2. RUMÄNISCH-DEUTSCHE KONFERENZ ZUM EUROPÄISCHEN INFORMATIONSRECHT

Jürgen Taeger/Mihaela Drăgan/Sebastian Louven (Hrsg.)

Rechtsfolgen der Digitalisierung im rumänisch-deutschen Ländervergleich

Beiträge zur 2. Rumänisch-Deutschen Konferenz 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.

Alle Rechte vorbehalten.

© OlWIR Verlag

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

Edewecht 2018

ISBN: 978-3-95599-053-4

INHALT

Jürgen Taeger

Vorwort VII

Alexis Daj

DAOs und Blockchain-Technologien: Ökonomisches Potenzial und Regulatorische Herausforderungen von Smart Contracts und Virtual Currencies 1

David Saive

Unification through distribution? 17

Carmen Lupsan

Blockchain und die DSGVO 27

Cristiana Fernbach/Cătălina Fînaru

GDPR compliance in the Industry 4.0 33

Boris Reibach

Die Regulierung von Algorithmen unter der DSGVO 43

Dennis-Kenji Kipker/Sven Müller

Internationale Cybersecurity-Regulierung 51

Sebastian J. Golla

Robocop streift durch das Netz: Grundrechtseingriffe durch die automatisierte Unterstützung von Polizeiarbeit im Social Web 67

Thorsten Feldmann

Presse- und Öffentlichkeitsarbeit unter der DSGVO 81

Anna K. Bernzen

Der EuGH als Lehrmeister: Was deutsche Gerichte beim Umgang mit den Medien von internationalen Gerichten lernen können 89

Kathrin Schürmann

Location Based Advertising – Eine Analyse aus datenschutz- und wettbewerbsrechtlicher Sicht 105

Hans-Christian Gräfe

Werbung auf Online-Plattformen: Influencer Marketing 115

Sebastian Louven

Kartellrechtliche Grenzen des Informationsaustauschs 135

Anselm Brandi-Dohrn

German Supreme Court on licensing agreements: a new understanding of the legal nature of licensing contracts 145

Michaela Braun-Noviello

Elektronische Verträge im rumänischen Recht 155

Matthias Baumgärtel

Chancen für ländliche Räume aufgrund der WiFi4EU-Verordnung 167

VORWORT

Das europäische Informationsrecht wird zunehmend durch gesetzgeberische Regulierungsaktivitäten geprägt. So soll die Datenschutzgrundverordnung (DSGVO) einen einheitlichen europäischen Rahmen für die Verarbeitung personenbezogener Daten schaffen, lässt jedoch eine Vielzahl an Fragen offen. Allerdings enthält diese in den Mitgliedstaaten unmittelbar geltende Verordnung eine Vielzahl an Öffnungsklauseln mit Anpassungsvorgaben und nationalstaatliche Regulierungsmöglichkeiten. Zudem kündigt sich die sogenannte ePrivacy-Verordnung (ePVO) für elektronische Kommunikation als nächstes Regelungswerk an, das wiederum stark mit dem allgemeinen europäischen Rechtsrahmen für elektronische Kommunikation verknüpft ist. Die Gesetzgebung zu Informations-, Digitalisierungs- oder Datensachverhalten ist zunehmend europäisch geprägt, lässt den Mitgliedstaaten aber auch weite Spielräume zur Gestaltung und wird in den durchaus unterschiedlichen Rechtskulturen der Unionsländer uneinheitlich angewendet.

Vor diesem Hintergrund ist es erfreulich, dass 2018 – passenderweise am 25. Mai 2018, dem ersten Anwendungstag der DSGVO – diese Entwicklungen auf der zum zweiten Mal an der Babeş-Bolyai-Universität Cluj-Napoca veranstalteten rumänisch-deutsche Konferenz zum Europäischen Informationsrecht diskutiert wurden. Die Konferenz geht auf eine Initiative der Deutschen Stiftung für Recht und Informatik (DSRI) zum länderübergreifenden Austausch insbesondere mit osteuropäischen Ländern zurück. Wieder konnten zahlreiche Referenten mit unterschiedlichen informationsrechtlichen Schwerpunkten für die zweitägige Konferenz gewonnen und die traditionell guten Beziehungen zwischen der Carl von Ossietzky Universität Oldenburg und der Babeş-Bolyai-Universität weiter ausgebaut werden. Für die Förderung der Konferenz danken die Herausgeber dieses Tagungsbandes dem Prorektor der Babeş-Bolyai-Universität, Univ.-Prof. Dr. Rudolf Gräf.

Gegenüber dem Vorjahr trugen noch mehr Referentinnen und Referenten vor, sodass zu den Themenschwerpunkten Panels gebildet werden konnten. Das erste Panel befasste sich mit der hochaktuellen Blockchain-Technologie, von der tiefgreifende Veränderungen in der Digitalwirtschaft erwartet werden, die auch mit Herausforderungen für die rechtswissenschaftliche Dogmatik verbunden sind. Das Europäische Datenschutzrecht, das auf eine Rechtsharmonisierung in der Europäischen Union hinwirken sollte, wurde ebenso kritisch beleuchtet, wie besorgniserregende Entwicklungen der IT-Sicherheit. Die Vorträge befassten sich auch mit den mittelbaren Auswirkungen der DSGVO auf das Medien- und Wettbewerbsrecht.

Schließlich griff die Konferenz aktuelle Diskussionen zur Regulierung von Algorithmen auf und befasste sich mit dem Einsatz automatisierter polizeilicher Recherchen in sozialen Netzwerken. Sehr fruchtbar waren die Diskussionen unter den rumänischen und deutschen Teilnehmern, weil sie mit ihren Rechtsansichten und Einschätzungen des EU-Sekundärrechts weitgehend übereinstimmten, sie aber doch bei der Rechtsanwendung Unterschiede in den beiden EU-Mitgliedstaaten identifizierten.

Ein Großteil der Vorträge der wissenschaftlich fruchtbaren Veranstaltung werden in diesem Tagungsband dokumentiert. Die Herausgeber bedanken sich bei allen Teilnehmern für ihr Engagement und freuen sich auf die 3. Rumänisch-Deutsche Konferenz zum Europäischen Informationsrecht im Mai 2019 in Cluj-Napoca.

Oldenburg, im August 2018

Prof. Dr. Jürgen Taeger

Carl von Ossietzky Universität Oldenburg

Direktor des Interdisziplinären Zentrums
für Recht der Informationsgesellschaft (ZRI)

Vorsitzender der Deutschen Stiftung
für Recht und Informatik (DSRI)

Prof. Dr. Mihaela Drăgan

Babeş-Bolyai-Universität Cluj-Napoca
Vizedekanin, Fakultät für Wirtschaftswissenschaften
und Unternehmensführung

Sebastian Louven

Carl von Ossietzky Universität Oldenburg
Interdisziplinäres Zentrum für Recht
der Informationsgesellschaft (ZRI)

DAOS UND BLOCKCHAIN-TECHNOLOGIEN: ÖKONOMISCHES POTENZIAL UND REGULATORISCHE HERAUSFORDERUNGEN VON SMART CONTRACTS UND VIRTUAL CURRENCIES

Av Ass. Prof. Dr. Alexis Daj

Transilvania University of Brasov –
Faculty of Economic Sciences and Business Administration
alexis.daj@unitbv.ro

Zusammenfassung

Bisher werden Decentralized Autonomous Organizations (DAOs) hauptsächlich im Finanzbereich oder im FinTech-Sektor (englisch „financial technology", verkürzt zu „FinTech") eingesetzt – während überwiegend die digitalen Währungen im Brennpunkt stehen. In der Zukunft könnten aber DAOs aufgrund ihrer ausgeklügelten Organisationsstruktur (und den daraus resultierenden schnellen Entscheidungswegen) und durch den Einsatz von auf Blockchain basierenden Smart Contracts und Virtual Currencies eine viel wichtigere Rolle in der globalen Wirtschaft spielen. Dieser Bericht wird einige beachtenswerte Aspekte bezüglich der regulatorischen Herausforderungen und des ökonomischen Potenzials identifizieren und erläutern.

1 Dezentrale Vertrauensnetzwerke – Ende der Institutionen?

Als Folge der expansiven Verbreitung automatisierter Prozesse (im FinTech-Sektor) oder von Legal-Tech-Anwendungen (im Bereich der juristischen Beratung) und der Internetnutzung im Allgemeinen werden wahrscheinlich weitreichende und noch unklare Konsequenzen hervorgerufen – insbesondere für die Gestaltung von Arbeitsprozessen in Anwaltskanzleien oder in Verbindung mit haftungsrechtlichen Fragestellungen (z.B. im Falle von Decentralized Autonomous Organizations – DAOs und von programmierten Verträgen – Smart Contracting).[1] Laut *Thomsen* wird die Digitalisierung „veränder(n), wie wir leben und wie wir arbeiten. Worauf wir uns einstellen und wie wir uns vorbereiten können".[2]

[1] *Bogenstahl/Ferdinand*, „Legal Techs – algorithmische Rechtsberatung" – Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Themenkurzprofil Nr. 12, Mai 2017.

[2] *BAVC*, „Legal Tech: Freund oder Feind der Juristen?", 2018.

Die Blockchain-Technologie ist zurzeit ein sehr polarisierendes Gesprächsthema und stellt erhebliche Herausforderungen für Rechtswissenschaftler und Juristen dar, weil „Technik und Recht unterschiedliche Sprachen sprechen", eröffnet aber auch neue Chancen. Die Verwirklichung dieser Gelegenheiten „setzt aber voraus, die Technologie und Philosophie hinter Blockchain zumindest dem Grunde nach und vom Prinzip her zu verstehen" um die rechtliche Erfassung von Geschäftsabschlüssen und -abwicklungen mit Hilfe von Blockchain möglich zu machen.[3]

Die digitalen Währungen (auch als „Kryptowährungen" bekannt) stehen überwiegend im Brennpunkt und haben als verfahrenstechnisches Fundament die Blockchain-Technologie. Die Bedeutung der Erschaffung von dezentralen Vertrauensnetzwerken wird auch von *Thiele/Ehrenberg-Silies* betont:

„Der Grundgedanke der Blockchain-Technologie ist es, eine nachvollziehbare, dezentral organisierte, unverletzliche und damit fälschungssichere Möglichkeit zu schaffen, um Transaktionen abbilden zu können, ohne auf eine zentrale Organisation oder Mittelsmänner wie Banken, Notare oder Treuhänder zurückgreifen zu müssen (Casey/Vigna 2015, Kap. 1, S. 1). Das Vertrauen in die korrekte Abwicklung der Transaktionen wird auf technologischem Wege mittels digitaler Signaturen und Verschlüsselungstechnologien erzeugt."[4]

Die Blockchain-Technologie ist „mehr als ein herkömmliches Computerprogramm, das bi- oder auch multilaterale Geschäftsabschlüsse beschleunigt und komfortabler macht. Es ist vielmehr eine Technologie, die das Betreten juristischen Neulands zumindest ermöglicht".[5] Die Hauptidee der Blockchain-Technologie ist, dass durch die Zusammenarbeit der Nutzer selbst dezentrale Vertrauensnetzwerke erschaffen werden können (siehe Abb. 1), die sichere und unvermittelte Transaktionen zwischen zwei oder mehr Nutzern befähigen und Intermediären ausschließen (da man Institutionen wie Behörden, Dienstleister oder Banken nicht immer trauen kann und weil Menschen öfters Fehler machen).

---

[3] *Buchleitner/Babl,* „Blockchain und Smart Contracts Vom Ende der Institutionen", Ecolex Fachzeitschrift für Wirtschaftsrecht 2017, 1-92, RspNr 1-39, www.ecolex.at, S. 4-14.

[4] *Thiele/Ehrenberg-Silies,* „Blockchain", Themenkurzprofil Nr. 1, Mai 2016; Karlsruher Institut für Technologie (KIT) 2016, S. 1., https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-001.pdf (abgerufen am 18.5.2018).

[5] *Buchleitner/Babl,* „Blockchain und Smart Contracts. Vom Ende der Institutionen", Ecolex Fachzeitschrift für Wirtschaftsrecht 2017, 1-92, Rsp-Nr 1-39, S. 4-14.

