1. RUMÄNISCH-DEUTSCHER WORKSHOP ZUM EUROPÄISCHEN INFORMATIONSRECHT

Jürgen Taeger/Sebastian Telle (Hrsg.)

Aktuelle Rechtsfragen im Informationsrecht in Rumänien und Deutschland

Beträge zum 1. Rumänisch-Deutschen Workshop zum Europäischen Informationsrecht

OlWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Gedruckt auf alterungsbeständigem säurefreiem Papier.

Oldenburger Verlag für Wirtschaft, Informatik und Recht
Rudolf-Kinau-Str. 54, 26188 Edewecht
mail@olwir.de

Edewecht 2017

ISBN: 978-3-95599-045-9

INHALT

VORWORT

Die Digitalisierung aller gesellschaftlichen Bereiche führte in den letzten Jahren zu starken Regulierungsaktivitäten des europäischen Gesetzgebers. Die Perspektiven der Geschäftsmodelle für das Internet schaffenden Wirtschaft und der Aufbau digitaler Geschäfts- und Produktionsprozesse in Unternehmen erfordern gesetzliche ‚Leitplanken', innerhalb derer sich die Unternehmen entwickeln können. Die öffentliche Verwaltung ist bemüht, das eGovernment und den elektronischen Rechtsverkehr auf der Grundlage normativer Vorgaben einzuführen. Tangiert sind durch die Digitalisierung stets die zu wahrenden Persönlichkeitsrechte der Betroffenen in ihrer jeweiligen Rolle als Subjekte in der Gesellschaft.

Längst ist es der Europäische Gesetzgeber, der auf den meisten Regulierungsfeldern die Kompetenz für die Verabschiedung von Richtlinien und Verordnungen inne hat und diese aktiv nutzt. Auch wenn bisweilen die Rechtsetzungsprozesse auf der europäischen Bühne quälend langsam zu sein scheinen, so sind die komplexen, in ihrer Fülle selbst von Experten kaum noch beherrschbaren und für die Rechtsunterworfen wegen der sehr speziellen Rechtssprache häufig nicht mehr verständlichen Regulierungsergebnisse doch überall sichtbar und prägend.

Wie weit die angestrebte Rechtsharmonisierung in der Europäischen Union auf dem Gebiet des Informationstechnologierechts tatsächlich geht, ist eine häufig gestellte kritische Frage. Richtlinie lassen Umsetzungsspielräume und Verordnungen enthalten, wenn im EU-Ministerrat keine Verständigung erzielt werden kann, Öffnungsklauseln. Daher ist es reizvoll, sich im grenzüberschreitenden Austausch zu informieren, wie das Europäisches Recht in den Mitgliedstaaten ‚gelebt' wird.

Es wurde deshalb im Vorstand der Deutschen Stiftung für Recht und Informatik (DSRI) die Idee eines länderübergreifenden Austausches zu Themen des Informationsrechts insbesondere mit osteuropäischen Ländern geboren. Die guten Beziehungen zwischen der Carl von Ossietzky Universität Oldenburg und der Babeș-Bolyai-Universität in Cluj-Napoca (Klausenburg/Rumänien) konnten genutzt werden, um einen Deutsch-Rumänischen Workshop zum Europäischen Informationsrecht am 17./18. März 2017 in Klausenburg zu organisieren. Jeweils sieben rumänische und deutsche Referentinnen und Referenten aus der Anwaltschaft und der Wissenschaft referierten und diskutierten zu aktuellen Rechtsfragen aus dem Medien- und Telekommunikationsrecht, aus dem Urheber- und Datenschutzrecht, zu Fragen der Haftung im Internet und zu Cybercrime. Zu den Referenten zählten Michaela Braun-Noviello (Bukarest), Ass. Prof. Alexis Daj (Brașov), Alexandra Epure (Bukarest), Thorsten Feldmann

(Berlin), Cristiana Fernbach (Bukarest), Dr. Sebastian Golla (Mainz), Alex Neumann (Zetel), Raluca-Isabela Oprisiu (Sibiu), Adrian Marcel Parvu (Cluj-Napoca), Conf. Univ. Dr. Ciprian Adrian Păun (Cluj-Napoca), Boris Reibach (Oldenburg), Kathrin Schürmann (Berlin), Dr. Volker A. Schumacher (Düsseldorf) und Sebastian Telle (Oldenburg).

Maßgebliche Unterstützung fand die Tagung bei dem Prorektor der Babeș-Bolyai-Universität, Univ.-Prof. Dr. Rudolf Gräf, der auch die Begrüßungsansprache hielt. Nachdrücklich wies er auf die Aktualität und die gesellschaftliche Bedeutung des rechtswissenschaftlichen Themas sowie auf die Notwendigkeit des grenzüberschreitenden Austausches über die Rechtsfolgen der Digitalisierung hin. Weiter sprach er sich dafür aus, den Dialog auch in den kommenden Jahren fortzusetzen.

Die Tagung hätte ohne die engagierte Unterstützung der Professorinnen Dr. Mihaela Drăgan und Dr. Mariana Muresan nicht stattfinden können. Dafür und für die so große Gastfreundschaft auch außerhalb des offiziellen Programms gilt der große Dank aller Teilnehmer.

Einige der Vorträge können in diesem Tagungsband dokumentiert werden.

Oldenburg, im Mai 2017

Prof. Dr. Jürgen Taeger

Vorsitzender des Vorstandes der
Deutschen Stiftung für Recht und Informatik (DSRI)

Direktor des Interdisziplinären Wissenschaftlichen
Zentrums Recht in der Informationsgesellschaft
Carl von Ossietzky Universität Oldenburg

DIE UMSETZUNG UND NOVELLIERUNG DER AVMD-RICHTLINE

Thorsten Feldmann, LL.M.

Rechtsanwalt
Fachanwalt für Urheber- und Medienrecht
JBB Rechtsanwälte, Berlin
feldmann@jbb.de

Zusammenfassung

Die Regulierung von Bewegtbildinhalten ist in Bewegung. Der Entwurf zur Änderung der Richtlinie 2010/13/EU vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste, AVMD-RL) liegt vor und wird derzeit diskutiert. Anlass genug, einen Blick auf die gegenwärtige Umsetzung in der Bundesrepublik Deutschland zu werfen und diese vor dem Hintergrund rasanten sozio-technischen Fortschritts zu bewerten.

1 Bestandsaufnahme

In manchen Nutzergruppen scheinen die Tage des klassischen Fernsehens gezählt. Bewegtbild wird heute vor allem von der medienaffinen Zielgruppe online geschaut. Die Nutzer lassen sich für Serien, Filme, Reportagen und Dokumentation nicht mehr auf Sendezeiten festlegen. Sie bevorzugen zunehmend nicht-lineare Dienste wie Mediatheken und Video-Plattformen, die sie vom Sofa auf ihren Smart-TVs ansteuern. Auch der Medienkonsum der Internetnutzer verschiebt sich hin zum Video. Bisherige Leser werden zu Zuschauern. Online-Anbieter stellen sich auf diese Entwicklungen ein. Kaum ein Content-Angebot kommt mehr ohne Videos aus. Zugleich sind Live-Video-Funktionalitäten im Social Web, etwa auf Facebook, auf dem Vormarsch, die es den Nutzern ermöglichen, das, was sie gerade sehen, mit dem Smartphone in Echtzeit an die Freunde oder in alle Welt zu übertragen. Darüber hinaus investiert Facebook derzeit in die Förderung sogenannter Long-Form-Videos auf der Plattform, der Facebook-Nutzern neue Vertriebs- und Vermarktungsmöglichkeiten eröffnet.

All‘ diese Entwicklungen werfen auch regulatorische Fragen auf, die teilweise bereits in der Vergangenheit von nationalen und europäischen Regelungen adressiert wurden. Diese Regelungen sind auf europäischer Ebene nun in der Diskussion. Auch der Europäische Gerichtshof musste sich jüngst mit Abrufdiensten beschäftigen.

2 Europarechtlicher Ausgangspunkt: Sekundärrecht

Europarechtliche Ausgangspunkt der Regulierung von Bewegtbildinhalten ist die Richtlinie 2010/13/EU vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste, AVMD-RL). Die AVMD-Richtlinie gilt für redaktionell verantwortliche Anbieter mit Sitz in EU-Mitgliedstaaten, die lineare Fernsehkanäle und Video-on-Demand-Dienste mit Inhalten anbieten, die als mit Fernsehsendungen vergleichbar („fernsehähnlich") gelten. Aufgrund des technologieneutralen Ansatzes der AVMD-Richtlinie werden dieselben Dienste auf dieselbe Weise reguliert, unabhängig von dem Gerät, auf dem sie konsumiert werden. Allerdings unterscheidet die Richtlinie zwischen Fernsehprogrammen (linearen Programmen) und nicht-linearen Diensten (Abrufdiensten). Wie noch zu zeigen sein wird, besteht insoweit ein Gleichlauf zu der unterschiedlichen Regulierungsdichte des deutschen Rundfunkstaatsvertrags, der auch einen zweistufigen Regulierungsansatz mit strengeren Vorschriften für lineare Dienste vorsieht. Obschon durch die AVMD-Richtlinie „die Mitgliedstaaten weder verpflichtet noch ermuntert" werden sollen, „neue Lizenz- oder Genehmigungsverfahren im Bereich audiovisueller Mediendienste einzuführen" (Erwägungsgrund 20), sieht die Richtlinie wie der Rundfunkstaatsvertrag für lineare Fernsehangebote strengere Regelungen zum Jugendschutz (Kapitel VIII AVMD-RL) vor, während für nicht-lineare Angebote ausdrücklich abgeschwächte Vorschriften gelten (Kapitel IV AVMD-RL). Vor allem aber müssen lineare audiovisuelle Angebote auch nach dem europäischen Normenkomplex spezielle Regelungen und zeitliche Grenzen für Teleshopping und Fernsehwerbung beachten (Kapitel VII AVMD-RL). Die AVMD-Richtlinie rechtfertigt in Erwägungsgrund 58 die unterschiedliche Behandlung von linearen und nicht-linearen Angeboten mit einem Verweis auf die Rechtsprechung des EuGH,[1] die im Falle von nicht-linearen Dienten angeblich von größeren „Auswahl- und Steuerungsmöglichkeiten der Nutzer" und „geringeren Auswirkungen auf die Gesellschaft" ausgeht. Wie unter 2.3 aufgezeigt werden wird, hat sich die Kommission inzwischen von diesen Grundannahmen offenbar verabschiedet.

3 EuGH-Rechtsprechung

Die europäische Rechtsprechung hat sich erst in einer Entscheidung mit dem sachlichen Anwendungsbereich der AVMD-Richtlinie beschäftigen dürfen.

Ein sich aus der AVMD-Richtlinie ergebendes Problem betrifft Internetangebote von Verlagen und anderen journalistisch-redaktionellen

Diensteanbietern, die ihre redaktionellen textbasierten Angebote mit audiovisuellen Inhalten anreichern. Die Schwierigkeit liegt in diesen Fällen in der Feststellung, ob die Bereitstellung derartiger audiovisueller Inhalte den „Hauptzweck" der Dienste darstellt und ob der Videobereich eines Online-Dienstes ein vom textbasierten Dienst zu trennender eigenständiger Dienst ist. Die Begriffsbestimmung des audiovisuellen Mediendienstes der AVMD-Richtlinie schließt nämlich in Artikel 1 Abs. 1 lit a) alle Dienste von der Regulierung aus, deren „Hauptzweck" nicht die Bereitstellung von Programmen ist, d. h. bei denen audiovisuelle Inhalte „lediglich eine Nebenerscheinung darstellen". Dazu zählen nach Erwägungsgrund 22 beispielsweise Internetseiten, die lediglich zu Ergänzungszwecken audiovisuelle Elemente enthalten.

In der Entscheidung „New Media Online"[1] rechnete der EuGH Videobereiche von Zeitungsportalen dem sachlichen Anwendungsbereich der Richtlinie zu. Er stellte sich damit gegen die Schlussanträge des Generalanwalts. Der Generalanwalt war noch der Auffassung, die Notwendigkeit einer dynamischen Auslegung des Begriffs „Sendung" führe dazu, dass Webportale angesichts der spezifischen Architektur der Multimediainhalte nicht unter die Definition fallen. Der Gerichtshof dagegen verwies auf die „Vergleichbarkeit einer Kurzvideosammlung mit einem von einem Fernsehveranstalter erstellten kompletten Sendeplan oder Katalog", wobei keine Bestimmung der AVMD-Richtlinie eine Anforderung hinsichtlich der Programmdauer enthalte.

Zu der entscheidenden Frage, ob die „audiovisuellen Elemente eine Nebenerscheinung darstellen und nur zur Ergänzung des Presseartikelangebots dienen", stellte der Gerichtshof fest, dies müsse einzelfallbezogen beurteilt werden, um eine Situation zu vermeiden, in der die Betreiber, die audiovisuelle Mediendienste anbieten, „ein multimediales Informationsportal verwenden könnten, um sich den in diesem Bereich für sie geltenden Rechtsvorschriften zu entziehen". Wörtlich führt der Gerichtshof aus:

> *„Im Ausgangsverfahren ist es Sache des vorlegenden Gerichts, zu prüfen, ob der in der Video-Subdomain angebotene Dienst in Inhalt und Funktion gegenüber den Presseartikeln des Verlegers der Online-Zeitung eigenständig ist. Wenn dies der Fall ist, fällt der Dienst in den Anwendungsbereich der Richtlinie 2010/13. Wenn der Dienst dagegen insbesondere wegen der zwischen dem audiovisuellen Angebot und dem Textangebot bestehenden Verbindungen untrennbar mit der journalistischen Tätigkeit dieses Verlegers verknüpft ist, fällt er nicht in den Anwendungsbereich der Richtlinie."*[1]

[1] EuGH, Urt. v. 21. Oktober 2015 - C-347/14, New Media Online gegen Bundeskommunikationssenat, Rn. 34.

Da die Website im konkreten Fall auch einen Bereich mit Videos unterhielt, die teilweise keinen inhaltlichen Bezug zu textbasierten Beiträgen aufwiesen, ging der Gerichtshof von einem „eigenständigen Dienst“ aus, der sich von den übrigen angebotenen Diensten unterscheidet. Damit dehnt der Gerichtshof den Regelungsgehalt von Art. 1 Abs. 1 lit a-i der AVMD-Richtlinie weit aus, in dem von einer Eigenständigkeit eines Teils eines Internet-Angebots keine Rede ist. Sachgerechter wäre es gewesen, einen Dienst, der anhand der Domain, des Brandings und der konkreten Gestaltung nach außen erkennbar als einheitlicher Dienst dem Nutzer entgegentritt, als multimediales Gesamtangebot zu begreifen und anhand publizistischer Kriterien zu ermitteln, in welchem Bereich der Schwerpunkt des journalistischen Angebots liegt, der dann als Hauptzweck gilt. Durch seine typisch dynamische Auslegung lehnt der Gerichtshof ein realitätsnahes Verständnis des „Hauptzwecks“ ab, indem er einen einheitlichen Dienst künstlich in zwei Teile zerlegt. Stattdessen konzentriert sich der Gerichtshof darauf, eine „Umgehung“ der Richtlinie verhindern:

> *„Bei dieser Prüfung kann nicht maßgebend sein, ob das fragliche audiovisuelle Angebot im Hauptbereich der betreffenden Website oder in einer ihrer Subdomains präsentiert wird, da sonst die Möglichkeit geschaffen würde, die Vorschriften der Richtlinie 2010/13 durch eine entsprechende Strukturierung der Website zu umgehen.“*

Der Gerichtshof ist demnach bestrebt, gerade auch journalistisch-redaktionelle Anbieter einer Regulierung zu unterwerfen, die aufgrund der ihnen zustehenden institutionellen Pressefreiheit aus gutem Grund bislang von regulatorischen Auflagen befreit waren.

Die Tiroler Tageszeitung Online, deren Angebot Gegenstand der gerichtlichen Auseinandersetzung gewesen ist, hat ihren Videobereich inzwischen geschlossen.

4 Umsetzung in der Bundesrepublik Deutschland

Der Umsetzungsakt der AVMD-Richtlinie in der Bundesrepublik Deutschland ist der Rundfunkstaatsvertrag (RfStV). Er gibt Antwort auf die Frage, ob und mit welcher Intensität ein audiovisuelles Angebot der öffentlich-rechtlichen Regulierung unterliegt. Anders als die europäischen Vorschriften klebt das deutsche Regulierungssystem dabei am Rundfunkbegriff. Dabei erfährt aber auch die Linearität als elementarer Bestandteil der Rundfunkdefinition des § 2 Abs. 1 RfStV Relevanz. Nicht-lineare Dienste sind folglich kein Rundfunk, ganz gleich, ob sie aus Text, Ton oder Video bestehen. Sie sind allenfalls Telemedien im Sinne der §§ 54 ff. RfStV. Die Regulierung für Telemedien ist bei Weitem nicht so dicht wie die des Rundfunks. Beispielsweise bedürfen Telemedien keiner Zulassung

durch die zuständige Landesmedienanstalt, auch dann nicht, wenn sie journalistisch-redaktionelle Qualität aufweisen oder fernsehähnlich daherkommen. Im Bereich des Rundfunks ist gemäß § 20b RfStV dagegen nur das reine Internetradio vom Zulassungserfordernis des § 20 RfStV befreit. Soweit ein Online-Angebot unter den Rundfunkbegriff zu subsumieren ist – linear, an die Allgemeinheit gerichtet, zum gleichzeitigen Empfang bestimmt, Inhalte orientieren sich zeitlich entlang eines Sendeplans, vgl. § 2 Abs. 1 RfStV – setzt die engmaschige Regulierung des Rundfunkrechts ein, die grundsätzlich das besagte Zulassungs- bzw. Anzeigeerfordernis (§§ 20, 20b RfStV), besondere inhaltliche und kommerzielle Beschränkungen (§§ 41 ff. RfStV) und eine behördliche Überwachung (z.B. §§ 35 ff. RfStV) vorsieht.

Wer seine private oder professionelle Meinung über ein technisches Mittel und auf eine Art und Weise verbreiten möchte, die der (einfache) Staatsvertragsgeber und eine staatliche Behörde als Rundfunk ansehen, muss den Staat konsultieren, ggf. diesen sogar um Erlaubnis bitten, und ihm eine Zulassungsgebühr zahlen. Vor dem Hintergrund der ständigen Rechtsprechung des Bundesverfassungsgerichts, wonach die Meinungsfreiheit ein besonderes Gut ist und Beschränkungen der Meinungsäußerungsfreiheit durch den einfachen Gesetzgeber besonderen Schranken unterliegen,[2] liegt die Grundrechtsrelevanz derartiger Regulierungsfragen auf der Hand.

4.1 Lineare Angebote

Der deutsche Rundfunkstaatsvertrag hat lineare Angebote seit jeher in seinen sachlichen Anwendungsbereich einbezogen. Die von ihm dabei an den Tag gelegte Großzügigkeit auch in Bezug auf non-visuelle Dienste wie beispielsweise Twitter hat mancherorts bereits berechtigtes Stirnrunzeln verursacht.[3] Vor dem Hintergrund der neuen technologischen Möglichkeiten zur Verbreitung von Bewegtbildinhalten im Internet stellt sich heute die Frage mehr denn je, ob der rechtstechnische Begriff des Rundfunks, wie der Rundfunkstaatsvertrag ihn verstanden wissen will, der zentrale Anknüpfungspunkt für die Entscheidung über Ob und Wie der Regulierung sein sollte.

Der Rundfunkstaatsvertrag deutet diese Zweifel selbst an, indem er manche linearen Angebote aus dem Rundfunkbegriff ausklammert und diese von einer Regulierung vollends freistellt. Allerdings hat der rund-

[2] BVerfG, Beschl. v. 15. Januar 1958 - 1 BvR 400/51, Lüth.

[3] *Koreng*, AfP 2009, S. 117.

funkrechtliche Dispens einen recht schmalen Anwendungsbereich: Kein Rundfunk sind gemäß § 3a RfStV nur Angebote, die

- jedenfalls weniger als 500 potentiellen Nutzern zum zeitgleichen Empfang angeboten werden,
- zur unmittelbaren Wiedergabe aus Speichern von Empfangsgeräten bestimmt sind,
- ausschließlich persönlichen oder familiären Zwecken dienen,
- nicht journalistisch-redaktionell gestaltet sind oder
- aus Sendungen bestehen, die jeweils gegen einzelne Entgelt freigeschaltet werden.

Nur reichweitenschwache private Angebote ohne meinungsbildenden Anspruch fallen aus dem Begriff und damit aus der rundfunkrechtlichen Regulierung heraus. Im Umkehrschluss bedeutet dies, dass eine nicht geringfügige Menge linearer Videoangebote, die sich im Netz finden lassen, vom Rundfunkbegriff erfasst werden dürften.

In Bezug auf Bewegtbilddienste ist eben nicht nur das klassische Fernsehprogramm Rundfunk. Auch der zu einer bestimmten Sendezeit ausgestrahlte und vorproduzierte Video-Blog oder ein einem bestimmten Programmablauf folgender Live-Stream im Web oder auf Facebook können Rundfunk sein. Journalistisch tätige Unternehmen oder Video-Blogger müssen aufpassen, sobald sie eine Sendung zu einer vorgeplanten Zeit im Internet ohne technische Beschränkung auf 500 gleichzeitige Abrufe zum Abruf bereitstellen und der Inhalt journalistisch-redaktionelle Ansprüche erhebt. Als Rundfunk ist beispielsweise das Diskussionsformat „#heiseshowXXL“ anzusehen, das der heise-Verlag anlässlich der CeBIT im Jahre 2016 in einer bestimmten Programmabfolge an seinem Messestand veranstaltete und per Stream im Internet live übertragen ließ.

#heiseshowXXL live auf der CeBIT 2016	
Montag, 14.3.	
10 Uhr	**iX:** Optimized Data Center: Selbsttest für RZ-Betreiber - *Tilman Wittenhorst, TechConsult*
11 Uhr	**heise Security:** Schutz und erste Hilfe: Banking- und Verschlüsselungs-Trojaner - *Dennis Schirrmacher*
12 Uhr	**Technology Review:** Übernehmen Roboter die Welt? - *Wolfgang Stieler*
13 Uhr	**Make:** Scannen und Drucken in 3D - *Peter König*
14 Uhr	**c't:** VR-Brillen - Hype oder Zukunft? - *Stefan Porteck*
15 Uhr	**IT-Recht:** Mit Strafrecht gegen Hass im Internet? - *Dr. Ulf Buermeyer (Richter am LG Berlin), Joerg Heidrich*
16 Uhr	**#heiseshow:** CeBIT-News und Netzpolitik - *Gerd Billen (Verbraucherschützer, Staatssekretär BMJV), Philip Banse, Jürgen Kuri*
17 Uhr	**After Show Quiztime:** CeBIT Jeopardy
Dienstag, 15.3.	
10 Uhr	**iX:** Developer World 2016: Software aus Deutschland - *Alexander Neumann*
11 Uhr	**heise Security:** Security-Fails – und was man daraus lernen kann - *Ronald Eikenberg*
12	**Technology Review:** Künstliche Intelligenz – überbewertet oder unterschätzt? - *Prof. Wolfgang Wahlster (CEO*

Programm der #heiseshowxxl, http://www.heise.de/newsticker/meldung/heiseshowXXL-News-Infos-Diskussionen-taeglich-live-von-der-CeBIT-3133362.html, abgerufen am 5. Juli 2016

Doch nicht nur Medienunternehmen sind in der Pflicht. Gerade infolge der Demokratisierung und Popularisierung der Medientechnologie liegt in vielen Fällen eine Lizenzierungspflicht auch bei natürlichen Personen nahe. Zumindest sind natürliche Personen keineswegs in lizenzrechtlichen Grundsatzfragen privilegiert. Der sendende Journalist wird daher im regulatorischen Ansatzpunkt genauso behandelt, wie ein klassischer Fernsehveranstalter, der sein Programm über Kabel oder Satellit ausstrahlt. Konsequenterweise haben sich einzelne Journalisten bereits mit einer Rundfunklizenz ausstatten lassen, weil sie in journalistisch-redaktioneller Art und Weise von den neuen Live-Funktionen auf Facebook und YouTube Gebrauch machen.

4.2 Nicht-lineare Angebote

Nicht-lineare Dienste, also On-Demand-Angebote, die die Zuschauer nicht alle gleichzeitig in Anspruch nehmen, sondern bei denen der individuelle Nutzer über die Zeit der Übermittlung auf seinen Bildschirm entscheidet, unterliegen in Deutschland einer nur eingeschränkten rundfunkrechtlichen Regulierung. Derartige nicht-lineare Angebote müssen nicht der Landesmedienanstalt angezeigt werden. Sie gelten als Telemedien im Sinne der §§ 54 ff. RfStV, wobei öffentlich-rechtliche Pflichten nur ansatz-

weise und maßgeblich nur dann bestehen, wenn sie journalistisch-redaktionellen Charakter aufweisen. Jenseits einer besonderen Impressumspflicht (§ 55 Abs. 2 RfStV) und der Verpflichtung zur Veröffentlichung von Gegendarstellungen (§ 56 RfStV) gibt es keine überbordend besondere Beschränkungen. So ist der Telemedienanbieter in der Vermarktung weit gehend frei: Er muss lediglich Werbung vom redaktionellen Angebot trennen und darf keine unterschwelligen Techniken einsetzen (§ 58 Abs. 1 RfStV). Auch für „fernsehähnliche" Telemediendienste gemäß § 58 Abs. 3 RfStV, die vom Anbieter in einem „Katalog" zum Abruf bereitgehalten werden, gelten ergänzend nur die werberechtlichen Selbstverständlichkeiten der §§ 7 und 8 RfStV – keine Menschenwürdeverletzungen, keine Schleichwerbung etc. –, die häufig ohnehin schon nach dem StGB, dem JMStV oder dem Lauterkeitsrecht verboten sind. Es finden auf den fernsehähnlichen Telemediendienst grundsätzlich aber gerade nicht die einschneidenden Werbedauerbeschränkungen der §§ 44, 45 RfStV und die Gemeinsamen Werberichtlinien der Landesmedienanstalten Anwendung, die dem Rundfunkveranstalter das Leben mitunter schwer machen und die gemäß § 49 Abs. 1 S. 1 Nr. 21, Abs. 2 RfStV mit harten Bußgeldern von bis zu EUR 500.000,00 geahndet werden können. Derartige Sanktionen können Anbietern nur dann auferlegt werden, wenn ihr fernsehähnlicher Telemediendienst gemäß § 2 Abs. 3 Nr. 5 RfStV aus Sendungen besteht, die „jeweils gegen Einzelentgelt freigeschaltet werden", also für klassische Pay-per-View-Angebote. Freilich haben gewöhnliche Videoangebote auf Abruf das Telemediengesetz und alle anderen anwendbaren Gesetze, insbesondere auch den JMStV, zu beachten. Von der Regulierungsdichte der linearen Dienste ist man aber recht weit entfernt.

4.3 Beobachtungen und Fragen

Nicht nur auf den ersten Blick muten die Unterschiede in der Regulierungsdichte bei linearen und nicht-linearen Diensten merkwürdig an: Wenn ein Journalist Videos vorproduziert und die Veröffentlichung in bestimmter Weise zeitlich taktet, ohne, dass der Nutzer den Beginn der Übertragung bestimmen kann, etwa, weil er sich interessant machen und seine Nutzer dazu anregen möchte, immer wieder zu einer bestimmten Zeit auf seiner Website oder seiner Facebook-Page vorbeizuschauen, liegt grundsätzlich lizenzierungspflichtiger Rundfunk vor. Dies ist insbesondere auch dann der Fall, wenn die Inhalte, fernsehähnlich flüchtig, nur gestreamt werden. Der Journalist darf eine derartige Tätigkeit zum Transport seiner Meinungen nicht ohne Weiteres entfalten. Wenn er es doch tut, betreibt er einen Piratensender, weil er entgegen § 20 Abs. 1 Satz 1 oder Abs. 2 Satz 1 ohne Zulassung Rundfunkprogramme veranstaltet, was ihm eine Untersagungsverfügung der zuständigen Landesmedienanstalt und gemäß § 49 Abs. 2 RfStV ein Bußgeld von bis zu EUR 500.000,00

einbringen kann. Der Journalist muss vielmehr vorab eine Fernsehlizenz beantragen, hierfür einen mindestens vierstelligen Betrag für das Genehmigungsverfahren aufwenden und vor allem auch negative Vermarktungseffekte in Form von Werbedauerbeschränkungen hinnehmen. Damit geht es dem Journalisten zwar immer noch besser als der live-streamenden juristischen Person des öffentlichen Rechts oder der live-streamenden Partei, die gemäß § 20 Abs. 3 RfStV keine Rundfunklizenz erhalten dürfen. Jedenfalls vermeidet der Journalist all‘ diese Probleme, wenn sich dafür entscheidet, alle seine vorproduzierten Videos auf einen Schlag oder schlicht planlos und dauerhaft im Internet zum Abruf bereit zu halten. Er muss keiner Behörde etwas melden und entgeht fast jedweder öffentlich-rechtlichen Pflicht, die sich nicht in menschlichem Anstand und juristischer Selbstverständlichkeit erschöpft.

Darüber hinaus sind häufig Angebote, die bei natürlicher Betrachtung Ein- und Dasselbe sind, regulierungsrechtlich vollkommen unterschiedlich zu beurteilen, je nach dem, zu welchem Zeitpunkt man den Inhalt einer Prüfung unterzieht. Im Zeitpunkt der linearen „Erstausstrahlung“, also beispielsweise der Live-Sendung auf der Website oder der Facebook-Page, finden die rundfunkrechtlichen Beschränkungen, beispielsweise in Bezug auf die Werbung (§ 44 RfStV i. V. m. den auf Basis des § 46 RfStV erlassenen Gemeinsamen Werberichtlinien der Landesmedienanstalten) Anwendung. Wird diese Sendung nach der Ausstrahlung, wie häufig, gespeichert und zum dauerhaften Abruf bereitgestellt, handelt es sich allenfalls um einen fernsehähnlichen Telemediendienst gemäß § 54 RfStV. Für ein und denselben Inhalt gelten vollends unterschiedliche Regelungskomplexe: Für Rundfunk greifen die inhaltlichen Programmgrundsätze des § 41 RfStV, für das Telemedium gemäß § 54 Abs. 1 RfStV nur die allgemeinen Gesetze und die verfassungsmäßige Ordnung. Während darüber hinaus die live gestreamte Erstausstrahlung nur eingeschränkt Werbung enthalten darf (§ 44 RfStV), kann dieselbe Sendung, wenn sie danach im Portal gespeichert und zum Abruf bereitgehalten wird, zeitlich unbegrenzt mit Werbung bestückt werden.

Urheberrechtlich mag eine solche Unterscheidung zwischen einer Sendung im Sinne des § 20 UrhG und einer öffentlichen Zugänglichmachung im Sinne des § 19a UrhG wegen der damit einhergehenden unterschiedlichen Intensität der Werknutzung sinnvoll und angemessen sein. Die Unterscheidung erschließt sich jedoch nicht bei dem auf Gefahrenabwehr ausgerichteten Medien-Ordnungsrecht. Diesbezüglich bewegt man sich nicht auf allzu dünnem Eis, wenn man die These wagt, dass von einem über das Internet ausgestrahlten linearen und flüchtigen audiovisuellen Dienst jedenfalls keine größeren Gefahren für die Gesellschaft ausgehen,

als von einem nicht-linearen, dauerhaft auf Abruf bereit gehaltenen Dienst mit exakt demselben Inhalt.

Umgekehrt geraten nun Online-Dienste, Verlage und Presseunternehmen, die seit jeher journalistisch-redaktionelle Inhalte in mitunter höchster Qualität frei von Beschränkungen im Internet zugänglich gemacht haben und aufgrund des gewandelten Nutzerverhaltens zunehmend auf Bewegtbildangebote angewiesen sind, um ihre Nutzer zu halten und ihre Dienste finanzieren zu können, in regulierungsrechtlich gefährliches Fahrwasser, wenn sie Angebote wie Facebook-Live oder Periscope nutzen. Die geradezu natürliche Weiterentwicklung des überkommenen Textangebots unter Nutzung redaktioneller Ressourcen zu programmierten und vielleicht auch fernsehähnlichen Video-Angeboten im eigenen Internetportal – beispielsweise die Einbindung eines Videos des Journalisten, der mittels seines Smartphones live aus dem Flüchtlingslager berichtet – katapultiert das Verlagshaus in gänzlich andere regulatorische Sphären, obwohl aus Sicht des Ordnungsrechts eine verstärkte Regulierung nach den §§ 20, 41 ff. RfStV anstelle der §§ 54 ff. RfStV bloß auf Grundlage der Linearität nicht zwingend geboten erscheint. Unabhängig davon blickt die Presse nicht ohne Stolz auf eine jahrzehntelange verfassungsrechtliche Tradition ohne jede staatliche Regulierung zurück, die sich vollends bewährt hat. Zu Recht scheint vor diesem Hintergrund die Notwendigkeit eines regulatorischen Paradigmenwechsels erklärungsbedürftig.

Die Unterscheidung zwischen linearen und nicht-linearen audiovisuellen Angeboten und die sich daraus ergebende unterschiedliche Regelungsdichte darf daher zu Recht hinterfragt werden. Überlegenswert wäre es, die Beschränkungen, die im Internet verbreiteten linearen Videodiensten auferlegt werden, zu lockern, indem sie den nicht-linearen Angeboten gleichgestellt werden. Der Gesetzgeber hat bewusst nicht-linearen Angeboten mehr Freiheiten eingeräumt. Nur auf dem Unterscheidungsmerkmal der Linearität beruhende Freiheitseinschnitte und Sanktionsandrohungen scheinen aufgrund der fehlenden Gefahrerhöhung nicht verhältnismäßig. Zu Recht werden auf europäischer Ebene derzeit die de lege lata bestehenden Regulierungsansätze hinterfragt. Wie im Folgenden aufgezeigt werden wird, gehen diese aber in die entgegengesetzte Richtung.

5 Der Vorschlag der Kommission zur Novellierung der AVMD-Richtlinie

In absehbarer Zeit wird die AVMD-Richtlinie aus dem Jahre 2010 ein Stück weit Geschichte sein. Denn am 25. Mai 2016 hat die Kommission nach einer seit dem Jahre 2013 durgeführten Konsultation einen Vor-

schlag zur Änderung der Richtlinie vorgelegt.[4] Als Grund für die Notwendigkeit einer Revision der Richtlinie führt die Kommission ausdrücklich das geänderte Nutzerverhalten hin zu Abrufdiensten und der eingeschränkten Nutzung des klassischen Fernsehens an:

„Die audiovisuelle Medienlandschaft verändert sich rasant durch die zunehmende Konvergenz von Fernsehen und Diensten, die über das Internet verbreitet werden. Immer mehr Verbraucher greifen über intelligente/vernetzte Fernsehgeräte und tragbare Geräte auf Abrufinhalte zu. Insbesondere junge Verbraucher schauen Videos, darunter auch von Nutzern selbst erstellte Inhalte, über das Internet. Das traditionelle Fernsehen hat in der EU bezüglich der Zuschauerzahlen, Werbeeinnahmen und Investitionen in die Inhalte (rund 30 % der Einnahmen) weiterhin eine starke Position inne. Es entstehen jedoch neue Geschäftsmodelle. Fernsehveranstalter weiten ihre Tätigkeiten im Internet aus, und neue Marktteilnehmer, die audiovisuelle Inhalte über das Internet anbieten (z.B. Anbieter von Video auf Abruf und Videoplattformen), werden zunehmend stärker und stehen im Wettbewerb um das gleiche Publikum. Allerdings gelten für Fernsehen, Videoabruf und von Nutzern erstellte Inhalte unterschiedliche Vorschriften, und auch die Verbraucherschutzniveaus variieren. In der Strategie für einen digitalen Binnenmarkt für Europa wird eine Überarbeitung der Richtlinie über audiovisuelle Mediendienste (AVMD-Richtlinie) gefordert, um diesen Veränderungen des Marktumfelds und der Nutzungsweisen sowie dem technologischen Wandel Rechnung zu tragen."

