellungnahmen zur Anhörung „Auswirkungen der Entwicklungen bei der Machine-to-Machine-Kommunikation auf die Nummerierung“, Bewertung zu Frage 7.1.

ist, (ii) die Nummer wegen „des Wesens“ der Anwendung „gar nicht aus dieser herausgelöst werden kann“ oder (iii) andere Anbieter „herausgelöste Nummern aus technischen Gründen gar nicht im Rahmen ihrer Anwendungen verarbeiten können“. [126] Die BNetzA stellt jedoch ausdrücklich klar, dass die Beurteilung von M2M-Diensten stets „im Einzelfall zu erfolgen“ hat.[127]

Diese Beispiele illustrieren, dass der geltende telekommunikationsgesetzliche Rahmen für den Bereich der Machine-to-Machine-Kommunikation oftmals nicht ausreichend flexibel ist und sich Anwendungsschwierigkeiten oft nur durch eine zweckgerichtete Auslegung der bestehenden Regelungen auf Grundlage einer Bewertung des Einzelfalls mildern lassen.

b. Erhebung, Verarbeitung, Nutzung und Speicherung von Standortdaten nach TKG und TMG

Die Erhebung, Verarbeitung und Nutzung von Standortdaten ist die technische Voraussetzung, um Nutzern standortbasierte Dienste anbieten zu können.

Standortbezogene Daten sind nur im TKG Gegenstand einer besonderen Regelung: Gemäß § 3 Nr. 19 TKG sind Standortdaten „Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben“.

Der Wortlaut der Regelung und die Tatsache, dass die Regelung im TKG vorgenommen wurde, erweckt den Eindruck, ihr liege die Vorstellung zu Grunde, dass der Telekommunikationsanbieter (insbesondere der Mobilfunkprovider[128]) die Positionierung vornimmt. Dies entspricht jedoch - wie dargelegt - einem älteren technischen Stand und trägt den neuen technischen Rahmenbedingungen von standortbezogenen Diensten nicht Rechnung.[129] Folgerichtig hat der europäische Gesetzgeber mit der E-Privacy-Richtlinie[130] und in der Folge der nationale Gesetzgeber mit der TKG-Novelle 2012[131] den Anwendungsbereich dieser Vorschriften erweitert. Er bezeichnet nunmehr (auch) solche Daten als Standortdaten, die von einem Telekommunikationsdienst erhoben und verwendet werden. Es ist unklar, ob damit nunmehr nicht nur die Positionsermittlung über die Funkzellenbestimmung sondern auch diejenige über die Nutzung der GPS-Sensoren des Endgeräts erfasst wird.[132]

Damit ist in vielen Fällen, in denen moderne Methoden zur Standortbestimmung verwandt werden (wie zum Beispiel mittels GPS-Sensoren in Smartphones, die von Smartphone-Apps genutzt werden), unklar, ob § 98 TKG anwendbar ist.[133]

---

[126] BNetzA, Auswertung der Stellungnahmen zur Anhörung „Auswirkungen der Entwicklungen bei der Machine-to-Machine (M2M) Kommunikation auf die Nummerierung“, Bewertung zu Frage 7.1.

[127] BNetzA, Auswertung der Stellungnahmen zur Anhörung „Auswirkungen der Entwicklungen bei der Machine-to-Machine (M2M) Kommunikation auf die Nummerierung“, Bewertung zu Frage 7.1.

[128] Der Mobilfunk wird in der Regelung ausdrücklich adressiert, vgl. § 98 Abs. 1 Satz 2 TKG.

[129] Vgl. oben, III.1.b.

[130] Vgl. Art. 2 lit. c Richtlinie 2009/136/EG Abl. EU L 337 v. 18.12.2009, S. 11.

[131] Gesetz zur Änderung telekommunikationsrechtlicher Regelungen v. 3.5. 2012, BGBl. I, 958 ff.

[132] Die Novellierung des § 98 TKG diente der Anpassung der Vorschrift an Art. 2 lit. c E-Privacy-Richtlinie (2009/136/EG; Abl. EU L 337 v. 18.12.2009, S. 11), vgl. BR-Drs. 129/11, S. 81. Deren Erwägungsgrund 56 benennt beispielhaft RFID-Empfangsgeräte, die mit dem Telekommunikationsnetz verbunden sind. Es bleibt unklar, ob sich dies auf Sensoren bezieht, die den Standort anderer Geräte bestimmen können, oder ob auch Endgeräte erfasst werden sollen, die ihren eigenen Standort bestimmen und diesen über einen Telekommunikationsdienst übertragen.

[133] Teilweise wird vertreten, dass die Regelungen des § 98 TKG auf den Erbringer des standortbezogenen Dienstes nicht anwendbar seien, sondern nur auf den TK-Diensteanbieter, der die Ortung vornimmt, vgl. R. Steidle,

Ist § 98 TKG anwendbar,[134] so ist Voraussetzung für die Verwendung von Standortdaten, dass sie zur Erbringung eines Dienstes mit Zusatznutzen erforderlich ist und dass die Daten anonymisiert wurden oder der Teilnehmer eingewilligt hat. Teilnehmer ist, wer den Vertrag mit dem Anbieter des Telekommunikationsdienstes (zum Beispiel den Mobilfunkvertrag) geschlossen hat.[135] Würde man § 98 TKG also auf Smartphone-Apps anwenden, so müssten die App-Anbieter sicherstellen, dass derjenige, der den Mobilfunkvertrag geschlossen hat, die Einwilligung in die Standortbestimmung erteilt. Das ist in der Praxis nicht umsetzbar. [136]

Wenn die Standortdaten an Dritte (andere Anbieter oder Teilnehmer) übermittelt werden, verlangt § 98 TKG darüber hinaus, dass die Einwilligung schriftlich erfolgen muss.[137] Auch das ist in der Praxis nicht sinnvoll: Soll der Anbieter einer Smartphone-App etwa seine Nutzer um ihre Adresse (bzw. die Adresse des „Teilnehmers“) bitten, damit er diesen ein Einwilligungsformular nebst Rücksendeumschlag zusenden kann?

Schließlich muss der Nutzer - das ist die Person, die den Dienst jeweils in Anspruch nimmt[138]- gemäß § 98 Abs. 1 Satz 2 TKG über jede Standortermittlung per Textmitteilung an das Endgerät informiert werden, es sei denn, der Standort wird nur auf dem Endgerät angezeigt. Dies ist im Falle von Smartphone-Apps wiederum kaum durchführbar, da ihnen die Nummer des Endgeräts nicht bekannt ist, sie also auch keine Textmitteilung an dieses versenden können. Darüber hinaus gilt die Regelung nur für Mobilfunkendgeräte. Die Informationspflicht entfällt also, wenn es sich um ein anderes Endgerät handelt, dessen Standort bestimmt wird. Wieso hier aber z.B. ein Unterschied in der Ortung eines Laptops mit eingebautem UMTS-Modem im Vergleich zu einem Laptop ohne ein entsprechendes Modem bestehen soll, ist nicht nachvollziehbar. Hinzu kommt, dass es auch Mobilfunkendgeräte gibt, die Textnachrichten gar nicht anzeigen können - was die Verpflichtung zur Übersendung von Textnachrichten an eben solche Mobilfunkendgeräte ad absurdum führt.[139]

Die Regelungen des § 98 TKG sind also für moderne standortbezogene Dienste untauglich.

Soweit die spezifischen Regelungen des TKG nicht einschlägig sind, kommt in der Regel der Telemediendatenschutz (§§ 11 ff. TMG) zur Anwendung. Telemediendienste sind alle elektronischen Informations- und Kommunikationsdienste, mit Ausnahme bestimmter

---

Datenschutz bei Nutzung von Location Based Services im Unternehmen, MMR 2009, 167, 170; T. Weichert, Datenschutz im Auto - Teil 1, SVR 2014, 201, 206 f.; A. Lober/A. Patzak, Datenschutz bei mobilen Endgeräten im Nutzungskontext, DSRITB 2012, 545, 559 f. Folgt man dieser Auffassung wäre das TKG kaum auf standortbezogene Dienste anwendbar.

134 Bei Standortdaten kann es sich auch um eine besondere Form der Verbindungsdaten handeln, vgl. R. Steidle, Datenschutz bei Nutzung von Location Based Services im Unternehmen, MMR 2009, 167, 168. Soweit deren Verarbeitung für die Herstellung der Verbindung notwendig ist, bleibt § 96 TKG einschlägig. Werden die Standortdaten zu anderen Zwecken verarbeitet, greift der speziellere § 98 TKG ein, vgl. J.-D. Braun, in: M. Geppert/R. Schütz (Hrsg.), Beck’scher TKG-Kommentar, 4. Aufl. 2014, Rn. 8 f.; a.A. R. Steidle, Datenschutz bei Nutzung von Location Based Services im Unternehmen, MMR 2009, 167, 169.

135 § 3 Nr. 20 TKG.

136 Vgl. hierzu für den Fall der Kommunikation von Maschine zu Maschine J. Scherer/C. Heinickel, Die TKG-Novelle 2012, NVwZ 2012, 585, 591.

137 § 98 Abs. 1 Satz 4 TKG.

138 Nach § 3 Nr. 14 TKG ist Nutzer „jede natürliche oder juristische Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt, ohne notwendigerweise Teilnehmer zu sein“ - der Begriff stellt also wiederum auf den Telekommunikationsdienst ab.

139 Zum Beispiel Router, die sich in das UMTS oder LTE Netz einbuchen und lokal ein WLAN errichten, über das dann Geräte ohne Mobilfunkeinrichtung das Internet nutzen können. In Zukunft werden zahlreiche Beispiele aus dem Internet of Things hinzu kommen.

Dienste, die dem TKG oder dem Rundfunkrecht unterfallen.[140] Viele standortbezogene Dienste rufen über das Internet Informationen von Servern des Anbieters ab. Beispielsweise beziehen Navigationsprogramme aktuelle Verkehrsinformationen aus dem Internet. Es handelt sich dann um Telemediendienste. Das TMG kennt keine spezifische Regulierung von Standortdaten. Standortdaten sind entweder Nutzungsdaten im Sinne des TMG oder nicht durch das TMG regulierte Inhaltsdaten.[141]

Standortdaten stellen Nutzungsdaten dar, soweit sie vom Diensteanbieter erhoben und verwendet werden und erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen, vgl. § 15 TMG. Dies ist beispielsweise bei Navigationsdiensten der Fall, bei denen der Diensteanbieter die Standortdaten erhebt und die ohne genaue und aktuelle Standortdaten nicht funktionieren können. In diesem Fall wird die Nutzung der Standortdaten durch § 15 TMG beschränkt. Sonst handelt es sich bei den Standortdaten um Inhaltsdaten, insbesondere dann, wenn sie den Inhalt der Kommunikation zwischen Nutzer und Anbieter des Telemediendienstes darstellen. Dies ist etwa der Fall, wenn ein Nutzer seine aktuelle Position aktiv in einem sozialen Netzwerk veröffentlicht und mit einem Kommentar verknüpft. Erhebung, Verarbeitung und Nutzung von Inhaltsdaten sind nicht Gegenstand des TMG, so dass das BDSG subsidiär zur Anwendung kommt. Die Einordnung hängt zu einem gewissen Grad also auch von der Gestaltung des Dienstes ab.

Zusammenfassend lässt sich festhalten, dass Standortdaten je nach technologischer und inhaltlicher Gestaltung des Dienstes den Regelungen des TKG, des TMG oder des BDSG unterliegen. Nur das TKG enthält Regelungen, die die besondere Relevanz von Standortdaten für das Individuum berücksichtigen und erweiterte Einwilligungs- und Informationspflichten vorsehen. Diese können in der Praxis von modernen standortbezogenen Diensten jedoch in vielen Fällen nicht befolgt werden.

c. Regulierung von Messenger-Diensten nach TKG, TMG und BDSG

Der datenschutzrechtliche Rahmen von Messenger-Diensten richtet sich je nach technischer Umsetzung des Diensteangebots nach dem TKG oder dem TMG und subsidiär nach den Regeln des BDSG. Obwohl - wie dargestellt[142] - Messenger-Dienste zunehmend SMS und auch klassische Sprachtelefonie ersetzen, gelten damit nicht immer die einschlägigen Datenschutzregeln des TKG.

Ob Messenger-Dienste als Telekommunikationsdienste anzusehen und damit die Regeln über den Schutz des Fernmeldegeheimnisses nach § 88 TKG und die Datenschutzvorschriften der §§ 91 ff. TKG anwendbar sind, hängt davon ab, ob sie ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen.[143] Dies hängt von der technischen Implementierung des Dienstes ab: Verwendet der Dienst Kommunikationsprotokolle, die unmittelbar auf dem physikalischen Netz aufbauen, spricht einiges für einen Telekommunikationsdienst.[144] Gleiches gilt, wenn der Anbieter technische Übertragungs- oder Vermittlungsfunktionen übernimmt.[145] Setzt der Dienst dagegen Kommunikationsprotokolle höherer Abstraktionsebenen ein, so dass der Diensteanbieter

---

[140] Vgl. § 1 Abs. 1 TMG; siehe auch oben II.1.a.
[141] Vgl. M. Arning/F. Moos, Location Based Advertising, ZD 2014, 126, 127.
[142] Vgl. oben II.1.b.(3).
[143] Vgl. § 1 Nr. 24 TKG.
[144] Der Dienst ähnelt dann letztlich dem Short-Message-Service im Mobilfunk. Allerdings sind derartige Messaging-Dienste heutzutage eher selten, die meisten machen sich die etablierte Abstraktion von der technischen Ebene durch das Internetprotokoll zu nutze und verringern so den Aufwand für die technische Umsetzung des Dienstes erheblich.
[145] Vgl. für den Bereich der Email-Dienste Erwägungsgrund 10 S. 3 Rahmen-RL.

nicht mehr an der Signalübertragung beteiligt ist oder übernimmt der Anbieter nur die Funktion eines Teilnehmerverzeichnisses, ohne an der Kommunikation selbst beteiligt zu sein, so liegt regelmäßig kein Telekommunikationsdienst vor und der Dienst unterliegt weder dem Telekommunikationsgeheimnis noch den Datenschutzregelungen des TKG.[146]

Sind die datenschutzrechtlichen Regelungen des TKG nicht einschlägig, richtet sich der Datenschutz bei Messenger-Diensten nach §§ 11 ff. TMG. Denn in aller Regel sind solche Messenger-Dienste Telemediendienste.[147] Die Datenschutzregelungen des TMG regulieren den Umgang mit Nutzungsdaten (§ 15 TMG) durch den Telemediendienstanbieter, während für die Inhaltsdaten das BDSG anwendbar bleibt.