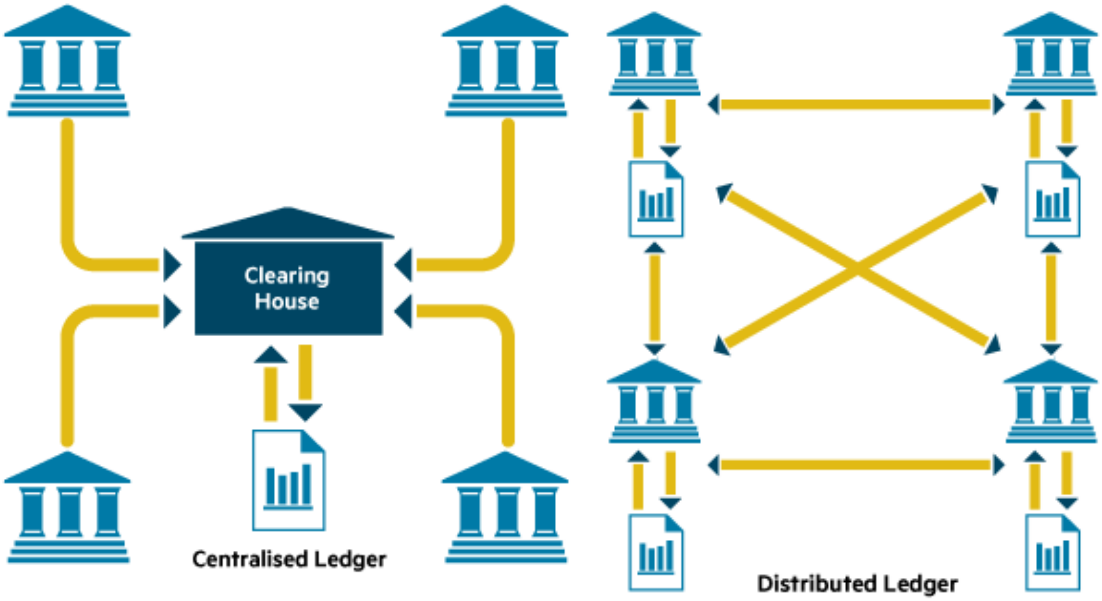

Abb. 1: Klassische Buchführung versus Blockchain:

Klassisch: Datenbank kontrolliert durch zentrale und vertrauenswürdige Instanz

Blockchain: Jeder Teilnehmer hat eine eigene Kopie der Datenbank (wird als „Distributed Ledger" Methode bezeichnet) – Quelle: Kofler (2018)[6]

Thiele/Ehrenberg-Silies sind der Meinung, dass Blockchain eine Basistechnologie darstellt, welche ein bemerkenswertes disruptives Potenzial aufweist, eine Technologie, „die weit über den ursprünglichen Anwendungsfall Kryptowährungen hinaus in allen Bereichen, in denen es um die Feststellung bzw. Übertragung von Eigentum an digitalen bzw. digitalisierbaren Gütern geht, eingesetzt werden könnte".[7]

2 Wissenschaftlichen Grundlage von Blockchain-Technologien

2.1 Konzept und Definitionen

Die Blockchain-Technologie ist eine neue Methode der Bestätigung und Überprüfung von Datentransaktionen, die in allen Fällen angewendet werden kann, wo normalerweise ein Vermittler benötigt wird um Informationen sicher zu verwalten und zu verifizieren. *Voshmgir* unterstreicht, dass es sich um „eine Form der Verteilung und Sicherung von Daten handelt, auf

[6] *Kofler*, „Blockchain", AKKT Forschungsgesellschaft 2018.

[7] *Thiele/Ehrenberg-Silies*, „Blockchain", Themenkurzprofil Nr. 1, Mai 2016.

deren Basis viele Funktionen zentral organisierter Informationssysteme dezentralisiert werden können".[8] Ergänzend, erläutern *Thiele/Ehrenberg-Silies* die Funktionsweise von Blockchain-Technologien:

„Das Verfahren fußt auf einem ausgeklügelten Algorithmus zur Verifizierung von Transaktionen So hat das zugrundeliegende Netzwerk eine dezentrale Peer-to-Peer-Struktur und nutzt keine zentralen Server. Informationen werden im Netzwerk unter allen Akteuren öffentlich geteilt und allen Akteuren gleichzeitig zugänglich gemacht. Weiterhin werden alle Transaktionen in Form von Datenblöcken gespeichert. Diese Datenblöcke werden mit einem Kodierungsverfahren bearbeitet und unter allen Teilnehmern verifiziert".[9]

Laut Fraunhofer-Institut für Angewandte Informations-technik (FIT) ist die Blockchain aber erst am Anfang ihrer Entwicklung und keine einheitlichen Definitionen haben sich durchgesetzt. Nichtsdestoweniger können einige aufschlussreiche Merkmale aus den folgenden Beispiele gewonnen werden:[10]

Während einige Forscher eine Blockchain als "ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die durch die Teilnehmer eines verteilten Rechnernetzes verwaltet werden" bezeichnen, deutet *Walport* eine Blockchain als "eine Art Datenbank, in der Einträge in Blöcken gruppiert werden. Diese Blöcke sind in chronologischer Reihenfolge über eine kryptographische Signatur miteinander verknüpft. Jeder Block enthält Aufzeichnungen valider Netzwerkaktivität seit dem Hinzufügen des letzten Blocks".

[8] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

[9] *Thiele/Ehrenberg-Silies,* „Blockchain", Themenkurzprofil Nr. 1, Mai 2016, S. 2.

[10] *Schlatt/Schweizer/Urbach/Fridgen*, „Blockchain: Grundlagen, Anwendungen und Potenziale", Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT 2016.

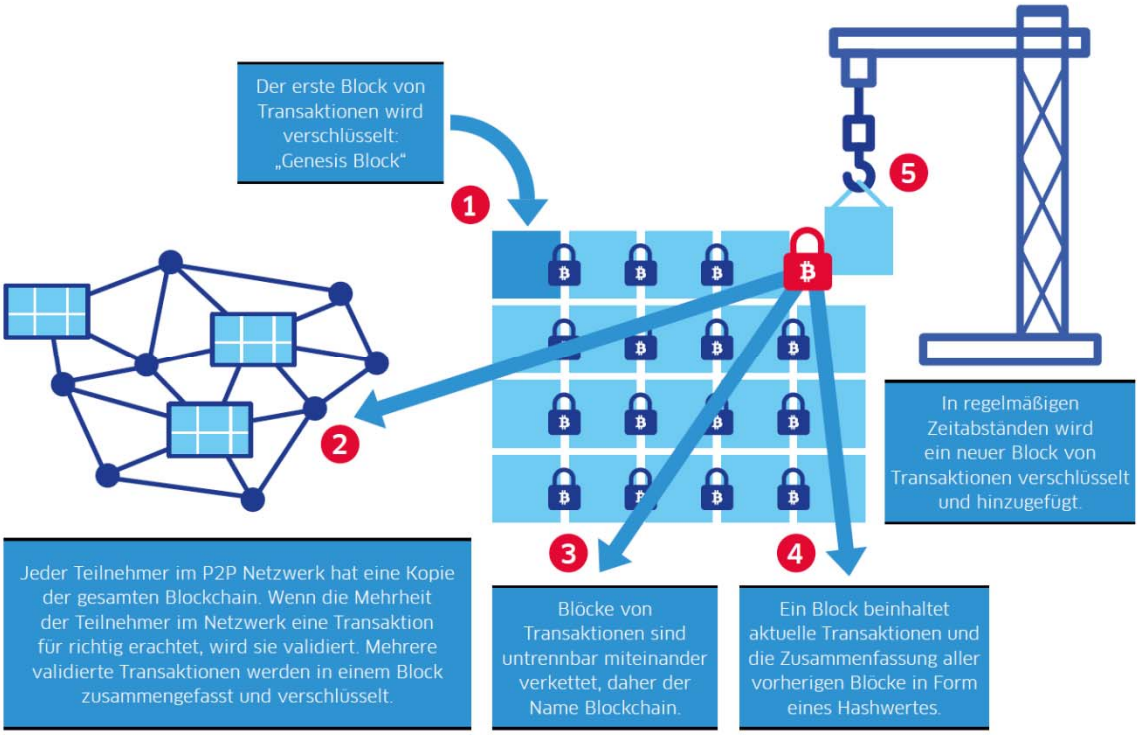

Abb. 2: Funktionsweise der Blockchain – Quelle: Voshmgir (2016)[11]

Die Funktionsweise der Blockchain wird in Abb. 2 von Shermin Voshmgir (2016) bildlich dargestellt. Das Schema erläutert die Tatsache, dass die Blockchain eine auf vielen Rechnern gleichzeitig gepflegte Datei ist, in der „sämtliche Transaktionen aller Teilnehmer vom gesamten Netzwerk per Mehrheits-Konsens validiert und abgespeichert werden“.

2.2 Wesentliche Bestandteile und Eigenschaften der Technologie

Laut *Thiele/Ehrenberg-Silies* wurde das System der Blockchain 2008 in Verknüpfung mit der Entwicklung der Kryptowährung Bitcoin - als digitales dezentrales Zahlungssystem - von *Nakamoto* beschrieben.

Näher kann man die Blockchain als digitales Register bezeichnen, „in dem alle Transaktionen seit Beginn der Nutzung der Technologie festgeschrieben werden“ mit dem Endzweck „finanzielle Interaktionen ohne den Einsatz von Dritten zwischen zwei Akteuren, die sich weder kennen, noch vertrauen müssen, durch den Einsatz von Technologie billiger, schneller und sicherer durchführen zu können, und dies unabhängig von staatlich oder anderweitig regulierten Instanzen“ zu ermöglichen.[12]

[11] *Voshmir*, „Blockchains, Smart Contracts und das Dezentrale Web“, Technologiestiftung Berlin 2016.

[12] *Thiele/Ehrenberg-Silies*, „Blockchain“, Themenkurzprofil Nr. 1, Mai 2016.

2.2.1 Blockchain Bestandteile

Buchleitner/Rabl betrachten die Bitcoin-Blockchain als „der erste Durchbruch zur ‚Abschaffung' von Intermediären wie Banken, Staaten, Finanzinstitutionen", indem ein eigenes „Währungssystem" errichtet wurde. Diese von der Anerkennung des Staates als legales Zahlungsmittel autonome digitale „Währung" existiert nur dank der Akzeptanz seiner Nutzer. Die Wissenschaftler sind der Meinung, dass die Hürde der Prüfung durch zentrale Institutionen (zur Verhinderung von „Double-Spending") mit Hilfe von Satoshi Nakamotos „Proof-of-Work"-Methode auf eine wirtschaftswissenschaftlich sinnvolle Weise überwunden wurde.[13]

Laut Fraunhofer-Institut für Angewandte Informationstechnik (FIT) werden die beigeordneten Verwaltungssysteme als „verteilte Konsenssysteme" etikettiert und „beruhen auf Kryptographie und Peer-to-Peer-Prinzipien (P2P), statt einer zentralen Autorität, um per Konsens eine netzwerkweite Verifikation des Status des Systems zu erreichen" siehe Abbildung 3.[14]

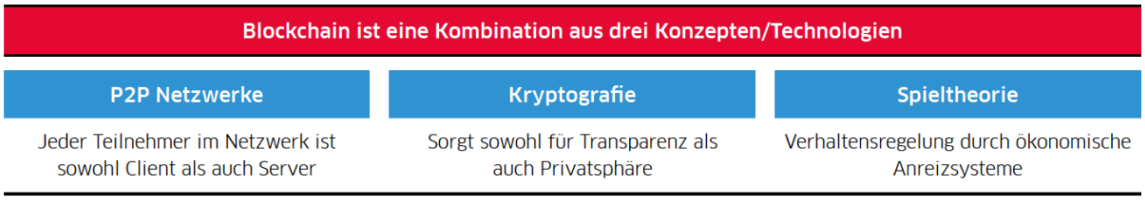

Abb. 3: Die wissenschaftlichen Grundlagen von Blockchain-Technologien – Quelle: Shermin Voshmgir (2016)[15]

Die Beschreibung der von *Thiele/Ehrenberg-Silies* schildert die Hauptbestandteile und die Funktionsweise der Blockchain-Technologie sehr verständlich:

„In einer Blockchain sind sämtliche jemals getätigten Transaktionen aller Nutzer, am Beispiel der Bitcoins – Kauf und Verkauf – in dezentraler Form in einem Peer-to-Peer-Netzwerk gespeichert. Neue Transaktionen werden an die bestehende Kette von Datenblöcken als neuer Datenblock angehängt. Die übertragenen Daten werden mithilfe eines speziellen Verfahrens kodiert, sodass ein unbefugter Eingriff in die Daten nicht möglich ist. Die Blockchain im Falle der Bitcoins ist somit vergleichbar mit

[13] *Buchleitner/Babl,* „Blockchain und Smart Contracts Vom Ende der Institutionen", Ecolex Fachzeitschrift für Wirtschaftsrecht 2017, 1-92, Rsp-Nr 1-39, S. 4-14.

[14] *Schlatt/Schweizer/Urbach/Fridgen,* „Blockchain: Grundlagen, Anwendungen und Potenziale", Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT 2016.

[15] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

einer öffentlich einsehbaren Buchhaltung eines Unternehmens, die alle Geschäftsvorgange beinhaltet. Jeder Block entspricht in dieser Analogie einer Seite in dem Transaktionsjournal."[16]

Im nächsten Abschnitt werden die wichtigsten Merkmale der Blockchain-Technologie aufgezählt und erläutert.

2.2.2 Blockchain Eigenschaften

Sowohl *Schlatt/Schweizer/Urbach/Fridgen* als auch *Voshmgir* synthetisieren die Haupteigenschaften von Blockchain und schlagen einige Klassifizierungsmöglichkeiten vor (siehe Abb. 4 und 5):

a) Blockchain-Systeme sind verteilte Systeme, die mehrere unabhängige Rechner (Netzknoten, die miteinander korrespondieren und sich synchronisieren) besitzen. Somit kann der Ausfall einzelner Rechner andere Rechner dabei nicht beeinträchtigen.

b) Jeder Netzknoten speichert mehrfach einen gemeinsamen Status des Systems, sodass der Ausfall einzelner Computer nicht den Verlust des Systemstatus involviert.

c) Ein anderes Unterscheidungszeichen von Blockchain-Systeme liegt darin, ob zur Beteiligung am Verwaltungsprozess der Blockchain eine Genehmigung benötigt wird (siehe Abbildung 4).

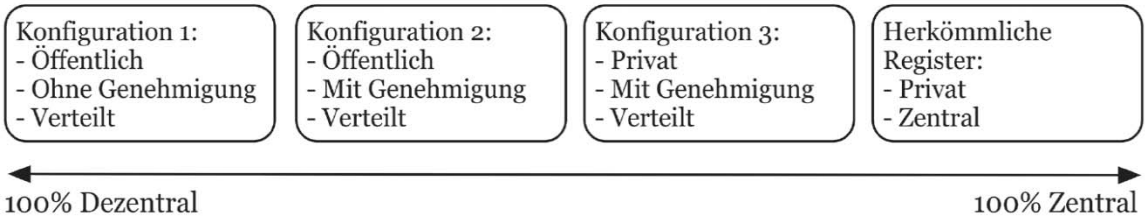

Abb. 4: Der Grad der Zentralisierung verschiedener Blockchain-Systeme (in Anlehnung an Walport 2015)
Quelle: Fraunhofer-Institut für Angewandte Informations-technik[17]

d) Im Zusammenhang mit den Peer-to-Peer-Prinzipien, können nach *Schlatt /Schweizer/Urbach/Fridgen* weitere Eigenschaften identifiziert werden:

- Die Netzteilnehmer stellen Hardwareressourcen zur Verfügung, um Inhalte bzw. Leistungen des Netzwerks bereitzustellen.