Die Kommission rückt damit nicht-lineare Dienste stärker ins Zentrum ihrer regulatorischen Überlegungen, in deren Konsequenz der sachliche Anwendungsbereich der Richtlinie und damit die Regulierung audiovisueller Dienste ausgeweitet werden.

Beispielsweise zementiert der Kommissionsvorschlag die durch den EuGH in der Entscheidung „New Online Media" verwässerte Regulierungsausnahme für den Fall, dass das Videoangebot nicht den „Hauptzweck" des gesamten redaktionellen Angebots darstellt. Der Vorschlag sieht in der Neufassung von neuer Artikel 1 Absatz 1 Buchstabe a-i) nunmehr vor,

> *„eine Dienstleistung […] bei der der Hauptzweck <u>oder ein trennbarer Teil der Dienstleistung</u> darin besteht, unter der redaktionellen Verantwortung eines Mediendiensteanbieters Sendungen zur Information, Unterhaltung oder Bildung der allgemeinen Öffentlichkeit über elektronische Kommunikationsnetze […] bereitzustellen"* (Hervorhebung nur hier)

als audiovisuellen Mediendienst einzustufen. Erwägungsgrund 3 des Vorschlags begründet ausdrücklich diese Ausweitung der Regulierung, dass in Anwendung des New Media Online-Urteils der „Hauptzweck" auch dann als erfüllt gelten sollte,

„wenn der Dienst audiovisuelle Inhalte enthält und eine Form hat, die sich von der Hauptaktivität des Diensteanbieters trennen lässt, beispielsweise eigenständige Teile von Online-Zeitungen mit audiovisuellen Sendungen oder von Nutzern erstellten Videos, soweit solche Teile als von ihrer Haupttätigkeit trennbar gelten können“.

Diese Änderung belegt zunächst, dass auch die Kommission offenbar nicht wirklich davon überzeugt ist, dass die Frage der Trennbarkeit eines Dienstes ausschlaggebend für die Beurteilung des „Hauptzwecks“ eines Dienstes ist; denn andernfalls hätte es keiner Änderung bedurft. Ferner hat die die Kommission bewusst davon abgesehen, die freiheitseinschränkende Auslegung des EuGH durch eine Klarstellung zurückzudrehen.

Ebenfalls zu einer Ausweitung der Regulierung für die Neufassung des Begriffs der „Sendung“, die identitätsstiftend für einen audiovisuellen Mediendienst ist: Das Kriterium der „Fernsehähnlichkeit“ entfällt. Stattdessen führt die Kommission im neuen Art. 1 Abs. 1 lit b) konkrete Beispiele an und fügt der bereits bestehenden Liste mit Spielfilmen, Sportberichten, Fernsehkomödien, Dokumentarfilmen, Kindersendungen und Originalfernsehspiele ausdrücklich „Kurzvideos“ hinzu. Der Benchmark für eine Regulierung ist damit nicht mehr das Angebot, das wir aus dem Fernsehen kennen, sondern der nicht professionell gestaltete Clip, wie er im Internet millionenfach anzutreffen ist.

Des Weiteren fallen nun neue Dienste, für die sich kein redaktionell Verantwortlicher finden lässt, in den Anwendungsbereich der AVMD-Richtlinie. Nun sind gemäß Art. 1 Abs. 1 lit. a) auch Videoplattformen audiovisuelle Mediendienste.

Natürlich bleibt abzuwarten, inwieweit der Vorschlag der Kommission für eine Neufassung der AVMD-Richtlinie Realität wird. Ebenso wird abzuwarten sein, wie der deutsche Gesetzgeber die Vorgaben einer in Kraft getretenen Richtlinie in nationales Recht umsetzt. Immerhin ist denkbar, dass er den Rundfunkmarkt liberalisiert, indem er den Rundfunk in der Regulierungsdichte den nicht-linearen Abrufdiensten anpasst. Aber die Tendenz des nun auf dem Tisch liegenden Vorschlags der Kommission kommt klar zum Vorschein: Es werden künftig mehr Bewegtbildinhalte in die Regulierung einbezogen.

6 Fazit

Sowohl auf europäischer als auch auf deutscher Ebene erweist sich der geltende Rechts- und Regulierungsrahmen für Video-Angebote im Internet als unbefriedigend. Die Linearität scheint als Rechtfertigungsgrund für unterschiedliche Regulierungsdichten ungeeignet. Insoweit sind die

Bestrebungen auf europäischer Ebene zur Änderung des geltenden Rahmens durch eine Revision der AVMD-Richtlinie zu begrüßen, wenn lineare und nicht-lineare Dienste in der juristischen Beurteilung einander angeglichen werden. Andererseits erweckt auch der erste Vorschlag der Kommission zur Neufassung der Richtlinie den Verdacht, in die falsche Richtung zu steuern, indem er Anbieter in eine traditionell fernsehmäßige Regulierung hineintreibt, ohne dass dies mit einem gesteigerten Gefährdungspotential begründet werden könnte. Deregulierung sieht jedenfalls anders aus. Insbesondere journalistisch-redaktionelle Dienste, die bislang ihre Medieninhalte vorwiegend in Textform verbreitet haben und insoweit vollkommen zu Recht noch nie einer staatlichen Regulierung ausgesetzt waren, könnten nun einer verstärkten staatlichen Beschränkung und Beobachtung unterworfen werden, die einer tragfähigen Begründung harren. Allein ein geändertes Nutzerverhalten vermag Grundrechtsbeschränkungen nicht zu rechtfertigen.

LITERATUR

Koreng, Ansgar: Staatliche Internetpräsenzen zwischen legitimer Öffentlichkeitsarbeit und dem Verbot des Staatsrundfunks. Podcasts, Videoblogs und der Rundfunkbegriff, AfP 2009, S. 117-121.

MEDIENRECHT IN RUMÄNIEN

Rechtsanwältin Michaela Braun-Noviello

Rechtsanwaltskanzlei Braun-Noviello in Heidelberg
Bogaru Braun Noviello & Associates BBNA in Bukarest
info@europe-lawyers.eu

Zusammenfassung

Mit diesem Beitrag wird ein Überblick über das rumänische Medienrecht präsentiert, wobei als Schwerpunkt die freie Meinungsäußerung im Verhältnis zu den Persönlichkeitsrechten näher dargelegt wird. Im aktuellen, internationalen Kontext rückt das Thema „Pressefreiheit" immer mehr in den Vordergrund der Debatten über die Demokratie. Daher wird sich dieser Beitrag zum Schluss auch mit einigen aktuellen Beispielen aus dem Bereich der Pressefreiheit und Persönlichkeitsrechte beschäftigen.

1 Gesetzgebung

Die wichtigsten, gesetzlichen Regelungen im Bereich des Medienrechts in Rumänien sind in den folgenden Gesetzen und Regierungsverordnungen, sowie in den Beschlüssen der Aufsichtsbehörde der audiovisuellen Medien (CNA) erfasst, welche im Wesentlichen die europäische Gesetzgebung in das Nationalrecht umsetzen:

- Gesetz über Audiovisuelle Mediendienste Nr. 504/2002 – setzt die Richtlinie 1989/552/EG und deren Novellierung durch die Richtlinie über audiovisuelle Mediendienste (Richtlinie 2007/65/EG) in das Nationalrecht um;
- Beschluss CNA Nr. 220/2011 über den Kodex für audiovisuelle Inhalte – wiederholt explizit die Prinzipien der Pressefreiheit, des Äußerungsrechtes und des Schutzes der Persönlichkeitsrechte und legt die deontologischen Berufsregeln fest (der Kodex);
- Beschluss CNA Nr. 320/2012 über audiovisuelle „on demand"-Dienstleistungen (zum Schutz von Kindern und Jugendlichen) – setzt die Richtlinie 2010/13/EG in das Nationalrecht um;
- Gesetz Nr. 365/2002 über E-Commerce setzt die Richtlinie 2000/31/EG in das Nationalrecht um;
- Gesetz Nr. 158/2008 über das Verbot irreführender Werbung und über die Voraussetzungen der erlaubten Vergleichswerbung;
- Gesetz Nr. 148/2000 über die Werbung;
- Gesetz Nr. 8/1996 über die Urheberrechte;
- das neue Bürgerliche Gesetzbuch;

- das neue Strafgesetzbuch.

2 Äußerungsrecht und Pressefreiheit

Art. 30 des Grundgesetzes – Äußerungsfreiheit – sieht vor:

- Die Äußerungsfreiheit der Gedanken, der Meinung oder der Glaube sowie der geistigen Werke aller Art, durch Sprache, Schrift, Bilder, Klang oder andere Mittel der Massenkommunikation ist unantastbar.
- Jede Art von Zensur ist verboten.
- Die Pressefreiheit bezieht sich konsequenter Weise auch auf die Freiheit, Publikationen und Zeitungen zu veröffentlichen. Keine Publikation kann unterdrückt werden.
- Per Gesetz kann die Verpflichtung der Anbieter von medialen Diensten begründet werden, ihre Finanzierungsquellen öffentlich zu machen.
- Die Äußerungsfreiheit darf nicht die Würde, die Ehre, das Privatleben der Person oder das Recht am eigenen Bild verletzen.
- Das Gesetz verbietet die Verunglimpfung des Staates und seiner Symbole sowie der Nation, die Anstiftung zum Aggressionskrieg, zum nationalen, sozialen, rassistischen oder religiösen Hass, zum Klassenkampf, zur Diskriminierung, zur territorialen Separation oder zur öffentlichen Gewalt sowie das obszöne oder sittenwidrige Verhalten.
- Die zivilrechtliche Haftung für veröffentlichte Informationen und geistige Werke obliegt dem Urheber, Verleger, Autor oder Organisator von künstlerischen Veranstaltungen, dem Eigentümer des Multiplikationsmittels, des Radio- oder Fernsehsenders, gemäß Gesetz. Alle Pressedelikte werden gesetzlich geregelt.
- Derzeit gibt es in Rumänien kein Pressegesetz und auch keine gesetzlich verankerten, spezifischen Pressedelikte. Die Journalistenbranche hat es bis dato geschafft, das Verabschieden eines Pressegesetzes zu verhindern.

Art. 31 des Grundgesetzes – Das Recht auf Information

(1) Das Recht auf Information des öffentlichen Interesses kann nicht eingeschränkt werden.

(2) Die öffentlichen und privaten Medien sind verpflichtet, eine korrekte Information der Öffentlichkeit zu gewährleisten.

(6) Die öffentlich-rechtlichen, audiovisuellen Medien funktionieren autonom und sind verpflichtet, den wichtigen, sozialen und politischen Gruppen das „Senderecht" (dreptul la antena) zu gewährleisten.

Art. 70 BGB Das freie Äußerungsrecht

Jede Person hat das Recht, sich frei zu äußern. Die Ausübung der Äußerungsfreiheit kann nur in den Fällen und unter den Voraussetzungen des Art. 75 BGB eingeschränkt werden.

Art. 75 BGB regelt die Voraussetzungen für die Einschränkungen des Äußerungsrechts durch Staatsbehörden.

(1) Einschränkungen, die gesetzlich festgelegt sind oder die durch internationale, von Rumänien unterzeichnete Abkommen über die Menschenrechte vorgesehen sind, stellen keine Verletzungen der genannten Rechte (Äußerungsrecht, Pressefreiheit) dar.

(2) Die gutgläubige Ausübung der Grundrechte und Freiheiten, die im Grundgesetz oder in den von Rumänien unterzeichneten internationalen Abkommen verankert sind, stellt keine Verletzung der genannten Rechte dar.

3 Schutz der Persönlichkeitsrechte

Art. 26 des Grundgesetzes – Schutz des Privatlebens

(1) Die Staatsbehörden respektieren und schützen die Intimsphäre, das Familien- und Privatleben.

(2) Die natürliche Person hat das Recht, über sich selbst zu bestimmen, wenn dadurch die Rechte und Freiheiten der Anderen, die öffentliche Ordnung und die guten Sitten nicht verletzt werden.

Art. 71 BGB Das Recht auf Privatleben

Das Privatleben der Person wird respektiert.

Eingriffe in das Privatleben (persönlichen Lebensbereich: Familie, Wohnsitz, Residenz, Korrespondenz) ohne Einwilligung der Person oder ohne Einhaltung der Voraussetzungen des Art. 75 BGB sind verboten.

Weiterhin ist jegliche Art der Verwendung von Korrespondenz, Manuskripten, persönlichen Unterlagen sowie von Informationen über das Privatleben der Person, ohne ihre Zustimmung oder ohne Einhaltung der Voraussetzungen des Art. 75 BGB, verboten.

Art. 72 BGB Das Recht auf Würde

Die Würde der Person wird respektiert.

Jede Verletzung der Ehre, Würde und des Rufes einer Person, ohne ihre Zustimmung und ohne Einhaltung des Art. 75 BGB, ist verboten.

Art. 73 BGB Das Recht am eigenen Bild

Jede Person hat das Recht am eigenen Bild.

In Ausübung dieses Rechtes ist jede Person berechtigt, jegliche Art von Wiedergabe ihres Aussehens oder ihrer Stimme oder die Verwendung einer solchen Wiedergabe zu verbitten oder zu verhindern. Art. 75 BGB findet Anwendung.

Art. 78 BGB Dem Andenken und dem Körper der Verstorbenen gebührt Respekt.

Art. 79 BGB Schutz des Andenkens der Verstorbenen

Das Andenken der Verstorbenen ist unter den gleichen Voraussetzungen geschützt wie das Recht am eigenen Bild und Privatleben.

Rechtsverletzungen:

Art. 74 BGB Verletzungen des Rechtes auf Privatlebens

Unter Vorbehalt des Art. 75 stellen folgende Handlungen eine Verletzung des Rechtes auf Privatleben dar:

- Das Betreten oder das Verbleiben in der Wohnung einer Person ohne deren Zustimmung, oder das Wegnehmen einer Sache aus der Wohnung einer Person, die sie rechtmäßig bewohnt;
- Das rechtswidrige Abhören von Privatgesprächen durch jegliche technische Mittel oder die vorsätzliche Verwendung einer durch rechtswidriges Abhören erlangten Aufnahme;
- Die Aufnahme und die Verwendung des Bildes oder der Stimme einer Person, die sich in einem Privatraum befindet, ohne ihre Zustimmung;
- Die Ausstrahlung von Bildern aus einem Privatraum ohne Zustimmung desjenigen, der den Privatraum rechtmäßig benutzt;
- Die Beobachtung des Privatlebens durch jegliche Mittel, unter Vorbehalt der gesetzlich geregelten Ausnahmen;
- Die Veröffentlichung oder Ausstrahlung von Informationen, Debatten, Ermittlungen oder Berichten in schriftlicher oder audiovisueller Form ohne Zustimmung der betroffenen Person;
- Die Ausstrahlung von Informationsmaterial, inklusive von Bildern von Personen während medizinischen Behandlungen in Krankenhäusern, sowie von persönlichen Daten bezüglich des Gesundheitszustandes, der Diagnose, Gesundheitsprognose, Behandlung, des Krankheitsbild und von anderen Aspekten, inklusive von Ergebnissen der Autopsie, ohne Zustimmung der Betroffenen Person, oder, wenn diese verstorben ist,

ohne Zustimmung der Angehörigen oder der dazu berechtigten Personen;

- Die bösgläubige Verwendung von Namen, Bildern, Stimme oder Ähnlichkeit einer Person mit einer anderen Person;
- Die Veröffentlichung oder Ausstrahlung von Korrespondenz, Manuskripten oder anderen persönlichen Unterlagen, inklusive von Daten über Wohnsitz, Residenz sowie Telefonnummer einer Person oder ihrer Familienangehörige, ohne deren Zustimmung oder ohne Zustimmung der verfügungsberechtigen Person.

4 Rechtsfolgen

4.1 Zivilrechtliche Rechtsfolgen

Art. 252 BGB

Die durch eine Verletzung der Persönlichkeitsrechte geschädigte Person ist berechtigt, vor Gericht das Verbot der Einleitung, die Aufhebung oder Beendigung sowie die Unterlassung jeder Art von rechtsverletzenden Handlungen zu beantragen. Weiterhin ist der Geschädigte zum Schadensersatz des durch die unerlaubte Handlung entstandenen Schadens sowie zur Veröffentlichung des Urteils auf Kosten des Schädigers berechtigt.

4.2 Strafrechtliche Sanktionen

Für schwerwiegende Verletzungen der Persönlichkeitsrechte sind strafrechtliche Konsequenzen vorgesehen. Die wichtigsten Straftaten zum Schutz der Persönlichkeitsrechte sind:

- Art. 208 StGB Nachstellung
- Art. 224 StGB Hausfriedensbruch
- Art. 226 StGB Verletzung des höchstpersönlichen Lebensbereichs
- Art. 302 StGB Verletzung des Briefgeheimnisses

Im Rahmen der Novellierung des Strafrechts 2009 wurden Straftaten wie Beleidigung, Verleumdung und Nötigung der Justiz (durch die Presse) aus der Sphäre des allgemeinen Strafrechts herausgenommen.

Seitdem gab es mehrere Gesetzesentwürfe zur Wiedereinführung der Beleidigung und der Verleumdung in das StGB als Straftaten, jedoch hat das Parlament, letztmalig im März 2016, diese Gesetzesentwürfe mit deutlicher Mehrheit abgelehnt.

Der Verfassungsgerichtshof begründete im Rahmen einer Verfassungsbeschwerde die verfassungskonforme Straffreiheit der genannten Taten damit, dass die Verpflichtung der Presse und der Medien im Allgemeinen

zur wahrheitsgemäßen und neutralen Veröffentlichung von Informationen des öffentlichen Interesses bereits gesetzlich verankert ist und der Verstoß gegen diese Pflicht zivilrechtlich sanktioniert wird. Unter diesen Umständen erschiene eine zusätzliche, strafrechtliche Sanktionierung als ungerechtfertigte und rechtswidrige „Doppelbestrafung".[1]

5 Schmale Grenze bei Verletzungen der Persönlichkeitsrechte im öffentlichen Bereich

In der Praxis ist folgender Rechtsirrtum verbreitet: wer sein Haus verlassen hat und sich an einem öffentlichen Ort befindet, also an einem Ort, der der Öffentlichkeit jederzeit zugänglich ist, der habe auf seine Privatsphäre verzichtet. Diese Ansicht ist falsch, denn, wenn sich eine Person auf der Straße, in einem Geschäft oder in einem Lokal befindet, bedeutet es nicht, dass sie auf ihre „Anonymität" verzichtet habe. Die bloße Anwesenheit einer Person an einem öffentlichen Ort bedeutet keinen Verlust ihres Rechtes auf Privatleben.

Vorsicht ist geboten, wenn eine Person sich an Veranstaltungen oder Ereignissen beteiligt, die das öffentliche Interesse betreffen (z.B. politische Wahlveranstaltungen, Sportereignisse, Streik). Bei der Teilnahme z.B. an einem Konzert oder einer Aufführung können von den Protagonisten nur mit Ihrer Zustimmung professionelle Bilder oder Aufnahmen gemacht werden. Von den Personen, die sich im Publikum befinden, ist die Einholung ihrer Zustimmung zur Aufnahme von Bildern nicht notwendig. Jedoch könnte das Herausnehmen oder Zoomen eines einzigen Gesichtes aus der Publikumsmenge und Veröffentlichung eines Porträts ohne Zustimmung der betroffenen Person unter Umständen auch eine Rechtsverletzung darstellen.[2]

Das Recht auf Privatleben besteht weiterhin auch am Arbeitsplatz. Daher ist der Arbeitgeber nicht berechtigt, z.B. die Telefongespräche, E-Mails oder die vom Arbeitnehmer abgerufenen Internetseiten aufzunehmen, ohne dass der Arbeitnehmer im Vorfeld darüber in Kenntnis gesetzt wird oder solche Eingriffe in sein Privatleben durch die Betriebsordnung oder Gesetz erlaubt sind. Davon gibt es einige Ausnahmen, z.B. wenn gegen den Arbeitnehmer der Verdacht des Diebstahles besteht oder um in einem Disziplinarverfahren Beweise zu sichern. z.B. dass der Arbeitnehmer den Messenger der Firma für seine Privatkorrespondenz benutzt (EGMR 61496/08 vom 12.1.2016 in der Sache Barbulescu vs. Romania)

---

1 *Turianu,* Dreptul 1/2000, S. 104.

2 *Lisevici/Halcu*, RRD 11/2014, S. 127.

Gem. Verordnung 52/2012 der Nationalen Aufsichtsbehörde für die Verarbeitung von Personaldaten dürfen keine Videoaufnahmegeräte zur Beaufsichtigung des Personals in den Büros der Angestellten installiert werden.

Das Privatleben von Personen des öffentlichen Lebens ist gleichermaßen geschützt, wenn die Informationen über ihr Privatleben das öffentliche Interesse nicht betreffen. Sodann ist z.B. verboten, ohne Zustimmung der betroffenen Person Bilder von Persönlichkeiten des politischen, öffentlichen oder künstlerischen Lebens zu veröffentlichen, wenn diese sich am Strand in ihrem Urlaub, mit ihren Familien, befinden, oder Informationen über intime Aspekte aus deren Leben zu veröffentlichen, zu verwenden oder zu verbreiten.

Bei der Beurteilung der Frage, ob eine Rechtsverletzung des Privatlebens einer Person des öffentlichen Lebens durch Veröffentlichung von Bildern oder Informationen betreffend private Angelegenheiten vorliegt, ist das berechtigte Interesse der Öffentlichkeit das wesentliche Entscheidungskriterium. [6] Demnach könnte es vom öffentlichen Interesse sein, mit wem sich ein hoher Politiker in seiner Freizeit trifft, wenn es sich dabei um vorbestraften oder gerade strafrechtlich verfolgten Personen handelt.

Unter welchen Voraussetzungen kann das öffentliche Interesse im Vordergrund stehen? Die Frage der Rechtmäßigkeit von Informationsveröffentlichungen aller Art, die das Privatleben von Personen des öffentlichen Lebens verletzen könnten, lässt sich anhand der konkreten Umstände des Falles beantworten. Dabei ist eine Interessensanalyse vorzunehmen.

Einige Fallkonstellationen haben sich in der Praxis wie folgt herauskristallisiert. Diese werden nachfolgend beispielsweise kurz aufgezählt:

1. Es liegt im allgemeinen, öffentlichen Interesse die Veröffentlichung der Information, dass gegen einen Politiker wegen Korruption ermittelt wird. Seine Ehe- oder Beziehungsprobleme sowie die Adresse seines Wohnsitzes interessieren die Öffentlichkeit dagegen nicht.
2. Es betrifft das öffentliche Interesse die Information, dass sich eine Person in einer akuten Suizidgefahr befindet, jedoch besteht kein öffentliches Interesse an der Veröffentlichung ihres Bildes. Hier ist viel mehr das Recht am eigenen Bild der betroffenen Person besonders zu schützen (EGMR 44647/98 vom 28.1.2003 Peck vs. UK).
3. Es liegt im öffentlichen Interesse, über ein Verbrechen und in dem Zusammenhang über eine (bekannte) gesuchte Person zu berichten, der die Verübung von Straftaten vorgeworfen wird, jedoch ist in diesem Zusammenhang die Veröffentlichung oder Verwendung von Informationen, die zu einer Identifizierung der Opfer führen könnten (z.B. Bild, Stimme, Adresse), verboten.

4. Es betrifft das öffentliche Interesse, wenn ein Politiker sich in seiner Freizeit mit einem Geschäftsmann trifft und ihm oder seinen Familienangehörigen bestimmte Funktionen oder Arbeitsstellen bei einer staatlichen Behörde oder öffentlich-rechtlichen Institution anbietet.
5. Es betrifft das öffentliche Interesse auch, wie hoch die Telefonrechnung eines Staatsbeamten für sein Diensttelefon ist und ob er im Anschluss an eine Dienstreise noch einige Tage mit seiner Familie am Ort der Dienstreise Urlaub gemacht hat und sich die Privatkosten dafür im Rahmen der Dienstreiseabrechnung hat ersetzen lassen.
6. Wenn gegen eine Person ein Ermittlungsverfahren geführt wird, liegt es im öffentlichen Interesse, darüber zu berichten, welches Objekt das Ermittlungsverfahren hat und welche Ergebnisse aktuell vorliegen. Jedoch stellt die Veröffentlichung von Bildern des Beschuldigten in Handschellen oder von Einzelheiten aus seinem Privatleben eine Verletzung seines Rechts auf Privatleben dar.

Im Ergebnis dieser Kurzanalyse ist festzuhalten, dass die Presse, in ihrer Rolle als „Wachhund der Demokratie", dem Interesse der Öffentlichkeit dienen und entsprechend sachlich und korrekt berichten soll. Dabei ist die Presse auch verpflichtet, auf die Unterscheidung zwischen Tatsachen und Meinungen ausdrücklich hinzuweisen.

Das kommerzielle Interesse der Medien soll keinesfalls lediglich der Neugierde der Öffentlichkeit bezüglich des Privatlebens der Personen des öffentlichen Lebens dienen.[3]

Die gebotene Gutgläubigkeit der Journalisten ist eine deontologische Pflicht und vereint inhaltlich die Legitimität des Zieles einer Berichterstattung, die Neutralität, die Mäßigkeit der Ausdrucksweise sowie die Einhaltung der Unschuldsvermutung.

6 CNA – die Nationale Aufsichtsbehörde der Audiovisuellen Medien

Die CNA wurde durch das Gesetz Nr. 504/2002 über Audiovisuelle Medien als Garant des öffentlichen Interesses gegründet. Die CNA ist die einzige Aufsichtsbehörde in dem Bereich der Audiovisuellen Medien, die befugt ist, Rechtsverordnungen zur Regelung des Lizenzverfahrens und des Inhaltes von audiovisuellen Programmen zu erlassen.

Weiterhin Ist CNA befugt, die audiovisuellen Dienstleister zu monitorisieren und gegen sie Sanktionen zu verhängen oder Empfehlungen auszu-

[3] *Ungureanu*, PR 2/2006, S. 119.

sprechen. Eine Gesetzesinitiative wurde der CNA jedoch nicht eingeräumt.

Die Hauptaufgabe der CAN ist es, für einen gerechten, auf dem Prinzip der Äußerungsfreiheit basierenden Wettbewerb auf dem audiovisuellen Dienstleistungsmarkt zu sorgen. Weiterhin muss die CNA dafür Sorge tragen, dass die audiovisuellen Medienanbieter ihre Dienste unter Einhaltung der gesetzlichen Voraussetzungen leisten und der Öffentlichkeit korrekte Information vermitteln. Dabei haben die Dienstleister die Persönlichkeitsrechte und die gesetzlichen Vorschriften zum Schutz der Minderjährigen zu respektieren und einzuhalten.

Zur Implementierung dieser Aufgaben hat die CNA 2006 die Verordnung über den deontologischen Kodex der audiovisuellen Medien herausgebracht (nachfolgend Kodex), die stets unter Beobachtung der EU-Richtlinien und Empfehlungen durch die Zusammenarbeit auf der europäischen Ebene sowie wegen der Entwicklungen auf der nationalen Ebene ergänzt wird.

Die CNA ist als autonome Aufsichtsbehörde unter parlamentarischer Kontrolle gegründet worden und wird von einem aus 11 Mitgliedern bestehenden Ausschuss geführt. Die Mandatsdauer der Mitglieder des Ausschusses beträgt 6 Jahre. Die Mitglieder werden vom Parlament ernannt, drei auf Vorschlag des Senats, drei auf Vorschlag der Kammer der Abgeordneten, zwei auf Vorschlag des Staatspräsidenten und drei auf Vorschlag der Regierung.

Gem. Art. 12 des Gesetzes 504/2002 erfüllen die Mitglieder des Führungsausschusses der CNA eine öffentliche Staatsfunktion, die der Funktion eines Staatssekretärs gleich steht.

Die Funktion als Mitglied des Führungsausschusses der CNA ist mit jeder anderen, öffentlichen oder privaten Funktion inkompatibel, mit Ausnahme einer didaktischen Tätigkeit, wenn daraus kein Interessenkonflikt entsteht.

Die Mitglieder des Führungsausschusses der CNA dürfen nicht an Handelsgesellschaften direkt oder mittelbar beteiligt sein, deren Tätigkeitsgegenstand in einem Bereich liegt, in dem ein Interessenkonflikt mit der Funktion als Mitglied des Führungsausschusses der CNA entstehen könnte. Weiterhin dürfen vorbestrafte Personen nicht zu Mitgliedern des Führungsausschusses der CNA ernannt werden. Bei Verstoß gegen diese Verbote wird die betroffene Person ihrer Funktion von Amts wegen enthoben.

Auf Vorschlag der spezialisierten Parlamentsausschüsse können Mitglieder des Führungsausschusses der CNA für den Fall, dass sie Ihre

Funktion auf eine Dauer von mehr als 6 Monaten nicht ausüben können oder für den Fall des Eintrittes der Rechtskraft einer strafrechtlichen Verurteilung, Ihres Amtes enthoben werden.

6.1 Rechtsverstöße in den rumänischen Medien – aktuelle Beispiele

1. Verfügung der CNA Nr. 96 vom 23.2.2017 über die Verhängung einer Sanktion – Bußgeld in Höhe von 12.000 RON - gegen den Fernsehsender „Antena 3".

Der Führungsausschuss hat nach Monitorisierung der Sendungen des Nachrichtformates „Tagesschau" in der Zeitspanne bis Januar 2017 mehrere Verstöße gegen Art. 40 und 57 des Kodex (beleidigende Äußerungen, nicht nachgewiesene Vorwürfe; das Recht auf Stellungnahme – *audiatur et altera pars* und Replik) festgestellt und den genannten Sender zur Zahlung eines Bußgeldes in Höhe von 12.000 RON sowie gem. Art 93Abs. 1 und 2 des Gesetzes 504/2002 zur dreimaligen Veröffentlichung eines Textes über die Sanktion innerhalb 24 Stunden ab Zustellung der Verfügung, in der Zeitspanne 18-22 Uhr, mindestens einmal in der Nachrichtenhauptsendung, verpflichtet:

„Die CAN hat den Sender Antena 3 zur Zahlung eines Bußgeldes in Höhe von 12.00 RON wegen der in den Sendungen „Tagesschau" vom 11. und 19. Januar 2017 begangenen Rechtsverletzungen, verpflichtet. In den genannten Sendungen haben sowohl der Moderator als auch die Gäste beleidigende Äußerungen und Vorwürfe gegen Personen vorgebracht, ohne dass diesen Personen die Möglichkeit zur Stellungnahme eingeräumt wurde. Das stellt ein Verstoß gegen Art. 40 des Kodex dar.

Weiterhin hat der Moderator in der genannten Sendung vom 29.1.2017 während der Veröffentlichung der Replik der Antikorruptionsstaatsanwaltschaft Kommentare gemacht. Dies ist im Art. 57 des Kodex verboten.

Es wird darauf hingewiesen, dass dieser Text nicht im Rahmen von Werbung veröffentlicht werden darf".

2. Verfügung der CNA Nr. 95 23.2.2017 über die Verhängung einer Sanktion – Bußgeld in Höhe von 15.000 RON gegen den Fernsehsender „Realitatea TV".

Infolge der Monitorisierung der Sendung "Machtspiele" vom 25.10.2016 hat der Führungsausschuss der CNA mehrere Verletzungen der Art. 30 und 40 des Kodex (Schutz des Privatlebens; Hinweise bezüglich der Unterscheidung zwischen Fakten und Meinungen, Verbot einer beleidigenden Äußerungsweise) festgestellt und eine Sanktion gegen den verantwortlichen Sender verhängt. Die CNA hat in der Begründung der Sanktion festgehalten, dass im Rahmen der genannten Sendung mehrere Bilder von Personen am Strand und bei privaten Freizeitaktivitäten ausgestrahlt

und von beleidigenden und abwertenden Kommentaren begleitet worden sind.

Der Sender wurde weiterhin zur Veröffentlichung des Textes nach Art. 93 des Gesetzes 504/2002 verpflichtet.

3. Verfügung der CNA Nr. 99 vom 28.2.2017 über die Verhängung einer Sanktion – Bußgeld in Höhe von 30.000 RON gegen den Fernsehsender „Antena 1".

Infolge der Monitorisierung der Sendung „Direkter Zugang" – die Art der Sendung wurde als „News Magazine" bezeichnet – in der Zeitspanne vom 20. bis 26. September 2016 zwischen 17:00 Uhr und 19:00 Uhr hat der Führungsausschuss der CNA mehrere Verletzungen der Art. 3 und 39 des Gesetzes 504/2002 sowie der Art. 3, 18 des Kodex (Neutralitätspflicht; Recht auf eine korrekte Information; Schutz der Minderjährigen) festgestellt und eine Sanktion gegen den verantwortlichen Sender verhängt.

Die CNA hat in der Begründung der Sanktion festgehalten, dass in der genannten Sendung das Privatleben und die intimen Beziehungen einer dreizehnjährigen Mutter in Einzelheiten und begleitet von abwertenden Kommentaren der Moderatoren und Gäste thematisiert wurden. Der Inhalt der Sendung wurde infolge der Monitorisierung durch CN als „nicht für Kinder geeignet" eingestuft, so dass die Sendung sowohl inhaltlich als auch bezüglich der Zeitspanne der Ausstrahlung hauptsächlich gegen den Schutz der Minderjährigen verstoßen hat.

Der Sender wurde weiterhin zur Veröffentlichung des Textes nach Art. 93 des Gesetzes 504/2002 verpflichtet.

7 Fazit

In Rumänien ist derzeit eine skurrile Art von kommerziellem Fernsehen festzustellen, wodurch die verschiedenen politischen Parteien versuchen, die Bevölkerung von „ihrem Recht" zu überzeugen und auch zu manipulieren.

Dadurch herrscht in der politisch gespaltenen Bevölkerung eine kontinuierliche Verwirrung. Das gleiche Ereignis wird von den verschiedenen TV-Sendern so unterschiedlich dargestellt und kommentiert, dass sich die Öffentlichkeit im Ergebnis überhaupt keinen objektiven Überblick über die Geschehnisse im eigenen Land verschaffen kann.

Die Verschwörungstheorien sind auf der Tagesordnung der Fernsehsender und sorgen letztendlich für die „Belustigung" und Unterhaltung der Massen.

Ein akutes Problem ist die Abschaffung der Rundfunkgebühr, die mit einem Gesetzesentwurf von der PSD (sozial-demokratischen Partei) eingebracht und vom Parlament verabschiedet wurde. Der Prüfungsantrag des Präsidenten *Johannis* ist abgelehnt worden, so dass die Abschaffung der Gebühr Anfang 2017 wirksam wurde.