Auf einen Messenger-Dienst können also - je nach technischer Gestaltung - die Datenschutzregelungen des TKG oder die des TMG Anwendung finden.[148] Verglichen mit den Regelungen des TKG, denen beispielsweise der Austausch von Kurznachrichten per SMS unterliegt, gewährleisten die Regeln des TMG nur begrenzten Schutz: Vergleichbar stark ausgeprägt ist das Schutzniveau bei *Informationen über das Vertragsverhältnis* zwischen Anbieter und Kunden. Im TKG unterliegen diese Daten als Bestandsdaten den Regelungen des § 95 TKG. Unter dem TMG handelt es sich ebenfalls um Bestandsdaten, die dem Schutz des § 14 TMG unterliegen.

Die *Umstände einzelner Kommunikationsvorgänge* (außer der Kommunikationsinhalte selbst) werden im TKG als Verkehrsdaten (§ 96 TKG), im TMG als Nutzungsdaten (§ 15 TMG) geschützt. Die Regelungen im TKG sind diesbezüglich aber deutlich strenger als die Regelungen im TMG. Dies zeigt sich beispielhaft daran, dass das TKG ein Einwilligungserfordernis bei der Verwendung der Daten für Werbezwecke vorsieht, während das TMG nur eine Widerspruchsmöglichkeit enthält.

Die *Inhalte der Telekommunikation* genießen unter dem TKG den höchsten Schutz. Der Zugriff auf diese Inhaltsdaten ist regelmäßig unzulässig (§ 88 TKG) und unter bestimmten Voraussetzungen strafbar (§ 206 StGB). Dagegen werden gerade diese Daten unter dem TMG gar nicht gesondert geregelt, so dass subsidiär das BDSG zur Anwendung kommt. Die Inhalte der Kommunikation über Messenger-Dienste stellen aus Sicht des Diensteanbieters damit normale personenbezogene Daten dar. Dies führt zu einer erheblichen Schwächung des Schutzniveaus.

So ermöglicht § 28 BDSG z.B. die Verwendung personenbezogener Daten für eigene Geschäftszwecke, für Zwecke Dritter und für die Strafverfolgung grundsätzlich auf Grundlage einer Abwägung zwischen den Interessen des Anbieters (bzw. des Dritten) und des Nutzers. Das TKG verbietet dagegen jeden über die zur Übermittlung der Information erforderlichen Zugriff auf die Inhalte der Kommunikation, Ausnahmen gibt es nur für die Strafverfolgung und dort nur mit richterlicher Anordnung.[149] In der Praxis lässt sich das Problem nur dann reduzieren, wenn man davon ausgeht, dass die Abwägung bei Messenger-Daten nahezu immer zugunsten des Geheimhaltungsinteresses des Nutzers ausgehen muss.

---

[146] Vgl. M. Schneider, WhatsApp & Co.- Dilemma um anwendbare Datenschutzregeln, ZD 2014, 231, 236. Auch im Übrigen ist das TKG dann nicht anwendbar. Der Dienst unterliegt dann keiner Regulierung.

[147] Dies gilt nicht, wenn sie Telekommunikationsdienste sind, die ganz in der Übertragung von Signalen bestehen. Dann gilt wie oben dargestellt das TKG, vgl. § 1 TMG. Auch für den Überlappungsbereich zwischen TMG und TKG (d.h. für Telekommunikationsdienste, die lediglich „überwiegend“ in der Übertragung von Signalen bestehen), gilt hinsichtlich des Datenschutzes vorwiegend das TKG (vgl. § 11 Abs. 3 TMG).

[148] M. Schneider, WhatsApp & Co.- Dilemma um anwendbare Datenschutzregeln, ZD 2014, 231, 236.

[149] Vgl. § 100a f. StPO.

Allerdings verhindert ein absolutes Verbot wie im TKG, dass ein Anbieter auf Grundlage einer unklaren Rechtsgrundlage Fakten schafft.

Darüber hinaus wird das Verarbeitungsverbot des TKG von der Strafbarkeitsdrohung des § 206 StGB flankiert. Eine ähnlich deutliche Sanktion gibt es im BDSG nicht, die Bußgeldtatbestände des § 43 BDSG werden in der Praxis kaum angewandt[150] und die Strafvorschrift des § 44 BDSG setzt eine besondere Bereicherungs- und Schädigungsabsicht voraus und umfasst nicht die bloße Mitteilung von Tatsachen.

Zusammenfassend ist festzuhalten: Obwohl Messenger-Dienste für die Nutzer als Ersatz für SMS und Telefonie eingesetzt und wahrgenommen werden, bietet ihnen der existierende Rechtsrahmen einen erheblich geringeren Schutz für die Kommunikationsinhalte als dies bei herkömmlichen Telekommunikationsdiensten (wie SMS und Telefonie) der Fall ist.

2. IT-Sicherheitsrecht: Geltende Rechtslage und Neuerungen durch das geplante IT-Sicherheitsgesetz

Auf europäischer Ebene will die EU Kommission mit einer Cybersicherheitsstrategie[151] einen umfassenden Schutz Kritischer Infrastrukturen erreichen. Kernstück dieser Cybersicherheitsstrategie ist der Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (sog. „NIS-Richtlinienvorschlag“)[152], der im März 2014 vom Europäischen Parlament mit einer Vielzahl von Änderungen angenommen wurde.[153] Die EU Kommission hat den überwiegenden Teil der vorgeschlagenen Änderungen angenommen.[154] Der NIS-Richtlinienvorschlag definiert zunächst Sektoren, die vom Anwendungsbereich der Richtlinie umfasst werden sollen[155] und sieht für Betreiber Kritischer Infrastrukturen in diesen Sektoren Verpflichtungen zur Implementierung von Sicherheitsmaßnahmen[156] sowie zur Meldung von Sicherheitsvorfällen[157] vor.[158] Darüber hinaus statuiert der NIS-Richtlinienentwurf umfassende Kooperationspflichten für die Mitgliedstaaten.[159]

Auf nationaler Ebene bestehen Verpflichtungen zur Implementierung von Sicherheitsmaßnahmen derzeit bereits in vereinzelten Sektoren.[160] Um für den Bereich der Kritischen Infrastrukturen insgesamt einen einheitlichen Mindeststandard der IT-Sicherheit zu gewährleisten, hat die Bundesregierung im August 2014 einen überarbeiteten[161] Referentenentwurf[162] zur Anhörung

---

150 Vgl. P. Gola, Aus den aktuellen Berichten der Aufsichtsbehörde (17): Die Bußgeldpraxis, RDV 2015, 26.

151 Cybersicherheitsstrategie der Europäischen Union - ein offener, sicherer und geschützter Cyberraum, 7.2.2013, JOIN (2013) 1 final.

152 COM (2013) 48 final, s. dazu auch D. Klett/T. Ammann, Gesetzliche Initiativen zur Cybersicherheit, CR 2014, 93, 95 f.

153 Legislative Entschließung des Europäischen Parlaments v. 13.3.2014 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM (2013) 48 - C7-0035/2013 - 2013/0027(COD).

154 Vgl. Antwort der EU Kommission v. 10.6.2014, SP (2014) 455.

155 Umfasst sind die Sektoren Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Internet-Knoten, Lebensmittelversorgungsketten, Gesundheit, Wassergewinnung und -versorgung (s. Art. 3 Abs. 8 lit. b, Annex II NIS-Richtlinienentwurf). Nicht umfasst sind dagegen Kleinstunternehmen i.S.d. Empfehlung 2003/361/EU, soweit diese Kleinstunternehmen nicht als Tochterunternehmen eines verpflichteten KI-Betreibers tätig sind.

156 Art. 14 Abs. 1 NIS-Richtlinienentwurf.

157 Art. 14 Abs. 2 NIS-Richtlinienentwurf.

158 S. dazu ausführlich C. Heinickel/L. Feiler, Der Entwurf für ein IT-Sicherheitsgesetz - europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis, CR 2014, 708, 709 ff.

159 Art. 8 ff. NIS-Richtlinienentwurf.

160 S. dazu oben, II.2.a.

161 Bereits 2013 hatte die Bundesregierung einen Referentenentwurf für ein IT-Sicherheitsgesetz vorgelegt (abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile, zuletzt abgerufen am 31.3.2015, der jedoch auf vielfältige Kritik

gestellt. Im Februar 2015 wurde der von der Bundesregierung verabschiedete[163] Entwurf eines IT-Sicherheitsgesetzes („IT-SiG-E“) dem Bundestag zur Beschlussfassung vorgelegt.

Bei dem IT-SiG-E handelt es sich um ein Artikelgesetz, das u.a. Änderungen des BSI-Gesetzes, des Atomgesetzes, des Energiewirtschaftsgesetzes, des Telemediengesetzes sowie des Telekommunikationsgesetzes vorsieht.

Der IT-SiG-E stärkt zum einen die Stellung des Bundesamts für die Sicherheit in der Informationstechnik („BSI“) als zentrale Stelle für die Gewährleistung von IT-Sicherheit und statuiert Koorperationspflichten von BSI und Regulierungsbehörden der betroffenen Sektoren.[164] Zum anderen führt der IT-SiG-E - durch Änderungen des BSI-Gesetzes[165] - für „Betreiber Kritischer Infrastrukturen“[166] Verpflichtungen zur Implementierung von IT-Sicherheitsmaßnahmen[167] sowie Meldepflichten im Falle von Sicherheitsvorfällen ein.

Der persönliche Anwendungsbereich der entsprechenden Verpflichtungen wird nicht durch die relevanten Vorschriften des BSI-Gesetzes i.d.F. des IT-SiG-E bestimmt. Die Ermittlung der Unternehmen, die als „Betreiber Kritischer Infrastrukturen“ anzusehen sind, soll vielmehr erst durch eine noch zu erlassende Rechtsverordnung des Bundesministerium des Innern erfolgen.[168] Die mittlerweile in den Entwurf aufgenommene[169] gesetzliche Definition des Begriffs des „Betreibers Kritischer Infrastrukturen“ enthält eine Liste der relevanten Sektoren[170] und stellt klar, dass nur solche Anlagen (bzw. Teile davon) Kritische Infrastrukturen darstellen, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Darüber hinaus ergeben sich aus der Begründung des IT-SiG-E allgemeine Kriterien, die nach dem Willen des Gesetzgebers für die Bestimmung des persönlichen Anwendungsbereichs der Verpflichtungen relevant sein sollen.[171] Der Umstand, dass die Adressaten der im IT-SiG-E vorgesehenen Verpflichtungen erst durch die zu erlassende Verordnung bestimmt und die Kriterien für die Qualifikation eines „Betreibers Kritischer Infrastrukturen“ nicht weitergehend gesetzlich konkretisiert wurden, stieß im Gesetzgebungsverfahren auf deutliche Kritik, da sie zu mangelnder

---

stieß. Der aktuelle Entwurf basiert zwar auf diesem Referentenentwurf, wurde jedoch in erheblichem Umfang überarbeitet.

162 Abrufbar unter http://www.computerundrecht.de/Entwurd_IT-Sicherheitsgesetz_1808.pdf, zuletzt abgerufen am 1.4.2015.

163 Dem voran ging ein Gesetzesentwurf der Bundesregierung aus dem Dezember 2014.

164 Hier insbesondere der Bundesnetzagentur als Regulierungsbehörde für den Telekommunikations- und Energiesektor.

165 Durch Einfügung von §§ 8a, 8b BSIG i.d.F. des IT-SiG-E

166 Ausgenommen sind Kleinstunternehmen i.S.d. Empfehlung 2003/361/EG der Kommission v. 6.5.2003.

167 § 8a BSI-G i.d.F. d. IT-SiG-E.

168 § 1 Abs. 10 BSI-G i.d.F. d. IT-SiG-E.

169 S. jetzt BT-Drs. 18/4096 v. 25.2.2015, § 2 Abs. 10 BSI-G i.d.F. d. ITSiG-E.

170 Erfasst sind die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Die Begründung des IT-SiG enthält zudem eine Liste von Dienstleistungen, die in den jeweiligen Sektoren „jedenfalls“ „kritische Dienstleistungen“ sein können vgl. BT-Drs. 18/4096 v. 25.2.2015, S. 31. Diese Liste ist jedoch zum einen nicht abschließend („jedenfalls“). Zum anderen sind die relevanten Dienstleistungen so weit gefasst, dass sie dem potentiell Betroffenen kaum Anhaltspunkte dafür geben, ob er als Betreiber einer Kritischen Infrastruktur angesehen werden wird oder nicht.

171 Maßgeblich sollen die Kriterien „Qualität“ und „Quantität“ sein, vgl. BT-Drs. 18/4096 v. 25.2.2015, S. 30 ff. Das Kriterium „Qualität“ bestimmt, welche Infrastrukturen „kritisch“ für das Funktionieren des Gemeinwesens sind (insbesondere mit Blick auf Sicherheit für Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung, die von einem Ausfall unmittelbar betroffen wären). Das Kriterium „Quantität“ bestimmt den Versorgungsgrad der Kritischen Infrastruktur; es sollen zur Konkretisierung dieses Kriteriums Schwellenwerte erarbeitet werden, die es den Betreibern der jeweiligen Anlagen ermöglichen sollen zu entscheiden, ob ihre Anlage als Kritische Infrastruktur i.S.d. Rechtsverordnung anzusehen ist.

Rechts- und Planungssicherheit für die potentiell betroffenen Unternehmen führe.[172] Dadurch, dass der IT-SiG-E für die Umsetzung der betreffenden Verpflichtungen Übergangszeiten vorsieht, die durch den Erlass der Rechtsverordnung in Gang gesetzt werden,[173] dürften die negativen Folgen der konkreten Bestimmung des Adressatenkreises erst durch Rechtsverordnung jedoch zumindest abgemildert werden.

Die Sektoren, die für die Bestimmung der Betreiber Kritischer Infrastrukturen relevant sind, sind nicht deckungsgleich mit den Vorgaben des NIS-Richtlinienentwurfs,[174] was zu Nachteilen für deutsche Betreiber Kritischer Infrastrukturen führen kann.[175]

Die von den Betreibern Kritischer Infrastrukturen zu implementierenden Sicherheitsmaßnahmen sollen dem „Stand der Technik" entsprechen. Die Begründung des IT-SiG-E enthält nunmehr, anders als noch der Entwurf aus dem Dezember 2014, eine Definition dieses Kriteriums.[176]

Ebenfalls durch unbestimmte Rechtsbegriffe geprägt sind die Voraussetzungen für die Pflicht zur Meldung von Sicherheitsvorfällen: So sind dem BSI „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, [unverzüglich zu melden], die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben …".[177] Eine gesetzliche Definition der unbestimmten Rechtsbegriffe sowie Kriterien für das erforderliche Maß der Eintrittswahrscheinlichkeit einer möglichen Beeinträchtigung (…„führen können") enthält der IT-SiG-E nicht.[178] Allerdings enthält die Entwurfsbegründung auch hier Anhaltspunkte, die zur Konkretisierung des Begriffs der „erheblichen Störung" herangezogen werden können.[179] Es verbleiben jedoch Unklarheiten, die im Ergebnis dazu führen könnten, dass es letztendlich den Betreibern Kritischer Infrastrukturen überlassen bleibt, zu entscheiden, ob sie im konkreten Fall einer Meldepflicht unterliegen oder nicht. Darüber hinaus sieht der IT-SiG-E keine Sanktionen für den Fall vor, dass ein Betreiber Kritischer Infrastrukturen die eigentlich gebotene

---

[172] BR-Drs. 643/1 v. 6.2.2015, S. 1; ebenso u.a. http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Entwurf_IT-Sicherheitsgesetz_19_08_2014.pdf.