---

[16] *Thiele/Ehrenberg-Silies,* „Blockchain", Themenkurzprofil Nr. 1, Mai 2016; Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), S. 1.

[17] *Schlatt/Schweizer/Urbach/Fridgen*, „Blockchain: Grundlagen, Anwendungen und Potenziale", Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT 2016.

- Es gibt keine zentrale Institution oder Verwaltung zur Abstimmung der Kommunikation zwischen den einzelnen Netzknoten.
- Der Konsensmechanismus (mittels dessen die Netzknoten den Systemstatus abstimmen) kann als die entscheidende Neuerung hinter Blockchain-Systemen betrachtet werden.

Öffentliche Blockchains	Private Blockchains	Konsortium Blockchains
· Unendlich viele Netzwerkteilnehmer · Jeder kann Transaktionen validieren · Protokoll öffentlich	· Ausgewählte und begrenzte Anzahl von Netzwerkteilnehmern · Nur ausgewählte Mitglieder können Transaktionen validieren · Protokoll nicht öffentlich	· Netzwerkteilnehmer nur innerhalb eines einzelnen Unternehmens · Nur ausgewählte Mitglieder können Transaktionen validieren · Protokoll kann öffentlich sein (open source) oder nicht öffentlich

Abb. 5: Arten von Blockchains und dazugehörige Eigenschaften - Quelle: Voshmgir (2016)[18]

e) In Verbindung mit **Bitcoin (als P2P-basiertes digitales Währungssystem)** können folgende Merkmale erkannt werden:

- Der Bitcoin ermöglicht als P2P Währungssystem, dass Transaktionen ohne einen Intermediär abgeschlossen werden können.
- Die Blockchain stellt ein dezentrales chronologisches Register aller vergangenen Transaktionen innerhalb des Bitcoin-Netzwerks dar.
- Die Rechnungseinheit Bitcoin (BTC) stützt sich auf zwei grundlegenden Konzepten der Kryptographie: Public-Key-Kryptographie bzw. digitalen Signaturen und kryptographischen Hash-Funktionen.
- Im Bitcoin-System existieren keine Konten oder Kontostände, sondern nur ein öffentliches Verzeichnis aller bisher durchgeführten Bitcoin-Transaktionen – die Bitcoin-Blockchain.
- „Bitcoins" sind lediglich Referenzen vergangener Transaktionen (die an spezifischen Adressen transferiert werden).
- Das Bitcoin-Netzwerk verwendet zwei Arten von Netzknoten, so genannte Mining-Netzknoten (die einzigen, die dafür sorgen, dass eine Transaktion in die Blockchain aufgezeichnet wird und dadurch auch neue Bitcoins – als Belohnung – generiert werden) und passive Netzknoten.
- Das Bitcoin-Netzwerk erreicht den Konsens über ein sogenanntes *Proof-of-Work*-Schema *(PoW)* (indem ein rechenintensives Problem

[18] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

gelöst wird – als Verhaltensregelung durch wirtschaftliche Anreizmechanismen), das die abusive Nutzung eines Dienstes verhindern soll.

- Eine Transaktion wird erst dann als abgeschlossen betrachtet, wenn sie in die Blockchain aufgezeichnet wurde.
- Es gibt allerdings eine Vielzahl an alternative Konsens-Methoden: Proof-of-Stake (PoS) – die Blockchain wird durch solche Netzknoten aufdatiert, die einen bedeutenden Anteil an der Währung bzw. generell Werten in der Blockchain haben; *Proof-of-Activity (PoA)* – eine Kreuzung von PoW und PoS samt einem Beweis für Aktivität innerhalb des Netzwerks; *Proof-of-Publication* oder *Proof-of-Storage*.[19]

3 Ökonomisches Potenzial und Anwendungsbereiche von Blockchain – Regulatorische Herausforderungen

3.1 Ökonomisches Potenzial - Wofür kann man die Die Blockchain-Technologie verwenden?

Die Erfindung des *World Wide Webs (WWW)* durch Tim Berners-Lee hat den Informationsaustausch revolutioniert. Danach folgte die als *Web 2.0* bekannte Weiterentwicklung und gestaltete das Web programmierbar und ermöglichte komplexe Anwendungen auf Basis von *Social Media* (soziale Medien) und die Entwicklung der *Sharing Economy*.[20]

Forscher wie *Voshmgir* sind der Auffassung, dass die Blockchain-Technologie - als ein „Baustein des *Web 3.0*" – ein „nächster großer Schritt in der Entwicklung der IT Branche und des dezentralen Internets" darstellen kann – ein Baustein, „der den Wertaustausch revolutioniert, indem er P2P-Transaktionen ohne zentrale Clearingstelle ermöglicht". Als Konsequenz kann man innovative Anwendungen in Form von *Smart Contracts*, *dezentrale Applikationen* (dApps) und *Dezentrale Autonome Organisationen (DAOs)* entwickeln.[21]

Ferner unterstreichen *Thiele/Ehrenberg-Silies*, dass – über die Kryptowährungen hinaus – die Blockchain-Technologie noch ausgedehntere Nutzungsmöglichkeiten bietet, „die die bisherigen Strukturen in verschiedenen Branchen verändern können":

---

[19] *Schlatt/Schweizer/Urbach/Fridgen*, „Blockchain: Grundlagen, Anwendungen und Potenziale", Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT 2016.

[20] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

[21] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

„So existieren beispielsweise Bestrebungen und erste Konzepte, um mithilfe der Blockchaintechnologie Wahlprozesse durchzuführen [...]. Ebenfalls eignet sich die Blockchain dazu, geistiges Eigentum zu verwalten und bisher durch Notare geleistete Dienstleistungen zu ersetzen [...]. Weiterhin könnten E-Governmentangebote entwickelt werden, die auf Basis der eindeutigen Identifikation einer Transaktion (und damit eines Nutzers) digitale Angebote für bürgernahe Dienstleistungen der Verwaltung, wie z.B. das Ausstellen oder die Beglaubigung von Dokumenten, ermöglichen. [...]. Hierzu zählen u.a. Wertpapierhandel, öffentliche Register (z.B. Grundbücher), elektronische Wahlen aber auch neuartige Konstrukte wie sich selbst vollziehende Verträge (Smart Contracts)".[22]

Buchleitner/Rabl betrachten den *Smart Contract* als ein „digitales Protokoll, das vorgegebene technologische Prozesse innerhalb einer Transaktion automatisch ausführt, ohne dass ein Dritter involviert ist" – sodass „vertragliche Vereinbarungen in *Programme* bzw. in eine *Programmiersprache*, den *Code* – der auf einer Blockchain läuft, umgesetzt und automatisch abgewickelt werden sollen, wenn bestimmte Bedingungen eingetreten sind". Aus wirtschaftlicher Sicht sind Smart Contracts deswegen attraktiv, weil „durch die automatisierte Abwicklung einzelne Vertragsbestimmungen ohne staatliche Vollstreckung und völlig automatisch durchgesetzt werden".[23]

Diese Sichtweise wird auch von anderen Wissenschaftler geteilt: laut *Voshmgir*, repräsentieren *Smart Contracts* „automatisch ausführbare Programme, die auf der Blockchain aufbauen und vordefinierte Transaktionsspielregeln im Programmcode abbilden". Folglich handelt es sich um eine Transaktion, die mittels eines Smart Contracts ausgeführt wird und „automatisch ausgeführt, wenn alle beteiligten Parteien die zuvor definierten Konditionen erfüllen". Demzufolge können auch *dApps (Decentralized Applications)* definiert werden. Sie sind „dezentrale Anwendungen vom Backend bis zum User Interface, die auf einer Blockchain laufen und einen oder mehrere Smart Contracts verwenden".[24] *Thiele/Ehrenberg-Silies* betonen:

„Mit zunehmender Verbreitung von blockchainbasierten Dienstleistungen und der steigenden Kapitalisierung von Kryptowährungen kann es in Zukunft dazu kommen, dass sowohl die Bedeutung der traditionell vom Staat übernommenen Funktionen als auch die Bedeutung des regulierten Bankensystems sinkt, wenn die beteiligten Akteure die Technologie nicht frühzeitig für ihre Zwecke adaptieren und nutzbar machen. Es könnte untersucht werden, welche blockchainbasierten E-Governmentlösungen sich im Sinne eines Bürokratieabbaus eignen könnten, z.B. um Amtsgänge, wie

[22] *Thiele/Ehrenberg-Silies,* „Blockchain", Themenkurzprofil Nr. 1, Mai 2016, S. 9.

[23] *Buchleitner/Babl,* „Blockchain und Smart Contracts Vom Ende der Institutionen", Ecolex Fachzeitschrift für Wirtschaftsrecht 2017, 1-92, Rsp-Nr 1-39, S. 4-14.

[24] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

z.B. das Ausstellen eines amtlich beglaubigten Dokuments, effizienter zu gestalten".[25]

In diesem Sinne können *DAOs (Decentralized Autonomous Organizations)* eine neue Form der Organisation darstellen, „deren Statuten, Geschäftsordnung, Gesellschaftsvertrag oder Satzung durch einen Smart Contract abgebildet und automatisch ausgeführt werden". Somit werden „die Spielregeln der Organisation im Vorfeld definiert und in die Smart Contracts programmiert. DAOs sind die höchste und komplexeste Form eines Smart Contracts".[26]

Buchleitner/Rabl erläutern das DAO-Prinzip, welches darauf stützt, dass die „Abwicklung" der Transaktionen von folgenden Regeln gelenkt wird:

a) *Unveränderbarkeit durch einzelne Teilnehmer* („Nur die Mehrheit der Teilnehmer soll durch Abstimmungsverhalten eine Adaptierung des Blockchain-Systems einleiten können").

b) *Unstoppbarkeit* („Unabhängig von Einzelnen läuft das Programm auf der Blockchain ab. Das Programm ist nur dann stoppbar oder änderbar, wenn die Mehrheit der Teilnehmer dem zustimmt").

c) *Unwiderlegbarkeit* („Sämtliche Ausführungen von Transaktionen werden transparent und für sämtliche Teilnehmer – auch auf alle Zeiten – im Internet, das heißt in der Blockchain, abgespeichert und sind auf diese Weise unwiderleglich dokumentiert").[27]

Laut Forschern wie *Kofler*, sind die Anwendungen der Blockchain-Technologie vielfältig und können auch in verschiedene Kategorien eingeteilt werden (siehe auch Abbildung 6):

a) *Der Zahlungsverkehr* (Kryptowährungen, Cross-border Payments, Smart Money etc.);

b) *Smart Contracts* (Versicherungspolicen, Energiewirtschaft, Rechtemanagement, DAOs etc.);

c) *Logistik – Industrie 4.0* (Supply Chain und IoT);

d) *E-Government* (Grundbücher, elektronische Gesundheitsakte, Echtzeit-Besteuerung etc.).

---

[25] *Thiele/Ehrenberg-Silies*, „Blockchain", Themenkurzprofil Nr. 1, Mai 2016, S. 10.

[26] *Voshmir*, „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

[27] *Buchleitner/Babl*, „Blockchain und Smart Contracts Vom Ende der Institutionen", Fachzeitschrift für Wirtschaftsrecht 2017, 1-92, Rsp-Nr 1-39, S. 5.

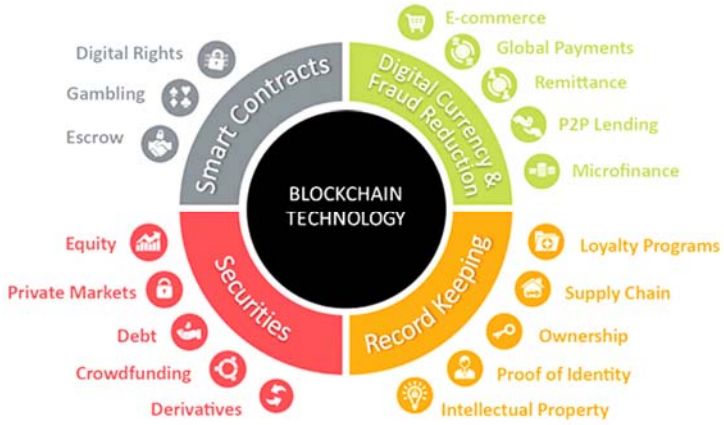

Abb. 6: Anwendungen von Blockchain (Quelle: aciworldwide.com - Kofler 2018)[28]

3.1.1 Regulatorische Herausforderungen der Blockchain und Dezentrale Internet-Probleme

Obwohl die Blockchain-Technologie viele Vorteile und nützliche Anwendungen aufweist, sind *Thiele/Ehrenberg-Silies* der Meinung, dass auch weiterhin gesetzwidrige Potenziale bestehen werden – wie z.B. durch den Gebrauch von Kryptowährungen, für Geldwäsche, Drogen- oder Waffenhandel. Sie unterstreichen zusätzlich die gegenwärtige Rolle der Kryptowährungen als „zentrales Zahlungsmittel im sogenannten *Dark Net*, ein anonymes Untergrundinternet abseits der von Suchmaschinen erreichbaren Seiten, welches seinerseits ein Peer-to-Peer-Netzwerk darstellt, das nur mit besonderen Hilfsmitteln betreten und genutzt werden kann".[29] Die gefährliche rechtliche Lage wird auch von *Voshmgir* erkannt:

„Die Grenzen verschwimmen oftmals, da auf der Blockchain komplett neue Marktmechanismen und wirtschaftliche Dynamiken eintreten, die von manchen als Crypto Economics bezeichnet werden und für die es noch keine Rechtsrahmen gibt".[30]

Auch in Bezug auf neue Geschäftsmodelle im Bereich der virtuellen Währungen fehlt eine effiziente Regulierung, da es ein grenzüberschreitendes Thema ist, welches nur global reguliert werden kann. *Hönig* untersucht das *Initial-Coin-Offering*-Verfahren *(ICO)* als ein neues Mittel zur Kapitalaufnahme von Unternehmen, deren Geschäftsmodell auf Kryptowährungen stützt, und betont, dass diese nicht regulierte Methode des Crowdfundings (auch als „sogenannte Schwarm- oder Gruppenfinanzierung" bekannt) eine

[28] *Kofler*, „Blockchain", AKKT Forschungsgesellschaft 2018.