Aus welchen Mitteln werden die öffentlich-rechtlichen TV und Radiosender finanziert? Vermutlich ausschließlich aus dem Staatsbudget. Somit können der politischen Intervention praktisch keine Grenzen mehr gesetzt werden.

LITERATUR

Popescu, Corina-Florenţa/Grigore-Radulescu, Maria-Irina: Aspecte privind respectarea dreptului la viata privata de catre mass-media, Pandectele Romane Nr. 10/2014, S. 17-28.

Lisevici, Andreea/Halcu, Bogdan: Dreptul la viata privata, RRD Nr. 11/2014, S. 127-132.

Turianu, Corneliu: Infracţiunile contra demnităţii şi presa, in: Dreptul, Nr. 1/2000, S. 104-108.

Ungureanu, Ovidiu: Dreptul la onoare şi dreptul la demnitate, Pandectele Române, Nr. 2/2006, S. 119-136.

www.infolegal.ro

www.gandul.ro

www.gardianul.ro

AKTUELLE ANPASSUNGEN IM DATENSCHUTZRECHT UND DATENSCHUTZ-GRUNDVERORDNUNG

Boris Reibach, LL.M.

Wissenschaftliches ‚Zentrum Recht in der Informationsgesellschaft' (ZRI)
Carl von Ossietzky Universität Oldenburg
boris.reibach@uni-oldenburg.de

Zusammenfassung

Die DSGVO wollte ursprünglich das Datenschutzrecht EU-weit harmonisieren. Aufgrund zahlreicher Öffnungsklauseln ist es jedoch dem nationalen Gesetzgeber in vielen Fällen freigestellt, Abweichungen vorzusehen. Deutschland hat auf der Bundesebene als erstes Land innerhalb der EU ein Umsetzungsgesetz verabschiedet, das die Öffnungsklauseln nutzt, dabei aber teilweise sogar so weit geht, dass einige Normen eines Tages für europarechtswidrig erklärt werden könnten.

1 Herausforderungen für das nationale und europäische Datenschutzrecht

Die Grundlage des europäischen Datenschutzrechts, die EG-Datenschutzrichtlinie (DSRL), stammt noch aus einer Zeit, als Begriffe wie „Big Data", „Cloud Computing" oder „Internet der Dinge" unbekannt waren. Seit 1995 ist sie in unveränderter Form die Basis für das mitgliedstaatliche Datenschutzrecht. Obwohl der technologische Fortschrift und die Digitalisierung alle Lebensbereiche nach und nach erfassten, wurde nur bei der elektronischen Kommunikation im Jahr 2002 eine eigenständige Richtlinie mit gesonderten Anforderungen erlassen.[1]

In beiden Fällen handelte es sich jedoch lediglich um Richtlinien auf europäischer Ebene, die in nationales Recht umgesetzt werden mussten. Folglich war das Datenschutzniveau in den einzelnen Mitgliedstaaten unterschiedlich hoch. Insbesondere datenaffine amerikanische Konzerne wie Facebook oder Microsoft ließen sich mit ihren europäischen Zentralen daraufhin in Ländern wie Irland nieder und beriefen sich bei EU-wie-

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 31.7.2002, S. 37.

ten Sachverhalten bislang erfolgreich vor Gericht auf das an ihrem Sitz geltende, niedrigere Datenschutzniveau.[2]

Mit einer europäischen „Grundverordnung", die durch weitere begleitende Rechtsakte hätte ergänzt werden sollen, wollte die EU-Kommission vor diesem Hintergrund und nach den Enthüllungen von *Edward Snowden* ein vollharmonisiertes Datenschutzrecht schaffen, das EU-weit einheitliche Standards setzt.[3] Trotz vieler Widerstände schafften es EU-Kommission, Parlament und Mitgliedstaaten nach mehrjähriger Verhandlungszeit, einen Kompromiss zu schließen und eine Europäische Datenschutzgrundverordnung (DSGVO) zu verabschieden, die am 27. April 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde.[4]

Freilich wich diese an zahlreichen Stellen vom ursprünglichen Vorschlag der EU-Kommission ab. Am schwersten wog jedoch, dass die vorgesehene vollharmonisierende Wirkung durch zahlreiche Öffnungsklauseln aufgeweicht wurde, so dass für die Mitgliedstaaten nun doch weite Spielräume zum Abweichen entstanden.[5] Manch einer spricht gar von einer „Richtlinie im Gewand einer Verordnung"[6] oder von einem „Hybrid zwischen Richtlinie und Verordnung".[7]

Gleichwohl ist die DSGVO gemäß Art. 99 Abs. 2 DSGVO in allen Mitgliedstaaten ab dem 25. Mai 2018 unmittelbar anwendbar. Im Folgenden soll daher ein Ausblick gegeben werden, welchen Einfluss die DSGVO auf das deutsche Recht hat und welche Maßnahmen seitens der Bundesgesetzgebers ergriffen wurden, um die für die nicht-öffentlichen Stellen geltenden Datenschutzanforderungen an die neuen Vorgaben anzupassen.

2 Wirkung der DSGVO und nationaler Spielraum

Die DSGVO wirkt unmittelbar und ist für alle Mitgliedstaaten verbindlich, Art. 288 Abs. 1 AEUV. Wo die DSGVO eine abschließende Regelung trifft, kann also entgegenstehendes Recht nicht angewendet werden.

---

2 VG Hamburg, Beschl. v. 3. März 2016 - 15 E 4482/15, ZD 2016, S. 243; OVG Schleswig, Beschl. v. 22. April 2013 - 4 MB 11/13, ZD 2013, S. 364.

3 *Priebe*, EuZW 2012, S. 163.

4 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016, S. 1.

5 *Laue/Nink/Kremer*, Das neue Datenschutzrecht, § 1 Rn. 114.

6 *Roßnagel*, DuD 2017, S. 269.

7 *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, S. 1.

Wenn es erlassen bleibt, dann generiert es allerdings Rechtsunsicherheit für den Rechtsanwender, der zunächst prüfen muss, inwieweit er das mitgliedstaatliche Recht noch anwenden kann.

Eine Möglichkeit zur Anpassung des mitgliedstaatlichen Rechts bei europäischen Verordnungen ist die Abschaffung der bisher geltenden, entgegenstehenden nationalen Normen, da sie ohnehin nicht angewendet werden dürfen. Bei der DSGVO ergibt sich aber die Besonderheit, dass sie zahlreiche Öffnungsklauseln unterschiedlicher Natur hat. Auf der einen Seite gibt es Regelungsgebote, die der nationale Gesetzgeber zwingend ausgestalten muss. Auf der anderen Seite gibt es Regelungsoptionen, die den Mitgliedstaaten eine Möglichkeit eröffnen, nationale Regeln aufzustellen, sie hierzu aber nicht verpflichten.

Wenn man sich die Gesamtheit der Öffnungsklauseln innerhalb der DSGVO ansieht, wird man feststellen, dass es mehr als 60 solcher Öffnungsklauseln gibt – nahezu jedes Kapitel hat seine eigenen Regelungen zum Abweichen vom europäischen Standard. Teilweise sind diese Öffnungsklauseln in separaten Artikeln enthalten, teilweise aber sehr versteckt innerhalb einer eigentlich harmonisierenden Vorschrift zu finden. Dies hat auch den Hintergrund, dass es sich auf der einen Seite um allgemein gehaltene Öffnungsklauseln handeln kann, die einen sehr weiten Gestaltungsspielraum einräumen (beispielsweise Art. 23 DSGVO), auf der anderen Seite aber auch sehr einzelfallbezogene Öffnungsklauseln existieren, die nur einen konkreten Sachverhalt betreffen (beispielsweise Art. 8 Abs. 1 S. 2 DSGVO).

2.1 Regelungsgebote innerhalb der DSGVO

Gebote, welche die Mitgliedstaaten verpflichten, im nationalen Recht Regelungen vorzusehen, finden sich nur vereinzelt in der DSGVO. Sie beschränken sich auf die folgenden fünf Bereiche:

- Zertifizierungen (Artt. 42 ff. DSGVO),
- Datenschutzaufsicht (Artt. 51 ff. DSGVO),
- Rechtsschutz (Art. 83 Abs. 8 DSGVO),
- Sanktionen (Art. 84 DSGVO) sowie
- Meinungs- und Informationsfreiheit (Art. 85 DSGVO).

2.2 Regelungsoptionen innerhalb der DSGVO

Anders als bei den Regelungsgeboten gibt es bei den fakultativen Öffnungen ein undurchsichtiges Geflecht, das dem nationalen Gesetzgeber den Spielraum nicht nur innerhalb der 99 Artikel eröffnet, sondern sogar bis in die Erwägungsgründe hineinreicht (vgl. beispielsweise EG 20 DSGVO).

Es bedurfte in Deutschland eines 525-seitigen Gutachtens, um alle einschlägigen Optionen aus der DSGVO herauszuarbeiten.[8]

Erschwerend kommt hinzu, dass der Spielraum, der dem nationalen Gesetzgeber gelassen wird, in der DSGVO selbst mit unterschiedlichen Begriffen bezeichnet wird. Wenn es um die Ergänzung durch nationale Regeln geht, dann ist mal von „spezifischeren Bestimmungen" (z.B. Art. 6 Abs. 2 DSGVO) und an anderer Stelle von „Rechtsgrundlagen" (z.B. Art. 6 Abs. 3 DSGVO) die Rede. Auch für abweichende mitgliedstaatliche Normen findet sich in der DSGVO ein uneinheitliches Vokabular: so gibt es hierfür die Begriffe der „Beschränkung" (z.B. Art. 23 DSGVO), aber auch der „Ausnahme" (Art. 89 DSGVO).

Als wichtigste Regelungsoptionen der Mitgliedstaaten sind zu nennen:

- Rechtsgrundlagen und spezifischere Bestimmungen für die Rechtmäßigkeit der Datenverarbeitung (Art. 6, 9, 17, 22 DSGVO),
- Altersherabsetzung bei der Einwilligung von Kindern für Dienste der Informationsgesellschaft (Art. 8 DSGVO),
- Beschränkungen bei den Betroffenenrechten (Art. 23 DSGVO),
- Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO),
- Datenverarbeitungen im Beschäftigungskontext (Art. 88 DSGVO),
- Ausnahmen für Forschungs- und Archivzwecke (Art. 89 DSGVO).

3 Status Quo in Deutschland

Die Anpassung des deutschen Rechts durch die DSGVO wird durch die – innerhalb der EU einmalige – Aufteilung der Gesetzgebungskompetenz und Aufsicht beim Datenschutz in Deutschland erschwert.

Mit dem BDSG existiert ein Datenschutzgesetz auf Bundesebene, das für den privaten Sektor und die Bundesbehörden gilt. Daneben enthalten zahlreiche weitere Gesetze auf Bundesebene datenschutzrechtliche Regelungen, beispielsweise das TKG, das TMG oder das SGB. Jedes Bundesland hat zusätzlich Landesdatenschutzgesetze erlassen, die für die öffentlichen Stellen der jeweiligen Länder gelten. Daneben gibt es auch auf Länderebene weitere Datenschutzregelungen in Fachgesetzen, beispielsweise in Krankenhaus-, Schul- oder Beamtengesetzen.

Die Aufsicht ist teilweise konträr zur Gesetzgebungskompetenz geregelt. Die Aufsichtsbehörden der Länder überwachen nämlich nicht nur die öffentlichen Stellen im jeweiligen Bundesland, sondern auch die Privat-

[8] *Kühling/Martini et al*, Die DSGVO und das nationale Recht, S. 1.

wirtschaft, mit Ausnahme der Post- und Telekommunikationsunternehmen. Post- und Telekommunikationsdienstleister unterliegen der Aufsicht der Bundesbehörde; sie überwacht zudem die öffentlichen Stellen des Bundes.

4 Umsetzungsgenese beim Bundesgesetzgeber

Die Bundesregierung hatte sich bereits sehr früh mit dem Regelungsbedarf aufgrund der DSGVO beschäftigt, nicht zuletzt wegen der anstehenden Bundestagswahl im Herbst 2017.[9] Man befürchtete, dass das neu zusammengesetzte Parlament, das erst Ende 2017 zusammentreten würde, es nicht schafft, das erforderliche Umsetzungsrecht noch vor dem 25. Mai 2018 zu erlassen. Das Bundesinnenministerium entschied sich deshalb für ein zweistufiges Vorgehen: man setzte sich das Ziel, in einem ersten Schritt noch vor der Sommerpause 2017 ein Datenschutz-Anpassungsgesetz auf Bundesebene zu beschließen, das zunächst die zwingenden Regelungsgebote sowie die aus Sicht der Bundesregierung vorrangigen Regelungsoptionen beinhaltet. Erst in einem zweiten Schritt sollte dann in der nächsten Legislaturperiode überlegt werden, ob weitere Regelungen erforderlich sind.

Bei den vorrangigen Regelungsoptionen war bereits ersichtlich, dass die DSGVO – anders als das BDSG – die Bereiche Arbeitnehmerdatenschutz, Videoüberwachung, Scoring, Werbung sowie Markt- und Meinungsforschung nicht konkret regelte. Hier war es für den bundesdeutschen Gesetzgeber also möglich, im Rahmen des Spielraums der Öffnungsklauseln national an das alte Schutzniveau des BDSG anzuknüpfen.

Das geplante Vorhaben wurde dann auch in die Tat umgesetzt, so dass Deutschland als erstes Land innerhalb der EU auf Bundesebene ein Anpassungsgesetz zu seinem Datenschutzrecht erlassen hat. Das sog. „Datenschutz-Anpassungs- und Umsetzungsgesetz-EU“ (DSAnpUG-EU) stellt ein neues BDSG („BDSG-2018“) auf Bundesebene auf, das zwar auf der einen Seite nur spärlich von den Möglichkeiten der Regelungsoptionen Gebrauch macht, auf der anderen Seite aber dort, wo es davon Gebrauch gemacht hat, wegen einer möglichen Überschreitung der mitgliedstaatlichen Regelungskompetenz Kritik erfahren hat.[10]

Nachfolgend soll also diese Umsetzungsgesetzgebung des Bundes beleuchtet werden – sowohl hinsichtlich der Regelungsgebote als auch hinsichtlich der Regelungsoptionen. Außer Betracht bleiben die im BDSG-

[9] So in einer Interviewfrage *Zimmer-Helfrich*, ZD 2016, S. 457.

[10] Vgl. die Stellungnahmen in der BT-Ausschuss-Drs. 18(4)824.

2018 erlassenen Umsetzungsnormen für die öffentlichen Stellen sowie alle Regelungen, die der Umsetzung der Richtlinie (EU) 2016/680[11] dienen.

5 Umsetzung der Regelungsgebote im BDSG-2018

5.1 Zertifizierungen

Art. 43 Abs. 1 S. 2 DSGVO fordert vom nationalen Gesetzgeber, sicherzustellen, dass Zertifizierungsstellen von der zuständigen Datenschutzaufsichtsbehörde und/oder einer nationalen Akkreditierungsstelle gemäß Verordnung (EG) 765/2008 akkreditiert werden. In Entsprechung dieses Erfordernisses regelt § 39 BDSG-2018 ein Zwittermodell: die Akkreditierung in Deutschland erfolgt durch die Deutsche Akkreditierungsstelle (DAkkS), die Aufsichtsbehörde wirkt aber bei der Entscheidung mit, weil die Akkreditierung im Einvernehmen mit der Aufsichtsbehörde erfolgen muss. Begründet wird die Entscheidung des Gesetzgebers damit, dass die DAkkS über „hohe Kompetenz und Erfahrung bei der Akkreditierung und über eine etablierte und erprobte Akkreditierungsinfrastruktur“ verfüge.[12]

5.2 Datenschutzaufsicht

Im BDSG-2018 ist aus kompetenzrechtlichen Gründen (vgl. oben, Ziff. 3) ausführlich das Aufsichtsorgan des Bundes, im Gesetz „die oder der Bundesbeauftragte“ genannt (BfDI), geregelt. Das Kapitel 4 normiert in den §§ 8-16 BDSG-2018 dessen Errichtung, Zuständigkeit, Unabhängigkeit, Ernennung und Amtszeit, Amtsverhältnis, Rechte und Pflichten, Aufgaben sowie Befugnisse. Auch die Abgabe des jährlichen Tätigkeitsberichts durch die oder den Bundesbeauftragten wird geregelt.

Die Ernennung soll nach § 11 Abs. 1 BDSG-2018 ohne Aussprache auf Vorschlag der Bundesregierung im Bundestag erfolgen. Dies steht im Widerspruch zu Art. 53 Abs. 1 DSGVO, der ein transparentes Verfahren zur Ernennung der Mitglieder der Aufsichtsbehörden fordert. Anforderungen an die Person, wie das Mindestalter von 35 Jahren oder die Beschränkung auf eine einmalige Wiederwahl, finden keine ausdrückliche Grundlage in der DSGVO. Der deutsche Gesetzgeber riskiert also bereits

[11] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4.5.2016, S. 89.

[12] BT-Drs. 18/11325, S. 107.

bei der Regelung der Bundesbehörde einen europarechtswidrigen Zustand.

Da für die Privatwirtschaft die Länder die Aufsicht übernehmen, verweist § 40 BDSG-2018 entsprechend auf die nach Landesrecht zuständigen Behörden, vermag deren Konstitution mangels Zuständigkeit aber freilich nicht zu regeln. Für den Fall einer länderübergreifenden Datenverarbeitung mit mehreren Niederlassungen in Deutschland wird von § 40 Abs. 2 BDSG-2018 der Ort der Hauptniederlassung im Sinne des Art. 4 Nr. 16 DSGVO für maßgeblich erklärt. Obwohl in der DSGVO nicht ausdrücklich enthalten, spricht § 40 Abs. 6 BDSG-2018 den Datenschutzbeauftragten der Privatwirtschaft ein Beratungsrecht zu – anders als im bisherigen BDSG haben dieses Recht aber nur Datenschutzbeauftragte, und nicht mehr auch die verantwortlichen Stellen selbst.

5.3 Rechtsschutz

Hinsichtlich des national sicherzustellenden Rechtsschutzes aus Art. 83 Abs. 8 DSGVO verweist § 20 BDSG-2018 beim Rechtsschutzerfordernis aus Art. 78 DSGVO auf den Verwaltungsrechtsweg und § 41 BDSG-2018 beim Rechtsschutzbedürfnis nach Verstößen auf das OWiG. Darüber hinaus gelten für Betroffene, verantwortliche Stellen und Auftragsverarbeiter auch generell die Rechtschutzmöglichkeiten des deutschen Zivil-, Straf- und öffentlichen Rechts.

5.4 Sanktionen

Bezüglich der sog. „anderen Sanktionen“, die jeder Mitgliedstaat nach Art. 84 DSGVO für Verstöße festzulegen hat und die neben den Geldbußen stehen, hat der deutsche Gesetzgeber mit § 42 BDSG-2018 Strafvorschriften eingefügt. Gegenüber dem BDSG steigt die Strafandrohung in § 42 Abs. 1 BDSG-2018 auf bis zu drei Jahre Freiheitsstrafe. Es handelt sich um einen neuen Tatbestand des gewerbsmäßigen Übermittelns oder Bereitstellens personenbezogener Daten einer großen Anzahl von Personen. Ansonsten verbleibt es bei der aus § 44 Abs. 1 BDSG bekannten Strafvorschrift der mit Gewinnerzielungs- oder Schädigungsabsicht erfolgenden, unzulässigen Datenverarbeitung.

5.5 Meinungs- und Informationsfreiheit

Zur Meinungs- und Informationsfreiheit findet sich im BDSG-2018 keine Norm, obwohl § 41 BDSG hierzu Regelungen getroffen hatte. Als Grund nennt der Bundesgesetzgeber seine mangelnde Gesetzgebungszuständigkeit. Da für das Pressewesen nunmehr ausschließlich die Länder zuständig seien, könne § 41 BDSG aus kompetenzrechtlichen Gründen nicht

beibehalten werden.[13] Der Bundesgesetzgeber gehe gleichwohl davon aus, dass die insofern zuständigen Landesgesetzgeber das Presseprivileg wie bisher absichern würden. Dies bleibt eine vage Hoffnung, da bislang jedenfalls keine dahingehenden Aktivitäten der Landesgesetzgeber stattgefunden haben.

6 Ausgestaltung ausgewählter Regelungsoptionen im BDSG-2018

Dem Plan des Bundesinnenministeriums folgend, konnten auch einige Regelungsoptionen durch Normierung nationaler Besonderheiten genutzt werden. Nachfolgend sind die wichtigsten nationalen Abweichungen von der DSGVO für nicht-öffentliche Stellen zusammengefasst:

6.1 Videoüberwachung

Der Gesetzgeber hat in Anlehnung an § 6b BDSG in § 4 BDSG-2018 die Überwachung öffentlich zugänglicher Räume geregelt, da sich in der DSGVO keine Normen zur Videoüberwachung finden lassen. Gleichwohl hat es der Gesetzgeber versäumt, in der Gesetzesbegründung die Öffnungsklausel zu benennen, auf die er die Beibehaltung der Videoüberwachungsvorschriften im BDSG-2018 stützt. Dies führt zu der absurden Situation, dass nach § 4 Abs. 1 BDSG-2018 die Videoüberwachung öffentlich zugänglicher Räume nur unter bestimmten, im BDSG-2018 genannten Fällen zulässig ist. Damit sind Videoüberwachungen entgegen den Vorgaben der DSGVO z.B. nicht mit einer Einwilligung oder mit vertraglichen Zwecken legitimierbar. Es erscheint deshalb sehr fraglich, ob § 4 BDSG-2018 europarechtskonform ist.

6.2 Verarbeitung besonderer Kategorien personenbezogener Daten

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten macht der deutsche Gesetzgeber von den Öffnungsmöglichkeiten des Art. 9 DSGVO Gebrauch. Er erlaubt in § 22 Abs. 1 BDSG-2018 über die in der DSGVO bereits geregelten Sachverhalte hinaus Fälle der Datenverarbeitung mit Daten nach Art. 9 Abs. 1 DSGVO. Damit sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung gemeint.

[13] BT-Drs. 18/11325, S. 79.

6.3 Zweckändernde Verarbeitung

Über den in Art. 6 Abs. 4 DSGVO enthaltenen Kompatibilitätstest hinaus, kann nach § 24 BDSG-2018 die Zulässigkeit von zweckändernden Verarbeitungen legitimiert werden, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich sind oder sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich sind und die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegen.

Es handelt sich damit um eine über Art. 6 und 9 DSGVO hinausgehende Erlaubnis, wobei bei besonderen Kategorien personenbezogener Daten nach § 24 Abs. 2 BDSG-2018 stets die Voraussetzungen der jeweiligen Ersterhebungsvorschrift mitzuprüfen sind. Allerdings sieht Art. 9 DSGVO keine Öffnung für zweckändernde Verarbeitungen vor, so dass § 24 Abs. 2 BDSG-2018 der europarechtlichen Vorgabe entgegensteht. Der Gesetzgeber beruft sich in seiner Gesetzesbegründung auf die Öffnungsklausel des Art. 6 Abs. 4 DSGVO,[14] vermag damit aber nicht zu überzeugen, da Art. 6 DSGVO gerade nicht für besondere Kategorien personenbezogener Daten gilt.

6.4 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Im Rahmen der Öffnungsklausel des Art. 88 DSGVO hat der deutsche Gesetzgeber die Regelungen des § 32 BDSG in § 26 BDSG-2018 weiterleben lassen.

Die Norm des § 26 BDSG-2018 ist allerdings auf neun Absätze angewachsen und enthält neben den Verarbeitungsvoraussetzungen (§ 26 Abs. 1 BDSG-2018), die nunmehr auch ausdrücklich die „Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten“ als Zweck vorsehen, auch eine Regelung zur Beurteilung der Freiwilligkeit einer Einwilligung im Arbeitsverhältnis (§ 26 Abs. 2 BDSG-2018). Entgegen ihrer Formfreiheit nach DSGVO, bedarf die Einwilligung im Arbeitsverhältnis nach § 26 Abs. 2 S. 2 BDSG-2018 in der Regel der Schriftform. Es wird zudem klargestellt, dass Betriebsvereinbarungen eine hinreichende Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten sein können (§ 26 Abs. 4 BDSG-2018).

[14] BT-Drs. 18/11325, S. 96.

6.5 Scoring und Bonitätsauskünfte

Mit § 31 BDSG-2018 erhält der Gesetzgeber die §§ 28a, 28b BDSG aufrecht. Es handelt sich um Regelungen zur Zulässigkeit des Scorings sowie zur Verwendung solcher von Auskunfteien ermittelten Scores. Sie sollen zum einen dem Schutz des Wirtschaftsverkehrs dienen und zum anderen auch Verbraucher vor Überschuldung schützen.[15]

Der Gesetzgeber schweigt sich allerdings wie bei vielen anderen Normen dazu aus, auf welche Öffnungsklausel er die Regelungen in § 31 BDSG-2018 stützt.[16] Darüber hinaus beschränkt der Gesetzgeber – ähnlich wie bei der Videoüberwachung in § 4 BDSG-2018 – die Zulässigkeit der Datenverarbeitung für das Scoring laut Wortlaut („nur zulässig") auf die in § 31 BDSG-2018 genannten Fälle, ohne dass ein Rückgriff auf die allgemeinen Normen der DSGVO möglich ist. Folglich wird auch § 31 BDSG-2018 mit hoher Wahrscheinlichkeit vom EuGH überprüft werden.

6.6 Betroffenenrechte

Das BDSG-2018 nutzt die weite Öffnungsklausel des Art. 23 DSGVO und regelt in den §§ 32-37 BDSG-2018 Einschränkungen der Betroffenenrechte der DSGVO. Während die DSGVO bereits einzelne Ausnahmen kennt, fügen §§ 32-37 BDSG-2018 weitere Ausnahmen hinzu. Allerdings sind die Regelungen im Rahmen des Gesetzgebungsverfahrens teilweise entschärft worden, so dass beispielsweise die ursprünglich geplante Erleichterung, bei unverhältnismäßigem Aufwand personenbezogene Daten nur zu sperren statt zu löschen, gestrichen wurde. Geblieben ist hingegen eine Sondererlaubnis für die automatisierte Entscheidung bei Leistungserbringungen durch Versicherer in § 37 BDSG-2018.

6.7 Datenschutzbeauftragte

Die Tradition des betrieblichen Datenschutzbeauftragten führt der deutsche Gesetzgeber auch im BDSG-2018 fort. Auf Basis der Öffnungsklausel des Art. 37 Abs. 4 DSGVO wird die Pflicht des bisherigen § 4 f BDSG, einen Datenschutzbeauftragten zu bestellen, wenn die verantwortliche Stelle in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, wenn eine Datenschutz-Folgenabschätzung (im BDSG noch „Vorabkontrolle") durchzuführen ist oder wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden, in § 38 BDSG-2018 aufrechterhalten.

---

[15] BT-Drs. 18/11325, S. 101.

[16] Mögliche Öffnungsklauseln finden sich aber bei *Taeger*, RDV 2017, S. 3 (6 ff.).

Auch die Stellung des Datenschutzbeauftragten bleibt wie bisher, da § 38 Abs. 2 BDSG-2018 auf die Regelungen zu den Datenschutzbeauftragten der öffentlichen Stellen in § 6 BDSG-2018 verweist. Die Datenschutzbeauftragten der nicht-öffentlichen Stellen genießen also den bisherigen Kündigungsschutz, sind zur Verschwiegenheit verpflichtet und haben ein Zeugnisverweigerungsrecht.

7 EuGH wird das BDSG-2018 untersuchen müssen

Wenngleich einige Regelungen für das deutsche Datenschutzniveau positiv zu bewerten sind, lässt bereits die hier aufgezeigte Auswahl der im BDSG-2018 enthaltenen Umsetzungsnormen befürchten, dass der deutsche Gesetzgeber teilweise über das Ziel hinausgeschossen ist. Offensichtlich war er sich in einigen Fällen selbst nicht so sicher, so dass er sich gar nicht erst bemüht hatte, bei strittigen nationalen Normen die entsprechend genutzte Öffnungsklausel der DSGVO zu benennen.

Als Verlierer bleiben damit die Rechtsanwender zurück, die ihre Prüfungen in der gesetzlichen Grauzone zwischen BDSG-2018 und DSGVO vornehmen müssen; alternativ bleibt dann aus Sicherheitsgründen nichts anderes übrig, als zunächst das strengste Recht zu beachten. Rechtsklarheit kann man nur nach etwaigen Entscheidungen des EuGH erhalten, die aber noch mehrere Jahre auf sich warten lassen werden.

LITERATUR

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/ Nink, David/Weinzierl, Quirin/Wenzel, Michael: Die DSGVO und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf, Münster 2016.

Laue, Philip/Nink, Judith/Kremer, Sascha: Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

Priebe, Reinhard: EU-Kommission: Vorschlag eines neuen europäischen Datenschutzrahmens, EuZW 2012, S. 163-164.

Roßnagel, Alexander: Entwurf eines neuen Bundesdatenschutzgesetzes, DuD 2017, S. 269-270.

Taeger, Jürgen: Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, S. 3-9.

OVER-THE-TOP-ANBIETER ALS TELEKOMMUNIKATIONSDIENSTE IM LICHTE DES GELTENDEN UND ZUKÜNFTIGEN TELEKOMMUNIKATIONSRECHTS

Sebastian Telle

Wissenschaftliches ‚Zentrum Recht in der Informationsgesellschaft' (ZRI)
Carl von Ossietzky Universität Oldenburg
sebastian.telle@uni-oldenburg.de

Zusammenfassung

In den letzten Jahren treten immer mehr Unternehmen auf, die Kommunikationsdienste über das offene Internet anbieten. Dabei üben sie einerseits auf andere Unternehmen einen hohen wettbewerblichen Druck auf, indem sie sich scheinbar sektorspezifischen Regelungen entziehen. Im Bereich der Telekommunikationsbranche stellen sogenannte Over-the-Top-Dienste (OTT) bisherige regulatorische Dogmen in Frage und sehen sich einer breit durch Politik, Gesellschaft und Wissenschaft geführten Debatte ausgesetzt, ob es ein Level Playing Field im Sinne einer Wettbewerbsgleichheit zwischen unterschiedlichen Akteuren der Branche geben sollte. Dieser Beitrag beschreibt die Einordnung von OTT-Angeboten als Telekommunikationsdienst nach geltendem Recht sowie im Rahmen der derzeitigen Überarbeitung des europäischen Telekommunikationsrechtsrahmens. Dabei werden in einem ersten Abschnitt technische, wirtschaftliche und regulatorische Hintergründe dargestellt. Im zweiten Abschnitt wird die derzeitige rechtliche Debatte über die Einordnung von OTT-Diensten als Telekommunikationsdienst im Sinne von § 3 Nr. 24 TKG erläutert. Schließlich diskutiert der dritte Abschnitt die aktuellen Änderungsvorschläge im Zusammenhang mit dem Richtlinienvorschlag über einen „Europäischen Kodex für Elektronische Kommunikation" (EKEK-Entwurf).[1]

1 Hintergründe

Over-the-Top-Dienste treten in verschiedenen Branchen auf und werden üblicherweise beschrieben als Angebote, die "über das offene Internet" erbracht werden.[24] Im Telekommunikationsbereich stellen Unternehmen dabei ihre Angebote IP-basiert der Öffentlichkeit zur Verfügung und bedienen sich auch der vorhandenen physikalischen Übertragungsinfrastruktur. Dabei treten sie zu konventionell auftretenden Unternehmen Wettbewerb. Diese stellen angesichts des immer stärker werdenden Wettbewerbsdrucks im Zusammenhang mit den Angeboten der OTT-

[1] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, COM[2016]590 final.

Anbieter die Forderung eines einheitlichen geltenden rechtlichen Maßstabs.[2]

1.1 Technische Hintergründe

Herkömmliche Telekommunikationsunternehmen erbringen ihre Dienste üblicherweise über Infrastrukturen, wie zum Beispiel Kabel, Switches oder Funkmasten. Dabei erbringen sie Telekommunikationsdienstleistungen entweder auf der Basis eigener physischer Netzinfrastrukturen oder aber als Reseller auf der Grundlage ihnen überlassener Infrastrukturen oder ihnen gegenüber erbrachter Dienstleistungen. OTT-Unternehmen erbringen ihre Dienste dagegen über das Internet, also ein weltweites Netzwerk aus verschiedenen zusammengeschalteten Netzwerken, die mittels offener Internetprotokolle gesteuert werden.[3] Der Internetzugang dient hier als grundsätzliche Voraussetzung, wird aber von den OTT-Anbietern nicht selbst bereitgestellt.

Hinsichtlich der Netzwerk-Architektur lassen sich OTT-Dienste grob in zwei gegensätzliche Modelle einordnen.[4] Auf der einen Seite können sie auf einer Client-Server-Struktur basieren, auf der anderen Seite erfolgt die Umsetzung auf der Grundlage einer Peer-to-Peer-Struktur. Im ersten Fall erfolgt die Kommunikation zwischen den Teilnehmern über eine zentralisierte logische Verbindung über einen Client-Server, der IP-Pakete im Zusammenhang mit einem Kommunikationsvorgang zuordnet und verteilt. Im zweiten Fall bestehen logische Verbindungen ausschließlich zwischen einzelnen Kommunikationsteilnehmern. Eine zentrale Infrastruktur, die Einfluss auf die Kommunikationsvorgänge hat und diese steuert, fehlt hier.

Beiden Modellen ist gemein, dass die Kommunikation sich des offenen Internet-Protokolls bedient, das im OSI-Modell auf der dritten Schicht eingeordnet wird. Auf dieser sogenannten Vermittlungsschicht werden Datenpakete weitervermittelt. Bei reinen Peer-to-Peer-Systemen werden die Informationen zwischen den an dem Kommunikationsvorgang Beteiligten über physikalische Infrastruktur von Dritten vermittelt, während bei einer Client-Server-Architektur die Vermittlung über die zentrale Infrastruktur des OTT-Anbieters erfolgt.

---

2 *Ufer*, Die Macht der Plattformen, 2017, S. 76 (77).

3 *Gersdorf*, K&R 2016, S. 91.

4 *Schumacher*, K&R 2015, S. 771 (772); *Kühling/Schall*, CR 2015, S. 641 (644).

1.2 Wettbewerbsökonomische Betrachtung

OTT-Dienste können in wettbewerblicher Hinsicht nach der Art und Weise des jeweiligen Angebots unterschieden werden.[5] So gibt es zum einen OTT-Inhaltsdienste, deren maßgeblicher Schwerpunkt auf der Bereitstellung bestimmter Hinhalte liegt. Hiervon sind auf der anderen Seite die OTT-Kommunikationsdienste abzugrenzen, mittels derer die Nutzer über das Internet kommunizieren können. Dabei können diese Dienste konventionelle Angebote ergänzen, indem sie weitere Inhalte, Dienste oder Funktionalitäten bereitstellen.