[173] §§ 8b Abs. 3 S. 1, 8c BSIG i.d.F. d. IT-SiG-E, BT-Drs 18/4096, S. 11 f.; P. Bräutigam/S. Wilmer, Big brother is watching you? - Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38, 39.

[174] S. dazu oben, Fn. 172.

[175] Ebenso O. Süme, IT-Sicherheitsgesetz - Bundesregierung muss europäische Einbettung sicherstellen, K&R 2/2015, Editorial.

[176] Diese lautet: „Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden" (BT-Drs. 18/4096 v. 25.2.2015, S. 26).

[177] § 8b Abs. 4 S. 1 BSIG i.d.F. des IT-SiG-E.

[178] Die Unbestimmtheit des persönlichen Anwendungsbereichs sowie die mangelnde gesetzliche Definition der im IT-Sig-E verwendeten unbestimmten Rechtsbegriffe ist einer der Hauptkritikpunkte der Stellungnahme des Bundesrates zum Gesetzesentwurf aus dem Dezember 2014, vgl. BR-Drs. 643/1/14 v. 27.1.2015, S. 1 f.

[179] So soll nach der Entwurfsbegründung, s. BT-Drs. 18/4096 v. 25.2.2015, S. 27 f., eine Störung dann vorliegen, wenn die Technik ihre Funktion nicht mehr erfüllen kann bzw. wenn versucht wurde, entsprechend auf sie einzuwirken. Erheblich sind insbesondere solche IT Störungen, die nicht automatisiert bzw. mittels der nach dem Stand der Technik zu implementierenden Maßnahmen mit wenig Aufwand behoben werden können. Eine Störung ist dagegen nicht erheblich, wenn es sich um täglich vorkommende Ereignisse (z.B. Spam, Schadsoftware, die der Virenscanner abfängt) handelt, die mit den zu implementierenden Sicherheitsmaßnahmen leicht zu beheben sind.

Meldung unterlässt.[180] Somit ist derzeit nicht ausreichend gewährleistet, dass durch die vorgesehenen Meldepflichten ein ausreichendes Maß an Transparenz der IT-Sicherheit gewährleistet werden kann.

3. Datenschutzrechtliche Fragestellungen im Zusammenhang mit OTT-Anbietern

Die oben unter II.3.a dargestellten ökonomischen Rahmenbedingungen für OTT-Anbieter basieren auf dem ökonomischen Wert, den personenbezogene Daten für OTT-Anbieter haben. Im Folgenden sollen daher praktisch besonders bedeutsame, den Wert der personenbezogenen prägende, datenschutzrechtliche Aspekte von OTT-Angeboten untersucht werden, nämlich (a) die rechtliche Einordnung personenbezogener Daten als Entgelt; (b) das Recht auf Datenportabilität; (c) der Rechtsrahmen für den internationalen Datenverkehr und (d) die von der geplanten EU-Datenschutzgrundverordnung zu erwartenden Neuerungen.

a. Personenbezogene Daten als Entgelt: Wahrung der subjektiven Äquivalenz bei Leistungsstörungen

Ökonomisch betrachtet kommt personenbezogenen Daten bei OTT-Angeboten ein wirtschaftlicher Wert zu (vgl. II.3.a). Damit stellt sich die Frage, ob personenbezogene Daten auch juristisch ein „Entgelt“ für Dienste und andere Leistungen (hier:) eines Unternehmers darstellen können. Unentgeltliche Leistungen werden im deutschen Zivilrecht oftmals privilegiert, beispielsweise hinsichtlich der Haftung. Betrachtet man personenbezogene Daten also als Entgelt für die Leistung des Unternehmers, verändert dies den Charakter der Vertragsbeziehung.[181]

Einige Stellungnahmen sprechen sich dafür aus, die Kommerzialisierung der personenbezogenen Daten auch im individuellen Vertragsverhältnis anzuerkennen.[182] Die Argumentation bezieht sich meist auf Internetdienstleister, die „kostenfreie“ Dienste[183] im Austausch für die Zustimmung zu Verarbeitung personenbezogener Daten anbieten. Der Nutzung dieser Dienste liege ein Austauschvertrag zugrunde, der die Diensterbringung durch den Anbieter gegen die Zustimmung zur Verarbeitung der eigenen personenbezogenen Daten betreffe.

Diese Ansicht beschreibt den Wert personenbezogener Daten, der ökonomisch unbestritten existiert, auch rechtlich.[184] Sie vermeidet zudem eine Zweiteilung zwischen datenschutzrechtlicher Einwilligung einerseits und Vertrag über die Erbringung der Dienstleistung andererseits. Eine solche Zweiteilung stünde grundsätzlich nicht im wirtschaftlichen Interesse der Anbieter, da diesen ohne „Anspruch“ auf die Einwilligung jederzeit der Widerruf der Einwilligung droht, was ihnen die Geschäftsgrundlage entziehen könnte.[185] Doch auch für den Nutzer wäre eine solche Zweiteilung nachteilig, da in diesem Fall die Verbraucherschutzvorschriften über Fernabsatzverträge regelmäßig nicht anwendbar wären.[186]

---

[180] Vgl. auch P. Bräutigam/S. Wilmer, Big brother is watching you? - Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38, 41.

[181] Vgl. zur Auswirkung der Entgeltlichkeit auf die Vertragstypologie, P. Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635, 636.

[182] Vgl. P. Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635, 640 f.; C. Hoffmann/ S. E. Schulz/K. C. Borchers, Grundrechtliche Wirkungsdimensionen im digitalen Raum, MMR 2014, 89, 90; F. Unseld, Die Übertragbarkeit von Persönlichkeitsrechten, GRUR 2011, 982, 987 f.

[183] Der Begriff „Dienst“ ist hier nicht in jedem Fall als dienstvertragliche Leistung zu verstehen, sondern wird eher im Sinne des (weiteren) englischen Begriffs „Service“ verwandt.

[184] Zur Herleitung insb. F. Unseld, Die Übertragbarkeit von Persönlichkeitsrechten, GRUR 2011, 982.

[185] P. Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635, 636.

[186] Vgl. § 312 Abs. 1 BGB.

De lege lata lässt sich eine Entgeltfunktion der Einwilligung in die Verarbeitung personenbezogener Daten jedoch nicht begründen.[187] Unter dem geltenden BDSG kann die datenschutzrechtliche Einwilligung nicht als Wirtschaftsgut betrachtet werden. Der Gesetzgeber hat bei der Einwilligung nicht das Ziel verfolgt, die wirtschaftliche Ausnutzung der personenbezogenen Daten zu regeln, sondern wollte vielmehr ihre Verarbeitung auf ein Minimum reduzieren.[188]

Auf das Recht, die Einwilligung jederzeit zu widerrufen kann der Nutzer - für die Nutzung der Daten zu Werbezwecken - nicht verzichten.[189] Mit diesem Widerrufsrecht gibt es aber auch keine endgültige Übertragung personenbezogener Daten an den Vertragspartner, der Nutzer behält stets ein Verfügungsrecht über „seine" personenbezogenen Daten.[190] Dieses Ergebnis mag in Anbetracht der wirtschaftlichen Relevanz der „Ressource" personenbezogene Daten unbefriedigend erscheinen. Es obliegt aber dem Gesetzgeber, das Datenschutzregime von einer Minimierung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf die Regelung der wirtschaftlichen Verwertung dieser „Ressource" umzustellen.

Entscheidet sich der Gesetzgeber - *de lege ferenda* - für eine solche Neukonzeption des Datenschutzrechts, müsste er Maßstäbe entwickeln, wann die Einwilligung in die Verarbeitung personenbezogener Daten als Entgelt gilt und unter welchen Umständen der Widerruf dieser Einwilligung zulässig bleibt. Darüber hinaus wäre zu regeln, wie Äquivalenzstörungen zu beheben sind, wenn personenbezogene Daten als Entgelt eingesetzt wurden. Wie ist die Einwilligung „zurückzugewähren", wenn der Kunde von einem Vertrag zurücktritt, ihn widerruft oder anficht? Wie sind Minderungen zu berechnen?

b. Das Recht auf Auskunft – und Datenportabilität?

Wie oben unter (II.3.a.2) dargestellt, entstehen den Wettbewerb erheblich beschränkende wirtschaftliche Lock-in-Effekte, wenn Kunden von OTT-Anbietern nicht über das Recht verfügen, ihre Daten zu portieren, d.h. die Daten in einem wiederverwendbaren Datenformat zu erhalten.

Die geltenden datenschutzrechtlichen Regelungen des Auskunftsrechts gewähren dem Betroffenen zwar einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten (§ 34 Abs. 1 Nr. 1 BDSG), sie ermöglichen es dem Betroffenen jedoch nicht, seine Daten zu portieren, d.h. von einem Diensteanbieter zu einem anderen Diensteanbieter zu übertragen.[191]

Nach § 34 Abs. 1 Nr. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen über die zu seiner Person gespeicherten Daten Auskunft zu erteilen. § 34 Abs. 6 BDSG normiert, dass die Auskunft auf Verlangen in Textform zu erteilen ist, d.h. in Form einer auf einem dauerhaften Datenträger gespeicherten lesbare Erklärung, in der die verantwortliche Stelle genannt ist (vgl. § 126b BGB). Ein dauerhafter Datenträger ist hierbei jedes Medium, (1) das es dem Empfänger ermöglicht, die auf dem Datenträger befindliche Erklärung so aufzubewahren oder zu speichern, dass sie ihm während eines für ihren Zweck

---

187 Vgl. T. Weichert, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463, 1467 ff.
188 Vgl. § 3a Satz 1 BDSG.
189 § 28 Abs. 4 Satz 1 BDSG; vgl. dazu P. Gola/C. Klug/B. Körffer, in: P. Gola/R. Schomerus, BDSG, § 28 Rn. 61.
190 T. Weichert, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463.
191 So im Ergebnis auch M. Dorner, Big Data und „Dateneigentum" - Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617, 625; vgl. auch N. Härting, Internetrecht, 5. Aufl., 2014, Berlin, S. 635.

angemessenen Zeitraums zugänglich ist, und (2) geeignet ist, die Erklärung unverändert wiederzugeben.

Nach der geltenden Rechtslage wäre es daher zulässig, einem Betroffenen Auskunft über seine Daten durch Übermittlung einer PDF-Datei zu erteilen. Damit würde zwar der Auskunftsanspruch erfüllt und dem Informationsbedürfnis des Betroffenen Rechnung getragen, eine automatisierte Weiterverwendung der Daten wäre dem Auskunftssuchenden jedoch praktisch unmöglich.

Will man beispielsweise seine E-Mails der letzten zwei Jahre von seinem bisherigen Cloud-basierten E-Mail-Anbieter zu einem anderen E-Mail-Anbieter portieren (d.h. gleichsam „mitnehmen"), so wird ein mehrere tausend Seiten langes PDF, das alle E-Mails enthält, wenig hilfreich sein.

Die derzeitige Ausgestaltung des Rechts auf Auskunft erfüllt daher nicht die Anforderungen eines Rechts auf Datenportabilität. Wie oben (unter II.3.a.(2)) ausgeführt, würde ein solches Recht den Wettbewerb fördern und die Markteintrittsschwelle für neue Anbieter wesentlich reduzieren.

c. Internationaler Datenverkehr

Um den oben (unter II.3.c.) beschriebenen Herausforderungen der Rechtsdurchsetzung gegen globale Diensteanbieter zu begegnen, ist es erforderlich, dass Datentransfers in Jurisdiktionen, in denen das Unionsrecht nicht gilt, reguliert werden, um so eine Umgehung des Rechts des Marktortes zu verhindern.[192]

Der internationale IT-Dienstleistungsmarkt hat dazu geführt, dass Datenübermittlungen an ausländische IT-Dienstleister in vielen Unternehmen aber auch für viele Konsumenten zum Regelfall geworden sind. Auch die Datenübermittlungen innerhalb international tätiger Konzerne sind aus dem heutigen Wirtschaftsleben kaum mehr wegzudenken.[193]

Im Folgenden soll daher ein Überblick über den geltenden Rechtsrahmen für den internationalen Datenverkehr gegeben werden:

(1) Datenexport in Drittländer ohne angemessenes Datenschutzniveau

Eine Datenübermittlung in ein Land, das nicht Mitglied des EWR ist und kein adäquates Datenschutzniveau bietet,[194] ist abgesehen von gewissen in § 4c Abs. 1 BDSG eng definierten Ausnahmen nur dann zulässig, wenn entweder zwischen dem Datenexporteur und dem Datenimporteur Standardvertragsklauseln[195] vereinbart wurden oder der Datenexporteur

---

[192] Mit Inkrafttreten der DS-GVO würde der Empfänger in vielen Fällen gem. Art. 3 Abs. 2 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zwar ohnedies der DS-GVO unterliegen. Hat er jedoch keine Vermögenswerte in der EU, so kann sich eine Vollstreckung schwierig gestalten, weshalb auch nach Inkrafttreten der DS-GVO ein Datenexport ein Mittel zur zumindest faktischen Umgehung des Marktortrechts sein kann.

[193] Vgl. U.S. Chamber of Commerce/Hunton & Williams LLP, Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity, 2014, https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf, zuletzt abgerufen am 4.4.2015.

[194] Ein adäquates Datenschutzniveau bieten grundsätzlich Andorra, Argentinien, die Färöer Inseln, Guernsey, die Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay. Vgl. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, zuletzt abgerufen am 22.3.2015.

[195] Bei Standardvertragsklauseln handelt es sich um von der Europäischen Kommission veröffentliche Vertragsvorlagen. Für eine Datenübermittlung von einer verantwortlichen Stelle an eine andere verantwortliche

und der Datenimporteur demselben Konzern angehören und für diesen sog. Binding Corporate Rules (BCR)[196] genehmigt wurden (und die Übermittlung im Übrigen auch innerhalb Deutschlands zulässig wäre).

Eine Sonderstellung nehmen Datenübermittlungen in die Vereinigten Staaten ein. Nach einer Entscheidung der Europäischen Kommission aus dem Jahre 2000[197] besteht dann ein adäquates Datenschutzniveau, wenn sich der Übermittlungsempfänger (das US-Unternehmen) zur Einhaltung der Safe Harbor Privacy Principles[198] verpflichtet. Seit den Enthüllungen von Edward Snowden wird von vielen jedoch die Adäquanz des Datenschutzniveaus von Safe Harbor bezweifelt.[199]

(2) Ist Safe Harbor zukunftssicher?