[29] *Thiele/Ehrenberg-Silies*, „Blockchain", Themenkurzprofil Nr. 1, Mai 2016.

[30] *Voshmir*, „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016, S. 27.

Lösung für Firmen darstellt um den „bekannten, streng regulierten Vorgang eines Börsengangs (Initial Public Offering, IPO)“ zu meiden. Als Schlussfolgerung, hebt *Hönig* die Rolle der internationalen Entscheidungsträger hervor:

„Initial Coin Offering (ICO) und Kryptowährungen sind Innovationen, die eine virtuelle, unregulierte und grenzüberschreitende Welt darstellen. Demgegenüber steht die reale Welt mit 194 Staaten und ihren Wirtschaftsräumen, in denen eigene Gesetze, Regeln und Normen gelten. Diese beiden Welten sind noch nicht miteinander kompatibel – das wird die Herausforderung der kommenden Jahre für die Entscheidungsträger in Politik, Wirtschaft und Gesellschaft werden.“[31]

In Deutschland geben die Positionen des Bundesverbands Öffentlicher Banken Deutschlands[32] wichtige Hinweise bezüglich der Zielsetzungen im Koalitionsvertrag im Bereich der „Erschließung des Potentials von Blockchain-Technologien und Verhinderung ihres Missbrauchs“:

- „Innovative Blockchain-Technologien ermöglichen neue Geschäftsmodelle. Dies gilt besonders auch für die deutsche Kreditwirtschaft.
- Den bestehenden Rechtsrahmen zu erweitern, ist nur dann notwendig, wenn die Anwendung bestehender Regulierung nicht greift.
- Eine technologiespezifische Regulierung sollte vermieden werden, um die Chancen des dezentralen Internets voll nutzbar zu machen. Aufgrund der Dezentralität ist ein auf Deutschland begrenzter Rechtsrahmen nicht ausreichend.
- Eine Regulierung von Kryptowährungen oder darauf basierenden Finanzinstrumenten sollte auf diese fokussiert sein und die Innovationschancen aus Blockchain-Technologien nicht gefährden.“

Die wichtigsten Erkenntnisse und Empfehlungen, die aus der Untersuchung zu „Blockchains, Smart Contracts und das Dezentrale Web“ Untersuchung von *Voshmgir* stammen, können aus den folgenden Zeilen entnommen werden – dementsprechend, werfen neuartige Anwendungen und Organisationsformen wie dApps oder DAOs gesellschaftsrechtliche Fragen auf, die noch zu klären sind:

- „Welches Recht gilt, wenn ein Unternehmen dezentral organisiert ist und keinen klassischen Firmensitz hat?

[31] *Hönig*, „Initial Coin Offering Studie zu Kryptowährungen und der Blockchain-Technologie“, Frankfurt University of Applied Sciences, Frankfurt am Main 2018, S. 3.

[32] VÖB-Positionspapier, Positionen des Bundesverbands Öffentlicher Banken Deutschlands: Politische Ziele der Digitalisierung in Deutschland, 22. März 2018, S. 4.

- Welche gesellschaftsrechtliche Form ist in so einem Fall sinnvoll und anwendbar?
- Auch steuerrechtliche Aspekte, Gewährleistungs- und Haftungsverpflichtungen u.v.m. sind derzeit kaum geklärt.
- Für Smart Contracts, die Verträge in Form von Programmcode sind, fehlt noch ausreichende Erfahrung in der Rechtspraxis, wie diese rechtssicher gestaltet werden können."[33]

Zum Schluss fällt auf, dass – obwohl die innerlichen *Blockchain spezifische Herausforderungen* und *Dezentrale Internet-Probleme* technischer und wirtschaftlicher Natur (wie z.B. das Risiko der Zentralisierung durch *Mining Pools* und die *„51 % Attack"* Gefährdung) relativ hoch sind, die wichtigsten Aufgaben werden im Regulierungsbereich auf nationaler und hauptsächlich internationaler Ebene liegen, um die Kluft zwischen nationalem Recht und das komplizierte Geflecht von internationalen multilateralen Verträgen zu verringern und um den Anforderungen einer globalisierten Internet-basierten Gesellschaft gerecht zu werde.

[33] *Voshmir,* „Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung Berlin 2016.

Literatur

Bogenstahl, Christoph/Ferdinand, Jan-Peter: Legal Techs – algorithmische Rechtsberatung. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Themenkurzprofil Nr. 12, Mai 2017, https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-012.pdf (abgerufen am 17.5.2018).

Buchleitner, Christina/Rabl Thomas: Blockchain und Smart Contracts Vom Ende der Institutionen. Ecolex Fachzeitschrift für Wirtschaftsrecht 2017, 1–92, Rsp-Nr 1–39, S. 4-14, https://www.kwr.at/fileadmin/res/2017/Presseartikel/ecolex_2017-01__4_Thomas_Rabl.pdf (abgerufen am 19.5.2018).

Hönig, Michaela: Initial Coin Offering Studie zu Kryptowährungen und der Blockchain-Technologie. Frankfurt University of Applied Sciences, Frankfurt am Main, Mai 2018, https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3 /Kontakt/Professor_inn_en/Hoenig/20180502_Bitcoin_Studie_fra_uas_Hoenig_V1.0.pdf (abgerufen am 12.6.2018).

Kofler, Johannes: Blockchain. AKKT Forschungsgesellschaft, 2018, https://www.aciworldwide.com/insights/expert-view/2017/march/blockchain-for-retailers-producing-real-business-benefits (abgerufen am 19.5. 2018).

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

Schlatt, Vincent/Schweizer, André/Urbach, Nils/Fridgen, Gilbert: Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik, 2016, https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf (abgerufen am 16.5.2018).

Thiele, Daniel/Ehrenberg-Silies/Simone: Blockchain. Themenkurzprofil Nr. 1 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Karlsruher Institut für Technologie (KIT), Mai 2016.

Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web. Technologiestiftung, Berlin 2016.

VÖB-Positionspapier: Positionen des Bundesverbands Öffentlicher Banken Deutschlands: Politische Ziele der Digitalisierung in Deutschland, März 2018, https://www.voeb.de/download/positionspapier-digitalisierung, (abgerufen am 12.6.2018).

WEB-BAVC: Legal Tech: Freund oder Feind der Juristen?, 2018, www.bavc.de/bavc/web/web.nsf/id/li_ib_02_2018_fa5.html (abgerufen am 18.5. 2018).

UNIFICATION THROUGH DISTRIBUTION?

David Saive

Interdisziplinäres Zentrum für Recht der Informationsgesellschaft (ZRI)
Carl von Ossietzky Universität Oldenburg
david.saive@uni-oldenburg.de

Summary

This article gives a brief presentation of the functions of the Blockchain-technology and the legal issues arising from the possible international distribution of all participants of the network. After that, international regulative approaches will be outlined and examined whether they provide sufficient rules for solving the legal problems. The article focuses on the rules guiding the applicable law and the place of jurisdiction. It shows that current legislative works are not sufficient and thus provides and explains an own Model Law on Blockchains (ML-B) at the end.

1 Bits, blocks and beyond

The Blockchain technology seems to have the power to disrupt every single corner of human interaction. Since the rise of Bitcoin and other cryptocurrencies, this assessment has become more and more true. Start-ups, bigger companies and national and international authorities are evaluating the benefits and risks of the usage of the technology. But what is so special about the technology?[1]

The term Blockchain refers to a purely distributed peer-to-peer data structure. Every user ("node") keeps a copy of the whole record by himself. New data is only added, if the majority of the nodes agrees to. The nodes evaluate, whether the new information complies with the formal requirements or not. An information which is contrary to already stored data will not become part of the storage. To prevent the data from tampering, a complex cryptographical procedure is executed ("hashing"). By hashing the information, a new string is created, which solemnly represents the underlying information. Blocks of information are connected through hashing all their hash-values and solving a certain task ("hash puzzle"). The task usually contains the finding of a certain number that must be added to the block, that the block hash-value complies with a special requirement, e.g. starting with three zeros or something similar. This process called "proof of stake" can only be solved by the usage of brute force, which makes the solving itself cost-intensive and the altering of the information contained, even more. New information is linked to the former by creating new blocks,

[1] Detailed view on the fundamental on functionalities of a Blockchain: *Saive*, CR 2018, S. 186-193.

which contain the hash of their predecessors. Therefore, Blockchains are most likely to store transaction histories.

2 Different usage, different Blockchain

There is no one and only Blockchain. The specifications of the Blockchain-architecture depend from the specific use-case. Cryptocurrencies need as many as possible participants or nodes to create acceptance. If only a few people are allowed to join the cryptocurrency network, broad acceptance cannot be reached. Therefore, a public Blockchain is needed, where everyone can join as a node and send and receive amounts of the currency used.

On the other hand, a private Blockchain is needed, where only a few persons are allowed to join the network. The access to the network is restricted from the start. A central instance or network administrator works as gatekeeper to grant access to the network. This Blockchain-architecture is also called consortium Blockchain.[2]

3 Tokenized trade

The Blockchain-technology can be used for many different use cases. The aforementioned cryptocurrencies are only one out of numerous applications. In general, a Blockchain is useful, when certain kind of information needs to be shared highly tamper resistant between many users at a time. This information can be of any kind, e.g. ownership of a certain object or even the object itself.

Even the ownership of real life assets can be tracked and proven by a Blockchain. By creating a so-called *asset backed token,* tangible or non-tangible assets can be connected to a digital token. This token represents the asset inside the Blockchain network and thus can be transferred between the nodes.

4 International approaches on the technology

Because of the purely distributed structure of the technology, the nodes may easily be spreaded all over the world. The only thing needed is a personal computer and access to the world wide web. Therefore, many legislations may affect the Blockchain technology. In the following, examples of international legislative work about Blockchains are given and examined, whether they cover all the legal aspects of the technology.

[2] *Dhillon/Metcalf/Hooper,* Blockchain Enabled Transactions, p. 41.

4.1 EU-Resolution on distributed ledger technologies and Blockchains

On 16th of May, 2018 the European Parliament passed a resolution to support distributed ledger technologies (DLT) and Blockchains. The resolution (2017/2772 (RSP)) called *distributed ledger technologies and Blockchains: building trust with disintermediation* deals with all the aspects, the Committee on Industry, Research and Design found important for DLTS and Blockchains. One of the main points of the resolution is, that a legal framework must be established to accompany the technical revolution caused by the introduction of DLT and Blockchain technology. Nonetheless it does not contain any binding rules for the usage of DLT or Blockchains.

4.2 UNCITRAL on Blockchain

The United Nations Commission on International Trade Law (UNCITRAL) was established to promote the harmonization and unification of international trade law. The idea that stood behind, was that harmonization of law will dismantle barriers of trade and therefore unify the world. UNCITRAL tries to reach this goal by developing model laws, that national legislations should use as role model for their own domestic laws.

Until today, UNCITRAL has not created any model laws directly addressing Blockchain-technology. Nevertheless, as *Takahashi* points out some of the older model laws do have an impact on the technology.[3]

4.2.1 Model Law on Electronic Commerce (1996) (EC Model Law)

Over twenty years before the Blockchain-technology was invented, UNCITRAL drafted the EC Model Law. UNCITRAL tried to prepare the law for the new technological development, especially the computer and early digital communication via internet. The EC Model Law was created neutral to technology, therefore it also applies to Blockchain-applications. Basically, it points out the requirements of an electronic conclusion of contract to be equivalent with the analogue ways.

4.2.2 Model Law on Electronic Signatures (2001) (ES Model Law)

The ES Model Law sets out the condition of how an electronic signature must be created, to fulfil the same function as the analogue signing of a document. A signature in general is needed, to proof the origin of a document and its authenticity and integrity. Since the ES Model Law is also constructed neutral to technology, Blockchain-based contractual agreements need to fulfil the conditions wherever a contractual agreement that requires a signature is represented through the network itself.

---

[3] For the following paragraph see: *Takahashi,* UNCITRAL works on Blockchains, p. 81 (81 ff.).

4.2.3 Model Law on Electronic Tradeable Records (2017) (ML-ETR)

The ML-ETR is the first Model Law at which UNCITRAL had Blockchains or distributed ledger technology in mind. The scope of the ML-ETR is to set standards for electronic tradeable records, such as Bill of Ladings or other to harmonize and therefore ease the international trade of these documents. Again, the principle of functional equivalent was used and outlined in the model law.

4.3 Functional equivalent as basic principle

The review of the international legislative efforts on the technology showed, that in fact, there is no international law on Blockchains. The international legislative work is neutral to technology. They rather try to provide a guideline for replacing analogue aspects of law and trade with digital solutions. The principle of *functional equivalents* is used, to include every thinkable technology.

5 Applicable law and place of jurisdiction in Blockchain-based claims

Due to the neutrality of technology, the special legal problems, that derive from the distributed architecture of the Blockchain, are neither covered by the UNCITRAL nor by the EU resolution. The main problem deriving from that is the question, which law shall be applicable and where the place of jurisdiction is in the case of claims between two or more nodes of a Blockchain.