In der Telekommunikationsbranche besonders auffallend ist jedoch, dass einige OTT-Dienste konventionelle Angebote in wettbewerblicher Hinsicht ersetzen.[6] Dies fällt besonders stark an dem Zusammenhang zwischen abnehmender Masse an SMS-Kommunikation und potenziell zunehmender Verwendung alternativer Messenger-Dienste wie zum Beispiel WhatsApp, Threema oder mittlerweile auch dem Facebook Messenger.[7] So verringerte sich die Zahl der in Deutschland versendeten SMS gegenüber dem Vorjahr von 16,6 Mrd. auf 12,7 Mrd.[8]

Weiterhin kann zwischen der Zugangs- und der Diensteebene unterschieden werden.[9] OTT-Dienste setzen einen bereits bestehenden Zugang zum Internet voraus. In dieser Hinsicht ist das OTT-Angebot kein wettbewerbliches Substitut für den Netzzugang. Allerdings treten auf der Diensteebene teilweise Substitutionseffekte auf, weshalb seit einiger Zeit eine marktbezogene Wettbewerbsgleichheit – auch „Level Playing Field" genannt – sowohl auf der gesetzgeberischen Ebene also auch im Rahmen der Rechtsanwendung durch die Regulierungsbehörden gefordert wird.[10]

1.3 Rechtliche Konsequenzen einer Einordnung als Telekommunikationsdienst

Die Relevanz einer Einordnung moderner OTT-Dienste als Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG ist hoch, da verschiedene Regelungen an dieses Merkmal anknüpfen. Dies betrifft die Regeln des Fernmeldegeheimnisses, des Kunden- und Datenschutzes, aber auch der öffentlichen Sicherheit. So sind Dienstanbieter und ihre Mitarbeiter gemäß § 88 Abs. 2 S. 1 TKG zur Wahrung des Telekommunikationsgeheim-

---

5 *Kühling/Schall*, CR 2015, S. 641 (642).

6 *Ufer*, Die Macht der Plattformen, 2017, S. 76 (77).

7 Siehe auch *Bundesnetzagentur*, Jahresbericht 2016, S. 145.

8 *Bundesnetzagentur*, Jahresbericht 2016, S. 58.

9 *Ufer*, Die Macht der Plattformen, 2017, S. 76 (79).

10 *Ufer*, Die Macht der Plattformen, 2017, S. 76 (80).

nisses verpflichtet und müssen gemäß § 93 TKG besonderen Informationspflichten betreffend die Erhebung und Verwendung personenbezogener Daten nachkommen. In diesem Zusammenhang stehen auch besondere Anforderungen an eine wirksame Einwilligung im elektronischen Verfahren nach § 94 TKG sowie gegenüber dem allgemeinen Datenschutzrecht strengere Voraussetzungen hinsichtlich der Erhebung und Verwendung von Bestands-, Verkehrs- oder Standortdaten. Im Bereich des Verbraucherschutzes sind vor allem die Vorschriften für Transparenzverpflichtungen nach §§ 43a und 45n TKG relevant. Außerdem sind dem Anwendungsbereich des TKG unterfallende Unternehmen der Bundesnetzagentur im Rahmen ihrer Befugnisse zur Auskunft oder Information verpflichtet. Schließlich könnten diese Unternehmen von Auskunftsverlangen durch bestimmte Behörden betroffen sein oder Verpflichtungen im Zusammenhang mit Überwachungsmaßnahmen nachkommen müssen. Maßnahmen im Zusammenhang mit einer möglichen Marktregulierung dürften wohl derzeit ausgeschlossen sein, da diese die Feststellung einer beträchtlichen Marktmacht auf einem als regulierungsbedürftig eingestuften Markt voraussetzt.[11] Dies verlangt wiederum eine derzeit so nicht absehbare Festlegung durch die EU-Kommission in einer Märkteempfehlung.

Eingangstor und exemplarisch für die rechtliche Diskussion über die Eigenschaft als Telekommunikationsdienst ist jedoch die Vorschrift des § 6 TKG, nach der die Erbringer von Telekommunikationsdiensten deren Aufnahme bei der Bundesnetzagentur anzumelden haben. Diese Regelung dient lediglich dem Zweck, der Behörde eine Übersicht über das Marktgeschehen zu ermöglichen, indem in der Branche aktive Unternehmen registermäßig erfasst werden. Dagegen sind – außer einer Bußgeldbewehrung gemäß § 149 Abs. 1 Nr. 2, Abs. 2 TKG bei Verstoß – keine unmittelbaren rechtlichen Folgen an die Meldung geknüpft und auch in wirtschaftlicher Hinsicht werden die betroffenen Unternehmen nicht erheblich eingeschränkt. Wird ein Unternehmen jedoch in diesem Zusammenhang von der Behörde als Telekommunikationsdienst eingeordnet, kann es ebenso von anderen Vorschriften des TKG, insbesondere aber auch Eingriffsbefugnissen betroffen sein. Für OTT-Anbieter kann ein erhebliches Interesse bestehen, nicht von diesen Vorschriften betroffen zu sein, weshalb sie sich bereits einer bloßen Meldepflicht zu entziehen versuchen.

[11] *Kühling/Schall*, CR 2015, S. 641 (653); *Ufer*, Die Macht der Plattformen, 2017, S. 76 (80).

2 OTT-Dienste als Telekommunikationsdienste de lege ferenda

Nach der grundlegenden Definition des § 3 Nr. 24 TKG sind Telekommunikationsdienste als diejenigen Dienste bezeichnet, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen und die regelmäßig gegen Entgelt erbracht werden. Dass auch das Internet als solches ein Telekommunikationsnetz ist, stellt § 3 Nr. 27 TKG klar. Im Zusammenhang mit der Einordnung von OTT-Angeboten als Telekommunikationsdienste im Sinne des § 3 Nr. 24 TKG wird zum einen diskutiert, wann diese Dienste mit einer mindestens überwiegenden Signalübertragung sind. In diesem Zusammenhang steht auch die Frage, welches Angebot oder welche Bestandteile hiervon überhaupt als Dienst anzusehen sind. Zum anderen wird für viele Angebote das Tatbestandsmerkmal der regelmäßigen Entgeltlichkeit infrage gestellt, da viele OTT-Angebote ohne ein unmittelbares monetäres Entgelt erfolgen.

2.1 Regelmäßige Entgeltlichkeit bei Plattformgeschäften

Entgeltlichkeit bedeutet dem Wortlaut nach zunächst, dass die Leistung des Dienstes mit einem Entgelt vergolten wird. Dies scheint jedoch gerade bei OTT-Diensten häufig zu fehlen. Viele dieser Unternehmen bieten ihre Dienste für Endkunden ohne einen zu zahlenden Betrag an. Zum Beispiel sind viele E-Mail-Dienste grundsätzlich kostenlos für den Endkunden. Auch für den Messenger WhatsApp müssen die Nutzer bis auf einen kurzen Zeitraum vor einigen Jahren gegenwärtig nichts bezahlen.

Aus diesem Umstand, dass der Leistung der OTT-Anbieter kein unmittelbares Entgelt gegenübersteht, könnten verschiedene Schlüsse gezogen werden. Zum einen könnte das fehlende unmittelbare monetäre Entgelt als Argument dafür herangezogen werden, dass überhaupt keine Entgeltlichkeit vorliegt, sodass das jeweilige Angebot kein Telekommunikationsdienst ist.[12] Es würde sich dann um unentgeltliche Dienste handeln, die nach dieser Argumentation vom Anwendungsbereich des Telekommunikationsgesetzes ausgeschlossen wären. Dass allein die vertragsrechtliche Ausgestaltung auf der Endkundenebene bereits über die Anwendbarkeit telekommunikationsrechtlicher Regelungen ausschlaggebend sein soll, erscheint angesichts des in § 1 TKG festgelegten Gesetzeszwecks und der in § 2 Abs. 2 TKG normierten Regulierungsziele aber widersinnig.

[12] *Schuster*, CR 2016, S. 173 (182 f.)

Zum anderen ließe sich argumentieren, die Anbieter würden sich zwar kein monetäres Entgelt gewähren lassen. Stattdessen würden die Nutzer jedoch mit ihren Daten bezahlen.[13] Diese Theorie erfreut sich zwar zunehmender Beliebtheit, überreizt jedoch zum einen die Relevanz von Daten als wirtschaftlicher Faktor und geht zum anderen am Wortlaut des § 3 Nr. 24 TKG vorbei. Zwar mögen Daten eine zunehmende wirtschaftliche Bedeutung erhalten und für Unternehmen besonders wichtig sein. Dennoch lassen sich Daten nur unzulänglich im Sinne eines Gegenwertes erfassen. So gibt es nicht den einen festen Wert für Daten. Der Wortlaut „entgeltlich" lässt sich darüber hinaus nicht auf jedes beliebige synallagmatische Austauschverhältnis ausdehnen, sondern verlangt eine Leistung und eine monetäre Gegenleistung. Die Entgeltlichkeit könnte weiterhin mit einer Bezahlung durch Aufmerksamkeit oder durch die Einräumung wirtschaftlich einem Entgelt äquivalenter datenschutzrechtlicher Einwilligungen begründet werden. Auch diese Theorien überstrapazieren den Wortlaut des § 3 Nr. 24 TKG.

Auf ein unmittelbares Entgelt wird es jedoch nicht ankommen. Zum einen impliziert der Wortlaut „regelmäßige Entgeltlichkeit" bereits, dass es nicht stets auf einen monetären Gegenwert ankommen muss.[14] Stattdessen soll maßgeblich allein eine gewisse Wirtschaftlichkeit sein.[15] OTT-Angebote sind überwiegend als sogenannte Plattform-Geschäftsmodelle ausgestaltet. Ein wesentliches Merkmal von Plattformen ist, dass es sich um Unternehmen mit mehrseitigen Markbeziehungen handelt, zwischen denen indirekte Netzwerkeffekte bestehen. Ein geeignetes Beispiel hierfür ist die Konstellation einiger Social-Media-Plattformen. Diese haben neben ihrer Kundengruppe der Endkunden häufig noch eine Markbeziehung zu einer weiteren Kundengruppe, die Werbung oder ähnliche Inhalte über die Plattform schalten lässt. In dieser Ausprägung kann sich das Verhalten der unterschiedlichen Kundengruppen jeweils positiv wie auch negativ auf das Verhalten der jeweils anderen Gruppe auswirken. Je mehr Endkunden auf der einen Marktseite bei einer Plattform angeschlossen ist, desto mehr Reichweite könnte die Plattform auf der anderen Seite den Geschäftskunden anbieten. Diese reichweitenbezogene Werbemöglichkeit wird dabei häufig gegenüber dem Plattformanbieter vergütet. Macht sich der Plattformbetreiber aber diese indirekten Netzwerkeffekte in einem zusammenhängenden Geschäftsmodell zunutze, kann er auch seine Kosten

[13] *Monopolkommission*, Sondergutachten 68, S. 44.

[14] *Kühling/Schall*, CR 2015, S. 641 (647).

[15] *Schumacher*, K&R 2015, S. 771 (775).

entsprechend verteilen.[16] Statt also gegenüber jedem einzelnen Teilnehmer der Plattform einen ausgerechneten positiven Geldbetrag zu verlangen, kann der Plattformbetreiber die Kostenlast einseitig auf eine Seite verlagern und nur von einer Nutzergruppe ein preisliches Entgelt verlangen, während er den Preis und damit das Entgelt auf der anderen Seite auf null rabattiert. Dieser auf null rabattierte Preis ist jedoch nach wie vor ein Preis, der die Entgeltlichkeit im Zusammenhang mit einer kommerziellen Diensteerbringung nicht ausschließt.[17]

2.2 Betrachtungsweisen eines Dienstes

Der Begriff „Dienst" im Sinne des § 3 Nr. 24 TKG wird unterschiedlich ausgelegt. Einerseits wird argumentiert, es könnten bereits nur diejenigen Bestandteile eines Angebots hierunter fallen, die gerade in der Signalübertragung bestehen. Dem liegt der Ansatz zugrunde, dass ansonsten eine übermäßige Regulierung auch von Angeboten erfolge, die gerade keine Signalübertragung darstellen. Eine isolierte Betrachtung entspricht allerdings nicht dem auch an der Sicherstellung einer effektiven Erfüllung öffentlich-rechtlicher und allgemeiner Aufgaben orientierten Gesetzeszweck des TKG. Die Aufspaltung eines Angebots in einen Teil, der in der mindestens überwiegenden Übertragung von Signalen besteht, und einen anderen Teil, bei dem dies nicht vorliegt scheidet aus drei weiteren Gründen aus. Erstens würde dies zu einem Zirkelschluss führen, bei dem die Definition des in der überwiegenden Signalübertragung bestehenden Dienstes von der vorherigen Abgrenzung von nicht in der überwiegenden Übertragung von Signalen bestehenden Diensten abhängt. Zweitens würde eine restriktive Auslegung wiederum dazu führen, dass allein die privatrechtliche Gestaltung allein durch den Anbieter ohne weitere Umstände über die Beantwortung dieser Frage führen würde. Drittens und hieraus folgend würde die dem TKG immanente Marktorientierung des TKG außer Acht gelassen. Wenn sich aber die Regulierungsziele für den Telekommunikationsbereich an Wettbewerb und dem Markt orientieren, dann muss dies auch für die Definition der sachlich betroffenen Dienste gelten. Dies bedeutet, dass als Dienst das Angebot angesehen kann, das für sich auf einem tatsächlichen oder potenziellen Markt angeboten oder nachgefragt wird. Es kommt also nicht auf die logisch abgrenzbare Übertra-

[16] *Schumacher*, K&R 2016, S. 771 (775); *Telle*, K&R 2016, S. 166 (167); kritisch dazu *Grünwald/Nüßing*, MMR 2016, S. 91 (93).

[17] *Kühling/Schall/Ruechardt*, CRi 2016, S. 134 (135f.); *Kühling/Schall*, CR 2016, S. 185 (196); *Kühling/Schall*, CR 2015, S. 641 (648); kritisch dazu *Schuster*, CR 2016, S. 173 (182 f.)

gungsleistung an, sondern auf die potenzielle Marktgängigkeit eines selbstständigen Angebots.[18]

2.3 Mindestens überwiegende Signalübertragung

Die wohl umstrittenste und für das geltende Recht noch nicht abschließend geklärte Frage ist an dieser Stelle jedoch, unter welchen Umständen bei IP-gestützten Diensten eine wenigstens überwiegende Signalübertragung vorliegt.

2.3.1 Verantwortlichkeit gegenüber den Nutzern

Auf der einen Seite wird darauf abgestellt, ob der Anbieter eine ausreichende Verantwortung über die Leistung gegenüber dem Endkunden hat. Dies ist jedenfalls für den sogenannten Reseller anerkannt, also wenn ein Unternehmen zwar selbst über keine Telekommunikationsinfrastruktur verfügt und auch selbst keine Signale überträgt, jedoch Telekommunikationsvorleistungen von Netzbetreibern oder Telekommunikationsdienstanbietern einkauft.[19] In diesem Fall habe der Reseller eine hinreichende Möglichkeit, auf den Lieferanten der Vorleistung einzuwirken und dadurch den eigentlichen Vorgang Signalübertragung jedenfalls rechtlich zu steuern.[20]

Dieser Ansatz ließe sich zwar grundsätzlich auch auf OTT-Anbieter übertragen. Denn ebenso wie beim Reselling werden bei diesen Angeboten fremde Übertragungsleistungen ausgenutzt, die sich das Unternehmen zurechnen lassen muss.[21] Gestützt wird dies durch eine Entscheidung des EuGH aus dem Jahr 2014, mit der das Gericht die Diensteigenschaft annahm, indem ein Unternehmen neben den Rundfunk- und Fernsehprogrammen auch den Transport dieser Inhalte bei anderen Unternehmen als Vorleistung einkaufe, weil es gegenüber seinen Endkunden für die Signalübertragung verantwortlich sei.[22] Hier tritt dann jedoch der Umstand hinzu, dass diese Unternehmen nicht nur keine tatsächliche sondern zusätzlich auch keine rechtliche Kontrolle über den Signalübertragungsvorgang haben, weshalb die Signalübertragung ausgeschlossen werden könne.[23]

---

[18] So auch VG Köln, Urt. v. 11. November 2015 – 21 K 450/15, CR 2016, 131; *Kühling/Schall*, CR 2016, S. 185 (189); *Kühling/Schall*, CR 2015, S. 641 (646).

[19] *Kühling/Schall*, CR 2015, S. 641 (650); Heun, CR 2008, S. 79 (80).

[20] *Gersdorf*, K&R 2016, S. 91 (96).

[21] *Kühling/Schall*, CR 2015, S. 641 (651).

[22] EuGH, 30. April 2014 – C-475/12, MMR 2015, 339 = K&R 2014, 513 - UPC DTH; *Kühling/Schall*, CR 2015, S. 641 (651); *Kühling/Schall*, CR 2016, S. 185 (186).

[23] *Gersdorf*, K&R 2016, S. 91 (97); *Schuster*, CR 2016, S. 173 (179).

Dies würde die Argumentation unterstützen, dass die wesentliche Leistung bei den meisten OTT-Angeboten darin besteht, mit Kommunikationsvorgängen zusammenhängende IP-Pakete zu verschlüsseln, sodass sie über das Internet den richtigen Weg finden.[24] Die Daten-Pakete werden hierbei aufgrund des standardisierten Internet-Protokolls übertragen, auf das der Anbieter jedoch weder tatsächlichen noch rechtlichen Einfluss habe.[25]

2.3.2 Funktional-wertende Betrachtung

Das VG Köln hatte in einer ersten verwaltungsgerichtlichen Entscheidung über die Einordnung eines OTT-Angebots als Telekommunikationsdienst, der einer Meldepflicht nach § 6 Abs. 1 TKG unterliegt, diese Frage positiv beantwortet und einen entsprechenden Verwaltungsakt der Bundesnetzagentur, mit der diese den Google-Dienst Gmail zur Abgabe einer entsprechenden Meldung verpflichtete, für rechtmäßig erklärt.[26] Dabei entschied die Kammer, dass die Einordnung als Dienst, der überwiegend in der Signalübertragung bestehe, sich nach einer auf den gesamten Dienst bezogenen richte, die sowohl die Nutzer- als auch die Anbietersicht sowie die gesetzgeberischen Intentionen in den Blick zu nehmen habe. Für den Nutzer stehen demnach nicht die inhaltlichen Komponenten im Vordergrund seines Interesses, sondern die raumüberwindende Kommunikation mit anderen Nutzern. Ebenso sprächen für eine Einordnung dieses Angebots als Telekommunikationsdienst die Regulierungsziele der Wahrung der Nutzer- und Verbraucherinteressen, der Sicherstellung eines chancengleichen Wettbewerbs sowie die Wahrung der Technologieneutralität nach § 2 Abs. 2 TKG.

2.3.3 Server-basierter Datenaustausch als Vorleistung

Schließlich ließe sich argumentieren, dass OTT-Angebote zwar keine rechtliche Funktionsherrschaft über die von Dritten bezogenen Vorleistungen haben, sondern nur faktisch ihre Dienste über die von Dritten aufgrund nicht unmittelbar wirkender Vereinbarungen vorgenommenen Übertragungsleistungen erbringen. Jedoch könnte OTT-Anbietern diese Internet-Konnektivität einerseits dadurch zuzurechnen sein, dass sie sich diese faktisch für ihre Zwecke zu eigen machen.[27] Weiterhin könnte die-

[24] EU-Kommission, Stellungnahme an das VG Köln vom 13.2.2014, wiedergegeben in der Entscheidung des VG Köln, Urt. v. 11. November 2015 – 21 K 450/15, CR 2016, 131 = K&R 2016, 141; *Schneider*, ZD 2014, S. 231 (236).

[25] *Schuster*, CR 2016, S. 173 (179 f.).

[26] VG Köln, Urt. v. 11. November 2015 – 21 K 450/15, CR 2016, 131 = K&R 2016, 141; mit Anmerkung von *Telle*, K&R 2016, S. 166 (167).

[27] *Kühling/Schall*, CR 2015, S. 641 (651).

ses faktische Zueigenmachen dem Unternehmen als Vorleistung zuzurechnen sein, wenn sie aufgrund der konkreten Ausgestaltung ihres Angebots den Übertragungsvorgang überhaupt erst initialisieren.

Maßgeblich ist für diese Zurechnung die Entscheidung des Dienstanbieters, welche Daten zwischen den Kommunikationsteilnehmern ausgetauscht werden, was regelmäßig der Fall bei einem Mail-Server mit einer Verzeichnisfunktion sein dürfte, über den statische Nutzerkennungen automatisch den jeweils zugeteilten dynamischen IP-Adressen der Nutzer-Anschlüsse zugewiesen werden.[28] Diese Entscheidung erfolgt regelmäßig über eine zentrale Server-Infrastruktur, die dann technologieneutral als Telekommunikationsvorleistung in einem Telekommunikationsnetz im Sinne des § 3 Nr. 27 TKG anzusehen ist, da mit ihr Telekommunikationsvorgänge selbstständig hergestellt werden können. Betreibt ein Unternehmen jedoch die Serverleistungen selbst, so hat es die erforderliche hinreichende tatsächliche und rechtliche Funktionsherrschaft auch über den Kommunikationsvorgang.[29]

Entscheidend für die Einordnung als Telekommunikationsdienst ist hiernach also allein, ob der OTT-Anbieter im Zusammenhang mit der IP-Konnektivität das Ob und Wie der Datenübermittlung entscheiden und steuern kann.[30] Dies wird bei reinen P2P-Modellen nicht zutreffen, da der eigentliche Übertragungsvorgang hier allein von dem Endkunden veranlasst und über Telekommunikationsnetze realisiert wird, an denen der OTT-Anbieter weder beteiligt ist noch in sonstiger Weise Einfluss nehmen kann.[31] Anders dürfte dies also bei einer Client-Server-Infrastruktur sein, wenn der Betrieb eines Servers, der über eine Verzeichnisfunktion die für die Internetübertragung erforderliche Zuordnung der statischen Nutzerkennungen zu den jeweiligen IP-Adressen ermöglicht, als Vorleistung und damit Grundlage der Erbringung der Kommunikationsdienste dient.[32]

---

[28] *Kühling/Schall*, CR 2016, S. 185 (186); *Kühling/Schall*, CR 2015, S. 641 (651); *Schumacher*, K&R 2015, S. 771 (774); *Telle*, K&R 2016, S. 166 (167).

[29] So bereits: *Kühling/Schall*, CR 2015, S. 641 (651).

[30] *Kühling/Schall/Ruechardt*, CRi 2016, S. 134 (138).

[31] *Grünwald/Nüßing*, MMR 2016, S. 91 (94); *Schumacher*, K&R 2015, S. 771 (773); *Schneider*, ZD 2014, S. 231 (236).

[32] *Kühling/Schall*, CR 2016, S. 185 (192); *Grünwald/Nüßing*, MMR 2016, S. 91 (95); *Schumacher*, K&R 2015, S. 771 (773); kritisch dazu: *Schuster*, CR 2016, S. 173 (177).

3 OTT-Dienste als elektronischer Kommunikationsdienst im EKEK-Entwurf

Die gegenwärtigen Unsicherheiten bei der Anwendung bisheriger regulatorischer Konzepte und Vorschriften auf neu auftretende Geschäftsmodelle haben den europäischen Gesetzgeber veranlasst, den Rechtsrahmen für elektronische Kommunikation weitreichend zu überarbeiten. Dieses Vorhaben steht im Zusammenhang mit der Strategie der EU-Kommission zur Schaffung eines digitalen Binnenmarktes.[33] Ein Teil dieses Reformvorhabens soll eine Richtlinie mit dem Namen „Europäischer Kodex für die Elektronische Kommunikation“ (EKEK-Entwurf) sein, mit der mehrere der bisherigen für das Telekommunikationsrecht geltenden Richtlinien in einem gemeinsamen Werk zusammengefasst und überarbeitet werden sollen. Dieser Entwurf sieht unter anderem vor, den als Anknüpfungspunkt für regulatorische Maßnahmen wesentlichen Begriff des elektronischen Kommunikationsdienstes zu erweitern, um gegebenenfalls auch OTT-Anbieter einer sektorspezifischen Regulierung zu unterwerfen.[34]

3.1 Erweiterung des Anwendungsbereichs

Der EKEK-Entwurf sieht in Art. 2 Nr. 4 eine Erweiterung des Begriffs elektronischer Kommunikationsdienst vor. Demnach soll es sich weiterhin um gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste handeln, die sich in drei wesentliche Dienstekategorien aufgliedern. Zum einen gehört hierzu der bereits bekannte Dienst, der ganz oder überwiegend in der Übertragung von Diensten besteht. Als positive Beispiele nennt die Definition hier bereits für M2M-Kommunikation oder Rundfunk genutzte Übertragungsdienste. Daneben tritt zum einen der Internetzugangsdienst im Sinne des Art. 2 Abs. 2 Nr. 2 des Telekom-Binnenmarkt-Verordnung, also ein öffentlich zugänglicher elektronischer Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet. Zum anderen soll als neu geschaffene Dienstkategorie der interpersonelle Kommunikationsdienst als elektronischer Kommunikationsdienst im Sinne des Art. 2 Nr. 4 EKEK-Entwurf anzusehen sein. Ausgenommen sind auch weiterhin Dienste, die lediglich in dem Angebot von Inhalten über elektronische Kommunikationsnetze und –dienste oder in einer redaktionellen Kontrolle über diese Inhalte bestehen.

[33] Scherer, MMR 2016, S. 713 (713).

[34] Scherer/Heinickel, MMR 2017, S. 71 (71); Scherer, MMR 2016, S. 713 (713).

Mit der Definition des interpersonellen Kommunikationsdienstes in Art. 2 Nr. 5 EKEK-Entwurf wird bezweckt, zukünftig auch OTT-Anbieter einer sektorspezifischen Regulierung zu unterwerfen, wenn sie zu herkömmlichen Telekommunikationsdiensten funktional äquivalente Leistungen anbieten.[35] In diesem Fall soll die Bestimmung nicht mehr nur durch das technisch geprägte Kriterium einer mindestens überwiegenden Signalübertragung erfolgen. Stattdessen sollen auch Dienste erfasst werden, die einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl an Personen ermöglichen, wobei die Empfänger von den die Kommunikation veranlassenden oder daran beteiligten Personen bestimmt werden. Nicht hierzu sollen aber wiederum Dienste zählen, bei denen die interpersonelle und interaktive Kommunikation untrennbar mit einem anderen Dienst verbunden ist und lediglich eine damit verbundene untergeordnete Nebenfunktion ermöglicht. Der Entwurf spricht hierzu den Kommunikationskanal in einem Online-Spiel als Beispiel an.[36]

Weiterhin soll es für die neue Dienstekategorie des interpersonellen Kommunikationsdienstes zwei Unterkategorien geben, nämlich einerseits den nummerngebundenen interpersonellen Kommunikationsdienst (Art. 2 Nr. 6 EKEK-Entwurf) und andererseits den nummernunabhängigen interpersonellen Kommunikationsdienst (Art. 2 Nr. 7 EKEK-Entwurf). Maßgebliches Kriterium ist hierbei, ob der interpersonelle Kommunikationsdienst mittels einer zugeteilten Nummerierungsressource oder über Nummern aus Telefonnummernplänen an das öffentliche Fernsprechnetz angebunden ist.

3.2 Kritikpunkte und Praxisfolgen

Der EKEK-Entwurf sieht keine Klarstellung vor, was als mindestens überwiegende Signalübertragung anzusehen sein kann. Die von dem EKEK-Entwurf im 15. Erwägungsgrund angesprochenen Unklarheiten

[35] EG 15 EKEK.Entwurf: „[…] Um einen wirksamen und gleichwertigen Schutz der Endnutzer bei der Nutzung von in der Funktionsweise gleichwertigen Diensten zu gewährleisten, sollte eine zukunftsorientierte Definition von elektronischen Kommunikationsdiensten nicht allein auf technischen Parametern fußen, sondern eher auf einem funktionalen Ansatz aufbauen. Der Umfang der erforderlichen Regulierung sollte angemessen sein, um die im öffentlichen Interesse liegenden Ziele zu erreichen. Obwohl „Signalübertragung" ein wichtiger Parameter für die Bestimmung der unter diese Richtlinie fallenden Dienste bleibt, sollte die Begriffsbestimmung auch andere Dienste erfassen, die Kommunikation ermöglichen. Aus der Sicht des Endnutzers spielt es keine Rolle, ob ein Anbieter die Signale selbst überträgt oder ob die Kommunikation über einen Internet-zugangsdienst übermittelt wird. […]"; *Scherer/Heinickel*, MMR 2017, S. 71 (71); *Scherer/Heckmann/Heinickel/Kiparksi/Ufer*, CR 2017, S. 197 (198).

[36] EG 17 EKEK-Entwurf.

sollen scheinbar allein durch die Erweiterung der Dienstekategorien beseitigt werden. Damit bleibt es bei der bestehenden Rechtsunsicherheit, bis der EuGH hier eine klärende Auslegung vornimmt.

Teilweise wird kritisiert, die Differenzierung zwischen nummerngebunden und nummernunabhängigen interpersonellen Kommunikationsdiensten sei nicht sachgerecht, da es sich um eine rein technische Abgrenzung handele und eine möglicherweise aus Sicht des Endnutzers bestehende funktionale Gleichwertigkeit unberücksichtigt bleibe.[37] Allerdings begründet die Kommission diese Unterscheidung damit, dass nummerngebundene Dienste in besonderer Weise eine öffentliche Ressource nutzen und sich damit an einem öffentlich gesicherten interoperablen Ökosystem beteiligen.[38] Deshalb könnten für einige Regelungspunkte besondere Vorschriften angebracht seien, die sich dann nach dem Bezug zu dieser öffentlichen Ressource richten. Dies gelte insbesondere für die Vertragslaufzeit, Transparenz, Angaben zur Dienstqualität, Nummernübertragbarkeit unter der Leitung des aufnehmenden Anbieters, Instrumente für die Verbrauchskontrolle, Werkzeuge für den Vergleich von Entgelten und Dienstqualität oder Vorschriften im Falle von Bündelverträgen zur Vermeidung von Lock-in-Effekten. Die Inanspruchnahme nummernunabhängiger interpersoneller Kommunikationsdienste auf spezifische regulatorische Pflichten sieht der EKEK-Entwurf im Übrigen nur bei Vorliegen eines öffentlichen Interesses vor, wie dies insbesondere bei Art. 40 EKEK-Entwurf der Fall ist.[39] Daneben sieht Art. 59 Abs. 1 UAbs. 1 lit. c) EKEK-Entwurf die Möglichkeit von Interoperabilitätsverpflichtungen für nummernunabhängige interpersonelle Kommunikationsdienste vor. Dies soll insbesondere in Betracht kommen, wenn die durchgehende Konnektivität zwischen Endnutzern wegen mangelnder Interoperabilität zwischen interpersonellen Kommunikationsdiensten bedroht ist.

Kritisch zu betrachten ist aber auch die in Art. 2 Nr. 4 2. HS EKEK-Entwurf erwähnte Ausnahme für Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.[40] Zum

---

[37] *Scherer/Heckmann/Heinickel/Kiparski/Ufer*, CR 2017, S. 197 (198).

[38] S. 14 Begründung EKEK-Entwurf; EG 42 EKEK-Entwurf: „Im Gegensatz zu anderen Kategorien elektronischer Kommunikationsnetze und -dienste im Sinne dieser Richtlinie profitieren nummernunabhängige interpersonelle Kommunikationsdienste nicht von der Nutzung öffentlicher Nummerierungsressourcen und sind nicht am öffentlich gesicherten interoperablen Ökosystem beteiligt. […]".

[39] S. 14 Begründung EKEK-Entwurf; *Gerpott*, K&R 2016, S. 801 (806).

[40] *Scherer/Heckmann/Heinickel/Kiparksi/Ufer*, CR 2017, S. 197 (198).

einen eröffnet diese Vorschrift Wertungsspielräume, die zu unterschiedlichen Auslegungen führen können, was wiederum zu einer Rechtsunsicherheit führen kann, die der EKEK-Entwurf gerade zu vermeiden sucht.[41] So ist – außer dem in der Begründung genannten Beispiel des Online-Spiels – nicht klar, wann eine untergeordnete Nebenfunktion vorliegt. Dies läuft auf eine ähnliche Problematik hinaus wie die Bestimmung einer mindestens überwiegenden Signalübertragung. Zum anderen ist das Verhältnis zum Merkmal der mindestens überwiegenden Signalübertragung missverständlich. Denn wenn ein Dienst überwiegend in der Übertragung von Signalen besteht, kann dies keine untergeordnete Nebenfunktion sein.

4 Zusammenfassung und Ausblick

Der Auftritt vieler OTT-Anbieter in der Telekommunikationsbranche hat zu einer Verunsicherung bei der Anwendung der geltenden Rechtsvorschriften für das Telekommunikationsrecht geführt. So ist die genaue Einordnung von OTT-Diensten bis zu einer höchstrichterlichen Klärung noch umstritten. Jedoch bedarf es aufgrund des grenzüberschreitenden Marktauftritts der OTT-Dienste und auch der fortschreitenden Internationalisierung der gesamten Branche einer europaweit geltenden Klarstellung. Der EKEK-Entwurf liefert hier keine befriedigende Lösung, sondern umgeht das Problem an mehreren Stellen. Zwar wird der Anwendungsbereich der sektorspezifischen Regulierung pragmatisch durch den neu geschaffenen Begriff der interpersonellen Kommunikationsdienste erweitert. Doch statt damit eine Problemstellung zu beseitigen, schafft der Entwurf viele neue. Innovativ sind die versteckten Reglungen hinsichtlich nummernunabhängiger interpersoneller Kommunikationsdienste. Hier bleibt abzuwarten, ob und welche konkreten Maßnahmen bei der anschließenden Umsetzung der Richtlinien-Vorgaben ergriffen werden, insbesondere im Hinblick auf mögliche Interoperabilität der OTT-Dienste untereinander.

[41] *Scherer/Heinickel*, MMR 2017, S. 71 (72); *Scherer/Heckmann/Heinickel/Kiparksi/Ufer*, CR 2017, S. 197 (198).

LITERATUR

Gerpott, Torsten J.: Vorschlag der Kommission zur Weiterentwicklung des europäischen Rechtsrahmens für den Telekommunikationssektor, K&R 2016, S. 801-808.

Gersdorf, Hubertus: Telekommunikationsrechtliche Einordnung von OTT-Diensten am Beispiel von Gmail. Rechtsgutachten im Auftrag der Google Inc., K&R 2016, S. 91-101.

Grünwald, Andreas/Nüßing, Christoph: Kommunikation over the Top. Regulierung für Skype, WhatsApp oder Gmail?, MMR 2016, S. 91-97

Kühling, Jürgen/Schall, Tobias: WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts. „Level playing field" de lege lata oder de lege ferenda?, CR 2015, S. 641-655.

Kühling, Jürgen/Schall, Tobias: E-Mail-Dienste sind Telekommunikationsdienste i.S.d. § 3 Nr. 24 TKG. Warum OTT-Kommunikationsdienste sehr wohl TK-Dienste sein können – zugleich Anmerkung zum Gmail-Urteil des VG Köln (Urt. V. 11.11.2015 – Az .21 K 450/15, CR 2016, 131) und Erwiderung auf die Aufsätze von Gersdorf, K&R 2016, 91 und Schuster, CR 2016, 173, CR 2016, S. 185-198.

Kühling, Jürgen/Schall, Tobias/Ruechardt, Corinne: Are Gmail, WhatsApp, and Skype "Electronic Communications Services" within the Meaning of the Framework Directive?. The State of the Debate about the Regulatory Future of OTT Communications Services, CRi 2016, S. 134-140.