Im Juli 2014 richtete der High Court of Ireland in einem vom Datenschutzaktivisten Max Schrems angestrengten Verfahren ein Vorabentscheidungsersuchen an den EuGH, mit dem die Frage beantwortet werden soll, ob nationale Behörden an die Entscheidung der Kommission aus dem Jahre 2000 über die Adäquanz von Safe Harbor gebunden sind (C-362/14). Sollte der EuGH entscheiden, dass nationale Behörden im Licht tatsächlicher Entwicklungen, die seit der erstmaligen Veröffentlichung der Entscheidung der Kommission eingetreten sind, eigene Ermittlungen anstellen müssen oder zumindest können, so würde dies dazu führen, dass zumindest in manchen Mitgliedstaaten die Adäquanz von Safe Harbor verneint würde.

Bis zur Entscheidung des EuGH in dieser Sache ist die Zukunftssicherheit von Safe Harbor daher jedenfalls in Frage gestellt.[200]

d. Neuerungen der Datenschutzgrundverordnung

Da der geltende datenschutzrechtliche Rahmen durch die Datenschutzgrundverordnung (DS-GVO) erhebliche Änderungen erfahren wird, soll deren Regelungsansatz im Folgenden kurz erörtert werden:

Stelle stehen zwei unterschiedliche Standardvertragsklauseln zu Auswahl, jene nach Entscheidung 2001/497/EG (Set I) sowie jene nach Entscheidung 2004/915/EG (Set II). Für Datenübermittlungen zwischen einer verantwortlichen Stelle und einem Auftragsverarbeiter sind die Standardvertragsklauseln gemäß Entscheidung 2010/87/EU zu verwenden. Vgl. Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, ABl. EU L 181, 4.7.2001, S. 19; Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl. EU L 385 vom 29.12.2004, S. 74; Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. EU L 39 vom 12.2.2010, S. 5.

196 BCR sind verbindliche konzernweit geltende Richtlinien, welche nach Genehmigung der zuständigen nationalen Datenschutzbehörden ein adäquates Datenschutzniveau im Konzern sicherstellen. Vgl. Artikel-29-Datenschutzgruppe, Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)“, WP 154, 2008, verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf, zuletzt abgerufen am 23.3.2015.

197 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (bekannt gegeben unter Aktenzeichen K(2000) 2441), ABl. EU L 215 vom 25.8.2000, S. 7.

198 Siehe Anhang I der Entscheidung 2000/520/EG (auszulegen im Lichte der FAQ in Anhang II der Entscheidung).

199 Vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015, https://www.datenschutz.hessen.de/k89.htm#entry4319, zuletzt abgerufen am 24.3.2015.

200 Der Schlussantrag des Generalanwalts wird für den 24.6.2015 erwartet.

Die DS-GVO wurde von der Europäischen Kommission im Jahre 2011 vorgeschlagen[201] und vom Europäischen Parlament in erster Lesung am 12.3.2014 mit 207 Änderungen angenommen.[202] Derzeit (März 2015) verhandeln die Mitgliedstaaten im Rat über einen gemeinsamen Standpunkt, der dann im Trialog zwischen Rat, Europäischer Kommission und Europäischem Parlament weiteren Verhandlungen zu unterziehen sein wird.

Da es sich um eine EU-Verordnung handelt, wird sie grundsätzlich in allen Mitgliedstaaten einheitliches Recht schaffen.[203] Eine einheitliche Rechtsanwendung sollte nach dem Entwurf der Kommission insbesondere dadurch sichergestellt werden, dass die Kommission nach der DS-GVO 26 Zuständigkeiten für die Erlassung von Durchführungsverordnungen erhalten sollte.[204] In der vom Europäischen Parlament angenommenen Fassung sind hingegen nur noch 10 Durchführungsverordnungsermächtigungen enthalten.[205] Es steht zu befürchten, dass im verbleibenden legislativen Prozess die Anzahl der Verordnungsermächtigungen noch weiter reduziert und so eine Rechtslage geschaffen wird, die sich für einen unmittelbaren Vollzug weniger gut eignet und vor allem über den Weg von Vorabentscheidungsverfahren eine nähere Determinierung durch den EuGH erfahren wird. Diese Rechtsunsicherheit wird durch „Leitlinien, Empfehlungen und bewährte Praktiken", die vom Europäischen Datenschutzausschuss (dem Nachfolger der Artikel-29-Arbeitsgruppe) beschlossen werden können,[206] voraussichtlich nur unzureichend kompensiert werden.

Im Unterschied zum Bereich des EU-Kartellrechts soll die Europäische Kommission für die DS-GVO keine Vollzugszuständigkeit erhalten. Die Vollziehung der DS-GVO soll vielmehr ausschließlich durch die Mitgliedstaaten erfolgen.

Die in der DS-GVO vorgesehenen Strafen sollen nach dem Vorschlag der Kommission bis zu EUR 1.000.000 oder im Fall eines Unternehmens bis zu 2 % des weltweiten Jahresumsatzes betragen. In der vom Europäischen Parlament angenommen Fassung sind sogar Strafen von bis zu EUR 100.000.000 oder im Fall eines Unternehmens bis zu 5 % seines weltweiten Jahresumsatzes vorgesehen.

Die DS-GVO sieht in der vom Europäischen Parlament angenommenen Fassung vor, dass ein Betroffener gegenüber einem für die Verarbeitung Verantwortlichen das Recht hat, seine personenbezogenen Daten in einem interoperablen gängigen elektronischen Format zu erhalten, wenn der Betroffene die Daten dem für die Verarbeitung Verantwortlichen zuvor zur Verfügung gestellt hatte und die Daten in weiterer Folge elektronisch verarbeitet wurden.[207] Soweit technisch machbar und verfügbar, sind die Daten auf Verlangen des

---

[201] Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endgültig.

[202] 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[203] Hiervon ausgenommen sein sollen Abwägungsfragen i.Z.m. dem Grundrecht auf freie Meinungsäußerung (Art. 80 DS-GVO), Abwägungsfragen i.Z.m. dem Recht auf Zugang zu amtlichen Dokumenten (Art. 80a DS-GVO), die Verarbeitung personenbezogener Gesundheitsdaten (Art. 81 DS-GVO) und die Datenverarbeitung im Beschäftigungskontext (Art. 82 DS-GVO) sowie die Datenverarbeitung im Bereich der sozialen Sicherheit (Art. 82a DS-GVO).

[204] Art. 86 DS-GVO i.d.F. COM (2012), 11.

[205] Art. 86 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

[206] Art. 66 Abs. 1 lit. b DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

[207] Art. 15 Abs. 2a Satz 1 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

Betroffenen sogar unmittelbar an einen anderen für die Verarbeitung Verantwortlichen zu übermitteln.[208]

Im Unterschied zur geltenden Rechtslage (siehe hierzu oben, III.3.b.) würde die DS-GVO in der vom Europäischen Parlament angenommenen Fassung daher ein Recht des Betroffenen auf Datenportabilität einführen. Ob dies ausreichend ist, um die oben unter II.3.a.(2) beschriebenen Lock-in-Effekte zu überwinden, wird unten im Folgenden unter IV.5. untersucht.

4. Urheberrecht in der grenzüberschreitenden Durchsetzung

Wie oben (II.4.) ausgeführt, stellen in vielen Mitgliedstaaten Website-Sperren das Mittel der Wahl zur grenzüberschreitenden Durchsetzung des Urheberrechts dar. Im Folgenden soll daher der in Deutschland geltende Rechtsrahmen für derartige Website-Sperren skizziert werden: Art. 8 Abs. 3 Information-Society-Richtlinie[209] (InfoSoc-RL) sieht vor, dass die Mitgliedstaaten sicherzustellen haben, dass die Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. In der Rechtssache UPC Telekabel Wien GmbH ./. Constantin Film Verleih GmbH[210] entschied der EuGH, dass es nach dem nationalen Recht, das diese Richtlinienbestimmung umsetzt, möglich sein muss, eine einstweilige Verfügung gegen einen Internet-Access-Provider zu erwirken, die diesen dazu verpflichtet, den Zugang zu einer urheberrechtsverletzenden Website zu sperren.[211] Eine entsprechende Bestimmung findet sich im UrhG jedoch nicht,[212] weshalb im Unterschied zu anderen Mitgliedstaaten der EU[213] in Deutschland bisher noch keine urheberrechtlichen Website-Sperrverfügungen erlassen wurden.[214] Zuletzt urteilte das OLG Köln, dass die Störerhaftung zwar grundsätzlich eine hinreichende Grundlage für eine Website-Sperre sei,[215] verweigerte diese im Ergebnis aber aus Gründen der Zumutbarkeit für den Internet-Access-Provider.[216]

5. Rechtsdurchsetzungsmöglichkeiten gegenüber globalen Diensteanbietern

Im Folgenden soll der derzeit geltende Rechtsrahmen für die Rechtsdurchsetzung gegenüber globalen Diensteanbietern in den Bereichen des Verbraucherschutzes, des Datenschutzes sowie im Regulierungsrecht skizziert werden. Dieser ist für die oben (II.3.c.) beschriebene Effektivität des für globale Diensteanbieter kraft Marktort geltenden Rechts von besonderer Bedeutung.

---

208 Art. 15 Abs. 2a Satz 2 leg cit.

209 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EU L 167 vom 22.6.2001.

210 EuGH 27.3.2014, RS. C-314/12.

211 J. B. Nordemann, Anmerkung zu EuGH, Urteil vom 27. März 2014 – C-314/12 – UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH („Kino.to“), ZUM 2014, 499; M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), GRUR 2015, 19; vgl. aber S. Maaßen, Unbestimmte Sperrungsverfügung gegen Internetprovider verstößt nicht gegen EU-Recht, GRUR-Prax 2014, 157 (Spruchpunkt 1 der Entscheidung verkennend).

212 Das OLG Hamburg sah in einer begehrten Sperre einen grundrechtsrelevanten Eingriff und lehnte eine Sperrverfügung mangels gesetzlicher Grundlage ab, OLG Hamburg, GRUR-RR 2014, 140, 145 f. – 3dl.am.

213 Vgl. ausführlich L. Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law - Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?, TTLF Working Paper No. 13, S. 22 ff, verfügbar unter http://www.law.stanford.edu/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf, zuletzt abgerufen am 22.3.2015.

214 Eine kompakte Judikaturübersicht bietet M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), GRUR 2015, 19.

215 OLG Köln, GRUR 2014, 1081, 1084, 1086 - Goldesel. So auch M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105, 115.

216 OLG Köln, GRUR 2014, 1081, 1095 - Goldesel.

a. Verbraucherschutz

Art. 11 Abs. 1 der Richtlinie über unlautere Geschäftspraktiken[217] (UGP-RL) sieht vor, dass die Mitgliedstaaten im Interesse der Verbraucher sicherzustellen haben, dass geeignete und wirksame Mittel zur Bekämpfung unlauterer Geschäftspraktiken vorhanden sind. Unlauterer Wettbewerb soll sich demnach nicht mehr lohnen.[218] Eine entsprechende Umsetzung findet sich insbesondere in § 10 UWG.

Der Anspruch aus § 10 UWG richtet sich auf Herausgabe des unlauter erzielten Gewinns ohne Rücksicht darauf, wer im Einzelnen geschädigt wurde. Anspruchslegitimiert sind rechtsfähige Verbände zur Förderung gewerblicher oder selbständiger beruflicher Interessen,[219] Verbraucherschutzorganisationen[220] sowie die Industrie- und Handelskammern (IHK).[221] Voraussetzungen des Gewinnabschöpfungsanspruchs sind eine vorsätzliche unzulässige geschäftliche Handlung sowie Gewinnerzielung zu Lasten einer Vielzahl von Abnehmern.[222] Liegen diese Voraussetzungen vor, ist der abgeschöpfte Gewinn unmittelbar an den Bundeshaushalt abzuführen.

In der Praxis ist jedoch problematisch, dass der Anspruchsberechtigte den Anspruch oftmals nicht beziffern kann.[223] Darüber hinaus fehlt angesichts der Tatsache, dass die anspruchslegitimierten Verbände zwar das Prozessrisiko tragen, aber alle eingenommenen Gelder an den Bundeshaushalt abführen müssen, der wirtschaftliche Anreiz zur Geltendmachung des Anspruchs.[224] § 10 UWG wird daher in der Literatur weitestgehend als „totes Recht“ angesehen.[225]

b. Datenschutz

Art. 24 der Datenschutzrichtlinie[226] sieht vor, dass die Mitgliedstaaten für Fälle von schuldhaften Datenschutzverstößen das Vorhandensein von Sanktionsmaßnahmen

---

[217] Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates v. 11.5.2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. EU L 149/22 vom 11.6.2005.

[218] C. Alexander, Marktsteuerung durch Abschöpfungsansprache, JZ 2006, 890, 893 f.; M. Goldmann, in: H. Harte-Bavendamm/F. Henning-Bodewig, UWG-Kommentar, 3. Aufl. 2013, § 10 Rn. 11.

[219] §§ 10 I, 8 III Nr. 2 UWG.

[220] Es sind dies gem. §§ 10 I, 8 III Nr. 2 UWG qualifizierten Einrichtungen, die nachweisen, dass sie in die Liste qualifizierter Einrichtungen nach § 4 des Unterlassungsklagengesetzes oder in dem Verzeichnis der Kommission der Europäischen Gemeinschaften nach Art. 4 der Richtlinie 98/27/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über Unterlassungsklagen zum Schutz der Verbraucherinteressen, Abl. EU L 166/51 vom 11.6.1998, eingetragen sind.

[221] Vgl. §§ 10 I, 8 III Nr. 4 UWG.

[222] Maßgebend sind hier die Umstände des Einzelfalls, es muss sich lediglich um einen größeren Personenkreis handeln, vgl. Begr RegE UWG 2004 zu § 10 Abs. 1, BT-Drs 15/1487 S. 24. Die Untergrenze liegt wohl bei drei Abnehmern (vgl. BGH NJW 2002, 128, 139; P. von Braunmühl, in: K.-H. Fezer, UWG-Kommentar, 3. Aufl. 2015, § 10 Rn. 196).

[223] H. Köhler, in: H. Köhler/J. Bornkamm, UWG-Kommentar, 33. Aufl. 2015, § 10 Rn. 15.

[224] Vgl. C. Alexander, Schadensersatz und Abschöpfung im Lauterkeits- und Kartellrecht, 2010, Tübingen, S. 505 ff.; S. Sieme, Die Auslegung des Begriffs „zu Lasten“ in § 10 UWG und § 34a GWB, WRP 2009, 914; A. van Raay, Gewinnabschöpfung als Präventionsinstrument im Lauterkeitsrecht, 2012, S. 181 berichtet, dass vom Inkrafttreten des § 10 UWG bis April 2011 nur EUR 47 305,78 aus lediglich vier erfolgreichen Verfahren an den Bundeshaushalt geflossen sind.