There are many possible cases, where nodes of the same Blockchain may file lawsuits against each other. In general, every time the information contained in the Blockchain database is linked to real life aspects, the nodes are interested in the correctness of the data. Especially when it comes to the trade of asset backed tokens, the correctness of the transfer history is crucial to the parties. If there is no way to take legal action against the wrongful owner, the rightful owner of the token, and therefore holder of the real-life asset is helpless.

In the following, the legal connection between the nodes of a Blockchain network shall be examined to find rules of international private law about the applicable law and place of jurisdiction. Eventually, a proposal of an international framework is provided to harmonize the treatment of Blockchain-based claims.

5.1 Legal connection between the nodes of a Blockchain

There are three possibilities of how the connection of the nodes among each other can be viewed under legal aspect. They might be connected by a

written or non-written contractual agreement. Further a tortious relationship between the nodes is possible, where a node manipulates the Blockchain database maliciously. Another legal possibility is, that the nodes form a company themselves. In the case of a token based Blockchain, the claims between the nodes may be of possessory or contractual nature.

While examining the legal connection it must be differentiated between the node of a public and a private Blockchain structure. In public Blockchains, the nodes are only connected by the Blockchain algorithm or smart contract, whereas in private Blockchains a central administration takes care of the connection between the nodes.

5.1.1 Contractual relationship

Every Blockchain network requires an underlying code structure or algorithm. It contains the basic architecture on how the network works, who can participate, what data is stored and which consensus mechanism is used. All participating nodes of the network agree with this algorithm. Nowadays this underlying algorithm is also called *smart contract*.[4] This term is then used when legal connections between people are governed by the algorithm. Best example of a smart contract is the chartering of a ship, where the ship can only be used, when the algorithm has confirmed the payment of the charter rate. If not, the usage of the machines is blocked automatically.

Some say, that a *smart contract is neither smart, nor a real contract*.[5] Where the first part is correct, the second part is not. All nodes of the network do agree on what subject the network is about and how the algorithm works. The smart contract might be considered as multipart *terms and conditions* between the nodes. The only difference between the smart contract and conventional contracts is, that they are written in code and automatically executed.

But that's not all. There might be a second agreement between all the nodes of a Blockchain-network. It is the implied agreement, that they all will comply with the smart contract.

In private Blockchains a third agreement enters the field. It's the agreement between all the nodes and the central administration, that they will comply to the rules of the central administration on the one hand and the central administration takes care about the network on the other hand.

---

4 *Sixt,* Bitcoins und andere dezentrale Transaktionssysteme, S. 14.

5 *Henglein,* Vortrag auf dem Cyber Security, Privacy and Blockchain High Tech Summit, Danmarks Tekniske Universitet, 21.9.2017.

Thus, every misbehaviour of a node might be seen as a breach of contract. Either the contract between the nodes itself or the central administration and the nodes.

5.1.2 Tortious connection in case of misbehaviour

If we compare the smart contract of a Blockchain network with the set of rules of a football game, another legal view on the connection between the nodes emerges. All players of a football match agree to comply with the rules of the game, exactly as the nodes agree on complying with the smart contract. If some football player fails to comply and commits a foul, e.g. by tackling another from the behind, the referee punishes him. If the tackled victim gets injured, he seeks for compensation. But, compensation is only granted, when the tackling player commits a harsh foul, far outside the rules of the game. Usually this is a matter of tort and not of contractual law.[6]

Transferred to the Blockchain, a node that does violate the smart contract by tampering it, would be subject to tort law as well. In this case, there is no difference between public and private Blockchains. It doesn't matter, whether the game is part of an official FIFA tournament, which decides who may join and what rules are to comply with or a casual Sunday league game between friends. The same tort rules apply. In Blockchain-terminology the FIFA is nothing less than a central administration, that looks after the nodes.

5.1.3 Quasi-Corporate law connection

Third, the connection between the nodes might be considered as quasi-corporate like.

Under German law, a partnership organised under the civil code (§ 705 ff. BGB) is formed, if more than two people decide to follow a common purpose. Any legal purpose is sufficient.[7]

Under Rumanian law, the *societate in nume collectiv* or general partnership in general consists out of two persons, that carry out trading operations, Art. 1, par. 1 and Art. 2, lit. a) HGG 31/1990. For creating a SNC a written founding document is needed, Art. 5, par. 3 HGG 31/1990.

Under English law, a general partnership can be established if more than two persons carry out a business in common with a view of profit, Partnership Act 1890, sec. 1 par. 1.

---

6 German law: *Förster,* MüKo BGB, § 823 Rn. 564 ff.; English law: Elliott v. Saunders & Liverpool FC (1994); Ben Colett v. Gary Smith & Middlesborough FC (2008).

7 *Schöne,* BeckOK BGB, § 705 Rn. 63; *Schäfer*, MüKo BGB, § 705 Rn. 144.

All the nodes of a Blockchain together form a new organization, whose only purpose is to create a network and maintain authenticity and integrity of the information stored in the distributed database. If tokens are used and traded amongst the nodes, the purpose of the connection between the nodes is trading of the tokens. Under German law this could be sufficient for founding a partnership under the civil code. The common purpose of the nodes is the maintenance of the Blockchain network itself. The requirement of a written document under Rumanian law speaks against the foundation of a SNC. Under English law, a view of profit is needed. This might only be fulfilled if the Blockchain network is used for commercial uses.

But there is another aspect, that speaks against a corporate relationship between the nodes. When it comes to disputes between the nodes, their interests are diametrically opposed. They are not arguing about the basic functionality of the underlying algorithm itself, but the legal correctness of the result of the algorithm, e.g. where the executed Blockchain transaction must be revoked because of wrong information entered into the algorithm. In these cases, the dispute does not derive from the "Blockchain-corporation" but from the misuse of the technology.

5.1.4 Interim result: *It's difficult*

The examination showed, that the legal assessment of the connection between the nodes is difficult. Neither of the provided solutions is able to convince. Most likely, the treatment of misbehaviour of one the nodes be treated as a breach of contract seems to be most convincing. Therefore, other approaches need to be found, to cope with the legal aspects of the technology.

5.1.5 Token based claims

In the case of token-based networks, another solution is conceivable. Asset-backed tokens represent real life values. If the represented value is a tangible good, claims concerning the rightful ownership of the token might be considered as matter of property law. There is no difference, whether the change of ownership or property is achieved by transferring the good itself or a token representing it digitally. Thus, asset-backed token traded in Blockchain-networks might be subject to (international) property law.

5.2 Applicable law

The search for the applicable law in terms of international disputes is as complicated as the finding of the substantive law. Still, there is not international legislation at sight, that treats with international harmonization of

private law. Only some EU-regulations[8] and a few bilateral agreements[9] had been ratified in the last decades. Whereas intra-European disputes may be solved by using the Rome-regulations, fully international disputes are hard to solve. It gets even harder, when it comes to the enforcement of judgements. Many countries require an expensive exequatur process before a foreign judgement can be enforced.[10]

5.3 Place of jurisdiction

Usually, the place of jurisdiction is linked to the defendant's place of residence.[11] Sometimes the place of performance shall be the place of jurisdiction.[12]

6 Proposal for a Model Law on Blockchains

To fill the gap of lacking international legislative works on Blockchains, a short proposal for an international Model Law on Blockchains (ML-B) shall be given in this last paragraph. Subject of the ML-B are mandatory rules for the applicable law and the place of jurisdiction. The ML-B does not contain any rules, that neither govern failures of the smart contract, nor any other substantive questions of the technology. This should be subject to the applicable national law. The ML-B differentiates between public and private Blockchains to satisfy all the users' needs. In addition, special rules for token-based claims are developed.

6.1 Applicable law

The main question governed by the ML-B is the question of the applicable law. Many different opportunities of linking a Blockchain-based claim to national law are possible: *law of the genesis block, law of claimant or defendant, law of the country with the closest connection to the network*. In private Blockchains the *law of the central administration* might be another possibility.

The law of the genesis block seems to be suitable, because inside the first block of the network, the whole architecture of the following Blockchain is manifested. Every following transaction or information send or executed

8 EC Regulation No. 593/2008 (Rome-I); EC Regulation No. 864/2007 (Rome-II).

9 Hague Civil Procedure Convention (1954); Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters (1988).

10 In Germany: par. 722 of the Code of Civil Procedure.

11 *Martiny,* MüKo BGB, Vor. Art. 1 Rom-I VO Rn. 40.

12 *Martiny,* MüKo BGB, Vor. Art. 1 Rom-I VO Rn. 41.

inside the network must comply with those given in the genesis block. Otherwise no Blockchain, but a fork is created.[13]

Although the genesis block sets the basis for the whole network, linking the law to the place, where the genesis block is created is not a suitable solution. In fact, it is not always clear, where exactly the genesis block has been created. Even if the place of creation is known, another problem arises. The place of creation might be the one, where the creation act was executed or the place of origin of the creator itself. Furthermore, the link between this national legislation and the whole network seems rather artificial. It is based on coincidence, whether the main part of the Blockchain is operated from the same country as the genesis block, or not.

Therefore, the national law with the closest connection to the Blockchain seems like a better solution. If the majority of the nodes operate from one country, the corresponding national law shall apply. Yet, two technical aspects thwart this approach. First, in public Blockchains the origin of the nodes is not always identifiable. Users may disguise their connection through proxy servers or VPN-tunnels. Second, the majority of the nodes' origin may change every second. Again, it's just a matter of coincidence whether the majority of the nodes is based in one country or another.

At least, in private Blockchains this problem can be prevented by linking the applicable law to the law of the central administration. This is an appropriate solution, because all nodes know at the beginning, that they were governed by a certain central authority.

The best solution for public Blockchains is to link the applicable law to the origin of the parties of the claim. Thereby an appropriate balance of the different interest can be achieved. The question deriving from this is, how law that has the closest connection to the parties can be identified. To answer this question a view on the principles developed on the term *closest connection* in Art. 4 par. 4 Rome-I-Regulation is helpful. Criteria e.g. the citizenship of the parties, the place to which the information stored in the Blockchain-database or the place of business indicate the closest connection.[14]

6.2 Place of jurisdiction

The place of jurisdiction shall be place of residence of the defendant. In private Blockchains the claimant may choose between the residence of the defendant or the location of the central administration.

[13] *Sixt*, Bitcoins und andere dezentrale Transaktionssysteme, S. 11.

[14] BeckOK BGB, Rom-I VO, Art. 4 Rn. 83.

6.3 Special rules on token-based claims

In case of asset-backed-token-based claims the applicable law can be identified by using the rule of *lex rei sitae*. The applicable law is the one, where the represented asset was located when the dispute between the parties arose.

7 International Approach is necessary

The struggle with identifying the applicable law and place of jurisdiction has shown impressively that international legislation works on Blockchains are vital. If the applicable law cannot be identified, no Blockchain-based dispute can ever be solved.

Thus, mandatory international agreements shall be erected, to bind the parties of the disputes deriving from the use of a Blockchain. The CISG could be used as a role model. This is a huge chance to reconnect the world in times of separation and protectionism. So, to speak, the distribution of the Blockchain nodes around the globe helps to overcome national borders.

Literatur

Bamberger, Georg/Roth, Georg/Hau, Wolfgang/Poseck, Roman (Hrsg.): Beck Online-Kommentar BGB, 45. Aufl., München 2018.

Dhillon, Vikram/Metcalf, David/Hooper, Max: Blockchain Enabled Transactions, Berkeley 2017.

Henglein, Fritz: Smart contracts are neither smart nor contracts, Vortrag auf dem Cyber Security, Privacy and Blockchain High Tech Summit, Danmarks Tekniske Universitet, 21.9.2017, http://www.diku.dk/~henglein/smart-contracts-are-neither.pdf.

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7. Aufl., München 2017.

Saive, David: Haftungsprivilegierung von Blockchain-Dienstleistern gem. § 7 ff. TMG, CR 2018, S. 183-193.

Sixt, Elfriede: Bitcoins und andere dezentrale Transaktionssysteme, Wiesbaden 2017.

Takahashi, Koji: UNCITRAL works on Blockchains, in: Proceedings of the Congress of United Nations Commission on International Trade Law, Vienna 2017, S. 81-95.

BLOCKCHAIN UND DIE DSGVO

Av Carmen Lupsan

Stalfort Legal. Tax. Audit.
clupsan@stalfort.ro

Zusammenfassung

Blockchains erfreuen sich unter anderem wegen des Schutzes, den die unveränderbare Speicherung von Daten mit sich bringt, einer wachsenden Beliebtheit und werden immer mehr in unterschiedlichen Bereichen eingesetzt. Dadurch wird einerseits eine hohe Sicherheit für die gespeicherten Daten gewährleistet, andererseits aber ist durch die Natur der Blockchain die Gewährleistung bestimmter Rechte und Pflichten gem. der DSGVO (fast) unmöglich. Dieser Beitrag möchte einige Widersprüche zwischen Blockchain und DSGVO hervorheben und gleichzeitig einige existierende Lösungsansätze aufzeigen. Ferner ist die Erkenntnis wichtig, dass Blockchain zukünftig in immer mehr Bereichen angewendet wird und entsprechend eine Lösung für die Konformität mit der DSGVO gefunden werden muss. Hierbei wird eine enge Zusammenarbeit erforderlich sein, um technische Ansätze zu finden, die mithilfe der gesetzlichen Anpassungen die Blockchain in die DSGVO-Konformität befördern sollten.

1 Blockchain-Arten

Die Anwendbarkeit der DSGVO auf Blockchain kann nur im Kontext der unterschiedlichen Arten der Blockchains beurteilt werden. Hierbei ist insbesondere zwischen den öffentlichen und privaten Blockchains zu unterscheiden. Obwohl es auch komplexere Blockchain-Konstruktionen (z.B. Hybride zwischen öffentlichen und privaten Blockchains) gibt, wird nur auf diese zwei Arten eingegangen.