Scherer, Joachim: Editorial: Ein europäischer Kodex für die Gigabit-Gesellschaft, MMR 2016, S. 713-714.

Scherer, Joachim/Heinickel, Caroline: Ein Kodex für den digitalen Binnenmarkt. Vorschlag der EU-Kommission für eine Reform des Rechts der elektronischen Kommunikation, MMR 2017, S. 71-77.

Scherer, Joachim/Heckmann, Dirk/Heinickel, Caroline/Kiparski, Gerd/Ufer, Frederic: Stellungnahme der DGRI zum Vorschlag der Europäischen Kommission für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation (COM[2016]590 final), CR 2017, S. 197-202.

Schneider, Mathias: WhatsApp & Co. – Dilemma um anwendbare Datenschutzregeln. Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZD 2014, S. 231-237.

Schumacher, Pascal: OTT-Dienste und Telekommunikationsrecht. Einordnung der neuen Dienste im Kontext der TK-Regulierung, K&R 2015, S. 771-776.

Schuster, Fabian: E-Mail-Dienste als Telekommunikationsdienste?. Warum OTT-Dienste keine TK-Dienste sein können – zugleich Erwiderung auf Kühling/Schall, CR 2015, 641 und VG Köln zu „Google Mail", CR 2016, S. 173-185.

Ufer, Frederic: OTT-Dienste und klassische TK-Anbieter, in: Die Macht der Plattformen. Tagungsband zur Telemedicus Sommerkonferenz 2016, Telemedicus-Schriftenreihe Band 3, Berlin 2017, S. 76-83.

WLAN UND STÖRERHAFTUNG – AKTUELLE ENTWICKLUNGEN

Rechtsanwältin Kathrin Schürmann

Schürmann Wolschendorf Dreyer Rechtsanwälte
schuermann@swd-rechtsanwaelte.de

Zusammenfassung

Grundsätzlich ist es Ziel der europäischen und deutschen Politik den Ausbau öffentlicher WLAN-Netze zu fördern. In Deutschland steht diesem Ziel das Haftungsmodell der Störerhaftung entgegen. Nach diesem Prinzip haftet auch derjenige, der ohne Täter oder Teilnehmer zu sein, in irgendeiner Form an einer Verletzung von Rechtspositionen beteiligt war. Demnach haften nach der deutschen Rechtsprechung auch Anbieter von WLAN-Netzen (z.B. in Restaurants oder Hotels) auf Unterlassung und Erstattung von Abmahnkosten, sofern der Zugang zum Netz nicht entsprechend gesichert ist, was dem erklärten Ziel, den Ausbau öffentlicher WLAN-Netze zu fördern, diametral wiederspricht. Infolge der nationalen und europäischen Rechtsprechung lassen jedoch aktuelle legislative Entwürfe eine Abkehr vom Modell der Störerhaftung erkennen.

1 Digitalisierung des Öffentlichen Raumes und die Haftung des WLAN-Anbieters

Mit der Digitalisierung des öffentlichen Raumes geht vor allem auch die Verbreitung öffentlicher WLAN-Netze einher. Zunehmend bieten Cafés, Restaurants, Einkaufszentren und Bars ihren Gästen offene WLAN-Netze an, die ohne Registrierung oder Anmeldung genutzt werden können. Auch ist es erklärtes Ziel der Politik, ein frei zugängliches WLAN-Netz im öffentlichen Raum „für jedermann“ anzubieten.

Mit dieser Digitalisierung des öffentlichen Raumes und der damit einhergehenden Möglichkeit der freien und anonymen Zugänglichkeit des Internets bietet sich neben vielen Vorteilen jedoch zugleich die Möglichkeit der Ausbreitung rechtswidriger Handlungen in „fremder Sphäre“, also im offenen WLAN-Netz eines Anbieters. Es stellt sich daher die in Deutschland viel diskutierte Frage, ob Anbieter von offenen WLAN-Netzen für Rechtsverletzungen durch Nutzer haften müssen und wenn ja, in welchem Umfang.

Viel Diskutiert sind hier vor allem Verletzungen urheberrechtlich geschützter Rechtspositionen, beispielsweise durch den illegalen Up- und Download von Audio- und Videodateien auf sog. „peer-to-peer“-Plattformen (Filesharing). Das Sharing entsprechender Datenpakete (Musik, Video) erfolgt dabei über eine Client-Software. Bei der Client-Software handelt es sich um Computerprogramme, mit denen die Inhaber einen

Netzwerk-Zusammenschluss mit dem Ziel virtueller (in der Regel kostenfreier) Tauschbörsen (z.B. eMule) bewirken, wodurch jedes Mitglied einen Zugang zu allen Daten innerhalb der Plattform erhält. Insbesondere erweitern sich die Zugriffsmöglichkeiten aller User während eines einzelnen Up- und Downloadvorgangs erheblich, da allen Usern während der Dauer des Up-/Downloads zusätzlich dieselbe Zugriffsmöglichkeit wie dem aktiv up-/downloadenden zusteht.[1] Insbesondere die rechtswidrige Vervielfältigung sowie das öffentliche Zugänglichmachen begründen dabei eine Urheberrechtsverletzung und Unterlassungs- sowie gegebenenfalls Schadensersatzpflichten nach § 97 Abs. 1 und 2 UrhG, nicht jedoch der einzelne Download als solcher.[2]

Während die urheberrechtliche Vorwerfbarkeit für Up- und Downloads mittels Client-Software bezüglich des Nutzers jeweils unproblematisch erscheint, stellt sich aus urheberrechtlich determinierter Haftungsperspektive die Frage nach der Vorwerfbarkeit gegenüber dem Inhabers eines WLAN-Routers, der sein WLAN nicht ausreichend durch ein Passwort schützt und somit ein „offenes WLAN" ermöglicht, welches sodann von Dritten – ohne Kenntnis – des WLAN-Anbieters zum Zugang zu solchen Tauschbörsen genutzt wird.

Es geht dabei um die Frage, inwieweit ein Anbieter eines solchen WLAN-Netzwerkes auf Unterlassung und Schadensersatz haftet. Die Diskussion bezieht sich dabei vor allem auf private und nebenbetriebliche WLAN-Anbieter, da für Access-, Cache- und Hostingprovider die Haftungsprivilegien in §§ 8-10 TMG gelten, welche Art. 12-14 der E-Commerce-Richtlinie (2003/31/EG) umsetzen.

Die grundsätzliche Linie der BGH-Rechtsprechung ging dabei bis zur Entscheidung „Sommer unseres Lebens" im Jahr 2010, von der aus § 97 UrhG abgeleiteten Unterlassungspflicht des WLAN-Anbieters nach den Grundsätzen der Störerhaftung aus. Die Literatur begründete ebenfalls mit den Grundsätzen der Störerhaftung zum Teil sogar eine über die reine Unterlassungspflicht hinausgehende Schadensersatzpflicht.[3] Von der BGH-Entscheidung „Sommer unseres Lebens" erhofften sich Wissenschaft und Praxis Klärung in Bezug auf mögliche Haftungskriterien und Umfänge.

---

1 Vgl. *Köster/Jürgens*, MMR 2002, S. 420 (421 f.); *Popescu*, VuR 2011, S. 327 (330ff).

2 Vgl. *Spindler/Schuster*, Recht der elektronischen Medien, § 97 UrhG, Rn. 1 ff.

3 Vgl. *Gierke*, WRP 1997, S. 892 ff.

1.1 Die BGH-ENTSCHEIDUNG: „SOMMER UNSERES LEBENS“

Sachverhalt: Der Inhaber eines privaten WLAN-Routers befand sich im Urlaub, als ein unbekannter Dritter über dessen WLAN-Zugang den Musiktitel „Sommer unseres Lebens“ auf der Tauschplattform „eMule“ zunächst hoch lud und sodann zum Download anbot. Der WLAN-Router war nur mit dem werkseitig festgelegten Standardsicherheitspasswort geschützt, das zwar der Änderung durch den Käufer des Routers offenstand, allerdings hatte der private WLAN-Inhaber in diesem Fall von der Möglichkeit keinen Gebrauch gemacht. Die Klägerin war die Rechteinhaberin des Musiktitels „Sommer unseres Lebens“ und begehrte vom Eigentümer des Routers Unterlassung, Erstattung der mit der Unterlassung verbundenen Abmahnkosten und Schadensersatz gemäß § 97 UrhG.

Enscheidung des BGH: Der Beklagte wurde nach den Grundsätzen der Störerhaftung auf Unterlassung und Erstattung der Abmahnkosten in Anspruch genommen. Dazu führte der BGH aus:

„Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt (…) Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers nach der Rechtsprechung des Senats die Verletzung von Prüfpflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist.[4]*“*

Da es nicht völlig außerhalb der Lebenswahrscheinlichkeit liege, dass Dritte private WLAN-Netze für Up-/Downloads von Musik nutzten, sei es dem Inhaber solcher Netze zumutbar, marktübliche Sicherungsmaßnahmen (wie die Festlegung eines eigenen sicheren und ausreichend langen Passworts) vorzunehmen, was der Beklagte vorliegend versäumt habe. Daher hafte er nach den Grundsätzen der Störerhaftung auf Unterlassung und Erstattung der Abmahnkosten.

Trotz dieser Grundsätze kommt nach dem BGH jedoch eine Schadensersatzhaftung mangels Beteiligung als Täter oder Teilnehmer (, die immer Vorsatz voraussetzen) einer Urheberrechtsverletzung nicht in Betracht.

[4] BGH, Urt. v. 12. Mai 2010 - I ZR 121/08, Sommer unseres Lebens.

1.2 STÖRERHAFTUNG VS. AUSBAU ÖFFENTLICHER WLAN-NETZE

1.2.1 DIE GRUNDSÄTZE DER STÖRERHAFTUNG

Als Störerhaftung bezeichnet man im deutschen Recht die Verantwortlichkeit eines in irgendeiner Art und Weise willentlich und adäquat kausal an der Verletzung eines geschützten Gutes Beitragenden, der – ohne Täter oder Teilnehmer zu sein – als sogenannter Störer auf Unterlassung der Rechtsverletzung in Anspruch genommen werden kann. Rechtliche Grundlage der Störerhaftung ist § 1004 Abs.1 BGB.

In analoger Anwendung dieser Norm entwickelte die Rechtsprechung die Haftung von „Störern", die auf andere/jede erdenkliche Art und Weise Rechtspositionen (also nicht nur das Eigentum, sondern alle Rechtspositionen, z.B. aus dem Persönlichkeits- und Urheberrecht abgeleitete Rechtspositionen) des Rechteinhabers beeinträchtigen. In Weiterentwicklung dieser Rechtsprechung entstanden viele Spezialgesetze in den jeweiligen Rechtsgebieten, die dieselben Abwehransprüche beinhalten, die in § 1004 Abs.1 BGB normiert sind.[5] Die Definition des Begriffs „Störer" ist dabei nicht eindeutig geklärt.

Grundsätzlich wird nach der Art der Störung zwischen Handlungs- und Zustandsstörern differenziert. Handlungsstörer ist dabei grundsätzlich (wer unmittelbar oder mittelbar) durch Tun oder Unterlassen schädigend auf eine fremde Rechtsposition (primär: Sache) einwirkt. Zustandsstörer ist demgegenüber der Eigentümer einer Rechtsposition (primär: Sache) von der (unmittelbar oder mittelbar) eine schädigende Handlung ausgeht.[6] Bezüglich der Störerhaftung und Filesharing-Plattformen liegt eine Konstellation der mittelbaren Zustandsstörung vor, die der spezialgesetzlichen Regelung des § 97 UrhG sowie den §§ 7, 8 TMG unterliegt.

Während diese Definition Elemente einer reinen Kausalhaftung zu beinhalten scheint, wird die reine Kausalhaftung im Urheberrecht durch das Kriterium der „Prüfpflicht" (so auch in der Entscheidung „Sommer unseres Lebens", fehlender Passwortschutz) eingeschränkt, wobei diese Prüfpflicht auch in sonstigen Fällen des Immaterialgüterrechts eingreift.[7]

---

[5] Vgl. *Ort*, Störerhaftung auf elektronischen Marktplätzen, 2009, S. 22 ff.; *Freytag*, Haftung im Netz, 1999, S. 60.

[6] Vgl. *Baldus*, in: MüKoBGB, § 1004 Rn. 156-160; *Bassenge*, in: Palandt, BGB, § 1004 R.15-25.

[7] Vgl. *Popescu*, VuR 2011, S. 327 (328); zur Rechtsprechung siehe BGH, Urt. v. 15. Oktober 1998 - I ZR 120/96, NJW 1999, 1960 – Möbelklassiker; BGH, Urt. v. 14. Juni 2006 - I ZR 249/03, GRUR 2006, 957 – Stadt Geldern.

1.2.2 ÄNDERUNG DES TMG UND KONTROVERSEN IN DER LITERATUR

Ziel der deutschen Politik ist es jedoch seit vielen Jahren, den Ausbau öffentlicher WLAN-Netze zu beschleunigen. Dem steht die BGH-Rechtsprechung jedoch entgegen, da das Haftungsrisiko für Betreiber öffentlicher WLAN-Netze ein Hemmnis darstellt. Nur durch eine starke Authentifizierung und Registrierung der User könnte dieses Risiko nach der Rechtsprechung ausgeschlossen werden, was aber gerade bei dem Angebot im öffentlichen Raum ein hohes Hemmnis für die User und erheblichen Aufwand für die Anbieter der öffentlichen WLAN-Hotspots darstellt. Dies wird auch als einer der Hauptgründe angesehen, warum in Deutschland die Verbreitung von öffentlichen WLAN-Netzen gegenüber anderen europäischen Ländern hinterherhinkt.

Um dieses Hemmnis zu beseitigen ergänzte der deutsche Gesetzgeber daher mit dem „Zweiten Gesetz zur Änderung des Telemediengesetztes“ vom 21.6.2016 § 8 TMG um einen Absatz 3 mit dem Ziel der „Privilegierung von WLAN-Betreibern“. Der neue Absatz 3 ist seit dem 27.7.2016 in Kraft. Ziel war es dabei, die Haftungsprivilegien für die in § 8 Abs.1 und Abs.2 TMG genannten Access-Provider auf WLAN-Provider auszudehnen, um dadurch den Ausbau von offenen WLAN-Netzen zu fördern.[8]

Neben dem Haftungsrisiko durch Abmahnkosten- und Unterlassungsansprüche führte die Rechtsunsicherheit über die Verwirklichung einer Störung vor der Gesetzesänderung zudem zu einem erheblichen Prozessrisiko, auch diesem sollte durch die Reform des § 8 TMG begegnet werden.[9]

Bis zum 21.6.2016 lautete § 8 TMG:

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,

2. den Adressaten der übermittelten Informationen nicht ausgewählt und

3. die übermittelten Informationen nicht ausgewählt oder verändert haben

Satz 1. Findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

---

[8] Vgl. *Paal*, in: Gersdorf/Paal, Beck’scher Online-Kommentar Informations- und Medienrecht, 15. Edition, Stand: 1.2.2107, § 8 TMG Rn. 42-46.

[9] Vgl. *Paal*, in: Gersdorf/Paal, Beck’scher Online-Kommentar Informations- und Medienrecht, 15. Edition, Stand: 1.2.2107, § 8 TMG Rn. 42-46.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

Der mit der Reform vom 21.6.2016 eingefügte **neue Absatz 3** lautet:

(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

1.2.3 AUSSCHLUSS DES HAFTUNGSRISIKOS DURCH ERGÄNZUNG DES § 8 TMG?

Trotz des erklärten gesetzgeberischen Ziels der Schaffung von Rechtssicherheit blieb eine entscheidende Frage ungeklärt: Umfasst die Haftungsprivilegierung in § 8 Abs.1 TMG aufgrund des neuen Abs.3 auch Unterlassungsansprüche (und damit verbundene Abmahnkosten) und mithin eine wesentliche Konstellation der Störerhaftung?

In der Gesetzesbegründung[10] lässt sich ein entsprechender Wille zur Ausdehnung auf Unterlassungsansprüche und Abmahnkosten erkennen. Zudem wird auf die Schlussanträge von Generalanwalt Szpunar vor dem EuGH im Fall McFadden (im Detail dazu sogleich) verwiesen, nach denen Art. 8 Abs. 1 und Abs.2 TMG *„daher nicht nur der Verurteilung des Anbieters solcher Dienste zur Leistung von Schadensersatz, sondern auch seiner Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Verletzung des Urheberrechts entgegen“* stehen. Damit wären Unterlassungsansprüche gegen den WLAN-Anbieter ebenfalls ausgeschlossen.

In der Literatur wird dennoch vertreten, dass die BGH-Entscheidung „Sommer unseres Lebens“ trotz der Änderung des TMG nicht anders ausgefallen wäre, da der BGH im Allgemeinen die Ansicht vertrete, dass Unterlassungsansprüche (und damit verbundene Abmahnkosten) nicht von § 8 Abs.1, 2 TMG umfasst seien, sondern lediglich Schadensersatzansprüche. Dementsprechend komme auch eine Anwendung im Bereich WLAN/Störerhaftung nicht in Betracht. Die Gesetzesänderung, die bis zum 21.6.2016 galt, erfasste damit nur Schadensersatzansprüche und brachte für Betreiber offener WLAN-Netze nicht die erhoffte Haftungserleichterung.

Das Fehlen entsprechender Klarstellungen im Gesetzeswortlaut und die Beschränkung auf Ausführungen in der Gesetzesbegründung konnte da-

[10] BT-Drs. 18/8645, 10.

mit keine echte legislative Klarstellung bewirken, da der I. Zivilsenat des BGH (zuständig für Fragen des Urheberrechts) eine Gesetzesbegründung nur dann berücksichtigt, wenn in ihr der Zweck des Gesetzes niedergelegt ist. Alle darüberhinausgehenden Ausführungen in der Gesetzesbegründung müssen grundsätzlich im Gesetzestext Ausdruck finden, um von der Rechtsprechung berücksichtigt zu werden. Die Frage nach der Auslegung von § 8 Abs.1 TMG blieb daher ungeklärt und die bisherige Rechtsprechung des BGH wonach § 8 TMG auf die auf § 7 TMG gestützte Störerhaftung keine Anwendung findet, schien weiter fortzubestehen.[11]

Die Klärung der Frage nach einer möglichen Ausdehnung der Haftungsprivilegierung auf Unterlassungs- und Abmahnansprüche ist auch deshalb von Bedeutung, weil in der Literatur die Reichweite des § 7 TMG umstritten ist:

§ 7Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

Grundsätzlich vertritt der überwiegende Teil der Literatur, dass aus § 7 Abs. 2 S. 2 TMG folge, dass die Haftungsprivilegierungen der §§ 8-10 TMG grundsätzlich und von vornherein nicht auf Beseitigungs- und Unterlassungsansprüche anwendbar seien, sodass auch ein Ausschluss der Störerhaftung gemäß § 8 TMG nicht in Betracht kommen könne, soweit Unterlassungsansprüche betroffen seien.[12]

Dies folge aus Erwägungsgrund 46 der E-Commerce-Richtlinie, wonach der Diensteanbieter, dem rechtswidrige Taten bekannt oder bewusst werden, unverzüglich einschreiten muss, um Informationen zu entfernen oder den Zugang zu ihnen zu sperren. Der entsprechenden Aufforderung

[11] Vgl. *Paal*, in: Gersdorf/Paal, Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, Stand: 1.2.2107, § 8 TMG Rn. 42-46.

[12] Vgl. *Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, Rn. 32 f.; *Lehment*, GRUR 2005, S. 210 (210); *Schultz*, WRP 2004, S. 1347 (1350 ff.); *Pankoke*, MMR 2004, S. 689 (690); *Hoffmann*, MMR 2002, S. 284 (286).

sei der deutsche Gesetzgeber nachgekommen, indem er Art. 7 Abs. 2 S. 2 „vor die Klammer“ der §§ 8-10 gezogen habe.[13]

Demgegenüber wendet ein anderer Teil der Literatur ein, dass Erwägungsgrund 45 der E-Commerce-Richtlinie dem nationalen Gesetzgeber einen Umsetzungsspielraum bezüglich der Entfernung und Sperrung von Informationen gewährt habe und § 7 Abs. 2 S. 2 TMG daher nach den allgemeinen Auslegungsregeln auszulegen sei. Der systematische Vergleich mit § 7 Abs. 2 S. 1 zeige, dass sich Abs. 2 S. 2 nur auf konkrete Informationen bzw. deren Entfernung und Sperrung beziehe, sodass auch nur insoweit die Störerhaftung von der Haftungsprivilegierung ausgeschlossen sei, als solche konkreten Informationen betroffen sind. Für die übrigen Fälle der Störerhaftung bleibe die Haftungsprivilegierung aber möglich.[14]

Hoffnung auf Klärung möglicher Haftungsfragen brachte das EuGH-Urteil im Fall *McFadden*.

2 DAS EUGH-URTEIL MCFADDEN[15]

2.1 DER SACHVERHALT

Der Betreiber (Tobias Mc Fadden) eines IT-Geschäftes (Schwerpunkt ist der Vertrieb und die Vermietung von Licht- und Tontechnik aller Art) betrieb ein öffentliches WLAN-Netz in seinem Geschäft. Dieses war bewusst ohne Passwort gestaltet, um die Aufmerksamkeit der Kunden umliegender Geschäfte, Passanten und Kunden zu erwecken.

Ein User dieses WLANs hatte ohne Kenntnis von Mc Fadden über dessen WLAN-Netz einen urheberrechtlich geschützten Musiktitel, an dem die Sony Music Entertainment Germany GmbH die Rechte hielt, ohne Erlaubnis im Internet hoch geladen und dort über eine sogenannte „Tauschbörse“ zum Download zur Verfügung gestellt. Aufgrund dieser Rechtsverletzung wurde Mc Fadden von der Rechteinhaberin auf Unterlassung und Schadensersatz verklagt. Aufgrund der unklaren Rechtslage im Hinblick auf die auf der E-Commerce-Richtlinie basierenden Haftungsprivilegien im deutschen TMG legte das LG München I dem EuGH die Frage vor, ob die Haftungsausnahme gemäß Art. 12 Abs.1 Nr. 1 E-

[13] Vgl. *Paal*, in: Gersdorf/Paal, Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, Stand: 1.2.2017, § 7 TMG, Rn. 54-57.

[14] Vgl. *Paal*, in: Gersdorf/Paal, Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, Stand: 1.2.2017, § 7 TMG, Rn. 54-57.

[15] EuGH, Urt. v. 15. September 2016 - C-484/14, K&R 2016, 733, McFadden.

Commerce RL, die durch Art. 8 Abs. 1 S.1 TMG in das deutsche Recht umgesetzt wurde, nicht jeglicher Haftung des WLAN-Betreibers – also auch der hier gegenständlichen mittelbaren Zustandsstörerhaftung – entgegenstehe.

2.2 DIE ENTSCHEIDUNG DES EUGH

Zunächst bejahte der EuGH die Frage, ob auch nebenbetriebliche Anbieter von WLAN einen Fall des „Dienstes der Informationsgesellschaft" nach Art. 12 Abs.1 E-Commerce-RL bzw. einen Fall des „Diensteanbieters" nach § 8 Abs.1 TMG darstellen. So sei der Begriff in der Richtlinie nicht legaldefiniert. In Anlehnung an den Dienstleistungsbegriff des AEUV sei jedoch bereits dann eine Dienstleistung zu bejahen, wenn für das Betreiben eines offenen WLAN-Netzes ein im weitesten Sinne kausale Gegenleistung erfolge. Dies sei v.a. bei Verknüpfung mit Werbezwecken in jedem Fall gegeben, da diese in die Kosten der beworbenen Güter und Dienstleistungen einbezogen werden.

Daran anknüpfend stellt sich allerdings eine in der Literatur bisher kaum behandelte Frage. Gelten die Grundsätze des EuGH-Urteils Mc Fadden auch für private Inhaber von WLAN-Routern, wie es im Rahmen der Entscheidung „Sommer unseres Lebens" des BGH der Fall war?

Diese Frage lässt der EuGH offen. Zwar lässt sich die Rechtsprechung des EuGH gerade auch auf Cafés, Bars, Restaurants übertragen, da deren WLAN-Kosten im weitesten Sinne auch auf die Kosten Speisen, Getränke, Übernachtungen umgelegt werden können. Offen und damit der Ausgestaltung der nationalen Gesetzgeber überlassen bleibt aber die Ausdehnung auf Gemeinden, Idealvereine, staatliche Hochschulen und Private. Der EU fehlt für eine mögliche Gleichstellung die Gesetzgebungskompetenz. Für Deutschland könnte ein Anhaltspunkt in der Anwendbarkeit des TMG für „alle Anbieter" (§ 1 Abs. 1 S.2 TMG) gesehen werden, ob die Rechtsprechung dem folgt, bleibt abzuwarten.[16] Zudem ist nach dem EuGH-Urteil nicht erforderlich, dass zwischen WLAN-Nutzer und Inhaber des WLAN ein Vertragsverhältnis zustande komme, sodass auch insoweit die Gleichstellung von nebenbetrieblichen Anbietern mit Privaten möglich bleibt.

Zur Störerhaftung entschied der EuGH, dass die Störerhaftung von Anbietern offener (d.h. nicht passwortgeschützter) WLAN-Netzen mit der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (E-Commerce-RL) grundsätzlich vereinbar sei, soweit sie Unterlassungsan-

[16] Vgl. EuGH, Urt. v. 15. September 2016 - C-484/14, K&R 2016, 733, McFadden, mit Anm. *Weisser*, ZD 2016, S. 578 (581 ff.).

ordnungen und darauf bezogene Abmahn- und Gerichtskosten betreffe. Demgegenüber seien Schadensersatzansprüche und darauf bezogene Abmahn- und Gerichtskosten nicht mit der Richtlinie vereinbar. Zur Begründung führte der EuGH Art. 12 Abs. 1 der E-Commerce-RL an. Liegen dessen drei Voraussetzungen vor, ist die Haftung auf Schadensersatz ausgeschlossen, da aus Art. 12 die Verpflichtung des Mitgliedstaates folge sicherzustellen, dass Diensteanbieter im Falle der Erfüllung der drei Voraussetzungen des Art. 12 Abs. 1 E-Commerce-Richtlinie[17] nicht für die übermittelten Informationen (z.B Up-/Downloads) verantwortlich sein dürfen.

Eine Abwägung der betroffenen Grundrechte und Grundfreiheiten von Nutzern und WLAN-Anbietern ergebe zudem, dass eine Sicherung des WLAN mittels Passwortes auch dann verhältnismäßig sei, wenn der Nutzer für die Erlangung des Passwortes seine wahre Identität preisgeben müsse. Demgegenüber sei eine Überwachung oder sogar die Einstellung des WLAN-Betriebes unverhältnismäßig.

Bezüglich der Passwortpflicht bleibt offen, ob jeder Nutzer ein individualisiertes Passwort erhalten muss. Dafür spräche, dass nur auf diesem Wege die Zurückverfolgung von Urheberrechtsverletzungen und die damit bezweckte Abschreckung des Nutzers möglich wäre. Die individualisierte Passwortvergabe könnte wegen des erhöhten Aufwandes aber zugleich Anbieter von WLAN-Netzen gänzlich von solchen Angeboten abhalten und würde damit dem Ziel der Digitalisierung des öffentlichen Raumes wieder entgegenstehen.[18] Anknüpfend an das EuGH-Urteil stellt sich die Frage, wo Verschlüsselungspflichten und Unterlassungsansprüche im TMG zu verorten wären.

2.3 AKTUELLE ENTWICKLUNG

Im Februar 2017 wurde ein Gesetzentwurf des Bundeswirtschaftsministeriums bekannt, der die Bestrebung öffentliche WLAN-Netzte auszubauen und gleichzeitig das Urheberrecht zu schützen, miteinander vereinbaren sollte. Demgemäß soll das Prinzip der Störerhaftung abgeschafft werden.

[17] Art. 12 Abs.1 E-Commerce-RL lautet: „Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist, sofern er a) die Übermittlung nicht veranlasst b) den Adressaten der übermittelten Information nicht auswählt c) die übermittelten Informationen nicht auswählt oder verändert“.

[18] Vgl. EuGH, Urt. v. 15. September 2016 – C-484/14, K&R 2016, 733, McFadden, mit Anm. *Weisser*, ZD 2016, S. 578 (581 ff.).

Mit dem Gesetzentwurf wird das EuGH-Urteil McFadden damit letztlich in Teilen umgesetzt. Verortet wurden die Regelungen zu Unterlassungs- und Verschlüsselungspflichten jedoch nicht in § 7 Abs. 2 TMG (wie zuvor teilweise diskutiert), sondern in einer Ergänzung des § 7 TMG um die Absätze 3 und 4 sowie einer Änderung des § 8 TMG.

Mit dem Gesetzentwurf würde der Umfang der Haftungsbeschränkung für Internetzugangsanbieter klar geregelt. Darüber hinaus werden diese von einem Großteil der bisher bestehenden Kostentragungspflicht, insbesondere bei Abmahnungen, befreit. Schließlich wird klargestellt, dass WLAN-Betreiber nicht von einer Behörde verpflichtet werden dürfen, Nutzer zu registrieren, ihr WLAN nicht mehr anzubieten oder die Eingabe eines Passworts zu verlangen, obgleich dies auf freiwilliger Basis weiterhin möglich bleibt. Ebenso soll klar geregelt werden, unter welchen Bedingungen Nutzungssperren im Einzelfall möglich sind, um die Wiederholung einer konkreten Rechtsverletzung zu verhindern. Insgesamt würde der deutsche Gesetzgeber mit diesem Entwurf damit seinen ihm durch das EuGH-Urteil *McFadden* eingeräumten Gestaltungsspielraum nutzen, da der EuGH Passwörter, Unterlassungsansprüche und Abmahnkosten nur für „möglich“ und „verhältnismäßig“, nicht jedoch für verpflichtend erklärt.

Zur Umsetzung dieser Vorgaben sollen neue Absätze in §7 TMG eingeführt werden, die neuen Absätze 3 und 4 sollen lauten:

„(3) Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen aufgrund von gerichtlichen oder behördlichen Anordnungen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.“

„(4) Wurde ein Dienst der Informationsgesellschaft von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 insbesondere die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.“

Demgemäß wird § 8 TMG ergänzend wie folgt geändert:

„(1) Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche."

Folgender Absatz 4 wird zudem angefügt:

„(4) Diensteanbieter nach § 8 Absatz 3 dürfen von einer Behörde nicht verpflichtet werden, 1. vor Gewährung des Zugangs

a) die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder

b) die Eingabe eines Passworts zu verlangen oder 2. das Anbieten des Dienstes einzustellen. Davon unberührt bleiben Maßnahmen auf freiwilliger Basis."

Zulässig wären damit Sperren, z.B. bestimmter Websites und illegaler Streamingportale, nach umfangreicher Interessenabwägung. Allerdings ist hier die technische Umsetzbarkeit v.a. für Smartphone-Apps bisher noch nicht vollständig abzuschätzen. Unzulässig wären nach diesem Entwurf demgegenüber Verpflichtungen zu Unterlassung, Schadensersatzansprüchen und die Verpflichtung zur Passwort-Verschlüsselung. Die Störerhaftung wäre damit insgesamt weitestgehend abgeschafft. Letztlich wird damit das Providerprivileg für Internetanbieter auch auf private und nebengewerbliche Anbieter (Hotels etc.) übertragen.

Grundsätzlich sind aktuell keine Anhaltspunkte dafür zu erkennen, dass die Grundentscheidung des § 1 Abs.1 S.2 TMG wonach das TMG „für alle Anbieter" gilt, nicht auch für die vorgeschlagene Gesetzesreform greifen soll. Mithin würde die Freistellung von Passwort- und Unterlassungspflicht auch Private und gänzlich unkommerzielle Anbieter betreffen. Der Schutzumfang wäre damit im Vergleich zum EuGH-Urteil McFadden sogar erhöht. Fraglich bleibt lediglich die praktische Umsetzbarkeit von Sperrungen einzelner Websites durch Private.

3 FAZIT

Das deutsche Modell der Störerhaftung würde infolge des EuGH-Urteils McFadden bei Inkrafttreten des Gesetzesentwurfes der Bundesregierung abgeschafft, da der Entwurf sogar über die Urteilsgrundsätze hinausgeht. Die genaue Umsetzung dieser Abschaffung hat jedoch noch keine endgültige Gesetzesform erlangt und es bleibt abzuwarten, ob und in welchen Form letztendlich eine Gesetzesänderung umgesetzt wird. Insbesondere für Hotels und Bars wird die Abschaffung der Passwortpflicht eine Erleichterung im Umgang mit Kunden bringen. Zudem müssen Hotels, Bars

und andere nebenbetriebliche Anbieter ohne Haftungsrisiko für Urheberrechtsverletzungen durch WLAN-Nutzer nicht mehr die aufwendige Individualisierung potentieller Urheberrechtsverletzer für Regressansprüche durchführen. Der Ausbau öffentlicher WLAN-Netzte scheint damit möglich. Aktuell wird der Gesetzentwurf der Bundesregierung zwischen verschiedenen Ministerien beraten und mit Verbänden abgestimmt.

LITERATUR

Freytag, Stefan: Haftung im Netz, Verantwortlichkeit für Urheber-, Marken- und Wettbewerbsrechtsverletzungen, Schriftenreihe Information und Recht, Band 1, München 1999

Gersdorf, Hubertus/Paal, Boris (Hrsg.): Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, München, Stand: 1.2.2017.

Gierke, Cornelie: Grenzen der wettbewerbsrechtlichen Störerhaftung, WRP 1997, S. 892-896

Köster, Olivier/Jürgens, Uwe: Haftung professioneller Informationsvermittler im Internet- Eine Bestandsaufnahme nach der Novellierung der Haftungsregelungen, MMR 2002, S. 420-425

Lehment, Cornelius: Haftung von Internet-Auktionshäusern, Urteilsanmerkung zu BGH, Urteil vom 11.3.2003 – Internet-Versteigerung, GRUR 2005, S. 210-211

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 7, 7. Aufl., München 2017.

Ort, Sven: Störerhaftung auf elektronischen Marktplätzen, Weinheim und München 2009.

Palandt, Otto (Begr.): Kommentar zum Bürgerlichen Gesetzbuch, 75. Auflage, München 2016.

Pankoke, Stefan: LG München I, Urteil vom 24.6.2004 – 17 HK O 10389/04 Beeinflussung von Suchmaschinen durch fremde Kennzeichennamen in Metatags – „Impuls", MMR 2004, S. 690-692.

Popescu, Corina-Florenţa: Verschuldensunabhängige Störerhaftung für den unzureichend gesicherten WLAN-Anschluss, VuR 2011, S. 327-333.

Reinbold, Fabian: Offene WLAN-Hotspots – Union und SPD schaffen Störerhaftung ab, Spiegel Online, 11.5.2016, http://www.spiegel.de/netzwelt/netzpolitik/stoererhaftung-union-und-spd-einigen-sich-auf-wlan-gesetz-a-1091731.html, zuletzt ab gerufen am 17.4.2017.

Schultz, Dennis: Die Haftung von Internetauktionshäusern für den Vertrieb von Arzneimitteln, WRP 2004, S. 1347-1355.

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 2. Auflage, München 2009.