[225] M. Goldmann, in: H. Harte-Bavendamm/F. Henning-Bodewig, UWG-Kommentar, 3. Aufl. 2013, § 10 Rn. 5.

[226] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EU L 281/31 vom 23.11.1995.

sicherzustellen haben. In Deutschland wird dies durch § 43 Abs. 3 BDSG umgesetzt, der die Durchführung von Bußgeldverfahren ermöglicht. Im Rahmen der Bußgeldverfahren können Verstöße gegen das BDSG mit Bußgeldern bis zu einer Höhe von EUR 300.000 geahndet und rechtswidrig erlangte Gewinne abgeschöpft werden.[227] Im Gegensatz zu § 10 UWG, bei dem rechtsfähige Verbände tätig werden müssen, handelt es sich bei der Gewinnabschöpfung im Rahmen des § 43 BDSG um ein staatliches Verfahren.

Die praktische Relevanz des Ordnungswidrigkeitsverfahrens zeigt sich darin, dass die Zahl der verhängten Bußgelder sowie auch deren Höhe in letzter Zeit stark zugenommen hat.[228]

c. Regulierungsrecht

Anders als im Daten- und Verbraucherschutzrecht existiert im Regulierungsrecht keine gemeinschaftsrechtliche Vorgabe.[229] Dennoch wurde 2004 im Rahmen der TKG-Novelle[230] § 43 TKG eingefügt, der sicherstellen soll, dass rechtswidrig erlangte Vorteile nicht einfach behalten werden dürfen.[231] Die Vorschrift ermöglicht daher die Abschöpfung wirtschaftlicher Vorteile, die auf einen schuldhaften Verstoß gegen das TKG oder gegen eine Verfügung der Bundesnetzagentur zurückgehen. Dem liegt der Gedanke zugrunde, dass sich der Verstoß ökonomisch nicht mehr lohnen soll.[232] Zudem besteht die Möglichkeit, wirtschaftliche Vorteile nach § 149 Abs. 2 TKG im Rahmen eines Ordnungswidrigkeitsverfahrens abzuschöpfen. Die Bedeutung des § 43 TKG ist in der Praxis gering.[233]

---

227 Vgl. § 43 Abs. 3 BDSG.

228 Vgl. P. Gola, Aus den aktuellen Berichten der Aufsichtsbehörden (17): Die Bußgeldpraxis, RDV 2015, 26, 27 auch m.w.N. und Beispielen aus der Praxis.

229 Vgl. J. Wimmer, in: H. Gersdorf/B. Paal (Hrsg.), Beck-OK TKG, Stand 1.2.2015, § 43 Rn. 2.

230 Telekommunikationsgesetz (TKG) vom 22. Juni 2004 (BGBl. I S. 1120).

231 K. Holthoff-Frank, in: M. Geppert/R. Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 43 Rn. 1; für eine instrumentelle Analyse der Gewinnabschöpfung nach § 43 TKG und eine Gegenüberstellung zu den Parallelvorschriften des GWB, EnWg sowie des UWG, vgl. A. Elbracht, Das Sanktionsinstrumentarium im TKG im Kontext der Rückführung sektorspezifischer Regulierung, 2009, S. 116 ff.

232 J. Wimmer, in: H. Gersdorf/B. Paal (Hrsg.), Beck-OK TKG, § 43 Rn. 1.

233 J. Neitzel/D. Hofmann, in: G. Spindler/F. Schuster (Hrsg.), Recht der elektronischen Medien, § 43 Rn. 5.

IV. Defizite der aktuellen Rechtslage und Empfehlungen für dessen Optimierung - „Digitaler Kodex“

1. Reduzierung der Komplexität der Rechtsregeln

a. Rechtskomplexität und Transaktionskosten

Die Komplexität des derzeitigen in der EU bestehenden Regelungsgefüges für die digitale Wirtschaft ergibt sich einerseits aus der Unterschiedlichkeit der in jedem Mitgliedstaat bestehenden Rechtsnormen, andererseits aus der hohen Regelungsdichte und der aus Grenzverwischungen resultierenden, oben (II.1.) exemplarisch dargestellten Gemengelage von Rechtsnormen, mit der gerade auch die Anbieter konvergenter Dienste konfrontiert sind.

Hierdurch erhöhen sich die durchschnittlichen Kosten, die für die Abwicklung einer ökonomischen Transaktion (z.B. die Erbringung eines digitalen Dienstes oder die Lizenzierung eines Musikrepertoires für den gesamten EWR) aufgewendet werden müssen; zu diesen Kosten zählen insbesondere die Kosten der Erfüllung regulatorischer Vorgaben (z.B. Einholung einer behördlichen Genehmigung), der Vertragsgestaltung sowie der Rechtsdurchsetzung.

Um die Rechtskomplexität und damit die Transaktionskosten zu mindern, wird häufig eine Rechtsvereinheitlichung auf Unionsebene befürwortet.[234] Die derzeit im nationalen Recht bestehende Regelungsdichte lediglich auf die Ebene des Unionsrechts zu verlagern, dürfte allerdings keine signifikante Reduktion der Transaktionskosten mit sich bringen, zumal auch derart weitreichende Änderungen der Rechtslage mit hohen Kosten verbunden sind.[235] Die eigentliche Herausforderung besteht vielmehr darin, die Regelungsdichte in den relevanten Rechtsbereichen zu vermindern - und zwar zunächst unabhängig davon, ob die Regelungen auf nationaler Ebene oder auf Unionsebene angesiedelt sind. Wie eine solche Reduzierung übermäßiger Regelungskomplexität aussehen könnte, lässt sich am Beispiel der Location Based Services illustrieren (nachfolgend, unter b.).

b. Schaffung eines einheitlichen Rechtsrahmens für Location Based Services

Der geltende Rechtsrahmen für standortbezogene Dienste ist unzureichend: Es ist unklar, welche Regelungen Anwendungen finden[236] und die einzige speziell auf Standortdaten bezogene Regelung ist in der Praxis in vielen Fällen nicht umsetzbar.[237]

Es ist daher empfehlenswert, die Erhebung, Verarbeitung und Nutzung standortbezogener Daten neu zu regeln; dabei liegt es nahe, die Rechtslage zu vereinheitlichen und einen einheitlichen Rechtsrahmen für die Erhebung, Verarbeitung, Übermittlung und Nutzung von Standortdaten zu schaffen.

---

[234] Vgl. z.B. European Commission - Fact Sheet, Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, 18. 1. 2015, http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm, zuletzt abgerufen am 2.4.2015, (die Ersparnisse durch eine Beseitigung des Fleckenteppichs der nationalen Datenschutzgesetze auf EUR 2,3 Milliarden pro Jahr bemessend). Ihre Forderung nach einer Vollharmonisierung des Urheberrechts begründete die European Copyright Society in einem Brief vom 19.12.2014 an Günther Oettinger ebenso mit der aus den nationalen Urheberrechtsgesetzen resultierenden Fragmentierung des Marktes anhand der nationalen Grenzen; http://www.ivir.nl/syscontent/pdfs/78.pdf, zuletzt abgerufen am 4.4.2015.

[235] A. Marciano/J.-M. Josselini, From Economic to Legal Competition - New Perspectives on Law and Institutions in Europe, 2003, Cheltenham, S. 66.

[236] § 98 TKG, TMG oder BDSG, vgl. oben, III.1.b.

[237] Vgl. oben, III.1.b.

Eine solche Neuregelung sollte unabhängig von der zur Erhebung der Standortdaten verwendeten Methode sein und würde an der Art der Daten anknüpfen. Derartige Sondervorschriften für bestimmte Kategorien von Daten sind im Datenschutzrecht nichts Ungewöhnliches. So gibt es die besonderen Arten personenbezogener Daten im BDSG oder die Unterscheidung zwischen Bestands- und Nutzungsdaten im TKG. Soweit es sich um Regelungen für die Wirtschaft handelt, ist - wie beim BDSG - die Gesetzgebungskompetenz des Bundes gegeben. Die Regelung wäre dann im Detail auf ihre europarechtliche Tauglichkeit zu prüfen, allerdings erlaubt insbesondere die Datenschutzrichtlinie spezielle Regelungen, so lange ihre Mindeststandards erfüllt werden. Mit Blick auf die anstehende EU-Datenschutzgrundverordnung, die zu einer Vollharmonisierung führen soll, wäre eine Regelung auf europäischer Ebene wünschenswert - allerdings auch schwerer zu erreichen.

Die Regelung sollte folgende Aspekte berücksichtigen:

Grundsätzlich sollte die Erhebung, Verarbeitung und Nutzung von Standortdaten die Einwilligung des Betroffenen voraussetzen. Allerdings sollte die Erteilung der Einwilligung auch elektronisch möglich sein, ein Schriftformerfordernis wie derzeit in § 98 Abs. 1 Satz 4 TKG ist in der Praxis nicht handhabbar und ist eher geeignet, den Datenschutz zu schwächen (da sie mangels Praktikabilität häufig ignoriert wird). Die Einwilligung wäre von der Person zu erteilen, deren Standort erhoben wird, in der Terminologie des TKG also vom Nutzer.[238] Sollen die standortbezogenen Daten auch für Werbezwecke genutzt werden, so könnte hierfür eine gesonderte Einwilligung vorgesehen werden.

Während die Einwilligung gegenüber einem Anbieter grundsätzlich für mehrere Ortungen zum gleichen Zweck erteilt werden kann, sollte der Nutzer die Möglichkeit haben, zu verlangen, über jede Ortung informiert zu werden und nachvollziehen zu können, wann welcher Dienst Standortdaten abgefragt hat. Die Form der Information sollte technologieneutral gehalten werden.[239] So wird vermieden, dass die Information nicht erfolgt, weil sie - wegen zu enger gesetzlicher Vorgaben - praktisch nicht durchführbar ist.

Der Nutzer sollte stets die Möglichkeit haben, die Ortung - auch für einzelne Dienste - zu unterbinden. Anbieter sollten dazu verpflichtet werden, ihre Dienste auch ohne Standortdaten anzubieten, soweit dies möglich ist (beispielsweise indem in einen Restaurantführer Adressen auch manuell eingetragen werden).

Die Erstellung von Bewegungsprofilen sollte grundsätzlich ganz verboten werden. Soweit sie für bestimmte Dienste notwendig sind, sollte der Nutzer ausdrücklich darüber informiert werden, dass Bewegungsprofile erstellt werden und diesbezüglich eine separate Einwilligung erteilen müssen. Die Nutzung der Bewegungsprofile für andere Zwecke als die Erbringung des Dienstes sollte ausgeschlossen werden.

2. Schaffung eines geeigneten Rechtsrahmens für IoT

Wie oben (III.1.a.) beschrieben, ist der derzeit geltende telekommunikationsrechtliche Rahmen für Machine-to-Machine-Dienste nicht sachadäquat. So können Konstellationen auftreten, in denen Anbieter von Machine-to-Machine-Diensten telekommunikationsrechtlichen Verpflichtungen unterliegen, die auf Kommunikationsdienste zugeschnitten sind, bei denen Menschen eine aktive Rolle spielen.

---

[238] Eine Einwilligung des „Teilnehmers“ wäre nicht umsetzbar, da Standortdaten auch verarbeitet werden könnten, ohne dass es einen Vertragsschluss gibt, wie zum Beispiel bei der standortbezogenen Werbung.

[239] Das Erfordernis, per „Textmitteilung“ zu informieren erzeugt einige praktische Probleme, zum Beispiel dann, wenn das Endgerät keinen Bildschirm hat.

Zwar lassen sich einige der dargestellten Anwendungsprobleme durch eine zweckgerichtete Auslegung der relevanten Tatbestandsmerkmale minimieren.[240] Zur Gewährleistung von Rechtssicherheit sollte dennoch eine Anpassung des TKG erwogen werden, welche die Anwendung der telekommunikationsrechtlichen Verpflichtungen im Kontext von Machine-to-Machine-Diensten sinnvoll begrenzt. Zu diesem Zweck sollte eine Definition des Begriffs der Machine-to-Machine-Dienste in das TKG aufgenommen werden. Diese kann sich an der entsprechenden Definition des GEREK orientieren (s. dazu oben, II.1.a.(1)).

Es sollte ferner gesetzlich klargestellt werden, dass die Klassifizierung von Machine-to-Machine-Diensten als Telekommunikationsdienste nicht auf Grundlage der einzelnen Bestandteile des Machine-to-Machine-Dienstes, sondern nach dem Schwerpunkt des Diensteangebots zu erfolgen hat.[241]

Insoweit kann die bereits im Telekommunikationsgesetz enthaltene Regelungskategorie „telekommunikationsgestützte Dienste“ (§ 3 Nr. 25 TKG) dazu dienen, konvergente Machine-to-Machine-Dienste, die zwar eine Übertragungsleistung beinhalten, deren Schwerpunkt jedoch auf der Bereitstellung der (Inhalte-)Leistung liegt, weitgehend vom Anwendungsbereich der Telekommunikationsregulierung auszunehmen. Durch die Erweiterung der Definition um einen nicht-abschließenden gesetzlichen Katalog von Regelbeispielen könnte der weite Anwendungsbereich dieser Dienstekategorie verdeutlicht werden; neben den bereits in der Gesetzesbegründung genannten Diensten,[242] können beispielsweise Machine-to-Machine-Dienste wie Telemetriedienste und andere konvergente Dienste wie z.B. Sicherheitsdienste im Connected-Car-Bereich aufgenommen werden.

Für diejenigen Machine-to-Machine-Dienste, die auch nach den oben dargestellten Änderungen als Telekommunikationsdienste anzusehen sind, sollte es in das pflichtgemäße Ermessen der BNetzA gestellt werden, bestimmte Machine-to-Machine-Dienstegruppen im Wege eines Dispens vom Anwendungsbereich telekommunikationsrechtlicher Vorschriften auszunehmen.

3. Anpassungsbedarf beim IT-Sicherheitsgesetz

Die Gewährleistung eines ausreichenden Maßes an IT-Sicherheit hängt, wie oben (unter II.2.) dargestellt, entscheidend davon ab, dass die Transparenz der IT-Sicherheit erhöht und ein einheitliches Mindestschutzniveau für Kritische Infrastrukturen geschaffen wird und dass die entsprechenden Maßnahmen mit den zu erwartenden Vorgaben auf europäischer Ebene abgestimmt werden.

Wegen der mangelnden Konkretisierung der Tatbestandmerkmale, die eine Meldepflicht auslösen können, bestehen Unklarheiten, welche die Eignung der Regelungen zur Schaffung von Transparenz beeinträchtigen. Der IT-SiG-E verwendet eine Vielzahl unbestimmter, ausfüllungsbedürftiger Rechtsbegriffe („erhebliche Störung“, „Beeinträchtigung der Funktionsfähigkeit“, „führen kann“), die in ihrem Zusammenspiel praktisch kaum handhabbar sind.