1.1 Unpermissioned Blockchains (öffentlich)

Unpermissioned Blockchains sind offen, dezentral und verteilt (*distributed ledger*) geführte Register. Jeder Teilnehmer am Blockchain, der Daten speichert und verarbeitet, hat dieselben Rechte und Befugnisse. Somit fügt jeder dieser Teilnehmer Informationen hinzu (neuer Block). Die Entscheidung über das Hinzufügen eines neuen Blocks wird durch Mehrparteienkonsens (*peer-to-peer consensus*) getroffen; alle Kopien werden daraufhin um diesen Block ergänzt.

1.2 Permissioned Blockchains (privat)

Permissioned Blockchains sind geschlossene (nur für bestimmte Teilnehmer zugängliche) Blockchains. Die Rechte und Befugnisse der Teilnehmer werden von einer zentralen Stelle eingeräumt. Dies bedeutet, dass bestimmte Teilnehmer berechtigt sind, neue Blocks hinzuzufügen, während

andere Teilnehmer lediglich die Befugnis haben, die Informationen einzusehen.

2 Blockchain im Rahmen der DSGVO

Während die DSGVO eine änderbare Speicherung von Daten fordert – z.B., um diese auf Anforderung der betroffenen Person ändern zu können, und von einem identifizierbaren Verantwortlichen und der Verarbeitung durch den Verantwortlichen oder einen Auftragsverarbeiter ausgeht, lebt die Blockchain gerade davon, dass die Daten unveränderbar und somit deren Verarbeitung als besonders sicher gelten. Hier gibt es nicht einen Verantwortlichen; jeder Teilnehmer kann vielmehr Blocks einfügen.

2.1 Was sind personenbezogene Daten im Blockchain?

Personenbezogene Daten werden im Blockchain (i) als Klartext, (ii) verschlüsselt oder (iii) durch Hashing verarbeitet. Während es eindeutig ist, dass Klartext und verschlüsselte Daten, die mit dem richtigen Schlüssel entschlüsselt werden können und somit auf die betroffene Person zurückzuführen sind, personenbezogene Daten darstellen, stellt sich die Frage, wie dies im Falle von Hashing zu deuten ist.

Eine Hashfunktion kann im Gegensatz zur Verschlüsselung nicht rückgängig gemacht werden. Obwohl das Hashing wesentlich sicherer als die Verschlüsselung ist, hat die WP 29 es ebenfalls als Pseudonymisierung ausgelegt und so behandelte Daten damit als personenbezogen gedeutet.[1]

Public keys, die im Rahmen der Transaktionen genutzt werden, obwohl sie nicht mehr einer bestimmten Person zugeordnet werden können, sind ebenfalls personenbezogene Daten, weil diese mithilfe der private keys wieder bestimmten Personen zugeordnet werden können.

2.2 Wer ist Verantwortlicher?

Der Verantwortliche gem. der DSGVO ist derjenige, der über den Zweck und das Mittel der Verarbeitung entscheidet. Die DSGVO geht davon aus, dass Daten entweder von einem Verantwortlichen oder von einem Auftragsverarbeiter verarbeitet werden.

Sollte es im Rahmen einer permissioned Blockchain möglich sein, unter Umständen die zentrale Stelle, die Teilnehmern Rechte und Befugnisse erteilt, als Verantwortlichen zu sehen, so ist es im Falle der unpermissioned Blockchains unmöglich, einen Verantwortlichen zu finden. Verantwortlicher können entweder alle oder kein Teilnehmer (Knoten) sein. Aus diesem Grund ist es auch schwierig, die Rechte und Pflichten sowie die durch

[1] WP 29 Opinion 5/2014 on Anonymisation Techniques, Pkt 4.

die DSGVO eingeräumten Grundsätze in der Blockchain umzusetzen und einzuhalten. Weiterhin stellt sich in dieser Situation auch die Frage der Haftung und Haftbarkeit. Eine unpermissioned Blockchain ist keine Rechtsperson als solche.

2.3 Beispiele von DSGVO-Grundsätzen, die nicht (oder nur schwierig) im Blockchain umgesetzt werden können

Aufgrund der unveränderbaren Speicherung von Daten in der Blockchain ist es fast unmöglich, die aufgrund der DSGVO (und übrigens auch zuvor) einzuhaltenden Grundsätze in der Blockchain umzusetzen. Aus diesem Grund ist es sehr wichtig, bestimmte technische Lösungen zu finden, die die große Kluft zwischen der DSGVO und Blockchain einigermaßen verringert.

2.3.1 Berichtigung und Löschung personenbezogener Daten

Aufgrund der Unveränderbarkeit der Blocks ist eine Berichtigung oder Löschung auf Anfrage der betroffenen Person nicht möglich. Blockchain lässt die Änderung eines Blocks nicht zu; es kann lediglich ein neuer berichtigender Block hinzugefügt werden. Dies bedeutet jedoch, dass auch die frühere Information weiterhin in der Blockchain bestehen bleibt und für alle sichtbar ist. Folgende Lösungsansätze wurden unter anderem angesprochen:

2.3.1.1 Off-chain Storage

Als Lösungsansatz wird die Aufbewahrung der personenbezogenen Daten außerhalb der unpermissioned Blockchain (*off-chain storage*) angesprochen. Dies ermöglicht es, von der zentralen Stelle die personenbezogenen Daten zu ändern, die in einer unpermissioned Blockchain nur mit einem Hashpointer verbunden und somit nicht im unpermissioned Blockchain gespeichert sind.

2.3.1.2 Redactable Blockchain

In einer redactable Blockchain kann die Hash-Verbindung aufgetrennt und der alte Block mit einem neuen geänderten Block ersetzt werden. Die Bearbeitung bleibt für alle ersichtlich (wie eine Narbe), zum alten Block erhalten jedoch nur die Teilnehmer, die an der Änderung beteiligt waren, Zugang. Somit sind die alten Informationen/Daten auch nur für diese ersichtlich.

2.3.1.3 Löschung des private key

Für die Löschung der personenbezogenen Daten wird schließlich die Löschung des private keys als Lösung betrachtet. Infolgedessen bleiben zwar die Daten in der Blockchain bestehen, der Zugang zu diesen Daten wird jedoch gesperrt. Obwohl dies keine Löschung im Sinne der DSGVO ist, muss unter Berücksichtigung der Merkmale einer Blockchains allerdings

auch angemerkt werden, dass die Rechte auf Berichtigung und Löschung der personenbezogenen Daten keine absoluten Rechte sind. Eine solche Lösung könnte durchaus als angemessene Maßnahme erachtet werden, was aber entsprechend vom Gesetzgeber bzw. vom Europäischen Datenschutzausschuss berücksichtigt und geregelt werden sollte.

2.3.2 Auskunftsrecht

Sollte eine betroffene Person, die nicht Teilnehmer an der Blockchain ist, wissen wollen, welche ihrer personenbezogenen Daten verarbeitet werden, so müsste sie der Blockchain beitreten, um so eine Kopie aller in der betreffenden Blockchain gespeicherten Daten zu erhalten. Ob dies als Auskunftsrecht unter der DSGVO gedeutet werden kann, ist allerdings fraglich.

2.3.3 Datenminimierung

Die personenbezogenen Daten müssen entsprechend eines festgelegten, eindeutigen und legitimen Zweckes verarbeitet werden und die Verarbeitung muss auf ein notwendiges Maß beschränkt sein. Hier sind die Schwierigkeiten ähnlich mit denjenigen, die unter Punkt 2.3.1 angesprochen wurden.

2.3.4 Speicherbegrenzung

Aufgrund des für die Blockchain essenziellen Merkmals der Transparenz ist eine Löschung nach Ablauf einer bestimmten Zeit nicht möglich.

2.4 Blockchain im Alltag

Obwohl die oben dargestellten Diskrepanzen zwischen Blockchain und DSGVO existieren, wird die Blockchain im Alltag immer häufiger in unterschiedlichen Situationen eingesetzt:

2.4.1 Blockchain in der Logistik

Gesellschaften mit Tätigkeiten im Bereich Logistik testen Blockchain, um einerseits eine höhere Effizienz durch die Verfolgung der Güter zu gewährleisten und andererseits die Zurückverfolgung der Lieferkette durch den Verbraucher zu erlauben. Nicht zuletzt ermöglicht dies, den Stand der Waren zu verfolgen und die Transparenz im Rahmen des Zollaufenthaltes zu erhöhen.

2.4.2 eHealth

Estland hat in seinem medizinischen System die Blockchain eingeführt. Patientendaten werden außerhalb der Blockchain eingetragen. Wenn auf Daten zugegriffen wird oder diese geändert werden, wird die entsprechende Aktivität in der Blockchain eingetragen und eine „keyless signature“ neben den Eintragungen gespeichert. Diese Signaturen dienen als elektronischer Zeitstempel, der beweist, wann Änderungen vorgenommen wurden.

2.4.3 Blockchain für bestimmte Sicherheiten

Frankreich hat einen Rechtsrahmen für die Verwendung der Blockchain-Technologie bei der Registrierung und Übertragung nicht-börsennotierter Sicherheiten geschaffen.

2.4.4 Bankdaten der Kunden im Blockchain

Immer mehr Banken aus Polen wollen in ihrem System Blockchain für eine Speicherung und einen sicheren Zugriff auf sensible Kundendaten implementieren. Diese Blockchain-Technologie ist eine Lösung, die eine vollständige Transparenz garantiert und eine nachvollziehbare Historie sowie den Zugriff auf alle kundenbezogenen Daten gewährleistet. Zusätzlich sei sie, so Billon, der Entwickler dieser DLT-Technologie DSGVO-konform, obwohl sie auf Blockchain-Technologie basiert.

2.4.5 Digitale Identität und e-voting

Durch Blockchain hat die Stadt Zug einerseits die Möglichkeit für ihre Bürger eingeräumt, eine E-ID zu erhalten, und andererseits ein elektronisches Abstimmungssystem implementiert.

Literatur

Finck, Michèle: Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18-01.

Marnau, Ninja: Die Blockchain im Spannungsverhältnis der Grundsätze der Datenschutzgrundverordnung, Informatik 2017, S. 1025-1036.

Salmensuu Cagla: The General Data Protection Regulation and Blockchains (January 1, 2018), Liikejuridiikka 1/2018.

GDPR COMPLIANCE IN THE INDUSTRY 4.0

RAin Cristiana Fernbach, LL.M., MBA/RAin Cătălina Fînaru

Stratulat – Albulescu SCA
cristiana.fernbach@stratulat-albulescu.ro,
catalina.finaru@stratulat-albulescu.ro

Summary

The world is more connected than ever, but we need to have a pragmatic vision about the future effects of the global digitalization and of the opportunities that this new and dynamic digital era brings to our attention. The legal framework must keep up the pace with the increased use of digital technologies and to address the challenges the use of personal data for interconnecting devices and for using cyber systems and intelligent robots brings. Innovative legal solutions must be designed and implemented on European and at a global level, that promote the digital evolution and protect the rights of the individuals.

1 Short History

In recent years it's become more difficult to distinguish the concept of "data protection" from the concept of "right to privacy". Right to privacy is an inalienable right of a natural person, whilst data protection is the process of safeguarding important information from corruption, compromise or loss. By protecting personal data, the right to privacy is partially respected.

Human rights are the basic rights and freedoms that belong to every person in the world, from the moment of birth until the moment of death. As the Universal Declaration of Human Rights states, "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[1]

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was concluded within the Council of Europe in 1981. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did.

As all member states of the European Union are also signatories of the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Commission was concerned that diverging data protection legislation would emerge and impede the free flow of data within the

[1] http://www.claiminghumanrights.org/udhr_article_3.html (last downloaded 19.7.2018).

EU zone. Therefore, the European Commission decided to propose harmonizing the data protection law within the EU. The resulting Data Protection Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data was adopted by the European Parliament and ministers from national governments in 1995 and had to be transposed into national law by the end of 1998.[2]

On the 25th of May 2016, Directive Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and free movement of such data ("General Data Protection Regulation" or "GDPR") came into effect, enforcing the already existing Data protection principles of the previous 20 years (Data Protection Directive 95/46/EC) and adding new rights for data subjects as well as new obligations for data controllers.

The GDPR contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects[3] inside the European Union, and applies to all enterprises, regardless of location, that are doing business with the European Economic Area.[4]

At the verge of the 20th century, traditional manufacturing and industrial practices combined with an increasingly technological world around us, has made the effort of maintaining the safety of a natural person's rights, in particular the privacy right, challenging.

Industry 4.0 is the name given to the move towards digitization and the use of the Internet of Things and cyber-physical systems such as sensors with the ability to collect data that can be used by manufacturers and producers.

The advancements in big data and powerful analytics mean that systems can trawl through huge sets of data and produce insights that can be acted upon quickly. The communications infrastructure that supports this, is secure enough to be used by heavy industries.

Smart factories will implement the use of information and communication technology for the evolution of the supply chain and production line, that will bring with it an increase of both automation and digitization. This

[2] https://en.wikipedia.org/wiki/Information_privacy_law#Europe (last downloaded 19.7. 2018).

[3] Identified or identifiable natural person.

[4] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (last downloaded 19.7. 2018).

means, machines will use self-optimization, self-configuration and even artificial intelligence to complete complex tasks in order to deliver vastly superior cost efficiencies and better-quality goods or services.[5]

2 Application and Principles of the General Data Protection Regulation

GDPR applies:

a) to the processing of personal data in the context of the activities of an establishment of a controller[6] or a processor[7] in the European Union, regardless of whether the processing takes place in the Union or not;

b) to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

c) to the processing of personal data by a controller not established in the European Union, but in a place where Member State law applies by virtue of public international law.

The core pillars of GDPR are represented by its fundamental principles, as follows:

a) **Lawfulness, fairness and transparency of data processing**: processing of personal data must happen in a lawful way and must be fair and transparent to data subjects;

b) **Purpose limitation**: personal data must be processed for the purpose(s) mentioned to data subjects at the time of collection;

c) **Data minimization**: limitation of processing personal data to the minimum of need in the scope of processing activity and established purpose(s);

d) **Accuracy of processed personal data**: processed personal data must be accurate and keep up to date;

---

[5] https://www.techradar.com/news/what-is-industry-40-everything-you-need-to-know (last downloaded 19.7.2018).