Tripp, Volker: Ende der WLAN-Störerhaftung, Europarecht steht echter Rechtssicherheit nicht im Weg, Digitale Gesellschaft, https://digitale gesellschaft.de/2016/05/ende-stoererhaftung-unterlassung, abgerufen am 17.4.2017.

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014.

Weisser, Ralf: EuGH – Keine Haftung des Betreibers öffentlicher WLAN-Netze – MC Fadden, ZD 2016, S. 581-583.

URHEBERVERTRAGSRECHT UND EUROPÄISCHES URHEBERRECHT

Dr. Volker Schumacher,

Fachanwalt für internationales Wirtschaftsrecht
Fachanwalt für gewerblichen Rechtsschutz
Lindenau Prior & Partner

schumacher@lindenau-prior.de

Zusammenfassung

In der digitalen Wissensgesellschaft sind das Urheber- und das IT-Recht von zentraler Bedeutung. Aus diesen wichtigen Rechtsbereichen soll der Artikel einen Überblick über das Softwarevertragsrecht (hierzu 1.) einschließlich des Themas „Open Source Lizenzen“ (hierzu 2.) geben sowie die neuere Entwicklungen im europäischen Urheberrecht (hierzu 3.) kurz skizzieren.

1 Softwarevertragsrecht

1.1 Grundsätze

In der täglichen Praxis des IT-Rechts nimmt das Softwarevertragsrecht einen großen Teil ein. Dabei ist insbesondere eines interessant: Die Frage nach dem Vertragstyp ist bei IT-Leistungen die entscheidende Weiche für die Verhandlung und Prüfung von IT-Verträgen. Das hat mehrere Gründe.

1.1.1 Was gilt, wenn nichts geregelt ist?

Für den Berater ist es unerlässlich, zu wissen, um was für einen Vertragstyp es sich bei den streitigen Leistungen handelt. Denn: Nur so lässt sich ermitteln, was für die Parteien gilt, wenn sie einen Punkt im Vertrag nicht geregelt haben.

Zwar versuchen die Parteien in komplexen IT-Projekten, möglichst jeden Punkt vertraglich abzubilden. Gleichwohl zeigt die Praxis immer wieder, dass die Probleme während eines IT-Projekts oft in anderer Form auftauchen, als dies von den Parteien beim Verhandeln eines Vertrags vorhersehen war. Nicht immer lassen sich die Probleme dann dadurch lösen, dass man den Vertragstext auslegt. Es stellt sich vielmehr ganz allgemein die Frage: Auf welche Regelungen des BGB müssen die Parteien zurückgreifen, um zu ermitteln, was für ihr IT-Projekt jetzt gilt.

1.1.2 Die Crux der Inhaltskontrolle des AGB-Rechts

Aus weiterem Grund ist es für den Anwalt unerlässlich, sich zunächst Gedanken darüber zu machen, was für einen Vertrag seine Partei eigentlich schließen will. IT-Verträge werden in der Praxis nur punktuell indivi-

duell verhandelt. Noch seltener werden sie „ausgehandelt“ im Sinne des § 305 Abs.1 BGB. Zumeist stellen IT-Anbieter ihre Leistung auf Basis von Standardverträgen bereit oder sie bedienen sich zumindest Musterklauseln, die sie bereits mehrfach an anderer Stelle verwandt haben. Damit unterliegen sie den Regelungen der AGB-rechtlichen Inhaltskontrolle.

Für den Kunden ist dies ein Segen. Für den Anbieter ein Fluch. Selbst bei zwischen zwei Unternehmen geschlossenen Verträgen gilt das AGB-Recht und beschränkt hier die Vertragsfreiheit erheblich. Gerade den aus dem Common-Law-Bereich stammenden Softwareunternehmen ist diese Inhaltskontrolle fremd. Dort werden die Vertragsfreiheit und eine stark am Wortlaut orientierte Interpretation hoch gehalten.

Nach dem deutschen AGB-Recht gilt: Eine vertragliche Regelung ist nach § 307 BGB unwirksam, wenn sie den Vertragspartner entgegen den Geboten von Treu und Glauben unangemessen benachteiligt. Eine solche unangemessene Benachteiligung ist anzunehmen, wenn eine Bestimmung mit dem wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist.

Jede vertragliche Regelung muss sich daher an den Grundgedanken der gesetzlichen Regelung messen lassen, die auf den Vertrag Anwendung finden würde, wenn nichts geregelt wäre. Die Entscheidung über den BGB-Vertragstyp gibt demnach für die Inhaltskontrolle des AGB-Rechts die entscheidende Richtung vor. Je nachdem, wie sich ein Vertrag oder eine einzelne Regelung unter die Vertragstypen des BGB einordnen lässt, kann die Regelung im Hinblick auf das AGB-Recht wirksam oder unwirksam sein.

Was im Dienstvertrag problemlos möglich ist, kann beim Werkvertrag demgegenüber ein grundstürzendes Abweichen von der gesetzlichen Regelung bedeuten.

1.1.3 Verhandlungsstrategie

Auch im Hinblick für die Verhandlungsstrategie ist die Frage nach dem Vertragstyp entscheidend.

Wenn der Kunde auf ein umfangreiches Gewährleistungsrecht zurückgreifen kann, wie beispielsweise im Werkvertragsrecht, reicht ihm möglicherweise eine sehr schlanke Regelung über seine Rechte bei Mängeln. Der Kunde hat kein Interesse daran, mit dem IT-Anbieter Vertragsklauseln zu diskutieren, die seine starken Gewährleistungsrechte aus den §§ 633 ff. BGB modifizieren. Im Zweifel wird sich die für ihn günstige Ausgangsposition nur verschlechtern.

Handelt es sich bei dem IT-Projekt aber um ein dienstvertragsähnliches Konstrukt, ist der Berater des Kunden gefordert. Der Dienstvertrag kennt

kein Gewährleistungsrecht. Ohne eine Regelung von „*Service-Level-Agreements*“ und einem detaillierten Haftungsregime, ist der Kunde im Falle der Schlechtleistung schutzlos.[1] Hier muss der Berater des Kunden darauf hinwirken, umfangreiche Regelungen im Vertragstext vorzusehen. Das setzt aber voraus, dass man zuvor für sich ermittelt hat, welcher Vertragstyp des BGB eigentlich auf die Leistung anwendbar ist.

1.1.4 Jede Leistung ist gesondert zu betrachten

Hierbei ist ein weiterer Grundsatz zu beachten: Jede Leistung eines IT-Vertrags ist gesondert zu prüfen.

Bei IT-Projekten sind zumeist mehrere komplexe Leistungen in einem Vertrag zusammengefasst (bspw. Outsourcing von Geschäftsprozessen samt Bereitstellung von Software). Manchmal sind die Leistungen sogar miteinander verwoben. Hier ist jede Leistung einzeln zu betrachten.

Es gilt der Grundsatz des typengemischten Vertrags. Nicht der Schwerpunkt der vertraglichen Leistung gibt vor, welcher Vertragstyp des BGB für alle Leistungen anwendbar ist. Vielmehr muss für jede Leistung die Frage neu aufgeworfen werden, welchem Vertragstyp des BGB unterfällt die Leistung.[2] Das ist auch sinnvoll. Denn nur so lassen sich Verträge flexibel handhaben und gestalten.

1.1.5 Die Leistungsbeschreibung ist das Wichtigste

Es gibt einen wesentlichen Grundsatz, der für jedes IT-Projekt gilt und nicht oft genug wiederholt werden kann: Eine vernünftige Leistungsbeschreibung ist für beide Parteien sinnvoll und vermeidet Streit.[3]

Es ist nur die eine Seite der anwaltlichen Arbeit, sich bei IT-Projekten ausgiebig um ein vertragliches Instrumentarium aus Service Level Agreements, Haftungsregelungen, komplexen Laufzeitbestimmungen samt „Termination Support“ sowie ausgetüftelten Change Request und Eskalationsverfahren im Streitfall zu kümmern. Das nutzt im Zweifel alles nichts, wenn die Parteien nicht nachvollziehbar dokumentiert haben, was sie eigentlich als geschuldete Leistung erwarten.

Hier ist der Anwalt gut beraten, seine Partei lieber einmal mehr daran zu erinnern, mit der Gegenseite zu dokumentieren, was Gegenstand der Leistungen sein soll. Oft gibt es auf jeder Seite genug Ausreden, sich jetzt gerade nicht um eine detaillierte Leistungsbeschreibung zu kümmern: „Wir sind uns absolut einig“, „wir müssen morgen starten“ oder „es ist

---

1 Zu Service Level Agreements *Schumacher*, MMR 2006, S. 12.

2 *Grüneberg*, in: Palandt, BGB, Überblick vor § 311 Rn. 19.

3 Zur Leistungsbeschreibung *Bräutigam*, IT-Outsourcing und Cloud Computing, S. 1105 ff.

ganz klar, worum es hier geht“. Wer die Durchführung des Projekts mit derartigen Floskeln priorisiert, sollte sich dabei kurz bewusst machen:

Wenn es zum Streit kommt, wird alles viel teurer, das Projekt nicht fertig und Zeit und Kosten einer Auseinandersetzung stehen in keinem Verhältnis zu dem Aufwand, sich bei Beginn um eine Dokumentation der Leistung zu kümmern.

1.2 Einzelne Vertragstypen

Die zentralen Vertragstypen im Softwarerecht lassen sich unter die vier wesentlichen Vertragstypen des BGB fassen: Kaufvertrag, Werkvertrag, Mietvertrag und Dienstvertrag.

1.2.1 Erwerb von Standardsoftware

Der bloße Erwerb von Standartsoftware unterfällt dem Kaufvertragsrecht.[4] Anders verhält es sich bei Verträgen über individuell herzustellende Software. Diese bestimmen sich nach werkvertraglichen Regelungen, wie der Bundesgerichtshof in der Entscheidung Internetsystem-Vertrag zusammenfassend dargestellt hat.[5] Software-Maintenance und Softwareerstellung

Dem Werkvertragsrecht unterfallen auch die in der Praxis auf dem Rückzug befindlichen Software-Wartungsverträge. Dies hat der Bundesgerichtshof bereits im Jahr 1984 entschieden.[6] Gleiches gilt für Verträge über die individuelle Erstellung von Software.[7]

1.2.2 Cloud- und SaaS-Verträge

Derzeit die favorisierten Praxislösungen für die Bereitstellung von Software sind Cloud- und servicebasierte Lösungen. Hier gibt es verschiedene Modelle *„SaaS“* (Software as a Service), *„IaaS“* (Infrasturcture as a Service) und *„PaaS“* (Platform as a Service). All diesen Modellen ist gemein, dass der Nutzer Software oder andere IT-Lösungen nicht mehr dauerhaft *„erwirbt“*, sondern *„as a Service“* nutzt. Das ist die klassische Situation des Mietvertrags nach §§ 535 ff. BGB.[8] Meist kamen dienstvertragliche Elemente hinzu.

---

[4] Hier: BGH, Urt. v. 22. Dezember 1999 - VIII ZR 299/98, NJW 2000, 1415.

[5] BGH, Urt. v. 8. Januar 2015 – VII ZR 6/14, NJW-RR 2015, 469 – Internetsystem-Vertrag.

[6] BGH, Urt. v. 5. Juni 1984 - X ZR 75/83, NJW 1984, 2160.

[7] BGH, Urt. v. 30. Januar 1986 - I ZR 242/83, BB 1986, 1319.

[8] Das ist naheliegend und schon seit einiger Zeit vom BGH zu den Vorgängern der Cloud-Lösungen entschieden worden, dem sogenannten “Application Software Providing”, BGH; Urt. v. 15. November 2006 -XII ZR 120/04. Gleichwohl gilt natürlich auch für Ver-

1.2.3 IT-Projektverträge

Die Einordnung von IT-Projektverträgen lässt sich nicht ohne weiteres einem bestimmten Vertragstyp zuordnen. Jedes Projekt ist individuell und muss daher auch im Einzelfall gesondert dahin betrachtet werden, wie es vertraglich eingeordnet werden kann.

Üblicherweise streiten die Parteien darüber, ob die in einem IT-Projekt die von einem Provider geschuldeten Leistungen dem Werkvertragsrecht oder dem Dienstvertragsrecht unterfallen. Wie gesagt, ist aus Kundenperspektive das Werkvertragsrecht immer wünschenswert.

Umgekehrt verhält es sich auf Anbieterseite. Für ihn ist der Dienstvertrag die sicherste Variante. Der Kunde kann im Fall der Schlechtleistung zwar kündigen, aber die Vergütung mangels Gewährleistungsrecht nicht mindern; es sei denn, er hat Servicelevel und ein entsprechendes Sanktionssystem vorgesehen.

Wenn keine Qualitätsparameter vorgegebenen sind, gilt bei beiden Vertragstypen für die Qualität der Leistung übrigens § 243 BGB: Der Anbieter schuldet nur eine Leistung mittlerer Art und Güte.

Damit ist dem Kunden sicherlich nicht gedient. Wer will schon eine Leistung mittlerer Art und Güte. Der Kunde ist entweder an einem sehr hohen Standard oder einer individuell maßgeschneiderten Qualität interessiert.[9] Daher gilt auch hier: Was Art und Qualität der Leistung angeht, kann man im Zweifel nicht genug regeln.

1.3 Spezielle Regelungen des Urheberrechts

Für die Gestaltung von Softwareverträgen reicht eine sichere Kenntnis des BGB nicht aus. Das liegt daran, dass Software gemäß § 69a ff. UrhG urheberrechtlich geschützt ist. Aus den Regelungen des Urhebergesetzes ergeben sich Besonderheiten für Softwareverträge. Folgende Regelungen sind in der Praxis am wichtigsten:

1.3.1 Rechte des Arbeitgebers/Dienstherren

Anders als bei Erfindungen und technischen Vorschlägen, bei denen die Regelung des Arbeitnehmererfinderrechts einschlägig sind, stehen Rechte an im Arbeits- oder Dienstverhältnis geschaffener Software nach § 69b UrhG automatisch und ohne jede weitere Vergütungspflicht dem Arbeitgeber oder Dienstherren zu. Diese Regelung ist wirtschaftlich unerläss-

träge über Cloud-Lösungen der Grundsatz des typengemischten Vertrags. Zum Ganzen *Bräutigam/Thalhofer*, IT-Outsourcing und Cloud-Computing, S. 1262 ff.

9 *Schumacher*, MMR 2006, S. 12 (12 f. m. w. N.).

lich. Wer in IT-Programmierer investiert, will auch über dessen Arbeitsergebnisse verfügen können.

1.3.2 Mindestrechte der Nutzer

Die §§ 69d Ansatz 2 und 3 sowie § 69e UrhG sprechen dem Anwender ein Minimum an Nutzerrechten zu. Er hat jeweils das Recht eine Sicherungskopie zu erstellen und Handlungen vorzunehmen, die der Herstellung der Interoperabilität der überlassenen Software dienen.

1.3.3 Erschöpfungsgrundsatz

Software wird kaum mehr auf Datenträgern gehandelt, sondern per Download „gekauft". Für den Weitervertrieb solcher per Download erworbenen Software war lange Zeit umstritten, ob der für sämtliche gewerbliche Schutzrechte zentrale Erschöpfungsgrundsatz (§ 17 Abs. 2 UrhG) gilt.

Der Urheber soll einmal die Möglichkeit haben, eine Vergütung für sein *„Werkstück"* zu erhalten. Danach sind seine Rechte verbraucht oder wie das Gesetz formuliert *„erschöpft"*.

Wie seit dem Used Soft-Urteil des Europäischen Gerichtshofs[10] feststeht, gilt der Erschöpfungsgrundsatz bei jedem erstmaligen Verkauf von Software. Ganz gleich, ob die Software, wie früher auf einem Werkstück oder online weitergegeben wird. Der Bundesgerichtshof hat sich der von EuGH vertretenen Auffassung inhaltlich komplett angeschlossen.[11]

Zugunsten des Urhebers ist bereits im ersten Korb der Urheberrechtsnovelle der Bestsellerparagraph (§ 32a UrhG) ins UrhG eingeführt worden.[12]

Im Kern kann der Urheber, auch wenn seine Rechte erschöpft sind, später eine angemessene Vergütung verlangen, wenn die damals vereinbarte Gegenleistung *„unter Berücksichtigung der gesamten Beziehungen des Urhebers zu dem anderen in einem auffälligen Missverhältnis zu den Erträgen und Vorteilen aus der Nutzung des Werkes steht"*. Kurzum: Entwickelt sich das Werk des Urhebers zu einem Bestseller, kann der Urheber nachträglich eine angemessene Vergütung von demjenigen verlangen, der den Bestseller vertreibt.[13]

---

[10] EuGH, 3. Juli 2012 - C-128/11, NJW 2012, 2565 – Used Soft.

[11] BGH, Urt. v. 17. Juli 2013 - I ZR 129/08, NJW 2014, 777 – Used Soft II; BGH, Urt. v. 11. Dezember 2014 – I ZR 8/13, NJW-RR 2015, 1138 - Used Soft III.

[12] *Dreier/Schulze,* UrhG, § 32a Rn. 1.

[13] Beispielsweise hatte die für das Verhältnis Urheberrecht und Designrecht prägende Geburtstagszug-Entscheidung, einen Bestsellerfall zum Gegenstand. Hier stellte sich die

1.3.4 Zweckübertragungsregel

In der Praxis von erheblicher Bedeutung ist die Zweckübertragungsregelung des § 31 Absatz 5 UrhG. Auch diese Regelung enthält ein Schutzprinzip zugunsten des Urhebers. Nach der Zweckübertragungsregel gilt der Grundsatz, dass ein Urheber nur so viel Rechte an seinem Werk überträgt, wie zur Erreichung des Vertragszwecks notwendig sind.[14] Sprich: Das Urheberrecht hat die Tendenz, beim Urheber zu verbleiben. Für die Vertragsgestaltung folgt daraus, dass der Verwerter tunlichst alle Nutzungsarten ausdrücklich aufführen muss, die er für die an den Urheber zu zahlende Vergütung erwartet.[15] Open Source Software

Schon das Zusammenspiel aus Regelungen des BGB und des Urheberrechts zeigt, wie komplex es ist, im Bereich von IT-Projekten zu beraten. Das Ganze lässt sich noch um eine Ebene erweitern:

Für die Erstellung von Software greifen Entwickler mittlerweile nicht selten auf Open Source Software zurück. Gerade im Bereich der Industrie 4.0 ist Open Source Software beliebt, um neue Anwendungen zu programmieren.

Aber nicht nur dort: Auch die öffentliche Verwaltung benutzt immer öfter Linux als Open-Source-Betriebssystem; klein- und mittelständische Unternehmen arbeiten intern mit Open-CMS; bei Endnutzern wird der Internetbrowser Mozilla immer beliebter.

Für das Softwarevertragsrecht ist der Umgang mit Open-Source-Lizenzen daher unerlässlich. Die Grundzüge der rechtlichen Besonderheiten von Open-Source-Software soll daher nachfolgend kurz skizziert werden:

1.1 Unterschiedliche Open Source Lizenzmodelle

Open-Source-Software oder Free-Software gibt es seit den 80-iger Jahren. Über die Zeit haben sich grundsätzlich zwei verschiedene Lizenzmodelle

Frage, ob der Kläger mit dem Geburtstagszug schon ein urheberrechtliches Werk oder nur ein schutzfähiges Design geschaffen hatte. Während der Entwerfer im Designrecht selbst bei einem Bestseller keine zusätzliche Vergütung verlangen kann, steht dem Urheber im Fall eines Bestsellers über § 32a UrhG ein solcher Anspruch zu. Daher war es für den klagenden Urheber in der Geburtstagszug-Entscheidung notwendig, dass seine Leistung als Werk der angewandten Kunst betrachtet wurde.

[14] BGH, Urt. v. 27. September 1995 - I ZR 215/93, GRUR 1996, 121 (122) – Pauschale Rechtseinräumung; *Dreier/Schulze*, UrhG, § 31 Rn 110 ff.

[15] *Dreier/Schulze*, UrhG, § 31 Rn 103 ff.

entwickelt: die sogenannten Copy-Left-Lizenzen und Permissive-Licenses auf der anderen Seite.[16]

Copy-Left-Lizenzen

Bei einer Copy-Left-Lizenz kann der Nutzer die Software zwar frei nutzen, bearbeiten und verändern. Allerdings muss er jede Weiterverwendung der so erstellten Software wieder einer Open Source Lizenz unterstellen. Dies bezeichnet man als viralen Effekt.[17]

Damit nicht genug: Der Nutzer der Open-Software ist auch verpflichtet, seinen Quellcode offenzulegen, so dass weitere Nutzer auch problemlos die *„neue"* Open Source Software weiterentwickeln und verwenden können.

Ein Beispiel für eine Copy-Left-Lizenz ist die GNU-Generell-Public-License (GPL). Sie ist die wichtigste und am weitesten verbreitetste Open Source Lizenz. Etwa zwei Drittel aller Open Source Software steht unter dieser Lizenz.[18] Das Betriebssystem Linux ist ein bekanntes Beispiel.

1.3.5 Permissive Licenses

Für Unternehmen sind solche Copy-Left-Lizenzen wenig interessant. Unternehmen haben kein Interesse daran, bei eigenen Entwicklungen den Quellcode offenzulegen. Verdienen lässt sich mit einer Copy-Left-Lizenz aus ihrer Sicht ebenfalls nichts. Das sieht bei permissive Licenses oder freizügige Open Source Lizenzen anders aus: Hier dürfen die Nutzer die erstellte Software proprietär vertreiben. Das bedeutet: Software, die durch Nutzung einer unter permissive Licenses gestellten Open Source Software programmiert wurde, kann zu anderen Bedingungen als die der vormals genutzten Open Source Software weiter vertrieben werden.[19] Beispiele für diese *„permissive"* Open Source Lizenzen sind die Massachusetts Institut of Technology License (MIT-Lizenz) und die Berkley-Software-Distribution-License (BSD-Lizenz).

1.2 Probleme bei der Nutzung von Open Source Software

In der Praxis ist der Einsatz von Open Source Software gerade bei Unternehmenskäufen ein Problem. Wenn ein Unternehmen eine Zielgesellschaft erwerben will, die Software herstellt, vertreibt oder für weitere IT-Leistungen nutzt, stellt sich regelmäßig die Frage, ob hierin Open Source Software enthalten ist. Denn: Wenn dies der Fall ist, gibt es Risiken für

[16] Zur Open Source Software *Dreier/Schulze*, UrhG, § 69a Rn 11 und § 69c Rn. 38.

[17] *Dreier/Schulze*, UrhG, § 69c Rn. 38.

[18] *Jaeger/Metzger*, GRUR 2008, S. 130.

[19] *Dreier/Schulze*, UrhG, § 69c Rn. 38.

das Geschäftsmodel. Im schlimmsten Fall ist die vertriebene Software so nicht nutzbar, da sie nicht gegen Entgelt vertrieben werden kann.

In der Praxis behelfen sich große Unternehmen meist mit einem so genannten *„Blue-Wash"*. Die fragliche Software wird *„blue gewashed"*, das heißt gereinigt, indem die Open Source Bestandteile durch proprietär erstellte Software ausgetauscht werden. Rechtlich werden solche *"Blue-Wash"*-Projekte zumeist mit umfangreichen Freistellungsvereinbarungen in Kaufverträgen flankiert. Der Verkäufer muss dafür einstehen, dass kein Dritter Rechte aus der verwandten Open-Source-Software herleitet.

1.3.6 Creative Commons

Nicht nur Software wird über Open Source Lizenzen *„frei"* vertrieben. Auch bei anderen urheberrechtlichen Werken gibt es Standard-Lizenzverträge, mit denen der Schöpfer Dritten auf einfache Weise Nutzungsrechte an seinen Werken einräumen kann. Solche Standardlizenzverträge mit der *„freie Inhalte"* entstehen, nennt man *„Creative Commons"*. Das lässt sich frei als *„schöpferisches Gemeingut"* übersetzen.[20] Häufig finden sich die Creative Commons bei der Nutzung von Bildern, Texten oder Musikwerken.

Unter der Creative Commons Public License (CCPL) werden unterschiedliche Vertragsmodule zur Verfügung gestellt.[21] Der Nutzer ist daher gut beraten, sich stets zu vergewissern, was er mit dem angeblich freien Inhalt machen darf. Die wichtigsten Einschränkungen des frei nutzbaren Werks lassen sich in folgende Module gliedern[22]:

- BY – Eine Verpflichtung zur Nennung des Namens des Urhebers
- NC – Das Werk darf nicht für kommerzielle Zwecke verwendet werden (Non-Commercial).
- ND - Das Werk darf nicht verändert werden (No-Derivatives).
- SA - Das Werk muss, nachdem es verändert worden ist, unter den gleichen Lizenzbedingungen weitergegeben werden (Share Alike).

Die Einschränkungen der Rechte erkennt man in der Regel schon im Namen der Lizenz. So bedeutet *„CC BY-SA"*, dass der Urheber des Werks auf eine Namensnennung besteht (BY), aber jegliche Form der Weitergabe und Vervielfältigung, Bearbeitung und Veränderung gestattet. Im Gegenzug ist der Nutzer aber verpflichtet, jegliche Materialien unter den

[20] Zu Creative Commons *Dreier/Schulze,* UrhG, § 69c Rn. 41.

[21] *Dreier/Schulze,* UrhG, § 69c Rn. 41.

[22] Näheres unter www.creativecommons.org.

gleichen Lizenzbedingungen weiterzugeben, die das Material des ursprünglichen Urhebers beinhalten (share alike).

1.3.7 Rechtsprechung zu Open-Source-Lizenzen

Das Feld der Open-Source-Lizenzen und freien Inhalte ist vergleichsweise jung. Es gibt daher bisher nur wenig Rechtsprechung. Das mag zum anderen aber auch daran liegen, dass es hier per se zu weniger Streitigkeiten kommt als bei proprietärer Software.

Betrachtet man die ergangenen Entscheidungen zu Open Source Software, so lässt sich folgendes festhalten: Open Source Software wird auf der Rechtsfolgenseite nicht anders behandelt, als andere urheberrechtlich geschützte Software. So hat das Landgericht Halle beispielsweise entschieden, dass der Verletzer einer unter den GPL-Bedingungen bereitgestellten Open Source Software auf Unterlassung verklagt werden kann. Er darf die unter dieser Bedingung erstellte Software nicht mehr ohne die GPL-Bedingungen und ohne Veröffentlichung des Source-Codes nutzen.[23]

Auch das übliche Instrumentarium bei Verletzung gewerblicher Schutzrechte und Urheberrechte steht dem Inhaber der Open Source Software zu. So kann der Verletzer auf Auskunft und Schadensersatz bei lizenzwidriger Nutzung von Open-Source-Software verklagt werden.[24]

Zur Schadensersatzpflicht hat das Landgericht Hamburg auch entschieden, dass derjenige, der Software erstellt und proprietär vertreibt, die Verpflichtung hat, sich zu vergewissern, dass er bei Erstellung seiner Software keine Open Source Software genutzt hat. Unwissenheit schützt den Software-Ersteller demnach nicht. Ein Verschulden des Verletzers wird auch bei der unerlaubten Nutzung von Open Source Software regelmäßig vorliegen.[25]

Allerdings ist das Thema Schadensersatz bei Open Source und Creative Common-Lizenzen schwierig. Denn: Die Open Source Software oder die freien Inhalte werden gerade unentgeltlich zur Verfügung gestellt.

Es stellt sich daher die Frage, welcher Schaden dem Rechteinhaber entsteht, wenn ein Dritter das Werk unerlaubt nutzt. Hierzu liegt eine Entscheidung des Oberlandesgerichts Köln vor, in der das Gericht entschie-

[23] LG Halle, Urt. v. 27. Juli 2015 - 4 O 133/15, MMR 2016, 417.

[24] LG Bochum, Urt. v. 3. März 2016 - I-8 O 294/15, MMR 2016, 553.

[25] LG Hamburg, Urt. v. 14. Juni 2013 - 308 O 10/13, CR 2013, 498; zum Verschuldensmaßstab im Urheberrecht generell: *Dreier/Schulze*, UrhG, § 97 Rn. 55 ff.

den hat, dass der Schadensersatz im Rahmen der Lizenzanalogie bei Creative Commons-Lizenzen unterstellten Werken gleich Null ist.[26]

In dem vom Oberlandesgericht Köln zu entscheidenden Fall hatte das Deutschlandradio eine von einer Bildagentur unter der Bedingung der *„Creative Commons Attribution Non-Commercial 2.0"*-Lizenz (CC-BY-NC) bekanntes Foto im Internet auf ihrer Webseite gezeigt. Den Namen des Fotografen nannte das Deutschland Radio nicht.

Das Oberlandesgericht hielt das folgerichtig für eine Verletzung der Lizenzbedingungen. Allerdings sei der Schadensersatz auf Erstattung der Abmahnkosten beschränkt: Zwar habe das Deutschlandradio die Lizenzbedingungen verletzt, da der Fotograf aber eine lizenzkostenfreie Nutzung des Bildes durch die Creative Common-Lizenz gestattet habe, könne ein Schaden nach der Lizenzanalogie gerade nicht bestehen, da der Fotograf eine Lizenz zum Nulltarif vergeben hätte.

Das erscheint plausibel – aber nur auf den ersten Blick. Denn eine kostenfreie Nutzung hat der Fotograf gerade nur dann eingeräumt, wenn die Lizenzbedingungen beachtet werden. Mit dem Lizenzverstoß sind daher sämtliche Nutzungsrechte weggefallen. Warum dann nicht eine vollständig unberechtigte Nutzung zu *„echten Schadensersatzansprüchen"* führen soll, erschließt sich nicht.[27]

Das Urteil des Oberlandesgerichts Köln zeigt exemplarisch: Viele Probleme im Bereich von Open Source Software sind ungeklärt.

Zudem werden sich die Probleme in Zukunft mehren. Gerade bei Industrie 4.0-Anwendungen wird üblicherweise Open Source Software benutzt. Wie aber soll bei in technischen Geräten eingebettete Software ein Urheber genannt werden und der Quellcode offengelegt werden? Eine von vielen Fragen, auf die die Praxis Antworten finden muss.

2 Europäisches Urheberrecht

2.1 Was ist „europäisches Urheberrecht"

Es gibt kein europäisches Urheberrechtgesetz. Anders als im Marken- und Geschmacksmusterrecht existiert keine Gemeinschaftsurheberrechtsverordnung. Gleichwohl ist das Urheberrecht durch verschiedenste Richtlinien immer weiter harmonisiert worden. Man kann daher durchaus von einem europäischen Urheberrecht sprechen.

---

[26] OLG Köln, Urt. v. 31. Oktober 2014 – 6 U 60/14, NJW 2015, 789.

[27] Hierzu auch OLG Köln, Urt. v. 31. Oktober 2014 – 6 U 60/14, NJW 2015, 789, mit Anm. *Schweinoch*, NJW 2015, S. 794.

Von besonderer Bedeutung ist insbesondere die „Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“ (Richtlinie 2001/29/EG). Diese Richtlinie ist auch als sogenannte Info-Soc-Richtlinie bekannt. Sie regelt im digitalen und im Online-Bereich verschiedene Rechte sowie urheberrechtliche Schrankenbestimmungen.

Neben der Info-Soc-Richtlinie sind die Computerprogrammrichtlinie 91/250/EWG und Datenbankrichtlinie 96/9/EG weitere wichtige urheberrechtsrelevante europäische Regelungswerke.

Die Harmonisierung auf europäischer Ebene findet aber nicht nur durch den Normgeber selbst statt. Die Rechtsprechung des EuGH konkretisiert momentan ein europäisches Urheberrecht immer weiter. Ein Beispiel aus der jüngsten Praxis ist die zu recht heftig kritisierte Entscheidung des Europäischen Gerichtshofs zur Haftung für Hyperlinks, die auf Internetseiten mit urheberrechtswidrigen Inhalten verweisen.[28]

2.2 Gesetzgeberische Neuerung

Die Schaffung eines funktionierenden digitalen Mindestmarkts ist derzeit ein wichtiges Ziel der Europäischen Kommission.

2.2.1 Aktionsplan

Ende 2015 hat die Europäische Kommission einen Aktionsplan für zukünftige Regelungen im Bereich des Urheberrechts veröffentlicht.[29]

In dem Aktionsplan betont die Kommission besonders folgende Ziele:

- Breiterer Zugang zu digitalen Inhalten in der gesamten EU,

[28] EUGH, Urt. v. 21. Januar 2016 - C-359/14, C-475/14, NJW 2016, 149 – GS Media; In diesem Verfahren hatte der Europäische Gerichtshof darüber zu entscheiden, ob das Verlinken auf ein urheberrechtlich geschütztes Werk, das ohne die Zustimmung des Rechteinhabers online gestellt wurde, eine „öffentliche Wiedergabe“ und somit eine Urheberrechtsverletzung darstelle. Konkret ging es um ein Nacktfoto der holländischen Moderatorin *Britt Decker* für das Magazin Playboy, das auf einer australischen Webseite illegal gezeigt wurde. Das holländische Unternehmen GS Media verlinkte auf diese Webseite. Der Europäische Gerichtshof entschied hier zunächst konsequent, dass das Verlinken grundsätzlich keine „öffentliche Wiedergabe“ darstelle. Wusste die verlinkende Person aber oder hätte sie vernünftigerweise wissen müssen, dass der verlinkte Inhalt rechtswidrig zum Abruf bereitgehalten wurde, stelle das Verlinken demgegenüber eine „öffentliche Wieder-gabe“ dar. Diese Entscheidung ist zu Recht kritisiert worden (hierzu beispielsweise *Hoffmann*, K&R 2016, 706), denn letzten Endes verwischt der EUGH damit Konturen eines europäischen Urheberrechts und lässt es zu einem unkalkulierbaren Billigkeitsrecht werden.

[29] http://europa.eu/rapid/press-release_IP-15-6261_de.htm.

- Ausnahmen vom Urheberrecht für eine innovative Gesellschaft (Schranken des Urheberrechts),
- Schaffung eines gerechten Marktes (gerechtere Verteilung der Wertschöpfung von Online-Inhalten),
- Bekämpfung der Piraterie und
- eine langfristige Zukunftsperspektive.

2.2.2 Verordnung über Portabilität von Online-Inhalten

Zudem hat die Europäische Kommission eine Verordnung zur Gewährleistung der grenzüberschreitenden Portabilität von Online-Diensten im Binnenmarkt erlassen.[30] Abonnenten von Online-Inhalt-Diensten soll es nun möglich sein, den abonnierten Online-Inhalt auch dann zu konsumieren, wenn sie sich vorübergehend in einem anderen Mitgliedsstaat aufhalten.

Konkret bedeutet dies: Die Kommission sorgt dafür, dass wir die Bundesliga auch im Urlaub sehen können.

Anders formuliert: Die neue Verordnung enthält zwar kein per-se-Verbot des Geoblocking, zumindest aber die Möglichkeit, Online-Inhalte vorübergehend innerhalb der Europäischen Union „mitzunehmen".

2.2.3 Richtlinie für ein Urheberrecht im Binnenmarkt

Die geplanten Änderungen am Urheberrecht werden aber insgesamt konkreter. Die Kommission hat am 14. September 2016 einen Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt veröffentlicht.[31]

Deren Highlights lassen sich wie folgt zusammenfassen:

- Neue Schrankenregelung zugunsten von Forschungs- und Bildungseinrichtungen sowie Archiven und Museen,
- eine europäische Bestsellerklausel;
- ein 20-jähriges Leistungsschutzrecht für Presseverleger.