Eine Konkretisierung, wann eine meldepflichtige Störung vorliegt, soll nach der Vorstellung des Gesetzgebers erst auf der Grundlage eines vom BSI in Zusammenarbeit mit den Betreibern und deren Aufsichtsbehörden zu entwickelnden Kriterienkatalogs erfolgen.[243] Bis diese Kriterien vorliegen,

---

[240] Dazu bereits oben, II.1.a.

[241] Dies ist beispielsweise in Österreich - zumindest in Teilen - durch eine Ausnahmeregelung für sog. „Nebendienstleistungen“ gewährleistet (vgl. Regierungsvorlage 128 BlgNR XXII. GP, S. 4 (zu § 3 Ziff. 9). Die Abgrenzung erfolgt nach dem Schwerpunkt der Dienstleistung als solches.

[242] BT-Drs. 15/2316, S. 58 nennt „beispielsweise“ Mehrwertdienste.

[243] BT-Drs. 18/4096 v. 25.2.2015, S. 28.

dürfte es für die Betreiber Kritischer Infrastrukturen nur schwer zu bestimmen sein, wann eine mögliche Störung oder Beeinträchtigung eine Meldepflicht auslöst. Um sicherzustellen, dass die vorgesehenen Meldepflichten ihren Zweck erfüllen, ist eine Präzisierung der Auslöser für die Meldepflicht von Betreibern Kritischer Infrastrukturen geboten.[244] Sollte eine entsprechende Präzisierung nicht bereits im Gesetz erfolgen, so sollten bereits mit Inkrafttreten der Meldepflicht Leitlinien vorgelegt werden, welche die Meldepflicht für die Verpflichteten handhabbar machen. Als Ausgangspunkt kann der Leitfaden zur Meldepflicht von erheblichen Sicherheitsvorfällen dienen,[245] den die BNetzA für den Telekommunikationsbereich erlassen hat.

Die praktische Wirkung der Meldepflicht könnte ferner dadurch eingeschränkt sein, dass der IT-SiG-E keine Sanktionen für den Fall vorsieht, dass Betreiber ihren Meldepflichten nicht nachkommen. Es sollten daher Regelungen aufgenommen werden, die es ermöglichen, einen Verstoß gegen die Meldepflichten angemessen zu sanktionieren. So wäre darüber hinaus sichergestellt, dass die Vorgabe des NIS-Richtlinienentwurfs zur Implementierung von Sanktionen zur Ahndung von Verstößen gegen die in Umsetzung der NIS-Richtlinie erlassenen nationalen Vorschriften eingehalten wird.[246]

Auch darüber hinausgehend sollte eine stärkere Abstimmung des IT-SiG-E an die zu erwartenden europarechtlichen Vorgaben erfolgen. Dies gilt insbesondere mit Blick auf die Auswahl der Sektoren, die für die Bestimmung der Kritischen Infrastrukturen relevant sind.

Zwar bezweckt der NIS-Richtlinienentwurf lediglich eine Mindestharmonisierung, so dass es den Mitgliedstaaten nicht verwehrt ist, Regelungen zu erlassen oder aufrechtzuerhalten, die ein höheres Schutzniveau gewährleisten als die Vorgaben der NIS-Richtlinie. Daher ist der deutsche Gesetzgeber grundsätzlich dazu befugt, auch Sektoren in den Anwendungsbereich der Verpflichtungen für Betreiber Kritischer Infrastrukturen einzubeziehen, die von dem NIS-Richtlinienvorschlag nicht genannt sind.

Eine ausschließlich in Deutschland umgesetzte Regulierung von Betreibern Kritischer Infrastrukturen in den Sektoren Transport- und Versicherungswesen, Informationstechnik (abseits von Internet-Knoten) sowie Finanzwesen (abseits von Banken und Finanzmarktinfrastrukturen) würde jedoch erhebliche Nachteile für deutsche Unternehmen im europäischen Wettbewerb bewirken.

Dies ließe sich allenfalls dann rechtfertigen, wenn mit dieser über die NIS-RL hinausgehenden Regulierung erhebliche Sicherheitsgewinne erzielt würden.

Dies ist allerdings nicht der Fall. Wie oben dargestellt (II.2.b.), besteht eine wechselseitige Abhängigkeit dieser Infrastrukturen untereinander,[247] die es verbietet, den Schutz Kritischer Infrastrukturen auf die nationale Ebene beschränken.[248] Daher hätte die Verpflichtung von Betreibern Kritischer Infrastrukturen zur Implementierung von Sicherheitsmaßnahmen und zur Meldung von Sicherheitsvorfällen in nur einem Mitgliedstaat kaum positive Wirkungen im Hinblick auf die

---

[244] BR-Drs. 643/14 v. 06.2.2015, S. 1.

[245] Abrufbar unter http://www.bundesnetzagentur.de/cln_1421/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/MitteilungSicherheitsverletzung/Mitteilungeinersicherheitsverletzung-node.html, zuletzt abgerufen am 31.3.2015.

[246] Art. 17 Abs. 1 NIS-Richtlinienentwurf; s. dazu auch P. Bräutigam/S. Wilmer, Big brother is watching you? - Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38, 41.

[247] BT-Drs. 18/4096 v. 25.2.2015, S. 2.

[248] S. EU Kommission, Communication on Critical Information Infrastructure Protection, S. 5.

Schaffung von Transparenz und die Erhöhung des Schutzniveaus für die betreffenden Infrastrukturen.[249]

Vor diesem Hintergrund sollte der IT-SiG-E in seinem persönlichen Anwendungsbereich auf die von der NIS-RL erfassten Betreiber Kritischer Infrastrukturen beschränkt werden.

4. Verbesserung des Schutzes von Persönlichkeitsrechten

Um die oben (II.3.a.) beschriebenen Herausforderungen im Zusammenhang mit der Behandlung personenbezogener Daten als Vermögenswert zu adressieren, sind eine Reihe von Anpassungen der rechtlichen Rahmenbedingungen denkbar:

a. Rechtliche Reaktion auf die Funktion personenbezogener Daten als Vermögenswert

Wie oben (III.3.a.) ausgeführt, kann die Zustimmung zur Verarbeitung personenbezogener Daten derzeit nicht im Rechtssinne als Entgelt angesehen werden. Dessen ungeachtet kommt personenbezogenen Daten in wirtschaftlicher Hinsicht die Funktion einer Gegenleistung zu.[250] Es sollte daher sichergestellt werden, dass ein fairer Wettbewerb zwischen entgeltlichen Diensten und „Gratis-Diensten" besteht, die eine Einwilligung zur Verarbeitung personenbezogener Daten voraussetzen. Ein Instrument zur Schaffung eines solchen „level playing field" sind Aufklärungspflichten: Wenn Art und Umfang der Datenverarbeitung, in die vor Verwendung eines „Gratis-Dienstes" einzuwilligen ist, im selben Maße transparent für einen Nutzer ist, wie der Euro-Preis einer entgeltlichen Dienstleistung, wird der Nutzer in die Lage versetzt, den von ihm verlangten „Preis" der Bereitstellung seiner personenbezogenen Daten mit dem Euro-Preis der entgeltlichen Dienstleistung zu vergleichen.

Dass vorformulierte Einwilligungserklärungen grundsätzlich der AGB-Kontrolle der §§ 305 ff BGB unterliegen,[251] stellt für sich allerdings keine Lösung dieses Problems dar. Denn wenn personenbezogene Daten gegenüber OTT-Anbietern aus wirtschaftlicher Sicht die Hauptleistung des Nutzers darstellen, sollte nicht erst aus dem Studium der AGB für den Nutzer ersichtlich werden, worin seine Hauptleistung besteht.

Um einen fairen Wettbewerb zu unterstützen, ist daher eine Erhöhung der Transparenz hinsichtlich der vom OTT-Anbieter vorgenommenen Datenverarbeitung erforderlich.

b. Schaffung eines klaren Rechtsrahmens für die wirtschaftliche Verwertung von Kundendaten

Wie oben (IV.4.a.) ausgeführt, besteht eines der zentralen Defizite der derzeitigen Rechtslage und Praxis der wirtschaftlichen Verwertung von Kundendaten darin, dass Einwilligungen in die Verwertung der Daten zwar einerseits die wirtschaftliche Funktion eines vom Nutzer zu leistenden Entgelts einnehmen, andererseits aber der Bedeutungsgehalt der Einwilligung für den Nutzer in vielen Fällen wenig transparent ist. Um den Nutzern eine informierte Entscheidung zwischen entgeltlichen Diensten und „Gratis-Diensten" zu ermöglichen - und auf diese Weise einen chancengleichen Wettbewerb zwischen „Gratis-Diensten" und Bezahldiensten zu ermöglichen -, sollten neuartige Wege beschritten werden.

Tatsächlich enthält die DS-GVO in der vom Europäischen Parlament angenommenen Fassung die Verpflichtung für verantwortliche Stellen, die Betroffenen durch die

---

[249] So auch C. Heinickel/L. Feiler, Der Entwurf für ein IT-Sicherheitsgesetz - europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis, CR 2014, 708.

[250] Vgl. M. Dorner, Big Data und „Dateneigentum" – Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617, 618; vgl. auch II.3.a.1.

[251] Vgl. z.B. BGH 11.11.2009, VIII ZR 12/08, CR 2010, 87 = ITRB 2010, 153 (Rössel) – HappyDigits.

Verwendung entsprechender Symbole über folgende Aspekte der Datenverarbeitung aufzuklären: (a) ob mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck der Verarbeitung erforderlich; (b) ob mehr personenbezogene Daten gespeichert werden, als für den jeweiligen Zweck der Verarbeitung erforderlich; (c) ob personenbezogene Daten zu anderen als den Zwecken verarbeitet werden, für die sie erhoben wurden; (d) ob personenbezogene Daten an gewerbliche Dritte weitergegeben werden; (e) ob personenbezogene Daten verkauft oder gegen Entgelt überlassen werden und (f) ob personenbezogene Daten verschlüsselt gespeichert werden.[252]

Eine derartige durch Symbole erfolgende Offenlegung der wichtigsten Aspekte der Datenverarbeitung ist grundsätzlich ein vielversprechender Lösungsansatz, da er eine leichte Wahrnehmbarkeit ermöglicht.

Die vom Europäischen Parlament gewählten Aspekte (insbesondere (a) bis (c)) sind allerdings für einen durchschnittlichen Nutzer allenfalls von geringer Aussagekraft: Mehr personenbezogene Daten (a) zu erheben oder (b) zu speichern, als für den jeweiligen Verarbeitungszweck erforderlich, würde auf Seiten des Nutzers ein klares Verständnis dafür voraussetzen, welche Daten für den jeweiligen Verarbeitungszweck tatsächlich erforderlich sind. Gleiches gilt für eine Verarbeitung für andere als die ursprünglich definierten Zwecke (c) stehen.

Darüber hinaus erscheint es unzweckmäßig, die Liste der in dieser Weise offenzulegenden Aspekte der Datenverarbeitung sowie die jeweiligen entsprechenden Symbole in der DS-GVO selbst zu regeln. Denn während zukünftige Änderungen der DS-GVO nur schwer bzw. mit großer Zeitverzögerung möglich sein werden, ist geradezu davon auszugehen, dass sich die Bedürfnisse der Praxis hinsichtlich der Transparenz unterschiedlicher Aspekte der Datenverarbeitung in den nächsten Jahren ändern werden.

Es sollte daher erwogen werden, die Festlegung der auf diese vereinfachte Weise offenzulegenden Aspekte der Datenverarbeitung einer Durchführungsverordnung der Europäischen Kommission oder einer Empfehlung des Europäischen Datenschutzausschusses (dem Nachfolger der Artikel-29-Arbeitsgruppe) vorzubehalten, wobei hierbei vorab einzuholenden Stellungnahmen der Wirtschaft besondere Bedeutung beigemessen werden sollte, da diese über unverzichtbare Expertise über die tatsächlich vorgenommenen Arten der Datenverarbeitung verfügt.

c. Einführung eines allgemeinen Kopplungsverbots

Die oben (unter a. und b.) beschriebenen Maßnahmen unterstellen, dass der Gesetzgeber die faktische Funktion der Einwilligung in die Verarbeitung personenbezogener Daten als Gegenleistung für Leistungen eines Unternehmers billigt. Dem würde ein Verbot entgegen stehen, die Einwilligung als Gegenleistung zu akzeptieren. Der Bundesrat hat in seiner Stellungnahme[253] zum „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Vorschriften von verbraucherschützenden Vorschriften des Datenschutzrechts“[254] vorgeschlagen, ein weitgehendes Kopplungsverbot zu schaffen. Demnach wäre es unzulässig, den Abschluss eines Vertrages von der Einwilligung des Vertragspartners in die Verarbeitung und Nutzung personenbezogener Daten zu Zwecken des Adresshandels und der Werbung abhängig zu machen; eine so erteilte Einwilligung wäre unwirksam. Dies kommt einem Verbot, die Einwilligung als Gegenleistung zu akzeptieren, nahe.

---

[252] Art. 13a DS-GVO i.d.F. der legislativen Entschließung des Europäischen Parlaments vom 12. März 2014.
[253] BR-Drs. 55/15(B).
[254] BR-Drs. 55/15.

Bisher kennt das BDSG ein Kopplungsverbot nur für den Fall, dass der Betroffene ohne Abschluss des Vertrages keinen Zugang zu gleichwertigen Leistungen hat.[255] In der Praxis spielt dieses Kopplungsverbot kaum eine Rolle. Kann der Unternehmer die Einwilligung nicht mehr zur Voraussetzung für die Erbringung eines Dienstes machen, so muss er sich die Diensterbringung anders vergüten lassen. Möglich wäre wohl noch,[256] kostenlose Verträge gegen Einwilligung und kostenpflichtige Verträge ohne Einwilligung anzubieten. Ob dieser doppelte Aufwand, Vergütungssysteme zu etablieren, tatsächlich in Kauf genommen wird, erscheint fraglich, möglich ist auch, dass Dienste auf die Einwilligung als Gegenleistung ganz verzichten.