[6] Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[7] Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

e) **Storage limitation**: personal data should not be keep longer that is strictly needed for the processing purpose(s);

f) **Integrity and confidentiality**: the processing of personal data should be done in a manner that a proper level of security with regards to the personal data is guaranteed;

g) **Accountability:** the controller is responsible for GDPR compliance and should be able to demonstrate that compliance.

3 GDPR – Cloud Killer?

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information.[8] Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant.

According to the Cloud Security Alliance, the top three threats in the cloud are Insecure Interfaces and Application Programming Interfaces' ("API"), Data Loss & Leakage and Hardware Failure – which accounted for 29 %, 25 % and 10 % of all cloud security outages respectively. Together, these forms shared technology vulnerabilities.

Given the fact that the data processor is that legal or natural person which processes personal data on behalf of the controller, typically a cloud service provider would be qualified as a processor when cloud users use its services. So, when cloud service providers process personal data which is stored within their database or servers on a cloud users behalf, they qualify as data controllers. The cloud service provider cannot do anything with the cloud user's data unless the cloud user instructs the provider to do so and the data remains within cloud user's control.

The most important GDPR specific challenges for a cloud service provider can be summarised as follows:[9]

- Effective implementation of a retention period within the cloud and a clear overview of the cloud service providers' backups, as the GDPR imposes the obligations, both for data locally stored and data stored in the cloud, of not keeping personal data for a period longer than needed for the predefined processing purpose(s);

[8] https://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext (last downloaded 19.7.2018).

[9] https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-update-the-impact-on-cloud-computing.html (last downloaded 19.7.2018).

- The relationship between cloud user and cloud service provider is data controller to data processor and this type of relationship must be a contractual one. The contract must define a breach event and describe a procedure that the cloud service provider will follow about notifying the cloud user without undue delay regarding any breaches. Moreover, the data processor has the obligation to assist the data controller ensuring compliance with that obligation in case of a data breach;
- If no adequate decisions have been made about the storage of personal data in countries outside the European Union ("EU") or the European Economic Area ("EEA"), appropriate safeguarding measures must be adopted;
- Facilitate the rights of data subjects, in particular data portability, since it must be possible for the data controller to retrieve processed personal data in a structured, commonly used and machine-readable format to provide that information to the data subject or any other controller;
- Maintain control and ownership of personal data processed by the cloud service provider as controller and not as processor;
- Performing of Data Protection Impact Assessment ("DPIA") and a Security Assessment by the cloud user to determine any risk of cloud usage. The cloud service provider as data processor has the obligation to contribute to audits, including inspections, conducted by the cloud user as controller or another auditor mandated by the controller.

Both the cloud service provider as processor and cloud user as controller must implement technical and organisational measures to ensure an appropriate level of security, to the inherent risks of the data being processed.

Depending on the nature of their core activities and/or the type of processed personal data, both the cloud service provider as processor and cloud user as controller shall designate a data protection officer, on the condition that this is required according to article 37 paragraph 1 GDPR.

4 Big Data VS "Big" GDPR

Big data represents:

- large datasets;
- the category of computing strategies and technologies that are used to handle large datasets.

The most important characteristics of big data can be summarized by the 6 V's:[10]

- **Volume**: these datasets can be orders of magnitude larger than traditional datasets;
- **Velocity**: data is frequently flowing into the system from multiple sources and is often expected to be processed in real time to gain insights and update the current understanding of the system;
- **Variety**: big data is often unique because of the wide range of both the sources being processed and their relative quality;
- **Veracity**: the variety of sources and the complexity of the processing can lead to challenges in evaluating the quality of the data;
- **Variability**: variation in the data leads to wide variation in quality;
- **Value**: the systems and processes in place are complex enough so that using the data and extracting actual value can become difficult.

One of the most important principles of the GDPR is the lawful processing. One of the legal bases established by the General Data Protection Regulation is data subject's consent but obtaining meaningful consent can be difficult. Novel and innovative approaches may foster consent collection.

On the other hand, relying on the legal basis of legitimate interests is not a risk-free solution, because there should always be a balance between interests and the rights of the individual.

Regarding the data minimization principle, it may be difficult to show that big data analytics are strictly necessary for the performance of some contract and big data analytics can result in the collection of personal data that is excessive for processing purposes.

The Data controller should pay more attention to the storage limitation period, because, given the fact that big data applications are capable of analysing large volumes of data, personal data could be retained for longer than necessary.

The core of data protection aspects is represented by data subject's rights and in this context, it may be difficult for data controllers to comply with the right to access personal data due to a vast quantity of personal data used in big data analytics.

In a growing number of high-profile corporate cybersecurity breaches, hackers have stolen some of the most sensitive data that consumers have,

[10] https://www.digitalocean.com/community/tutorials/an-introduction-to-big-data-concepts-and-terminology (last downloaded 19.7.2018).

including identification numbers, passwords and financial information.[11] In this context, the most famous security incidents can be remembered as follows:

- Facebook's Security Incident – the breach exposed that Cambridge Analytica had begun to collect data on 50 million Facebook users from 2014 onwards;
- Uber's Security Incident – the breach exposed names, email addresses and phone numbers of 50 million people worldwide, plus the personal details of 7 million drivers;
- Greenwich University's Security Incident – the breach exposed the personal data of 19,500 students, including information on some students' mental health problems.

5 New Challenges for Artificial Intelligence

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems.[12]

Big data and artificial intelligence have a close bidirectional relationship which can be analysed both from the artificial intelligence perspective and from the big data perspective. So, artificial intelligence, through machine learning, needs a vast amount of data to learn. From the perspective of big data, artificial intelligence techniques are used to extract value from big datasets.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to privacy.

When developing and designing such products, services and applications and considering the technological state of the art, producers of the products need to ensure they are able to fulfil their data protection obligations. In this context, a robotics engineer should ensure that private information is kept secure and limited to appropriate use. In addition, a robotics engineer should guarantee that individuals are not personally identifiable, aside from exceptional circumstances and in such case only with clear, unambiguous, informed consent. Human informed consent should be pursued and obtained prior to any man-machine interaction. As such, robotics designers

[11] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (last downloaded 19.7.2018).

[12] https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence (last downloaded 19.7.2018).

have a responsibility to develop and follow procedures for valid consent, confidentiality, anonymity, fair treatment and due process. Designers must comply with all requests that require any related data to be destroyed and removed from any datasets.

Given the fact that artificial intelligence uses personal data of data subjects, special attention must be given to the principles of GDPR, which must be met for each such data processing.

The GDPR principles responsible for the most complex challenges in relation to artificial intelligence are as follows:

- **Fairness principle**: this principle requires that personal data is used in a relevant and correct manner and should not use information relating to racial or ethnic origin, political opinion, religion or philosophical belief, trade union membership, genetic status, health status or sexual orientation if this would lead to arbitrary discriminatory treatment;
- **Purpose limitation principle**: in cases where previously-collected personal data is to be re-used, the controller must consider whether the new purpose is compatible with the original one;
- **Data minimization principle**: the data controller should evaluate that the data collected is accurate, relevant and limited to the processing purposes
- **Transparency principle**: the data subject must be informed in a transparent manner as the use of artificial intelligence is a form of automated processing and in some cases the decision is taken by the robot.

6 Blockchain from a GDPR Perspective

We are living in a digital world and blockchain is a digitized, decentralized and public ledger of all cryptocurrency transactions.

Blockchain databases are particularly interesting because they allow - **at least in theory** - transactions between parties without having to disclose their identity directly to the contracting party or the public. However, studies have shown that the address of a service user can be traced back to its IP address, which in turn can be traced back to a specific internet connection or connection owner.[13]

In 2014, Article 29 Working Party, provided guidance on the difference between pseudonymised and anonymised data in its Opinion 05/2014 (WP

[13] https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html (abgerufen am 19.7.2018).

216). This distinction is important in relation to blockchain as data protection rules do not apply to anonymised data; as such data cannot be traced back to a living individual. However, the threshold for data to qualify as anonymised is very high. The guidance states that "anonymization results from processing personal data in order to irreversibly prevent identification". Data controllers must have regard to all means likely to be used for identification (either by the controller or any third party). Because hashing permits records to be linked, hashing will generally be considered a pseudonymisation technique, not an anonymization technique. This high standard will continue to apply under the European General Data Protection Regulation.

Encrypted personal data can often still be traced back to a person if enough effort is put into it by experts or someone holds the key to decryption. Therefore, encrypted data will often qualify as personal data and not as anonymous data. This means that in most instances the privacy rules will be applicable to at least some of the data involved in blockchain systems.[14]

When a business model is designed based on blockchain technology and participants are not required to provide their prior consent, other means or functions regarding the authenticating of the transaction and its validity, have to be developed. The legal base of processing of personal data in such cases might be:

- Either the performance of a contract or the necessity of processing personal data in order to take steps to enter into a contract, or
- legitimate interest of the controller, but these interests should not be overridden by the interests or fundamental rights and freedoms of the data subject.

7 Outlook on the Future

The world is more connected than ever, but we need to have a pragmatic vision about the future effects of the global digitalization and of the opportunities that this new and dynamic digital era brings to our attention.

As the industry 4.0 and whole concept of digitalisation continues to expand, the challenges for ensuring a safe environment for personal data is growing. Moreover, the future legal framework must provide means for balancing the human rights with the benefits of the digital industry.

[14] https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf (abgerufen am 19.7.2018).

It remains to see if and how the Directive on privacy and electronic communications will address and solve the specific challenges of the Industry 4.0 and what will be the strategy for growing opportunities for digital industry.

Literatur

Deloitte: Blockchain from a perspective of data protection law A brief introduction to data protection ramifications, https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html (last downloaded 19.7.2018).

Ellingwood, Justin: An Introduction to Big Data Concepts and Terminology, DigitalOcean v. 28.9.2016, https://www.digitalocean.com/community/tutorials/an-introduction-to-big-data-concepts-and-terminology (last downloaded 19.7.2018).

Hogan, Lovells: A Guide to Data Protection and Blockchain, https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf (last downloaded 19.7.2018).

ICO: Big data, artificial intelligence, machine learning and data protection https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (last downloaded 19.7.2018).

Moore, Mike: What is Industry 4.0? Everything you need to know, techradar vom 24.4.2018, https://www.techradar.com/news/what-is-industry-40-everything-you-need-to-know (last downloaded 19.7.2018).

Ryan, Mark D.: Cloud Computing Privacy Concerns on Our Doorstep. Communications of the ACM, January 2011, Vol. 54 No. 1, S. 36-38 (online verfügbar unter https://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext (last downloaded 19.7.2018).

Tolsma, Alex: GDPR and the impact on cloud computing. The effect on agreements between enterprises and cloud service providers, https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-update-the-impact-on-cloud-computing.html (last downloaded 19.7.2018).

DIE REGULIERUNG VON ALGORITHMEN UNTER DER DSGVO

Boris Reibach, LL.M.

Interdisziplinäres Zentrum für Recht der Informationsgesellschaft (ZRI)
Carl von Ossietzky Universität Oldenburg
boris.reibach@uni-oldenburg.de

Zusammenfassung

Algorithmen sind Teil unseres digitalisierten Alltags geworden. Mit der zunehmenden Digitalisierung steigt aber auch die Macht der Algorithmen, die zahlreiche Entscheidungen ohne menschliche Einflussnahme treffen. Nicht zuletzt seit dem Facebook-Skandal um Cambridge Analytica werden Stimmen laut, die eine gesetzliche Regulierung der Nutzung von Algorithmen fordern. Hinsichtlich der Datenschutzkomponente einer solchen Regulierung hätte die DSGVO eine moderne Antwort auf die mit Algorithmen verbundenen Risiken bieten können. Der Gesetzgeber hat diese Chance allerdings nicht genutzt und nur sehr eingeschränkte Regelungen zu Algorithmen in der DSGVO verankert.

1 Die Macht der Algorithmen

Aus unserem Alltag sind Algorithmen nicht mehr wegzudenken. Sie sind Teil unseres Lebens geworden – egal, ob beim Shopping, im Social Web, in der Bank oder bei der Erledigung von Behördengängen. Von den zehn wertvollsten Unternehmen der Welt sind es bereits drei (Alphabet, Tencent und Facebook), die ihr Geld ausschließlich mit auf Algorithmen basierenden, datengetriebenen Geschäftsmodellen verdienen:

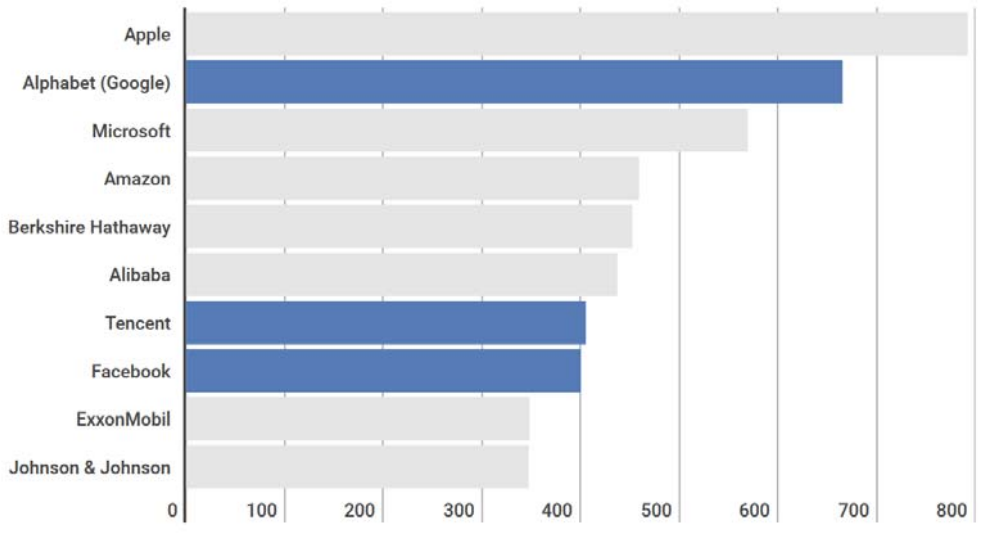

Abb. 1: Die zehn wertvollsten Unternehmen der Welt (Quelle: Financial Times)

Algorithmen entscheiden beispielsweise darüber, welche Werbung uns angezeigt wird. Sie bestimmen auch darüber, welche Route wir bei einer Navigation nehmen. Darüber hinaus berechnen sie, ob wir auf Rechnung zahlen können oder gar einen Kredit bekommen. Algorithmen bestimmen also unsere Alltagsaktivitäten, sie greifen – oftmals unbemerkt – erheblich in unsere Grundrechte ein. Ihre unausweichlichen Nebenwirkungen sind Diskriminierungen, denn sie sind gerade dazu gemacht, den Einzelfall im Sinne einer programmierten Abfolge von Berechnungen zu bewerten und damit ohne menschlichen Eingriff zu entscheiden.