Zu begrüßen sind sicherlich die neuen Schrankenregelungen, die länderübergreifende Forschung vereinfachen. Gerade auch so interessante Projekte wie der rumänisch-deutsche Workshop zum Europäischen Informationsrecht können in Zukunft hiervon profitieren. Bei grenzüber-

[30] https://ec.europa.eu/transparency/regdoc/rep/1/2015/DE/1-2015-627-DE-F1-1.PDF; zum Ganzen *Spiegel*, Ich packe meinen Koffer und nehme mit… in: Taeger, Smart World – Smart Law, 2016, S. 693; *Raue/Ettig*, K&R 2016, S. 79.

[31] Abrufbar unter http://www.computerundrecht.de/EU-Kommission-Richtlinie-Urheberrecht-Binnenmarkt.pdf.

schreitenden Forschungsprojekten muss Klarheit herrschen, dass Inhalte für Forschungszwecke länderübergreifend genutzt werden können.

Sicherlich auch zu befürworten ist die europäische Bestsellerklausel. Der Entwurf will eine Berichtspflicht für Verwerter einführen, die regelmäßig und unaufgefordert Auskunft über Werknutzungen und die damit verbundenen Erlöse geben sollen. Im Rahmen eines Streitbeilegungsverfahrens ist auch ein Anspruch auf Nachvergütung vorgesehen, ähnlich der in Deutschland bekannten Bestsellerklausel. Hier mag man im Detail Änderungen diskutieren, im Grunde geht der Vorschlag aber in die richtige Richtung.

Schwer nachzuvollziehen ist aber die Tatsache, dass sich der europäische Gesetzgeber nunmehr für ein Leistungsschutzrecht für Presseverleger stark macht. Das Leistungsschutzrecht für Presseverleger kann man auf deutscher Ebene als schlicht gescheitert ansehen.[32] Das umstrittene Leistungsschutzrecht hat nicht zu der gewünschten (und zu Recht umstrittenen) Vergütung für Presseverleger geführt. Es läuft in der Praxis leer und behindert dafür Innovationen an anderer Stelle.

In puncto Leistungsschutzrecht wirkt es aber so, als gehe die Europäische Kommission nach dem Grundsatz vor: Wenn das nationale Leistungsschutzrecht nicht funktioniert, erhöhen wir die Dosis und führen es auf europäischer Ebene ein.[33]

Davon sollte die Europäische Kommission Abstand nehmen. Das Leistungsschutzrecht für Presseverleger behindert neue Geschäftsmodelle im Medienbereich. Was Europa aber braucht ist ein Urheberrecht, das dem technologischen Wandel gerecht wird und Innovationen fördert, es aber gleichzeitig schafft Urheber an den Erlösen der Verwertung zu beteiligen, wo es fair und notwendig ist.

Es bleibt abzuwarten, ob dies in Zukunft gelingen wird.

[32] Zur Kritik am Leistungsschutzrecht auf nationaler Ebene: *Wieduwilt*, K&R 2010, S. 555; *Höppner*, K&R 2013, S. 73.

[33] *Kritik* unter https://irights.info/artikel/eu-kommission-mehr-vom-alten-statt-neuem-urheberrecht/27902.

LITERATUR

Bräutigam, Peter (Hrsg.): IT-Outsourcing und Cloud-Computing, 3. Aufl., Berlin 2013.

Dreier, Thomas/Schulze, Gernot: Urheberrechtsgesetz, 5. Aufl., München 2015.

Höppner, Thomas: Technisch-ökonomische Aspekte des Leistungsschutzrechts für Presseverleger, K&R 2013, S. 73-82.

Hofmann, Franz, Der Linksetzer auf urheberrechtswidrige Inhalte als Urheberrechtsverletzer – oder doch besser als Störer, K&R 2016, S. 706-709.

Jaeger, Till/Metzger, Axel: Die neue Version 3 der GNU Public License, GRUR 2008, S. 130-137.

Palandt, Otto (Begr.): Bürgerliches Gesetzbuch, 76. Aufl., München 2017.

Rauer, Nils/Ettig, Diana: Die Strategie für einen digitalen Binnenmarkt – Erste Schritte für eine Modernisierung des Urheberrechts, K&R 2016, S. 79-83.

Schumacher, Volker: Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen, MMR 2006, S. 12-17.

Schweinoch, Martin: Anmerkung zu OLG Köln, Urt. v. 31.10.2014 – 6 U 60/14 – Auslegung von Creative Commons-Lizenzen", NJW 2015, S. 794-795.

Spiegel, Johanna: Ich packe meinen Koffer und nehme mit… Meine Online-Inhalte, in: Jürgen Taeger (Hrsg.), Smart World – Smart Law – Weltweite Netze mit regionaler Regulierung, Tagungsband DSRI-Herbstakademie 2016, Edewecht 2016, S. 693-707.

Wieduwilt, Hendrik: Das neue Leistungsschutzrecht für Presseverlage – eine Einführung, K&R 2010, S. 555-561.

PRAKTISCHE UND STEUERLICHE VORTEILE FÜR SOFTWARE-UNTERNEHMEN IN RUMÄNIEN

Rechtsanwältin Alexandra Epure, LL.M.

EPURE & LOHMANN SCA
Alexandra.Epure@anwaltskanzlei.ro

Zusammenfassung

Die Software-Industrie ist in Rumänien in den letzten Jahren zum größten Generator von Arbeitsplätzen geworden. Das letzte Jahr 2016 sowie das letzte Jahrzehnt waren ein erfolgreiches Jahr für die Branche. Der Umsatz von Softwaregesellschaften, nämlich Softwareherstellern und Dienstleistern, hat sich um 21 % erhöht, rund um 3 Milliarden EUR. [116] In dem vergangenen Jahr erreichte die Softwarebranche, in denen auch die Telekomunikationsunternehmen einbezogen sind, einen Anteil von 5,6 % des Bruttoinlandsproduktes. Ein wichtiger Faktor für den Schwung der Softwareindustrie ist die Steuerbefreiung zum Vorteil der Mitarbeiter der Branche. Die Angestellten der Softwarebranche erfreuen sich über eine Begünstigung der Einkommensteuer, die in Rumänien in der Höhe von 16 % liegt. Die Steuerbefreiung gilt ab 2004,[116] damals mit beschränkten Grenzen für die Mitarbeiter im Vergleich zur aktuellen Form. In den vergangenen Jahren ist der rumänischen Gesetzgeber zwecks Unterstützung der steuerlichen Vorteile der Branche mit neuen Änderungen gekommen. Im Folgenden werden diese Steuerbegünstigung und die Bedingungen dafür behandelt.

1 Allgemeiner Überblick

Die Hauptregelungen sind im Art. 60 Abs. 2 des Steuergesetzbuches zu finden, und das Verfahren und die Einzelheiten wurden im Laufe der Jahre durch die Zusammenarbeit mehreren Ministerien beschlossen.

2015 ist ein Beschluss durch die Zusammenarbeit mehreren Ministerien – Kommunikationsministerium, Bildungsministerium, Ministerium für Arbeit und Sozialpolitik und Finanzministerium – bezüglich der steuerlichen Vorteile in Kraft getreten. Vor dem Hintergrund, dass dieser Beschluss mehrere Fragen und Unklarheiten auf dem rumänischen Markt zur Folge hatte, gab es vom rumänischen Gesetzgeber 2016 einen neuen Beschluss Nr. 872/5932/2284/2903/2016 betreffend die Einbeziehung der EDV-Programme an der kreativen Arbeit.

Der Minister für Kommunikation hat mitgeteilt, dass ab August 2017 neue Regelungen betreffend die Steuerbefreiung für Angestellte mit sekundärem Bildungsabschluss veröffentlicht werden. Die Begünstigung soll ab Januar 2018 in Kraft treten und wird sowohl auf Angestellte mit

mittlerem Bildungsabschluss als auch auf den Outsourcing-Bereich erweitert werden.

2 Rechtliche Rahmenbedingungen

Damit die Softwareunternehmen von der Steuerbefreiung einen Vorteil ziehen können, sind mehrere Bedingungen sowohl auf der Seite des Arbeitsgebers als auch auf der Seite des Arbeitsnehmers zu erfüllen.

2.1 Bedingungen betreffend den Arbeitsgeber

Gemäß der neuen Verordnung ziehen die Arbeitnehmer der rumänischen juristischen Personen des öffentlichen Rechts von keiner Lohn- und lohnähnlicher Steuerbefreiung Vorteil. So bleiben als Befreiungsbegünstigte nur juristische Personen des privaten Rechts übrig.

Eine Neuheit ist auch die Tatsache, dass die im Laufe des Geschäftsjahres errichteten bzw. die gesetzlich unter Neuorganisierung befindlichen Gesellschaften von der Erfüllung der Umsatzerzielung aus der Softwareverlegung im Vorjahr, im Errichtungsjahr und im folgenden Jahr bzw. im Jahre ausgeschlossen sind, in dem die Neuorganisierung stattgefunden hat. Demzufolge ziehen die neu errichteten Gesellschaften sowie die umgewandelten Gesellschaften aus der Steuerbegünstigung einen Vorteil. Dies war nicht vorher möglich, da eine andere Bedingung bestand.

2.1.1 Tätigkeitsgegenstand

Es gab in der Praxis viele Fragen über den Gegenstand der befreiungsbegünstigten Gesellschaften. Eine der Unklarheiten für die Softwarehersteller war, ob auch die Verlegung von softwaresubsidiären Produkten von der Befreiung Vorteil ziehen. Durch die letzte Veränderung erklärt der Gesetzgeber diese Frage, indem er präzisiert, dass das Ziel der Softwareverlegung die Erlangung eines Endprodukts oder einer Komponente eines zur Vermarktung bestimmten Produkts ist.

Das Unternehmen soll einen bestimmten Tätigkeitsgegenstand durchführen. Der Tätigkeitsgegenstand erfolgt gemäß der Klassifizierung der Tätigkeiten in Rumänien,[1] die in der Gründungsurkunde der Gesellschaft vorgesehenen Tätigkeiten müssen die folgenden sein:

- NACE 5821 Verlegen von Computerspielen
- NACE 5829 Verlegen von sonstiger Software

[1] Ordnung Nr. 337/20.4.2007 des Nationalen Statistikinstituts über die Aktualisierung der Klassifizierung der Tätigkeiten in der nationalen Wirtschaft. Die NACE Tätigkeiten entsprechen den in der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft, Rev. 2 (2008) vorgesehenen Tätigkeiten.

- NACE 6201 Programmierungstätigkeiten
- NACE 6202 Erbringung von Beratungsleistungen auf dem Gebiet der Informationstechnologie
- NACE 6209 Erbringung von sonstigen Dienstleistungen der Informationstechnologie

Diese Tätigkeit muss bei der Betriebsstätte bzw. beim Firmensitz des Arbeitgebers erklärt werden.

2.1.2 Arbeitsplatzeinstufung

Der Arbeitgeber muss in den Arbeitsverträgen und in der Jobbeschreibung die EDV-spezialisierten Stellen angeben: Die betreffenden Arbeitnehmer müssen auf den folgenden Stellen angestellt werden (gemäß der Beilage zum gemeinsamen Ordnung Nr. *872/5932/2284/2903/2016*):

Datenbasisadministrator

Beschreibung: „Tätigkeiten für Fachgutachtung und praktische Assistenz im Management der Datenbasissysteme und in der Verwendung der Informationsdaten zum Reagieren bei den Erfordernissen des Informationssystems in jedem Lebenszykluszeitpunkt gemäß definierten Qualitätskriterien".

Analyst

Beschreibung: „Tätigkeiten für die Durchführung der Analyse zum Zwecke der Definierung der Spezifikationen für den tatsächlichen Bau solcher EDV-Systeme, die den Erfordernissen der Nutzer entsprechen".

Informatiksystemingenieur

Beschreibung: „Tätigkeiten, die analytische und Planfähigkeiten mit adäquaten Software- und Hardwarekenntnissen zum Zwecke der Definierung, Planung, Verlegung, Erprobung, Implementierung und Veränderung der EDV-Systeme verbinden, die Software als Hauptbestandteil enthalten".

EDV-Systemingenieur

Beschreibung: „Tätigkeiten für die Anpassung bzw. Harmonisierung der Hardware- bzw. Softwarelösungen und Betriebssysteme sowie der bestehenden oder den realen oder geschätzten Nutzernotwendigkeiten adaptierten Anwendungen, zum Zwecke der Erfüllung der Erfordernisse in Hinsicht auf die Deckung der Beanspruchungsebenen (Reaktionszeit)".

EDV-Projektmanager

Beschreibung: „Tätigkeiten für die Koordinierung der EDV-großanwendungsspezifischen Entwicklungssysteme, inkl. der Koordinierung des Personals und der Überwachung der Projekterfordernisse (notwendige Infor-

mationen/Daten, Programmierung, Analyse). Die Projektmanager entwickeln, planen, analysieren, schätzen und setzen Prioritäten für die zu verlegenden Komponenten, sowie für die Projektphasen und -termine".

Programmierer

Beschreibung: „Tätigkeiten für die Verlegung von Rechnerprogrammen gemäß vordefinierten Spezifikationen und für ihre Zusammensetzung in kohärente Systemen, inkl. der Erprobung zum Zwecke der Sicherung der Spezifikationsangemessenheit".

EDV-Systemplaner

Beschreibung: „Tätigkeiten, die analytische und Planfähigkeiten aufgrund Fachkenntnisse mit Software- und Programmierungssprachenkenntnissen zum Zwecke der Verlegung und Implementierung funktionaler Lösungen verbinden, die vordefinierten Erfordernissen bzw. organisationalen Notwendigkeiten entsprechen".

EDV-Systemprogrammierer

Beschreibung: „Tätigkeiten, die analytische und Planfähigkeiten mit adäquaten Software- und Hardwarekenntnissen zum Zwecke der Definierung, Planung, Verlegung, Erprobung, Implementierung und Veränderung der EDV-Systeme verbinden, die Software als Hauptbestandteil enthalten".

2.1.3 Organigramm des Arbeitgebers

Der Arbeitgeber muss in seinem Organigramm die EDV-spezialisierten Abteilungen in der Gesellschaft angeben. Die Stellen müssen Teil solcher EDV-spezialisierten Abteilungen sein, wie z.B. Rechenzentrum, Direktion, Abteilung, Amt, Dienst, Büro, Fach bzw. ähnliches.

2.1.4 Gesonderte Bilanzaufstellung

Eine zusätzliche Bedingung für einen nicht neugegründeten Unternehmer wäre die Durchführung der Softwaretätigkeiten im vorigen Jahr und eine gesonderte Eintragung des Einkommens aus dieser Tätigkeiten in seiner Bilanzaufstellung.

2.2 Bedingungen betreffend den Arbeitsnehmer

Die Bestimmungen der Verordnung gelten nicht nur für rumänische Staatsbürger, die bei der Programmierung tätig sind, sondern auch für ausländische Bürger der sonstigen EU-Mitgliedstaaten, des Europäischen Wirtschaftsraumes und der Schweiz, vorausgesetzt, dass ihre Diplome gemäß der rumänischen Gesetzgebung für gleichwertig erklärt werden. Das Diplom eines ausländischen Staatsbürgers muss mittels der Fachstrukturen des Ministeriums für Nationale Erziehung und Wissenschaftliche Forschung als gleichwertig erklärt werden.

Der Arbeitnehmer muss ein nach der Fertigstellung einer langfristigen Hochschulform bzw. der 1. Lizenzhochschulreihe gewährtes, durch eine akkreditierte Hochschulinstitution ausgestelltes Diplom innehaben.

2.3 Akte bei dem Arbeitgeber mit begünstigen Angestellter

Es ist wichtig, einen Dossier mit solchen Arbeitnehmern, die sich in diese Begünstigung einreihen, in der Gesellschaft zu führen. Der Dossier wird bei einer Kontrolle den zuständigen Organen vorgelegt. Der Dossier muss die folgenden Unterlagen enthalten:

- den Gesellschaftsvertrag mit dem entsprechenden Gegenstand (die oben erwähnten NACE-Codes);
- das Organigramm der Gesellschaft, wo die EDV-spezialisierten Abteilungen ersichtlich sind;
- für jeden Arbeitnehmer, der von der präferentiellen Behandlung Vorteil zieht:
- die Jobbeschreibung;
- eine beglaubigte Kopie des Studiendiploms;
- eine beglaubigte Kopie des Arbeitsvertrags;
- die getrennt erstellte Zahlungsliste für die Arbeitnehmer, die von der Lohnsteuerbefreiung Vorteil ziehen;
- die interne, vom befugten Führungsorgan des Arbeitgebers genehmigte Bestellung, die den Verlegungsvorgang von EDV-Programmen nachweist;
- die analytische Bilanz, in der sich die Erträge aus der Verlegung von EDV-Programmen distinkt gespiegelt werden.

Die Führung des Dossiers und die Einstufung des Angestellten als für die Steuerbefreiung begünstigter Angestellte ist die Aufgabe des Arbeitgebers, der dafür verantwortlich ist.

2.4 Vergleichsübersicht

Zur Hervorbringung des Unterschieds zwischen einem steuerbefreiungsbegünstigten und einem nichtbegünstigten Arbeitnehmer stellten wir eine Vergleichsübersicht mit der beispielsweisen Annahme eines verhandelten monatlichen Nettolohns von 7.500 lei (d.h. ca. EUR 1.666) zusammen. Es ist erkennbar, dass im unteren Beispiel ein Endjahreserlös sowohl für den Arbeitnehmer als auch für den Arbeitgeber 25.200 lei (d.h. ca. EUR 5.600) wäre.

Abrechnung Bruttogehalt	107,808 lei	8,984 lei	Abrechnung Bruttogehalt	128,340 lei	10,695 lei
Renten-versicherung 10.5 %	11,328 lei	944 lei	Angestellter mit Steuerbefreiung	Jahres-wert	Monatswert
Kranken-versicherung 5.5 %	5,940 lei	495 lei	Krankenversicherung 5.5 %	7,068 lei	589 lei
Arbeitslosen-versicherung 0.5 %	540 lei	45 lei	Arbeitslosen-versicherung 0.5 %	648 lei	54 lei
			Einkommen-steuer 16 %	17,148 lei	1,429 lei
Netto Gehalt	90,000 lei	7,500 lei	Netto Gehalt	90,000 lei	7,500 lei
Arbeitgeber-beiträge (15.8+5.2+0.5 +0.85+0.25+ 0.15) %	24,564 lei	2,047 lei	Arbeitgeber-beiträge (15.8+5.2+0.5+ 0.85+0.25+0.15)%	29,232 lei	2,436 lei
Arbeitgeber-kosten	132,372 lei	11,031 lei	Arbeitgeberkosten	157,572 lei	13,131 lei

2.5 Beispiele aus der Praxis – Freiberufler – steuerpflichtiges lokales Einkommen

Selbständiger Freiberufler	Jahres wert	Monats wert
Steuerpflichtiges lokales Einkommen 2017 Cluj	50,380 lei	
Einkommensteuer 16 %	8,061 lei	
Krankenver-sicherung 5.5 %	2,771 lei	
Renten-versicherung 10.5 %	5,290 lei	
Rentenver-sicherung 26.3 %	13,250 lei	
Steuerpflichtiges lokales Einkommen ohne MwSt. mit Renten-versicherung 10.5 %		
Netto jährliches Einkommen	116,250 lei	9,688 lei
Firma zahlt	132,372 lei	
Steuerpflichtiges lokales Einkommen ohne MwSt. mit Rentenver-sicherung von CAS 26.3 %		
Netto jährliches Einkommen	108,290 lei	9,024 lei
Firma zahlt	132,372 lei	

Selbständiger Freiberufler	Jahres wert	Monats wert
Steuerpflichtiges lokales Einkommen 2017 Bukarest	28,000 lei	
Einkommensteuer 16 %	4,480 lei	
Kranken-versicherung 5.5 %	1,540 lei	
Renten-versicherung 10.5 %	2,940 lei	
Renten-versicherung 26.3 %	7,364 lei	
Steuerpflichtiges lokales Einkommen ohne MwSt. mit Rentenver-sicherung von 10.5 %		
Netto jährliches Einkommen	123,412 lei	10,284 lei
Firma zahlt	132,372 lei	
Steuerpflichtiges lokales Einkommen ohne MwSt. mit Rentenver-sicherung von CAS 26.3 %		
Netto jährliches Einkommen	118,988 lei	9,916 lei
Firma zahlt	132,372 lei	

Trotz der Steuerbefreiungsvorteile bevorzugen einige Firmen in der Praxis, mit Freiberuflern zu arbeiten. In diesem Sinne haben wir eine Tabelle vorbereitet, um die Vorteile der Zusammenarbeit mit einem Freiberuflerprogrammierer im Vergleich zu einem Arbeitnehmer zu erkennen. In der Tabelle unter Pkt. 2.5 sind wir von dem Betrag ausgegangen, den der Arbeitgeber pro Jahr für einen Arbeitnehmer bezahlt, der 7,500 lei/ Monat, d.h. 132,372 Lei pro Jahr, erwirbt.

Ein anderer steuerlicher Vorteil für einen Freiberufler im Bereich der Software ist die Tatsache, dass er von der Einkommensnorm Vorteile zieht. Im Falle der Steuerpflichtigen, die Einkommen aus selbstständigen Tätigkeiten erwerben, und zwar andere Einkommen als aus freien Berufen und geistigen Eigentumsrechten, wird das jährliche Nettogewinn aufgrund Einkommensnormen am Ort der Tätigkeitsabwicklung festgesetzt.

Die Einkommensnorm stellt einen festen Betrag dar, der je nach der Gegebenheiten der Tätigkeit und des Tätigkeitsgebiets durch die territorialen öffentlichen Steuerverwaltungen[2] vorgeschrieben wird, vorausgesetzt dass sich die betreffende Tätigkeit im Verzeichnis der selbstständigen Tätigkeiten befindet, wofür das Nettoeinkommen aufgrund jährlicher Einkommensnormen festgestellt werden kann. In unserem Vergleich haben wir zwei Lokalitäten in Rumänien ausgewählt, wo die Softwareaktivität entwickelt ist, nämlich Cluj und Bukarest.

Die Einkommensnorm für das Jahr 2017 ist für diese Lokalitäten unterschiedlich, wie es aus der ersten Tabellenreihe ersichtlich ist, und zwar Cluj 50.380 lei, und Bukarest 28.000 lei.

Die Berechnungen werden für in Cluj und Bukarest eingetragene Freiberufler erstellt, die noch keine MwSt. bezahlt haben; das heißt, sie haben ein Einkommen unter 65.000 EUR pro Jahr und sie übersteigen die Einkommensstufe von 100.000 EUR pro Jahr nicht; über dieser Stufe würden sie von den Vorzügen der Einkommensnorm keinen Vorteil mehr ziehen.

Ein Freiberufler im Softwarebereich kann wählen, wieviel er beim Rentenversicherungsbudget zu bezahlen wünscht; er kann 10,5 % oder 26,3 % wählen, und die in diesem Sinne gemachten Kalkulationen sind auch in der Tabelle ersichtlich.

So kann man ersehen, dass bei Gesamtkosten einer Softwarefirma von 132,372 lei pro Jahr eine als Freiberufler organisierte Person einen jährlichen Nettoerlös von 108.290 lei/Jahr bzw. 9.024 lei/Monat in Cluj und

[2] Die Einkommensnorm wird durch die Steuerverwaltungen jährlich veröffentlicht. Die Einkommensnorm für 2017 befindet sich auf der ANAF Webseite https://static.anaf.ro/static/10/Anaf/AsistentaContribuabili_r/Normevenit2017/Norme.

118.988 lei/Jahr bzw. 9.916 lei/Monat in Bucuresti hat. Im Vergleich zum Einkommen eines Arbeitnehmers im EDV-Bereich, welches laut der Tabelle 2.4 7.500 lei pro Monat wäre, ist der Erlös eines Freiberuflers höher, und zwar 9.024 lei/Monat in Cluj und 9.916 lei/Monat in Bukarest. Einige Gesellschaften bevorzugen die Zusammenarbeit mit einem Freiberufler auch wegen der Tatsache, dass in diesem Fall die Haftung an den letzten transferiert wird.

Aber die Zusammenarbeit mit einem Freiberufler kann nicht mit der gleichen Konstanz wie bei einem Arbeitsvertrag mit einem Arbeitnehmer erfolgen. Widrigenfalls gibt es die Möglichkeit einer Steuerprüfung, in der das verträgliche Verhältnis zu einem Freiberufler als ein klassisches Arbeitnehmer-/Arbeitgeber-Verhältnis neu klassifiziert werden kann.

Mit dem Ziel, der Abwanderung von Programmierern entgegenzuwirken, hat der rumänische Staat für den EDV-Bereich Privilegierungen in Form steuerrechtlicher Erleichterungen verabschiedet, die die Arbeitnehmer von der Zahlung der Steuer auf gehaltsartige Einkommen befreit. Neben den gehaltsbezogenen Möglichkeiten bestehen für den Unternehmer im Softwarebereich auch sonstige steuerliche Vorteile. Folglich ist Rumänien zu einem wichtigen Hub für große EDV- und Programmierungsgesellschaften geworden. Die durch ANIS[118] veröffentliche Studie sagt voraus, dass der Software- und EDV-Dienstleistungsbereich 2019 den Umsatz von 5,5 Milliarden Euro erzielen wird. Nach der auffallenden gegenwärtigen Entwicklung werden die Exporte von EDV-Produkten gegen Ende dieses Jahrzehntes moderat erhöht werden. Aber Einschätzungen aus der Industrie erwarten eine Erhöhung des internen Markts, der zurzeit bei etwa einer Milliarde Euro pro Jahr liegt.

LITERATUR

Pierre Audoin Consultants: Studie von Pierre Audoin Consultants für ANIS (Arbeitgeberverband der Software- und Service-Industrie in Rumänien) Software and IT Services in Romania, 3 Aufl., 2016.

Seceleanu, Adrian: Studiu ANIS: Industria de software şi servicii IT a depăşit în 2015 valoarea de 3 miliarde de euro (de. Die Softwareindustrie hat 3 Millarden EUR in 2015 überschritten), Ziarul Financiar 19.5.2016 (http://www.zf.ro/business-hi-tech/studiu-anis-industria-de-software-si-servicii-it-a-depasit-in-2015-valoarea-de-3-miliarde-de-euro-1534 3421)

Muscalu, Stelian: Industria IT&C a ajuns la 5,6 % din PIB (de. Die Softwareindustrie erreichte 5,6 % des Bruttoinlandsproduktes) Digi 24, mai 2016 (http://www.digi24.ro/stiri/actualitate/evenimente/industria-itc -a-ajuns-la-56-din-pib-519750)

Industria IT in Romania, 15.1.2016, (http://pgrom.ro/indus tria-it-in-romania/)

STRAFTATBESTÄNDE DER COMPUTER-KRIMINALITÄT IN DEUTSCHLAND UND RUMÄNIEN

Dr. Sebastian J. Golla/Stefanie Winkler

Johannes Gutenberg-Universität Mainz
golla@uni-mainz.de

Zusammenfassung

Dieser Beitrag betrachtet die Straftatbestände der Computerkriminalität in Deutschland und Rumänien. Er konzentriert sich hierbei auf die Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen nach Art. 2 – Art. 5 Cybercrime Convention (CCC) und versucht, die wichtigsten Unterschiede der beiden Regelungsregime aufzuzeigen.

1 Computerkriminalität in Deutschland und Rumänien

Die Computerkriminalität ist ein seit langer Zeit ein wachsendes internationales Phänomen. Welche Risiken von globalem Ausmaß etwa von Hackerangriffen ausgehen, belegte zuletzt eindrucksvoll der Fall „Wannacry“: Anfang Mai 2017 gelang es Hackern, eine Sicherheitslücke in Windows-Programmen auszunutzen, dadurch Computersysteme zu befallen und darauf Daten zu verschlüsseln. Zur Freigabe der Daten forderten die Hacker von den Betroffenen die Zahlung von Lösegeld unter Androhung, diese ansonsten zu löschen. Betroffen waren Computersysteme in über hundert Ländern, darunter solche von Großunternehmen wie Renault oder der Deutsche Bahn AG.[1]

Auch in Deutschland und Rumänien ist die Computerkriminalität von hoher Relevanz. In Deutschland belegt dies die Polizeiliche Kriminalstatistik (PKS) des BKA für das Jahr 2016,[2] nach der 107.751 Fälle von Computerkriminalität mit einem Anteil von ca. 1,69 % an der Kriminalität

[1] Frankfurter Allgemeiner Zeitung vom 15. Mai 2017, abrufbar unter http://www.faz.net/agenturmeldungen/dpa/was-steckt-hinter-der-erpressungs-software-wanna-cry-15016863.html (zuletzt abgerufen am 24. Mai 2017).

[2] BKA, Polizeiliche Kriminalstatistik, 2016, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2016/pks2016_node.html (abgerufen am 24. Mai 2017).

insgesamt[3] erfasst wurden. Auch angesichts der Häufung schadensträchtiger Fälle ist das Thema der Computerkriminalität aktueller denn je. In Rumänien existiert zwar keine umfassende öffentliche Statistik über das Aufkommen der Computerkriminalität, nach Angaben der rumänischen Polizei gab es aber allein im Jahr 2016 in diesem Bereich 3.848 Strafanzeigen, es kam zu 900 Vernehmungen und die rumänische Polizei deckte 30 auf Computerkriminalität spezialisierte kriminelle Vereinigungen auf.[4] Auch international wird Rumänien als Herkunftsland von Cyberattacken wahrgenommen. Die Stadt Râmnicu Vâlcea in der Kleinen Walachei erlangte beispielsweise zweifelhaften Ruhm als Metropole des internationalen Online- und Kreditkartenbetrugs.[5]

Freilich lässt sich Computerkriminalität kaum als nationales Phänomen betrachten. Es ist ein internationales Anliegen, sie zu bekämpfen. Um dies zu ermöglichen, ist eine gewisse Harmonisierung der rechtlichen Regelungen unumgänglich. Die Cybercrime Convention (CCC)[6] ist dabei das aktuell wichtigste Harmonisierungsinstrument. Dieses Übereinkommen des Europarates wurde 2001 ausgehandelt. Unterzeichner waren neben den Mitgliedsstaaten des Europarates (darunter Deutschland und Rumänien) auch Japan, Kanada und die USA. Durch Verbesserung der internationalen Kooperation, Harmonisierung nationaler Vorschriften und Entwicklung einheitlicher Ermittlungsinstrumente sollte eine wirksame Bekämpfung der Datennetzkriminalität bewirkt werden.

---

[3] Unter Computerkriminalität versteht die PKS Internetkriminalität sowie Computerkriminalität im engeren Sinne. Als Internetkriminalität werden alle Delikte erfasst, bei denen das Internet als Tatmittel eingesetzt wird. In Betracht kommen etwa Äußerungs- und Verbreitungsdelikte (z.B. Drohungen per Email) sowie Straftaten, bei denen „das Internet als Kommunikationsmedium bei Tatbestandsverwirklichung" genutzt wird. Unter den Begriff der Computerkriminalität im engeren Sinne fallen Straftaten, „bei denen EDV als Tatbestandsmerkmal genannt ist" (§§ 202a ff., § 263 f., 269, 270, 303 a f. StGB-De und Vorschriften des UrhG); vgl. BKA, Richtlinien für die Führung der Polizeilichen Kriminalstatistik i.d.F. vom 1. Januar 2016, S. 12 f., abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2016/pks2016_node.html (zuletzt abgerufen am 24. Mai 2017); LKA BW, Cyberkrimi-nalität/Digitale Spuren, S. 39 f., abrufbar unter https://www.polizei-bw.de/Dienststellen/LKA/Documents/2012_Cyberkriminalitaet_Digitale_Spuren.pdf (zuletzt abgerufen 24. Mai 2017).

[4] Poliția Română, Atacurile cibernetice: Criminalitatea din spatele monitorului, abrufbar unter https://www.politiaromana.ro/ro/comunicate/atacurile-cibernetice-criminalitatea-din-spatele-monitorului (zuletzt abgerufen am 24. Mai 2017).

[5] Bhattacharjee, How A Remote Town In Romania Has Become Cybercrime Central, abrufbar unter https://www.wired.com/2011/01/ff_hackerville_romania/all/1 (zuletzt abgerufen am 24. Mai 2017).

[6] Convention on Cybercrime; vgl. Gesetz zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität (BGBl. 2008, Teil II Nr. 30, S. 1242).

Die CCC verpflichtet ihre Mitgliedstaaten auch dazu, Maßnahmen zur Harmonisierung des materiellen Strafrechts zu treffen. Dies betrifft unter anderem die Regelung der Strafbarkeit von Urheberrechtsverletzungen, Computerbetrug, Kinderpornographie und Verstößen gegen die Sicherheit von Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen („CIA"-Delikte). Letzterer Bereich lässt sich als Computerkriminalität im engeren Sinne verstehen.[7] Es handelt sich um Straftatbestände, die sich tatbestandlich auf Computersysteme und Daten beziehen und diese selbst schützen. Dieser Beitrag beschränkt sich auf eine Betrachtung dieser Delikte im deutschen und rumänischen Recht. Die Strafbarkeit von Vorbereitungshandlungen im Sinne von Art. 6 CCC (§§ 202c, 303a Abs. 3, 303b Abs. 5 StGB-De und Art. 365 StGB-Ro) soll hierbei zunächst außen vor bleiben.

In der CCC finden sich die Regelungen zu diesen Delikten in Art. 2 – Art. 5, im deutschen Strafgesetzbuch (StGB-De) in §§ 202a ff., 303a f. sowie im rumänischen Strafgesetzbuch (StGB-Ro)[8] in Art. 360 ff. Das StGB-Ro und mit ihm die Delikte der Computerkriminalität wurden zuletzt in den Jahren 2009 und 2012 grundsätzlich reformiert.[9] Die Änderungen traten am 1. Februar 2014 in Kraft.[10]

2 „CIA"-Delikte im deutschen und rumänischen Recht

Schon systematisch sind die Regelungen im deutschen und rumänischen Recht unterschiedlich verortet. Im StGB-Ro sind die „CIA"-Delikte als Taten gegen die Sicherheit und Integrität von Computersystemen und Daten im StGB-Ro in einem Zusammenhang geregelt.[11] Im StGB-De hingegen finden sich die Delikte verteilt auf zwei Abschnitte: Während die Strafbarkeit des rechtswidrigen Zugangs und rechtswidrigen Abfangens im 15. Abschnitt des besonderen Teils unter den Delikten zum Schutze

---

[7] Es gibt allerdings unterschiedliche Verständnisse des Begriffes Computerkriminalität; vgl. LKA BW, Cyberkriminalität/Digitale Spuren, S. 39 f. abrufbar unter https://www.polizeibw.de/Dienststellen/LKA/Documents/2012_Cyberkriminalitaet_Digitale_Spuren.pdf (zuletzt abgerufen am 24. Mai 2017).

[8] Auf Englisch abrufbar unter http://www.legislationline.org/documents/section/ criminal-codes/country/8 (zuletzt abgerufen am 24. Mai 2017).

[9] Vgl. dazu *Ioniță*, The major modifications of legal provisions of the cybercrime offences made by the legislator in the process of implementation of the new criminal code, Union of Jurists of Romania Law Review 2014, 32 ff., abrufbar unter http://www.internationallawreview.eu/fisiere/pdf/5_2.pdf (zuletzt abgerufen am 24. Mai 2017).