Eine Bewertung des Vorschlags, ein allgemeines Kopplungsverbot einzuführen, allein aus juristischer Sicht fällt schwer. Sie hängt letztlich von der politischen Entscheidung ab, ob der Gesetzgeber die Nutzung personenbezogener Daten als Wirtschaftsgut anerkennen oder verhindern möchte. In letzterem Fall könnte sich das Kopplungsverbot bei einer auf den nationalen Markt beschränkten Betrachtung als hilfreich erweisen. Zu prüfen wären aber die Auswirkungen auf die Position deutscher (insbesondere auch kleinerer) Unternehmen im internationalen Wettbewerb: Werden die Daten von einem Unternehmen erhoben, das in einem anderen EU-Staat niedergelassen ist und in Deutschland keine Niederlassung hat (das können auch internationale Konzerne mit einer Tochter in einem anderen Mitgliedstaat sein), so findet das BDSG keine Anwendung (§ 1 Abs. 5 Satz 2 BDSG). Diese Unternehmen hätten das Kopplungsverbot dann nicht zu beachten.

d. Ausweitung der Klagemöglichkeiten von Verbänden gegen Datenschutzverstöße

Der aktuell diskutierte „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Vorschriften von verbraucherschützenden Vorschriften des Datenschutzrechts“ erstreckt die Möglichkeiten von Verbraucherverbänden und Kammern, Unterlassungsansprüche gegen Unternehmen durchzusetzen, ausdrücklich auch auf Verstöße gegen datenschutzrechtliche Vorschriften. Bisher ist dies nur über den Umweg des Verstoßes gegen Marktverhaltensregeln (§ 4 Nr. 11 UWG) möglich. Dabei ist aber nach wie vor umstritten, welche Regelungen des Datenschutzes Marktverhaltensregeln darstellen.[257]

Der Vorschlag ist aus unserer Sicht geeignet, die Beachtung datenschutzrechtlicher Regelungen zu fördern. Verbände haben durch ihre Klagen nach dem UKlaG bereits einige Klärungen im Bereich des AGB-Rechts bewirkt und es steht zu erwarten, dass sie auch im Bereich des Datenschutzes die Entwicklung von case law vorantreiben werden. Im Unterschied zu einzelnen Betroffenen verfügen Verbände oftmals über die erforderlichen Mittel und die juristische und technische Expertise, um gegen Datenschutzverstöße vorgehen zu können. Da der Kreis der Anspruchsberechtigten im UKlaG beschränkt ist,[258] dürfte auch die Gefahr einer weiteren (rechtsmissbräuchlichen) Abmahnwelle gering sein.[259]

Problematisch erscheint allerdings die so entstehende „Doppelzuständigkeit“ von Datenschutzbehörden und Verbänden. Konflikte könnten beispielsweise auftreten, falls eine Datenschutzbehörde eine bestimmte Verarbeitung im Rahmen ihrer Beratung in

---

[255] § 28 Abs. 3 Satz 3 BDSG; damit sind vor allem Monopolstrukturen gemeint, die in der Praxis aber nur selten auftreten.

[256] Bei wortlautgetreuer Auslegung wäre auch diese Variante unzulässig, denn der Abschluss des kostenlosen Vertrages wird eben auch von einer Einwilligung abhängig gemacht. Allerdings wird in der Stellungnahme des Bundesrates festgestellt, dass der Einwilligende selbst entscheiden können soll, ob er „für das Angebot mit Daten oder Euro bezahlen will“, BR-Drs. 55/15(B), S. 6.

[257] Vgl. E. Weidlich-Flatten, Verbraucherschutzverbände als Heilsbringer für den Datenschutz, ZRP 2014, 196, 197.

[258] Vgl. §§ 3 ff. UKlaG.

[259] So auch E. Weidlich-Flatten, Verbraucherschutzverbände als Heilsbringer für den Datenschutz, ZRP 2014, 196, 197.

Datenschutzfragen (§ 38 Abs. 1 Satz 2 BDSG) für zulässig erachtet und die Zivilgerichte dies auf Klage eines Verbands hin anders sehen und Unterlassung oder Beseitigung verlangen. Hier scheint es erwägenswert, beispielsweise eine Vermutung der Rechtmäßigkeit der Verarbeitung zu schaffen, wenn die Verarbeitung bereits behördlich geprüft wurde.

5. Gewährleistung von Datenportabilität

a. Lock-in-Effekte durch unzureichendes Recht auf Datenportabilität

Wie oben (III.3.b.) beschrieben, gibt es nach geltender Rechtslage kein Recht auf Datenportabilität. Um den Wettbewerb zwischen OTT-Anbietern zu fördern und die Markteintrittsschwelle für neue Anbieter zu reduzieren, wäre die Einführung eines solchen Rechts begrüßenswert.

Die DS-GVO wird voraussichtlich ein Recht auf Datenportabilität normieren. Wie oben (III.3.b.) ausgeführt, handelt es sich hierbei um ein Recht des Betroffenen gegenüber der verantwortlichen Stelle. Fungiert die verantwortliche Stelle als IT-Dienstleister (z.B. als Cloud Computing Provider) und besteht die Marktgegenseite aus Betroffenen, so ist dieses Recht auf Datenportabilität durchaus geeignet, die gewünschte wettbewerbsfördernde Wirkung zu erzielen. Denn in diesem Fall haben die Kunden in der Tat ein Recht, ihre Daten zu einen anderen Anbieter zu portieren und sind daher geringeren Switching Costs ausgestzt.

Sofern der IT-Dienstleister als Auftragsverarbeiter seiner Kunden fungiert, d.h. wenn die Marktgegenseite aus verantwortlichen Stellen und nicht aus Betroffenen besteht, greift das im Entwurf der DS-GVO vorgesehene Recht auf Datenportabilität allerdings nicht. Hat ein Einzelhandelsunternehmen beispielsweise sein Customer Relationship Management (CRM) System an einen externen IT-Dienstleister ausgelagert, so hätte das Einzelhandelsunternehmen nach dem Entwurf der DS-GVO kein gesetzliches Recht, die Daten in einem strukturierten, gängigen, wiederverwendbaren Format zu erhalten. Auch nach geltender Rechtslage hat eine verantwortliche Stelle kein derartiges gesetzliches Recht gegenüber seinem Auftragsverarbeiter.[260]

Dies stellt allerdings eine Regelungslücke dar, weil viele IT-Dienstleister, insbesondere OTT-Anbieter, einen wesentlichen Teil ihres Umsatzes mit Geschäftskunden tätigen, die nach den oben beschriebenen Grundsätzen kein Recht auf Datenportabilität hätten und, so die Befürchtung mancher, gegenüber großen IT-Dienstleistern auch eine zu schwache Verhandlungsposition hätten, um ein solches vertraglich zu erwerben.[261]

Die Ausgestaltung des Rechts auf Datenportabilität als ausschließliches Recht der Betroffenen ist daher nur in geringem Maße dazu geeignet, die oben beschriebenen Lock-in-Effekte von OTT-Diensten zu mindern. Zielführender wäre die Schaffung eines umfassenderen Rechts auf Datenportabilität (hierzu sogleich II.b.)

---

[260] Vgl. zur österreichischen Rechtslage OGH 15.4.2010, 6 Ob 40/10s wonach nach Beendigung von Personalverrechnungsdienstleistungen die Übergabe der Lohnverrechnungsdaten im PDF-Format und TXT-Format ausreichend sei, dass keine weitergehende Pflicht besteht, die vorhandenen Daten in einem ganz bestimmten, für den Auftraggeber am besten zu handhabenden Format zu übergeben, sei bereits nach dem Gesetzwortlaut eindeutig zu lösen.

[261] Mitteilung der Europäischen Kommission über die Freisetzung des Cloud-Computing-Potenzials in Europa, COM (2012) 529, 27.9.2012, 6, 13 (mit Verweis auf „nicht verhandelbare Standard-Vertragsbedingungen“).

b. Wettbewerbsförderung durch Schaffung eines umfassenden Rechts auf Datenportabilität

Um die Umstellungskosten für Kunden zu reduzieren und so den Wettbewerb zu fördern, sollte ein Recht auf Datenportabilität in zweifacher Hinsicht geschaffen werden:

Erstens als Recht der Betroffenen gegenüber der verantwortlichen Stelle: Die DS-GVO enthält in der vom Europäischen Parlament angenommenen Fassung bereits eine entsprechende zweckmäßige Regelung.[262] Da die DS-GVO voraussichtlich erst Ende des Jahres 2015 verabschiedet werden wird und eine Übergangsfrist von zwei Jahren vorgesehen ist,[263] ist mit der Durchsetzbarkeit der Regelung frühestens für Ende 2017 zu rechnen. Es sollte daher erwogen werden, der DS-GVO in diesem Punkt vorzugreifen und bereits jetzt ein Recht auf Datenportabilität als Betroffenenrecht in § 34 BDSG zu verankern.

Zweitens als Recht der verantwortlichen Stelle gegenüber dem Auftragsverarbeiter: Es sollte darauf hingewirkt werden, dass in Art. 26 DS-GVO ein Recht der verantwortlichen Stelle gegenüber dem Auftragsverarbeiter normiert wird, die vom Auftragsverarbeiter für die verantwortliche Stelle verarbeiteten Daten in einem interoperablen gängigen Format zu erhalten. Nur durch eine solche Ausdehnung des Rechts auf Datenportabilität auf verantwortliche Stellen kann das Ziel der Wettbewerbsförderung tatsächlich erreicht werden.

6. Verbesserung von Rechtsdurchsetzungsmöglichkeiten

Schwächen der Rechtsdurchsetzung gegen ausländische Unternehmen zeigen sich exemplarisch im Bereich des Urheberrechtsschutzes, für den auf Grundlage der InfoSoc-RL gesetzgeberischer Handlungsbedarf besteht (dazu a.), aber auch in den Bereichen des Verbraucher-, Datenschutz- und Regulierungsrechts, für die eine Stärkung des Instruments der Gewinnabschöpfung zu erwägen ist (dazu b.) sowie angesichts der praktischen Probleme des nationalen Verwaltungsvollzugs ein Vollzugsdefizit zu konstatieren ist (dazu c.).

a. Rechtsdurchsetzung gegen ausländische Rechtsverletzer

Wie oben (III.4.) dargestellt, gibt es derzeit in Deutschland (anders als beispielsweise in Österreich[264]) keine ausdrückliche, die Regelungen des Art. 8 Abs. 3 InfoSoc-RL umsetzende gesetzliche Grundlage für einstweiligen Verfügungen gegen Internet-Access-Provider, mit denen diese zur Sperrung urheberrechtsverletzender Websites verpflichtet werden könnten. Zuletzt entschied das OLG Köln, dass die Störerhaftung zwar grundsätzlich eine hinreichende Grundlage für eine Website-Sperre sei,[265] verweigerte diese im Ergebnis aber aus Gründen der Zumutbarkeit für den Internet-Access-Provider.[266] Da der EuGH in seiner Entscheidung UPC Telekabel Wien GmbH ./. Constantin Film Verleih GmbH[267] die Zumutbarkeit von Website-Sperren zwar einer Einzelfallprüfung durch das nationale Gericht vorbehalten, aber dennoch grundsätzlich bejaht hat,[268] ist die vom OLG Köln gewählte Linie grundsätzlich nicht mit Unionsrecht vereinbar.[269]

---

[262] Art. 15 Abs. 2a Satz 1 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

[263] Art. 91 Abs. 2 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

[264] Vgl § 81 Abs. 1a UrhG.

[265] OLG Köln, GRUR 2014, 1081, 1084, 1086 – Goldesel. So auch M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105, 115.

[266] OLG Köln, GRUR 2014, 1081, 1095 - Goldesel.

[267] EuGH 27. 3. 2014, C-314/12.

[268] EuGH 27. 3. 2014, C-314/12, Rn. 53.

[269] Zu berücksichtigen ist insbesondere, dass (i) es ausreichend ist, dass „unerlaubte Zugriffe auf die Schutzgegenstände […] erschwert werden“ (EuGH 27. 3. 2014, C-314/12, Rn. 62), insofern die Existenz von Umgehungsmöglichkeiten eine Bejahung der Zumutbarkeit nicht entgegensteht und (ii) die Kosten der Implementierung einer Sperre relativ

Die unzureichende Umsetzung der InfoSoc-RL[270] erweist sich als ein kaum überwindbares Hindernis für die Durchsetzung des deutschen Urheberrechts gegenüber ausländischen Rechtsverletzern. Website-Betreibern wie kinox.to ist es derzeit weiterhin möglich, ihren Nutzern unter Verstoß gegen § 19a UrhG tausende Kinofilme per Streaming anzubieten.

In Umsetzung des Art. 8 Abs. 3 InfoSoc-RL sollte daher eine ausdrückliche gesetzliche Grundlage geschaffen werden,[271] die es ermöglicht, einen Internet-Access-Provider im Wege der einstweiligen Verfügung zur Sperrung einer urheberrechtsverletzenden Website zu verpflichten. Allerdings bedarf eine solche Regelung einer Reihe flankierender Maßnahmen, um einerseits eine hinreichende Rechtmäßigkeitskontrolle von Websitesperren zu gewährleisten und andererseits einen fairen Interessensausgleich zwischen Rechteinhabern und Internet-Access-Providern zu ermöglichen:

Erstens sollte die Implementierung einer Website-Sperre einem Richtervorbehalt unterworfen werden, um sowohl missbräuchliche als auch irrtümliche Sperren zu vermeiden und insbesondere das Risiko eines Overblocking zu reduzieren (vgl. hierzu bereits II.4.).

Zweitens sollten Internet-Access-Provider einen Anspruch auf Kostenersatz für die Implementierung und Aufrechterhaltung von Website-Sperren erhalten. Schließlich werden die Internet-Access-Provider im Interesse der Rechteinhaber tätig, so dass es angemessen erscheint, die Kostentragung den Rechteinhabern zu überlassen.

Drittens sollten sowohl Betreiber gesperrter Websites als auch Nutzer einen Rechtsbehelf zur Verfügung haben, um die Rechtmäßigkeit einer Website-Sperre einer nochmaligen gerichtlichen Prüfung zu unterziehen.[272]

b. Erhöhung der Effektivität des für globale Diensteanbieter geltenden Rechts

Die Effektivität des für globale Diensteanbieter geltenden Rechts ist insbesondere dadurch gemindert, dass es häufig keine hinreichenden positiven oder negativen Anreize für rechtskonformes Marktverhalten gibt (s. dazu III.5.).

Während für den Bereich des Datenschutzes und des Regulierungsrechts durchaus praktikable Möglichkeiten der Gewinnabschöpfung bestehen (s. dazu III.5.), ist der lauterkeitsrechtliche Anspruch auf Gewinnabschöpfung gem. § 10 UWG totes Recht, da die erstrittenen Gelder an den Bundeshaushalt abzuführen sind, der klageführende Verband aber im Falle des Unterliegens die Prozesskosten zu tragen hat. Will man dem Gewinnabschöpfungsanspruch gem. § 10 UWG praktische Bedeutung verleihen, sollte daher erwogen werden, die Pflicht zur Abführung der erstrittenen Gelder an den Bundeshaushalt

---

gering sind – vgl. hierzu L. Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law - Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?, TTLF Working Paper No. 13, 6 ff, verfügbar unter http://www.law.stanford.edu/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf

270 Vgl. A. Nazari-Khanachayi: Access-Provider als urheberrechtliche Schnittstelle im Internet, GRUR 2015, 115, 121, der ausdrücklich von einer Unionsrechtswidrigkeit des deutschen Rechts *de lege lata* spricht.

271 So auch M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105, 115; A. Ohly, Gutachten zum 70. Deutschen Juristentag – Urheberrecht in der der digitalen Welt - Brauchen wir neue Regelungen zum Urheberrecht und dessen Durchsetzung?, 2014, S. 122 f.; M. Leistner, Urheberrecht in der digitalen Welt, JZ 2014, 846, 856; A. Nazari-Khanachayi: Access-Provider als urheberrechtliche Schnittstelle im Internet, GRUR 2015, 115, 121.

272 Derzeit könnten nur Nutzer ihre Rechte gegenüber ihrem Internet-Access-Provider aus ihrem Vertragsverhältnis gerichtlich geltend machen; Betreibern gesperrter Websites steht dieser Weg hingegen nicht offen. Vgl. M. Leistner/K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105, 110.

entfallen zu lassen. Dies würde für die aktivlegitimierten Verbände finanzielle Anreize schaffen, gegen rechtswidriges Marktverhalten vorzugehen.

Für die Marktteilnehmer würde hierdurch ein stärkerer wirtschaftlicher Anreiz geschaffen, rechtskonform zu agieren, wodurch auch die Effektivität des insbesondere für globale Diensteanbieter geltenden Rechts verbessert würde.

c. Stärkung von Rechtsdurchsetzungskompetenzen

Die Durchsetzung des Rechts des Marktortes in der Europäischen Union gegenüber globalen Anbietern konvergenter Dienste ist vor allem wegen der praktischen Schwierigkeiten des nationalen Vollzugs (s. dazu II.3.c.) defizitär.

Nach der EU-Kartellrechtsverfahrens-VO[273] besteht bei der Vollziehung des europäischen Kartellrechts - das grundsätzlich nur zur Anwendung kommt, wenn der Handel zwischen Mitgliedstaaten beeinträchtigt wird[274] - eine duale Zuständigkeit der Europäischen Kommission und der nationalen Wettbewerbsbehörden. Die Europäische Kommission hat allerdings die Möglichkeit, durch Einleitung eines eigenen Verfahrens die Zuständigkeit an sich zu ziehen.[275]

Um die Herausforderungen der Durchsetzung europäischen Rechts gegen globale Dienste zu bewältigen (vgl. II.3.c.), wäre es denkbar, eine ähnliche duale Zuständigkeit auch für andere vollharmonisierte Rechtsbereiche, wie z.B. das Datenschutzrecht, zu entwickeln. Allerdings dürfte die Einführung einer solchen dualen Zuständigkeit zumindest derzeit politisch kaum durchsetzbar sein und würde im Übrigen der Entwicklung hin zu einem europäischen Verwaltungs- und Regulierungsverbund[276] zuwiderlaufen.

Anstatt neue Vollzugskompetenzen für die Europäische Kommission zu schaffen, bildet der europäische Gesetzgeber zunehmend Zusammenschlüsse nationaler Regulierungsbehörden, die durch Stellungnahmen und Empfehlungen auf eine einheitliche Regulierungs- und Vollzugspraxis hinwirken. Als Beispiele seien GEREK im Bereich des Telekommunikationsrechts[277], die Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER)[278] sowie die Artikel-29-Datenschutzgruppe[279] bzw. der Europäische Datenschutzausschuss nach der DS-GVO[280] genannt.

Die bestehenden Kompetenzen des GEREK sowie der Artikel-29-Datenschutzgruppe sollten geprüft und ggf. ausgeweitet werden, um eine stärkere Zusammenarbeit zwischen den

---

273 Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln, ABl. EU L 1 vom 4.1.2003.

274 Vgl. Art. 3 Abs. 1 EU-Kartellrechtsverfahrens-VO.

275 Art. 11 Abs. 6 EU-Kartellrechtsverfahrens-VO.

276 S. hierzu G. Britz, Vom Europäischen Verwaltungsverbund zum Regulierungsverbund? EuR 2006, 46 ff, und W. Weiß, Der Europäische Verwaltungsverbund, 2010, Berlin. Zum Rechtsschutz im europäischen Verwaltungs- und Regulierungsverbund s. J. Scherer, Strukturen des Rechtsschutzes gegen Maßnahmen von Regulierungsbehörden - Gemeinschaftsrechtlicher Rahmen und nationalstaatliche Ausgestaltung, in: L. Gramlich/C. Manger-Nestler (Hrsg.), Europäisierte Regulierungsstrukturen und -netzwerke, 2011, S. 93 ff.

277 Vgl. Verordnung (EG) Nr. 1211/2009 des Europäischen Parlaments und des Rates vom 25. November 2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros, ABl. EU L 337 vom 18.12.2009.

278 Vgl. Verordnung (EG) Nr. 713/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Gründung einer Agentur für die Zusammenarbeit der Energieregulierungsbehörden, ABl. EU L 211 vom 14.8.2009, S. 1.

279 Vgl. Art. 29 Datenschutzrichtlinie.

280 Vgl. Art. 66 DS-GVO i.d.F. der legislative Entschließung des Europäischen Parlaments vom 12. März 2014.

nationalen Behörden und ein effizientes Einschreiten gegen grenzüberschreitend rechtswidrig handelnde Akteure zu ermöglichen. Darüber hinaus sollte erwogen werden, derartigen Zusammenschlüssen nationaler Regulierungsbehörden nicht nur die Kompetenz zur Erlassung von Stellungnahmen und Empfehlungen einzuräumen, sondern ihnen auch die Kompetenz zu gewähren, bindende Regelungen zu erlassen.

7. Verbesserung des Datenschutzes bei Messenger-Diensten

Wie dargestellt zeigt sich die Konvergenz der Dienste auch daran, dass Nutzer heute für ihre Individualkommunikation unterschiedliche Dienste nutzen, die auf verschiedenen technischen Implementierungen basieren, die sie aber alle von ihrem Smartphone aus nutzen können. Neben Diensten, die unmittelbar über das Telekommunikationsnetz erbracht werden (z.B. Sprachtelefonie, SMS, MMS), gibt es insbesondere Dienste, die über das Internet abgewickelt werden. Unter diesen kommt den Messenger-Diensten eine große und weiter wachsende Bedeutung zu. Ob diese Dienste den datenschutzrechtlichen Regelungen des TKG oder des TMG unterfallen, hängt vor allem von der technischen Umsetzung ab. Insbesondere peer-to-peer Messenger werden häufig nicht dem TKG unterfallen (vgl. III.1.c.).

Aus Sicht der Nutzer ist es jedoch unerheblich (und regelmäßig auch kaum erkennbar), ob der genutzte Messenger-Dienst Server/Client-basiert oder peer-to-peer-basiert arbeitet. Daher sollten einheitliche Anforderungen an die Vertraulichkeit von Messenger-Diensten gelten, unabhängig von deren technischen Implementierung. Bei der Schaffung eines solchen einheitlichen Rechtsrahmens liegt es nahe, von den Regelungen zum Fernmeldegeheimnis und den datenschutzrechtlichen Regelungen des TKG auszugehen (§§ 88, 91 ff. TKG). Denn die Messenger-Dienste werden häufig als Ersatz für klassische Telekommunikationsdienste wie Telefonie oder SMS genutzt (vgl. II.1.b.(3)).

Voraussetzung für die Schaffung eines einheitlichen Rechtsrahmens für Messenger-Dienste, ist eine sinnvolle Abgrenzung des Anwendungsbereichs. Außerdem wäre der Umgang mit gemischten Diensten festzulegen, also solchen Diensten, die sowohl Messenger-Dienste als auch sonstige Telemediendienste beinhalten. Beispiele hierfür sind Dienste zur gemeinsamen Arbeit an Dokumenten, die auch eine Chat-Funktion implementieren. Hier die gesamte Regulierung des TKG anzuwenden, erscheint uns unverhältnismäßig. Allerdings könnten auch auf diese Dienste einige der strengeren Anforderungen des Datenschutzteils des TKG übertragen werden. Folgende Kriterien könnten verwendet werden, um Messenger-Dienste von anderen Diensten abzugrenzen:

Messenger-Dienste ermöglichen eine individuelle, nicht-öffentliche Kommunikation (beispielsweise sollten Dienste wie Twitter oder Posts auf einer Facebook-Seite nicht erfasst werden). Als individuell können dabei auch Konferenzschaltung gelten, an denen eine abgeschlossene Gruppe von Personen teilnimmt. Die Kommunikation findet unmittelbar statt. Allerdings kann die Kommunikation auch dann noch unmittelbar sein, wenn die Inhalte zwischengespeichert werden, falls ein Teilnehmer vorübergehend nicht erreichbar ist.

Die Art der Inhalte der Kommunikation sollte keine Rolle spielen. Ob es sich um Text, Sprachaufnahmen oder Bilder handelt, spielt für die Schutzbedürftigkeit der Kommunikation keine Rolle.

Die Kommunikation findet bei Messenger-Diensten zwischen Menschen statt. M2M-Dienste sollten keiner zusätzlichen Regulierung unterliegen (vgl. IV.2.).

Hinsichtlich der Anforderungen an die Vertraulichkeit der Kommunikation können dann §§ 88, 91 ff. TKG insbesondere hinsichtlich der Differenzierung zwischen Bestands-, Verbindungs- und Inhaltsdaten als Vorlage genutzt werden.

V. Zusammenfassung der Optimierungsvorschläge

Die Untersuchung hat ergeben, dass der bestehende Rechtsrahmen nicht durchgängig dazu geeignet ist, den Herausforderungen, die sich durch die Konvergenz der Netze und Dienste ergeben, angemessen zu begegnen.

Auf Grundlage der Untersuchung wurde der folgende Anpassungsbedarf identifiziert:

Die Erhebung, Verarbeitung und Nutzung von Standortdaten sollte - unabhängig von der Technologie, die zur Standortbestimmung verwendet wird - spezifischen Einwilligungs- und Informationspflichten unterliegen. Dazu gehört, dass Dienste grundsätzlich auch ohne Standortermittlung angeboten werden müssen, dass die Nutzer über die Standortbestimmung informiert werden müssen und dass für die Erhebung, Verarbeitung und Verwendung von Standortdaten die Einwilligung des Nutzers erforderlich ist.

Um den Nutzen, den die Machine-to-Machine-Kommunikation für Industrie und Gesellschaft bringen kann, zu verwirklichen, ist es erforderlich, die Besonderheiten dieser Dienste angemessen zu berücksichtigen. Wir schlagen daher vor, die geltenden Regelungen des TKG so anzuwenden bzw. anzupassen, dass die Regulierung von Machine-to-Machine-Diensten sinnvoll begrenzt wird. Soweit Machine-to-Machine-Dienste dennoch in den Anwendungsbereich des TKG fallen, sollte die BNetzA die Möglichkeit erhalten, Machine-to-Machine-Dienste vom Anwendungsbereich solcher Vorschriften auszunehmen, die auf die menschliche Kommunikation zugeschnitten sind.

Der Entwurf eines IT-Sicherheitsgesetzes soll in Umsetzung der Aussagen des Koalitionsvertrags dazu beitragen, durch die Schaffung von Transparenz und die Einführung von einheitlichen Sicherheitsstandards den Schutz von IT-Infrastrukturen, -Systemen und -Diensten zu verbessern. Um dieses Ziel zu erreichen, sollte - insbesondere im Hinblick auf die von den Verpflichtungen betroffenen Sektoren - eine engere Abstimmung des Entwurfs an die zu erwartenden europarechtlichen Vorgaben erfolgen. Darüber hinaus sollten die Tatbestandmerkmale, die eine Meldepflicht auslösen können, zur Vermeidung von Rechtsunsicherheit konkretisiert werden. Verstöße von Betreibern Kritischer Infrastrukturen gegen die Meldepflicht sollten sanktionierbar sein.

Um einen fairen Wettbewerb zwischen entgeltlichen Diensten und OTT-Angeboten zu ermöglichen, die zwar „gratis“ angeboten werden, aber eine Einwilligung in die Verarbeitung personenbezogener Daten voraussetzen, ist eine Erhöhung der Transparenz hinsichtlich der von OTT-Anbietern vorgenommen Datenverarbeitung erforderlich. Die Datenverarbeitung, in die der Nutzer einwilligt, sollte im selben Maße transparent sein, wie der Euro-Preis einer entgeltlichen Dienstleistung. Zu diesem Zweck sollte eine vereinfachte Offenlegung durch die Verwendung von grafischen Symbolen erwogen werden.

Um den Wettbewerb zwischen OTT-Anbietern zu fördern und die Markteintrittsschwelle für neue Anbieter zu reduzieren, sollte ein Recht auf Datenportabilität geschaffen werden, d.h. ein Recht, seine Daten in einem strukturierten, gängigen, wiederverwendbaren Format zu erhalten. Dieses Recht sollte nicht nur (wie in der DS-GVO vorgesehen) Betroffenen gegenüber einer verantwortlichen Stelle, sondern auch verantwortlichen Stellen gegenüber ihren Auftragsverarbeitern zustehen.

Um eine Rechtsdurchsetzung gegen ausländische Urheberrechtsverletzer zu erleichtern, sollte eine ausdrückliche gesetzliche Umsetzung von Art. 8 Abs. 3 InfoSoc-RL erfolgen, die es ermöglicht, einstweilige Verfügungen gegen einen Internet-Access-Provider zu erwirken, mit denen dieser zur Sperrung einer urheberrechtsverletzenden Website verpflichtet wird. Derartige Website-Sperren sollten einem Richtervorbehalt sowie einer Kostentragung durch den Rechteinhaber unterliegen. Außerdem sollten für Nutzer und Website-Betreiber Rechtsbehelfe verfügbar sein, um bereits erlassene Sperrverfügungen einer nachträglichen Rechtmäßigkeitskontrolle zu unterziehen.

Um die Effektivität des auch für globale Diensteanbieter geltenden Rechts des lauteren Wettbewerbs zu erhöhen, sollte erwogen werden, Verbände, welche einen Anspruch auf Gewinnabschöpfung gemäß § 10 UWG durchsetzen, von der Verpflichtung zu befreien, die erstrittenen Gelder an den Bundeshaushalt abzuführen. Dies würde für alle Marktteilnehmer einen stärkeren wirtschaftlichen Anreiz schaffen, rechtskonform zu agieren und so unabhängig von der Finanzkraft der Marktteilnehmer für einen faireren Wettbewerb sorgen.

Der Rechtsrahmen für Messenger-Dienste sollte ein ähnliches Niveau für den Schutz der Kommunikationsinhalte vorsehen, wie dies heute für Telekommunikationsdienste der Fall ist, also eine strenge Vertraulichkeit dieser Kommunikationsinhalte und ein Verbot, sie für andere Zwecke als die Erbringung der Kommunikationsdienstleistung zu verarbeiten. Dies sollte unabhängig von der technischen Implementierung des Messenger-Dienstes gelten.