[10] Art. 246 Gesetz Nr. 187/2012, veröffentlicht im Gesetzblatt Rumäniens, Teil 1, Nr. 757.

[11] Titel VII, Kapitel VI des besonderen Teils StGB-Ro.

des persönlichen Lebens- und Geheimbereichs geregelt sind (§§ 202a ff. StGB-De), findet sich die Strafbarkeit des Eingriffs in Daten und Systeme im 27. Abschnitt im Zusammenhang mit der Sachbeschädigung (§§ 303a f. StGB-De). Der Grund für diese Aufteilung der Regelungen liegt darin, dass der Gesetzgeber die Strafbarkeit des Zugangs zu und des Abfangens von Daten in einem Sachzusammenhang mit der Verletzung des Briefgeheimnisses (§ 202 StGB-De) und der Vertraulichkeit des Wortes (§ 201 StGB-De) sah, obwohl Zugang und Abfangen keine Verletzungen des persönlichen Lebens- oder Geheimbereichs voraussetzen.[12]

2.6 Rechtswidriger Zugang und rechtswidriges Abfangen (Art. 2 und Art. 3 CCC)

2.6.1 Zugang zu Daten und Computersystemen

Art. 2 CCC verpflichtet die Vertragsparteien, den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon unter Strafe zu stellen. Typische hiervon erfasste Phänomene sind Password Cracking und Phishing.

2.6.1.1 Deutschland

Im deutschen Recht setzt § 202a StGB-De Art. 2 CCC um. Strafbar macht sich nach § 202a Abs. 1 StGB-De, „[w]er unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft." Geschütztes Rechtsgut ist das formelle Datengeheimnis[13] bzw. die formelle Verfügungsbefugnis[14] an Daten. § 202a StGB-De setzt keine inhaltliche Qualität der geschützten Daten voraus. Dies wird in der Literatur zum Teil kritisiert.[15]

Tatobjekt sind nicht für den Täter bestimmte und besonders gesicherte Daten. Gemäß § 202a Abs. 2 StGB-De sind nur solche Daten erfasst, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Sinnlich wahrnehmbare Daten sind vom Tatbestand damit nicht erfasst. Dies betrifft etwa ausgedruckte Informationen oder Barcodes.[16] Ungesicherte Daten werden durch § 202a

[12] BT-Drs. 10/5058, S. 28.

[13] BT-Drs. 10/5058, S. 29; *Graf*, in: MüKo-StGB, 2. Aufl. 2012, § 202a Rn. 2.; *Weidemann*, in: v. Heintschel-Heinegg, StGB, § 202a Rn. 2.

[14] *Fischer*, StGB, 64. Aufl. 2017, § 202a Rn. 2; Weidemann, in: v. Heintschel-Heinegg, StGB, § 202a Rn. 2.

[15] Vgl. *Hilgendorf*, in: LK-StGB, § 202a Rn. 6.

[16] *Graf*, in: Müko-StGB, § 202a Rn. 17; *Hilgendorf*, in: LK-StGB, § 202a StGB Rn. 10; *Welp*, CR 1992, S. 291 ff.

nicht geschützt.[17] Die tatbestandlich erforderliche Zugangssicherung erfordert allerdings kein besonders hohes Schutzniveau.[18] In der Überwindung der Zugangssicherung (z.B. einem Passwort) manifestiert sich eine kriminelle Energie, die die Strafwürdigkeit begründet.[19]

Tathandlung ist das Verschaffen des Zugangs zu den Daten für sich oder einen anderen. Eine Kenntnisnahme der Daten ist hierzu nicht erforderlich; es genügt bereits eine Zugriffsverschaffung zu dem Informations- oder Computersystem im Sinne eines „elektronischen Hausfriedensbruchs".[20] Eine Strafbarkeit des Versuchs ist nicht vorgesehen. Begründet wurde dies mit der Gefahr der Überkriminalisierung und der ebenso fehlenden Strafbarkeit des Versuchs in § 202 StGB-De und der Strafvorschrift des BDSG.[21] Der Strafrahmen beträgt bis zu drei Jahre Freiheitsstrafe oder Geldstrafe.

2.6.1.2 Rumänien

Im rumänischen Recht setzt Art. 360 StGB-Ro Art. 2 CCC um. Nach Art. 360 Abs. 1 StGB-Ro ist der unbefugte Zugang zu einem Computersystem mit Strafe bedroht. Der Tatbestand formuliert hierfür keine weiteren einschränkenden Voraussetzungen und ist in mehrerlei Hinsicht weiter als § 202a Abs. 1 StGB-De. Zunächst sind nicht Daten, sondern Computersysteme Tatobjekt. Der Begriff des Computersystems wird hierbei im Sinne von Art. 1 lit. a) CC auszulegen sein.[22] Zwar geht der Zugang zu einem Computersystem grundsätzlich mit dem Verschaffen von Daten einher, allerdings erfasst der Zugang zu Systemen auch bereits die bloße Möglichkeit jedweden Datenzugriffs auf diesen und erleichtert zumindest praktisch die für eine Verurteilung notwendige Feststellung strafbaren Verhaltens.[23]

Dem Wortlaut nach ist keine besondere Zugangssicherung erforderlich, weshalb auch ungesicherte Systeme unter den Tatbestand fallen können. Dies wird auch im systematischen Zusammenhang mit der Qualifikation in Abs. 3 klar, die eine besondere Zugangssicherung erfordert. Dies ist ein

---

[17] BT Drucks. 16/3656, S. 10.

[18] *Ernst*, NJW 2003, S. 3233 (3236); *Fischer*, StGB, § 202a Rn. 9.

[19] *Hilgendorf*, in: LK-StGB, § 202a StGB Rn. 3.

[20] *Ernst*, NJW 2007, S. 2661 (2661); *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 18.

[21] BT-Drucks. 10/5058, S. 28.

[22] Ein Computersystem ist demnach „eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen".

[23] BT-Drucks. 18/10182, S. 12.

gravierender Unterschied zum deutschen Recht. Auch der Versuch der Tat ist – anders als im deutschen Recht – gemäß Art. 366 StGB-Ro mit Strafe bedroht.

Im Vergleich zum deutschen Recht ist auch der erhöhte Strafrahmen auffällig. Der rechtswidrige Zugang zu einem Computersystem ist mit Freiheitsstrafe von drei Monaten bis drei Jahren oder Geldstrafe bedroht.

Artikel 360 Abs. 2 und Abs. 3 StGB-Ro regeln außerdem Qualifikationen zu dem Tatbestand in Abs. 1. Handelt der Täter, um Computerdaten zu erlangen, wird er gemäß Artikel 360 Abs. 2 StGB-Ro mit Freiheitsstrafe von nicht unter sechs Monaten und bis zu fünf Jahren bestraft. Artikel 360 Abs. 3 StGB-Ro sieht eine Freiheitsstrafe von nicht unter zwei Jahren und bis zu sieben Jahren vor, wenn die Tat sich auf ein Computersystem bezieht, zu dem der Zugang für bestimmte Nutzer durch Verfahren, Geräte oder spezialisierte Programme eingeschränkt oder verboten ist. Damit ist die Qualifikation in Art. 360 Abs. 3 StGB-Ro im Ergebnis eher mit § 202a Abs. 1 StGB-De vergleichbar als der Grundtatbestand in Abs. 1, da nur hier eine besondere Zugangssicherung vorausgesetzt wird.[24] Der überaus hohe Strafrahmen ist bei diesem Tatbestand besonders auffällig. Die Vorgängervorschrift Art. 42 Abs. 3 Gesetz Nr. 161/2003 sah sogar einen noch höheren Strafrahmen von drei bis zwölf Jahren Freiheitsstrafe vor.[25]

2.6.2 Abfangen von Übermittlungen

Gemäß Artikel 3 CCC sind die Mitgliedsstaaten verpflichtet, das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, unter Strafe zu stellen. Typische Phänomene sind dabei das Abhören von Leitungen oder WLANs.

2.6.2.1 Deutschland

Umgesetzt wurde diese Vorschrift im deutschen Recht in § 202b StGB-De. Nach dieser Norm wird mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe bestraft, wer sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Dateien im Sinne des § 202a Abs. 2 StGB-De aus einer nicht öffentlichen Datenübermittelung oder aus

[24] Die Vorgängervorschrift von Art. 360 Abs. 3 StGB-Ro sprach lediglich von „Sicherungsmaßnahmen“, Art. 42 Abs. 3 Gesetz Nr. 161/2003.

[25] Vgl. *Ioniță*, The major modifications of legal provisions of the cybercrime offences made by the legislator in the process of implementation of the new criminal code, Union of Jurists of Romania Law Review 2014, S. 32 (34 f.).

einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Geschütztes Rechtsgut ist wie bei § 202a StGB-De das formelle Geheimhaltungsinteresse des Verfügungsberechtigten.[26]

Für den Datenbegriff gilt die Legaldefinition des § 202a Abs. 2 StGB-De. Anders als bei § 202a StGB-De müssen die Daten aber nicht besonders gesichert sein. Erfasst werden alle Formen der elektronischen Datenübermittelung, unabhängig davon, ob die Übermittelung leitungsgebunden oder etwa per Funk erfolgt.[27] Unter den Tatbestand fallen jedoch nur Daten, die sich im Zeitpunkt der Tat in einem Übertragungsvorgang befinden. Nicht erfasst werden bereits gespeicherte Daten, die früher übermittelt wurden.[28] Zudem dürfen die Daten nicht für den Täter bestimmt sein.[29] Nicht öffentlich ist die Datenübermittelung, wenn sie sich an einen beschränkten Personenkreis richtet.[30] Dabei kommt es nicht auf Art oder Inhalt der Daten an.[31]

Erweitert wird der Tatbestand durch die Tatvariante der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage (z.B. WLAN-Router).[32] Im Gegensatz zur ersten Tatvariante ist es nicht erforderlich, dass die Daten aus einer Übermittlung abgefangen werden. Vielmehr genügt das Verschaffen gespeicherter oder rechnerintern verarbeiteter Daten.[33] Mit dem Merkmal „unter Anwendung von technischen Mitteln" erfährt der Tatbestand eine Einschränkung, die eine Überkriminalisierung verhindern soll.[34] Dennoch ist dieses Merkmal weit auszulegen, so dass auch Codes, Passwörter und Software einbezogen werden.[35] Anders als in § 202a StGB-De reicht als Tathandlung nicht das bloße Verschaffen des Zugriffs aus. Vielmehr ist das Erlangen der Verfügungsmacht über die Daten notwendig.[36] Ebenso wie bei § 202a StGB-De ist bei § 202 b StGB-De der Versuch nicht mit Strafe bedroht.

---

[26] BT-Drs. 16/3656, S. 11; *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 2.

[27] *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 3f.

[28] BT-Drs. 16/3656, S. 11; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 202b Rn. 4; *Eisele*, in: Schönke/Schröder, StGB, § 202 b Rn. 4.

[29] *Fischer*, StGB, § 202b Rn. 3.

[30] *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 4a.

[31] *Hilgendorf*, in: LK-StGB, § 202b Rn. 9.

[32] *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 5.

[33] *Graf*, in: Müko-StGB, § 202b Rn. 13.

[34] BT-Drs. 16/3656, S. 11.

[35] BT-Drs. 16/3656, S. 11; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 202b Rn. 7.

[36] *Hilgendorf*, in: LK-StGB, § 202b Rn.13.

2.6.2.2 Rumänien

Im rumänischen Recht setzt Art. 361 StGB-Ro Art. 3 CCC um. Nach Art. 361 Abs. 1 StGB-Ro wird mit nicht unter einem Jahr und bis zu fünf Jahren Freiheitsstrafe bestraft, wer unbefugt eine Übermittlung von Computerdaten, die nicht öffentlich ist und für ein solches Computersystem bestimmt ist, aus einem solchen Computersystem stammt oder innerhalb eines Computersystems durchgeführt wird, abfängt. Dieser Tatbestand ist § 202b StGB-De sehr ähnlich.

Während in § 202b StGB-De die Rede von einer Datenverarbeitungsanlage ist, stellt Art. 361 StGB-Ro auf den Begriff des Computersystems ab. Hieraus ergeben sich allerdings allenfalls marginale Unterschiede. Nach Art. 1 lit. a) CCC handelt es sich bei einem Computersystem um „eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen". Unter dem Begriff der Datenverarbeitungsanlage versteht man die funktionelle Einheit von Geräten, die die Datenverarbeitung ermöglicht.[37]

Die von Art. 361 StGB-Ro erfassten Tathandlungen erscheinen dadurch etwas weiter als bei § 202b StGB-De, dass zumindest der Wortlaut der rumänischen Regelung eine Anwendung von technischen Mitteln nicht erfordert. Nach Art. 361 StGB-Ro Abs. 2 ist auch das unbefugte Abfangen von elektromagnetischen Abstrahlungen aus einem Computersystem, die Träger von Computerdaten mit nichtöffentlichen Informationen sind, strafbar. Es gilt der gleiche Strafrahmen wie nach Abs. 1. Der Versuch der Tat ist gemäß Art. 366 mit Strafe bedroht.

Auch bei Art. 361 StGB-Ro ist der im Vergleich zum deutschen Recht deutlich höhere Strafrahmen auffällig, wobei auch hier der Strafrahmen gegenüber der Vorgängervorschrift nach unten verschoben wurde.[38]

2.7 Eingriff in Daten und Systeme (Art. 4 und Art. 5 CCC)

2.7.1 Eingriff in Daten

Nach Art. 4 Abs. 1 CCC haben die Vertragsparteien das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe zu stellen.[39]

---

[37] *Weidemann*, in: Heintschel-Heinegg, StGB, § 303b Rn. 13.

[38] Art. 43 Gesetz Nr. 161/2003; vgl. *Ioniță*, The major modifications of legal provisions of the cybercrime offences made by the legislator in the process of implementation of the new criminal code, Union of Jurists of Romania Law Review 2014, S. 32 (35).

2.7.1.1 Deutschland

In Deutschland setzt § 303a Abs. 1 StGB-De Art. 4 Abs. 1 CCC um. Demnach macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Geschützt wird das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit von Daten.[40] Auf einen wirtschaftlichen, wissenschaftlichen oder ideellen Wert kommt es dabei nicht an.[41] Tatobjekt sind Daten i.S.d. § 202a Abs. 2 StGB-De, wobei eine besondere Sicherung nicht erforderlich ist.[42]

Die „Fremdheit" der Daten wird nicht als Voraussetzung angesehen, der Tatbestand ist aber einschränkend auszulegen: Geschützt sind lediglich Daten, über die ein anderer die Verfügungsbefugnis hat.[43] Tathandlungen sind das Löschen (Unlesbarmachen), Unterdrücken (dem Berechtigten entziehen), Unbrauchbarmachen (bestimmungsgemäßen Gebrauch beeinträchtigen) oder Verändern (inhaltliche Umgestaltung) von Daten. Durch Überschneidungen der Tathandlungsbeschreibungen soll ein umfassender Schutz erreicht werden.[44]

Gemäß Absatz 2 ist auch der Versuch strafbar. Die Tat ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bedroht.

2.7.1.2 Rumänien

In rumänischem Recht ist Art. 4 CCC in Art. 362 StGB-Ro umgesetzt. Nach dieser Norm wird mit nicht unter einem Jahr und bis zu fünf Jahren Freiheitsstrafe bestraft, wer rechtswidrig Computerdaten verändert, löscht, unbrauchbar macht oder den Zugang zu solchen Daten beschränkt. Der Versuch ist wie im deutschen Recht strafbar (Art. 366 StGB-Ro). Auch hier wurde der Strafrahmen gegenüber der Vorgängerregelung herabgesetzt,[45] bleibt aber im Vergleich zum deutschen Recht überaus hoch.

2.7.2 Eingriff in ein System

Art. 5 CCC verpflichtet die Mitgliedsstaaten, die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Über-

---

[39] Nach Abs. 2 der Vorschrift könne sich die Vertragsparteien das Recht vorbehalten, als Voraussetzung vorzusehen, dass das Verhalten zu einem schweren Schaden geführt haben muss.

[40] *Haft*, NStZ 1987, S. 6 (10); *Hoyer*, in: SK-StGB, § 303a Rn. 2.

[41] *Fischer*, StGB, § 303a Rn. 2.

[42] *Hoyer*, in: SK-StGB, § 303a Rn. 3.

[43] *Hilgendorf*, in: Satzger/Schluckebier/Widmaier, StGB, § 303a Rn. 5.

[44] *Fischer*, StGB, § 303a Rn. 8; *Weidemann*, in: v. Heintschel-Heinegg, StGB, § 303a Rn. 7.

[45] Art. 44 Abs. 1 Gesetz Nr. 161/2003.

mitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe zu stellen.

2.7.2.1 Deutschland

Im deutschen Recht setzt § 303b StGB-De Art. 5 CCC um. Nach § 303 b Abs. 1 StGB-De wird mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er eine Tat nach § 303a Abs. 1 StGB-De begeht, Daten im Sinne von § 202 a Abs. 2 StGB-De in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert. Geschütztes Rechtsgut ist das Interesse am störungsfreien Funktionieren einer eigenen oder fremden Datenverarbeitung, da Beeinträchtigungen empfindliche (wirtschaftliche) Schäden verursachen können.[46] Der Begriff der Datenverarbeitung ist weit auszulegen,[47] erfährt jedoch über das Merkmal „von wesentlicher Bedeutung" eine Einschränkung.[48]

Als Tathandlungen nennt § 303b Abs. 1 StGB-De die Veränderung von Daten,[49] das Eingeben (Zuführen) oder Übermitteln (Weiterleitung) von Daten mit Schädigungsabsicht[50] und einen Sacheingriff in eine Datenverarbeitungsanlage oder einen Datenträger (äußerliche Einwirkung).[51] Als Taterfolg muss eine erhebliche Störung, d.h. eine nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs der Datenverarbeitung eingetreten sein.[52] Erheblich ist eine Beeinträchtigung, wenn für die Beseitigung ein „beträchtlicher Aufwand entweder an Zeit, an Mühen oder an Kosten" notwendig ist.[53]

§ 303b Abs. 2 StGB-De regelt eine Qualifikation zu Abs. 1. Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, liegt der Strafrahmen bei bis zu fünf Jahren Freiheitsstrafe oder Geldstrafe. Die

---

[46] *Wolff*, in: LK-StGB, § 303b Rn. 1.

[47] BT-Drs. 10/5058, S. 35; vgl. auch § 3 Abs. 4 BDSG 2009.

[48] Vgl. *Wolff*, in: LK-StGB, § 303a Rn. 4.

[49] Im Sinne von §§ 303a Abs. 1, 202a Abs. 2 StGB-De. Es handelt sich um eine Qualifikation zu § 303a StGB-De; *Fischer*, StGB, § 303 b Rn. 11; *Hoyer*, in: SK-StGB, § 303b Rn. 14.

[50] Durch diese Tatvariante werden beispielsweise „Denial-of-Service-Attacken" erfasst; *Stree/Hecker*, in: Schönke/Schröder, StGB, § 303b Rn. 7.

[51] *Hoyer*, in: SK-StGB, § 303b Rn. 14.

[52] *Fischer*, StGB, § 303b Rn. 9.

[53] *Schumann*, NStZ 2007, S. 675 (679); *Hoyer*, in: SK-StGB, § 303b Rn. 7.

Begriffe Betrieb und Unternehmen werden dabei weit ausgelegt. Beispielsweise ist auch eine karitative Einrichtung vom Normzweck erfasst.[54] Das Kriterium „von wesentlicher Bedeutung" liegt bei einer Datenverarbeitung für einen Betrieb vor, wenn sie „für die Organisation und die Verwaltungs- und Arbeitsabläufe grundlegend" ist, so dass die nötigen Daten zumindest vorübergehend nicht zur Verfügung stehen oder nur durch erheblichen Mehraufwand eingeholt werden können.[55] Bei Privatpersonen ist auf die Bedeutung der Datenverarbeitung für die Lebensgestaltung abzustellen.[56] Als wesentlich gelten Daten, wenn sie der Erwerbstätigkeit, der wissenschaftlichen, künstlerischen oder schriftstellerischen Tätigkeit dienen.[57]

§ 303b Abs. 4 StGB-De enthält eine Strafzumessungsregel für besonders schwere Fälle. Solche liegen unter anderem vor, wenn ein großer Vermögensverlust bei Betrieben, Unternehmen oder Behörden entsteht, die Tat gewerbs- oder bandenmäßig begangen wird oder schwere Folgen für die Allgemeinheit entstehen.[58] Der Versuch ist gemäß § 303b Abs. 3 StGB-De mit Strafe bedroht.

2.7.2.2 Rumänien

Im rumänischen Recht ist Art. 5 CCC in Art. 363 StGB-Ro umgesetzt. Mit zwei bis sieben Jahre Freiheitsstrafe wird bestraft, wer unbefugt den Betrieb eines Computersystems erheblich stört, indem er Daten eingibt, überträgt, verändert, löscht oder beschädigt oder den Zugriff auf Daten beschränkt.

Im Tatbestand finden sich im Gegensatz zu § 303b StGB-De kaum einschränkende Voraussetzungen. Anders als in § 303b StGB-De ist vor allem nicht Voraussetzung, dass Datenverarbeitungsvorgänge „von wesentlicher Bedeutung" sind, womit Art. 363 StGB-Ro zumindest dem Wortlaut nach auch Bagatellfälle umfasst. Eine einschränkende Auslegung könnte jedoch aufgrund der hohen Strafandrohung erfolgen. Es besteht zudem zumindest die Voraussetzung einer „erheblichen" Beeinträchtigung. Auch eine Schädigungsabsicht ist bei den Tathandlungen „Eingeben" und „Übertragen" in Art. 363 StGB-Ro nicht Voraussetzung.

Im Vergleich zum deutschen Recht ist auch hier der hohe Strafrahmen (zwei bis sieben Jahre Freiheitsstrafe) auffällig. Die Vorgängervorschrift

[54] *Fischer*, StGB, § 303b Rn. 15.

[55] *Winkelbauer*, CR 1986, S. 824 (830); *Hoyer*, in: SK-StGB, § 303b Rn. 11.

[56] *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 303b Rn. 5.

[57] Vgl. BT-Drs. 16/3656, S. 13.

[58] *Wolff*, in: LK-StGB, § 303b Rn.34; BT-Drs. 16/3656, S. 14.

Artikel 45 Gesetz Nr. 161/2003 sah für Eingriffe in den Betrieb von Computersystemen sogar einen noch höheren Strafrahmen von drei bis zu fünfzehn Jahren Freiheitsstrafe vor.[59] Anders als § 303b StGB-De regelt Art. 363 StGB-Ro keine Qualifikation oder besonders schwere Fälle.

2.8 Datenübermittlung

Eine Strafbarkeit der Übermittlung bzw. Übertragung von Daten ist in Kapitel II Abschnitt 1 Titel 1 der CCC nicht direkt vorgesehen. Allerdings enthalten sowohl das deutsche als auch das rumänische Recht im Zusammenhang mit den „CIA"-Delikten Straftatbestände, die sich vor allem auf die Übermittlung von Daten beziehen.

2.8.1 Deutschland

In Deutschland ist vor allem § 202d StGB-De zu nennen, der die „Datenhehlerei" unter Strafe stellt. Nach § 202d Abs. 1 StGB-De macht sich strafbar, wer Daten im Sinne von § 202a Abs. 2 StGB-De, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Der seit 18. Dezember 2015 geltende Tatbestand soll dazu dienen, Strafbarkeitslücken beim Handel mit rechtswidrig erlangten Daten wie Kreditkartendaten oder Zugangsdaten zu Online-Banking, E-Mail-Diensten oder sozialen Netzwerken im Internet bzw. Darknet zu schließen.[60] Schützen soll der Tatbestand das formelle Datengeheimnis bzw. die formelle Verfügungsbefugnis an Daten.[61]

In der Literatur wird der Tatbestand teilweise heftig kritisiert.[62] Dies hat den Grund, dass schon zweifelhaft ist, ob er die „formelle Verfügungsbefugnis" an Daten konzeptionell schützen kann und ob die vom Gesetzgeber behaupteten Strafbarkeitslücken tatsächlich bestehen. Zudem werden Bedenken hinsichtlich der Vereinbarkeit des Tatbestandes mit dem straf-

[59] Vgl. *Ioniță*, The major modifications of legal provisions of the cybercrime offences made by the legislator in the process of implementation of the new criminal code, Union of Jurists of Romania Law Review 2014, S. 32 (36).

[60] BT-Drs. 17/14362, S. 1; 83. Konferenz der Justizministerinnen und Justizminister, Beschluss TOP II.2.

[61] BR-Drs. 249/15, S. 24 f.; BT-Drs. 18/5088, S. 3, 26 f., 45 ff.

[62] Vgl. *Franck*, RDV 2015, S. 180; *Golla/v. zur Mühlen*, JZ 2014, S. 668; *Selz*, in: Taeger, Internet der Dinge, Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 915; *Singelnstein*, ZIS 2016, S. 432 ff.; *Stuckenberg*, ZIS 2016, S. 526.

rechtlichen Bestimmtheitsgebot aus Art. 103 Abs. 2 GG sowie der Pressefreiheit (Art. 5 Abs. 1 S. 2 Var. 1 GG) geäußert.[63]

2.8.2 Rumänien

Im rumänischen Recht stellt Art. 364 StGB-Ro die nicht autorisierte Übertragung von Computerdaten aus einem Computersystem oder von einem Datenspeichermedium unter Strafe. Art. 364 StGB-Ro stellt (wie Art. 360 StGB-Ro) weder Anforderungen an die Sicherung der Daten, noch sind besondere subjektive Merkmale zu erfüllen (wie die Bereicherungs- oder Schädigungsabsicht bei § 202d StGB-De). Da Art. 364 StGB-Ro auch keine rechtswidrige Vortat erfordert oder sich auf die Aktivitäten von Mittelsmännern richtet, ist die Vorschrift eher mit § 202a Abs. 1 StGB-De in der Variante des einem anderen Verschaffens vergleichbar als mit § 202d StGB-De. Der Strafrahmen beträgt nicht unter einem Jahr und bis zu fünf Jahre Freiheitsstrafe.

3 Fazit

Im Unterschied zu der deutschen Regelung sind die „CIA-Delikte" des rumänischen Rechts tatbestandlich tendenziell weiter und mit deutlich höheren Strafen bedroht. Besonders die Strafbarkeit des Zugangs zu Computersystemen nach Art. 360 StGB-Ro geht deutlich über die Regelung in § 202a Abs. 1 StGB-De hinaus, da das rumänische Delikt keine besondere Zugangssicherung voraussetzt und sich auf Computersysteme statt auf Daten bezieht. Die rumänische Regelung bewegt sich insgesamt auch näher am Wortlaut der CCC und regelt die „CIA"-Delikte anders als das StGB-De in einem einzigen Abschnitt.

Die hohen Strafandrohungen im rumänischen Recht, in dem diverse „CIA"-Delikte mit im Mindestmaß erhöhten Freiheitsstrafen bedroht sind, führen auch in der Praxis zu Verurteilungen. So kam es in jüngerer Zeit zu mehreren Aufsehen erregenden Fällen. Beispielsweise verurteilte ein Strafgericht in Cluj den rumänischen Staatsbürger Biro Endre Mark im März 2017 wegen unbefugten Zugriffs auf Computersysteme[64] zu einer

[63] Die Weite des Tatbestandes ist besonders deshalb problematisch, weil er dadurch geeignet ist, den Umgang mit Materialien von „Whistleblowern" unter Strafe zu stellen sowie Recherche und Hilfstätigkeiten für die Presse zu erschweren. Vor allem aufgrund der Auswirkungen des Tatbestandes auf die Pressefreiheit ist unter dem Aktenzeichen 1 BvR 2821/16 eine Verfassungsbeschwerde gegen § 202d StGB-De anhängig, an der ein Autor dieses Beitrages als Mitverfasser mitgewirkt hat; vgl. dazu näher https://freiheitsrechte.org/datenhehlerei/ (zuletzt abgerufen am 24. Mai 2017).

[64] Zu Gunsten des Angeklagten wurde hierbei die Vorgängervorschrift von Art. 360 StGB-Ro (Art. 42 Gesetz Nr. 161/2003) angewandt.

Freiheitsstrafe von drei Jahren auf Bewährung. Der ehemalige Angestellte des Unternehmens Vitacom Electronics, einem Vertrieb für Elektronik und IT-Komponenten, habe in seiner Zeit als Mitarbeiter dort unberechtigt auf Datensätze im Unternehmen zugegriffen.[65] In einem weiteren, noch laufenden, Verfahren ist der rumänische Staatsangehörige Simion Borș angeklagt, unbefugt auf die Website des rumänischen Präsidenten zugegriffen zu haben.[66] Auch hier steht eine Freiheitsstrafe im Raum. Allerdings sind sowohl im Fall Biro Endre Mark als auch im Fall Simion Borș Entscheidungen des Rumänischen Verfassungsgerichts zu erwarten. Es ist mit Spannung zu abzuwarten, wie sich das Gericht dabei zu Art. 360 StGB-Ro äußern wird.

In Deutschland ist die Zahl der Verurteilungen zu Freiheitsstrafen wegen „CIA"-Delikten gering.[67] Allerdings ist auf materieller Ebene auch im deutschen IT-Strafrecht eine gewisse Tendenz zur Expansion des Strafrechts zu erkennen; konkret deuten die Einführung des § 202d StGB-De (Datenhehlerei) und das Vorhaben zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme („Digitaler Hausfriedensbruch")[68] in diese Richtung. Es ist jedoch zweifelhaft, ob diese Expansion notwendig ist, um Schutzlücken zu schließen. Die tatsächlichen Probleme scheinen in der Computerkriminalität vor allem in der praktischen Durchsetzung der bestehenden Vorschriften zu liegen.[69]

---

[65] Tribunalul Cluj, Urt. v. 9. März 2017 – 3388/117/2015. Eine Zusammenfassung des Falles findet sich in der Gazeta de Cluj vom 20. März 2017, abrufbar unter http://gazeta decluj.ro/trei-ani-de-inchisoare-pentru-fostul-angajat-vitacom-acuzat-ca-accesat-ilegal-conturile-societatii-vasile-vita/ (zuletzt abgerufen am 24. Mai 2017).

[66] Eine Zusammenfassung des Falles findet sich in der Gazeta de Cluj vom 30. März 2016, abrufbar unter http://gazetadecluj.ro/hackerul-clujean-care-spart-site-ul-presedintiei-scapa-de-masura-controlului-judiciar/(zuletzt abgerufen am 24. Mai 2017).

[67] Nach der Strafverfolgungsstatistik des Statistischen Bundesamtes kam es im Jahr 2015 zu 42 Verurteilungen nach § 202a StGB-De (davon eine Freiheitsstrafe), zu zwei Verurteilungen nach § 202b StGB-De (keine Freiheitsstrafe), zu 37 Verurteilungen nach § 303a StGB-De (davon eine Freiheitsstrafe) und zu 15 Verurteilungen nach § 303b StGB-De (davon eine Freiheitsstrafe); Statistisches Bundesamt, Rechtspflege Strafverfolgung, Fachserie 10, Reihe 3, abrufbar unter http://www.destatis.de/DE/ Publkationen/Thematisch/Rechtspflege/ StrafverfolgungVollzug/Strafverfolgung.html (zuletzt abgerufen am 24. Mai 2017).

[68] Im Juni 2016 legte Hessen im Bundesrat einen Gesetzesantrag zur Einführung eines entsprechenden § 202e StGB-De vor; BR-Drs. 338/16.

[69] *Golla*, Risiken und Nebenwirkungen bei der Fortbildung des Internetstrafrechts, in: Stiftung der Hessischen Rechtsanwaltschaft, Die Internetkriminalität boomt, 2017, S. 153 (169 f.).

LITERATUR

Bhattacharjee, Yudhijit: How A Remote Town In Romania Has Become Cybercrime Central, wired.com, 31.01.2011, https://www.wired.com/2011/01/ff_hackerville_romania/all/1 (zuletzt abgerufen am 24. Mai 2017).

Ernst, Stefan: Das neue Computerstrafrecht, NJW 2007, S. 2661-2666.

Ernst, Stefan: Hacker und Computerviren im Strafrecht, NJW 2003, S. 3233-3239.

Fischer, Thomas: Strafgesetzbuch mit Nebengesetzen, 64. Aufl., München 2017.

Franck, Lorenz: Datenhehlerei nach dem künftigen § 202d StGB, RDV 2015, S. 180-183.

Golla, Sebastian/von zur Mühlen, Nicolas: Der Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei: Zur Legitimation und Zweckmäßigkeit eines allgemeinen Perpetuierungsdelikts im Informationsstrafrecht, JZ 2014, S. 668-674.

Golla, Sebastian: Risiken und Nebenwirkungen bei der Fortbildung des Internetstrafrechts – Datenhehlerei, Digitaler Hausfriedensbruch und alternative Regelungsansätze, in: Stiftung der Hessischen Rechtsanwaltschaft (Hrsg.), Die Internetkriminalität boomt: Braucht das Strafgesetzbuch ein Update?, Göttingen 2017, S. 153-181.

Haft, Fritjof: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) – Teil 2: Computerdelikte, NStZ 1987, S. 6-10.

Ioniță, Gheorghe-Iulian: The major modifications of legal provisions of the cybercrime offences made by the legislator in the process of implementation of the new criminal code, Union of Jurists of Romania Law Review 2014, S. 32-45, http://www.internationallawreview.eu/fisiere/pdf/5_2.pdf (zuletzt abgerufen am 24. Mai 2017).

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ulrich (Hrsg.): Strafgesetzbuch (StGB), 4. Aufl., Baden-Baden 2013.

Lenckner, Theodor/Winkelbauer, Wolfgang: Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (III), CR 1986, S. 823-831.

Leipziger Kommentar: StGB, 12. Aufl., Berlin 2008-2009.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.): Münchener Kommentar: StGB, 2. Aufl., München 2012.

Satzger, Helmut/Schluckebier, Wilhelm/Widmaier, Gunter (Hrsg.): StGB, 3. Aufl., Neuwied 2017.

Schönke, Adolf/Schröder, Schröder (Begr.): Strafgesetzbuch, 29. Aufl., München 2014.

Schumann, Kay H.: Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, S. 675-680.

Selz, Ilan Leonard: Gesetzentwurf zur Strafbarkeit der sogenannten Datenhehlerei, in: Jürgen Taeger (Hrsg.), Internet der Dinge, Digitalisierung von Wirtschaft und Gesellschaft, Edewecht 2015, S. 915-931.

Singelnstein, Tobias: Ausufernd und fehlplatziert: Der Tatbestand der Datenhehlerei (§ 202d StGB) im System des strafrechtlichen Daten- und Informationsschutzes, ZIS 2016, S. 432-439.

Stuckenberg, Carl-Friedrich: Der missratene Tatbestand der Datenhehlerei (§ 202d StGB), ZIS 2016, S. 526-533.

Wolter, Jürgen (Hrsg.): Systematischer Kommentar: StGB, 9. Aufl. 2016

Von Heintschel-Heinegg, Bernd (Hrsg.): StGB Kommentar, 2. Aufl., München 2015.

Welp, Jürgen: Strafrechtliche Aspekte der digitalen Bildverarbeitung (I), CR 1992, S. 291-296.