Manch einer spricht also von einer „Herausforderung für die Rechtsordnung“[1] oder gar von der „Macht der Algorithmen“.[2] Und in der Tat nähern wir uns einer „Black-Box-Gesellschaft“,[3] in der die von den algorithmischen Berechnungen betroffenen Personen nicht mehr überblicken können, was mit ihren Daten geschieht. Die in Computersystemen steckenden Algorithmen wirken – zum größten Teil unbemerkt – auf unser von der Verfassung als selbstbestimmt garantiertes Leben ein und können in Sekundenbruchteilen Entscheidungen treffen. Oftmals sind es nicht nur die von der Verarbeitung betroffenen Personen, die keinen Einblick in die Abläufe der Algorithmen haben. Selbst Unternehmen und Behörden, die im Rahmen der Beauftragung von Dienstleistungen oder beim Outsourcing Technologien mit Algorithmen einsetzen, sind sich oft nicht im Klaren darüber, was die eingesetzten Systeme mit personenbezogenen Daten tun.

2 Algorithmen-TÜV vs. DSGVO

Es verwundert deshalb nicht, dass Stimmen laut werden, welche diese Macht der Algorithmen regulieren wollen. So ist die Rede von einem „Algorithmen-TÜV“,[4] der insbesondere nach dem Facebook-Skandal um Cambridge Analytica auch auf EU-Ebene diskutiert wird.[5] Nur mit einer starken Regulierung, so die Forderung, könne man den Gefahren der algorithmischen Gesellschaft begegnen. Beim Blick auf die möglichen Rechtsbereiche einer Regulierung kommen insbesondere das Datenschutzrecht,

1 *Martini*, JZ 2017, S. 1017.

2 *Boehme-Neßler*, NJW 2017, S. 3031.

3 *Pasquale*, The Black Box Society, S. 8 ff.

4 Vgl. meinungsbarometer.info v. 15.6.2017, https://www.meinungsbarometer.info/beitrag/Deutschland-braucht-den-Algorithmen-TueV_2269.html (abgerufen am 20.6.2018).

5 Vgl. zeit.de v. 17.4.2018, https://www.zeit.de/politik/ausland/2018-04/mark-zuckerberg-facebook-datenskandal-vera-jourova-eu-kommission-regulierung (abgerufen am 20.6. 2018).

das Wettbewerbsrecht, das Nichtdiskriminierungsrecht sowie sektorspezifische Regelungen in Betracht.[6] Nachfolgend soll deshalb geprüft werden, ob zumindest die DSGVO hinreichende Schutzmechanismen für die Betroffenen beim Einsatz von komplexen Algorithmen bietet.

Die Gesetzgeber der DSGVO sind u.a. mit dem Ziel angetreten, dem Bürger mehr Transparenz bei der Verarbeitung seiner personenbezogenen Daten zu gewähren. Es verwundert deshalb nicht, dass die Betroffenenrechte in der DSGVO – anders als im BDSG vor dem 25. Mai 2018, wo die Betroffenenrechte noch in den Schlussregelungen ein Nischendasein führten – einen prominenten Platz eingenommen haben und unmittelbar nach den Legitimationstatbeständen in den Art. 12-22 DSGVO ausführlich geregelt werden. Dabei wurden die Transparenzmaßnahmen gegenüber den betroffenen Personen am detailliertesten geregelt – Art. 13 DSGVO beispielswiese enthält einen Katalog mit zwölf Punkten, über die Verantwortliche die betroffenen Personen im Zeitpunkt der Erhebung personenbezogener Daten informieren müssen. Für die automatisierte Entscheidungsfindung ist in Art. 13 Abs. 2 lit. f DSGVO eine Regelung aufgenommen worden, nach der aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer Verarbeitung mitzuteilen sind. Auch das Recht auf Auskunft zu den eigenen personenbezogenen Daten nach Art. 15 DSGVO ist im Gegensatz zur bisherigen Rechtslage unter dem BDSG a.F. erweitert worden.[7] Dass Transparenz für den Gesetzgeber eine sehr wichtige Rolle spielt, wird auch bei der Regelung des Art. 5 Abs. 1 lit. a DSGVO deutlich: innerhalb der dort geregelten Grundsätze steht die Transparenz an erster Stelle. Kann man also davon ausgehen, dass die DSGVO hinreichende Maßnahmen trifft, um die uns im Alltag begegnenden Algorithmen zu regulieren?

3 Regulierung der Algorithmen in der DSGVO

3.1 Grundsatz der Fairness

Aus Art. 5 Abs. 1 lit. a DSGVO ergibt sich, dass jedweder Einsatz von Algorithmen zur Verarbeitung personenbezogener Daten sich am Prinzip von „Treu und Glauben“ orientieren muss. In der deutschen Sprachfassung wird für das englische „fair“ der Begriff „Treu und Glauben“ verwendet – für die Betrachtung der Algorithmusregulierung bietet es sich aber an, das englische „fair“ auch in die deutschen Sprachfassung hineinzulesen und die Verwendung nur solcher Algorithmen zuzulassen, die mit Blick auf beide

[6] Vgl. das ABIDA-Gutachten, abrufbar unter http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf (abgerufen am 20.6.2018).

[7] *Bäcker,* in: Kühling/Buchner, DS-GVO BDSG, Art. 15 Rn. 46.

Parteien – Verwender und betroffene Person – ausgewogen sind. Entscheidend wäre dann, dass

- der Verwender nicht wissentlich auf ein milderes Mittel verzichtet, das die betroffene Person weniger stark beeinträchtigt und für den jeweiligen Zweck gleich geeignet ist;
- die Verwendung des Algorithmus keine völlig überraschenden, negativen Folgen für die betroffene Person hat, die nicht vorhergesehen werden können und auch keine Widersprüchlichkeiten in sich trägt;
- keine unlautere Ausnutzung eines Machtgefälles zwischen der betroffenen Person und dem Verantwortlichen stattfindet;
- keine unbillige Einwirkung auf den Betroffenen zu dessen Nachteil erfolgt.

Damit darf im Ergebnis die Berechnungsformel des Algorithmus nicht nur zulasten des Betroffenen ausgestaltet werden. Vielmehr setzt der Grundsatz von Treu und Glauben – in Zusammenschau mit dem Grundsatz von Privacy by Design (Art. 25 Abs. 1 DSGVO) – voraus, dass sich Verantwortliche, die sich Algorithmen bedienen, über die Fairness ihrer Algorithmen Gedanken machen und hierüber Rechenschaft ablegen müssen (Art. 5 Abs. 2 DSGVO). Tun sie dies nicht, werden Verstöße dagegen mit dem höchsten Bußgeld der DSGVO nach Art. 83 Abs. 5 lit. a DSGVO geahndet. Somit kann bereits hier festgehalten werden, dass die DSGVO mit dem Grundsatz der Fairness einen ersten Basis-Schutz bei der missbräuchlichen Verwendung von Algorithmen zur Verarbeitung personenbezogener Daten bietet.

3.2 Relatives Verbot der automatisierten Entscheidung im Einzelfall

Die DSGVO sieht über den Grundsatz der Fairness hinaus in Art. 22 DSGVO ein ausdrückliches, aber eingeschränktes Verbot der automatisierten Einzelentscheidung vor. Art. 22 Abs. 2 DSGVO regelt, dass ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen, wozu gerade auch algorithmische Berechnungen ohne menschliches Eingreifen gehören, die betroffenen Personen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, nur in folgenden Fällen zulässig sind:

- Erforderlichkeit für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen;
- Zulässigkeit aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt;
- Ausdrückliche Einwilligung der betroffenen Person.

Damit findet auf den ersten Blick in der DSGVO eine starke Regulierung von Algorithmen statt. Bei genauerer Betrachtung wird jedoch erkennbar, dass sehr vage bleibt, was mit „rechtlichen Wirkung“ oder „ähnlicher erheblicher Beeinträchtigung“ gemeint sein könnte.[8] Ist davon beispielsweise bereits das Anzeigen eines individuellen Preises, wie dies bei Online-Shops und im Online-Marketing die Regel ist, betroffen oder sind reine Angebote noch keine Entscheidung, die eine rechtliche Wirkung entfalten? Auch reicht bereits das Hinzuziehen einer kurzen Begleitentscheidung einer natürlichen Person aus, um nicht mehr von Anwendungsbereich des Art. 22 DSGVO erfasst zu sein.[9] Darüber hinaus sind die zugelassenen Fälle in Art. 22 Abs. 2 DSGVO so weitgehend und zusätzlich auch mit einer Öffnungsklausel für die Mitgliedstaaten verbunden, dass die Verwendung von insbesondere komplexen Algorithmen in der Regel möglich bleibt. Damit wird das relative Verbot der automatisierten Entscheidung im Einzelfall nach Art. 22 DSGVO nur selten die Verwendung von komplexen Algorithmen verhindern können. Stattdessen können die Vorschriften zu den Informations- und Auskunftspflichten regulierend eingreifen.

3.3 Grundsatz der Transparenz

Zunächst ist gem. Art. 5 Abs. 1 lit. a DSGVO der Grundsatz der Transparenz zu beachten. Personenbezogene Daten müssen dabei in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.[10] Hier setzt die DSGVO genau an der Stelle an, die bisher bei der Algorithmusverwendung am häufigsten kritisiert wurde – die mangelnde Aufklärung über die Verwendung und die Art und Weise ihrer Funktionalität durch die Verantwortlichen. Die DSGVO versucht, dem mit Pflichten zur Bereithaltung von leicht zugänglichen, verständlichen und in einer klaren und einfachen Sprache abgefassten Informationen und Mitteilungen (ErwG 39 S. 3 DSGVO) entgegenzuwirken. Auch hier können Verstöße mit dem höchsten Bußgeld der DSGVO nach Art. 83 Abs. 5 lit. a DSGVO geahndet werden.

Im Gegensatz zum Grundsatz der Fairness wird der Grundsatz der Transparenz zusätzlich durch spezielle Vorgaben der DSGVO konkretisiert:

3.3.1 Informationspflichten

Nach Art. 13 Abs. 2 lit. f DSGVO ist die betroffene Person zum einen über das Bestehen einer automatisierten Entscheidungsfindung im Einzelfall nach Art. 22 DSGVO und, falls eine solche stattfindet, aussagekräftige In-

---

8 Ebenso kritisch *Hladjk,* in: Ehmann/Selmayr, DS-GVO, Art. 22 Rn. 9; *Kamlah,* in: Plath, BDSG DSGVO, Art. 22 Rn. 7.

9 *Schulz*, in: Gola, DS-GVO, Art. 22 Rn. 12 ff.

10 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, Art. 5 Rn. 11.

formationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zum Zeitpunkt der Datenerhebung zu unterrichten. Selbige Informationspflichten treffen auch einen Verantwortlichen, der die Daten von Dritten erhebt (Art. 14 Abs. 2 lit. g DSGVO), allerdings möglicherweise mit einer zeitlichen Verzögerung von maximal einem Monat nach Datenerhebung (Art. 14 Abs. 3 DSGVO).

Hier findet sich also die Pflicht der Verantwortlichen, die involvierte Logik des Algorithmus offenzulegen.[11] Ob davon auch die Formel selbst umfasst ist, bleibt offen. Der BGH hat dies unter alter BDSG-Rechtslage für die Score-Formel der SCHUFA abgelehnt.[12] Es werden deshalb Stimmen in der Literatur laut, die diese Rechtsprechung unter der DSGVO als nicht mehr vertretbar ansehen.[13]

Diese Regelung gilt allerdings nur für Verarbeitungen, die mithilfe einer automatisierten Entscheidung im Einzelfall erfolgen, so dass – wie oben dargestellt – in den seltensten Fällen Anwendung finden wird. Verantwortliche werden nämlich entweder keine rechtlich wirkende Entscheidung daran knüpfen oder den Algorithmus nicht ausschließlich voll automatisiert durchlaufen lassen, sondern noch einen manuellen Prüfschritt einfügen, um der Offenlegung des Algorithmus zu entgehen. Die gut gemeinte Informationspflicht nach Art. 13 Abs. 2 lit. f DSGVO wird deshalb in der Praxis kaum zu mehr Transparenz bei Algorithmen führen und ist deshalb nicht geeignet, das Informationsdefizit von betroffenen Personen hinsichtlich der allgegenwärtig vorkommenden Algorithmen aufzulösen.

3.3.2 Auskunftsrecht

Darüber hinaus können Betroffene nach einer etwaigen Datenerhebung Auskunftsrechte im Rahmen des Art. 15 DSGVO geltend machen. Dabei ist ihnen – wortgleich zu Art. 13, 14 DSGVO – nach Art. 1 Abs. 1 lit. h DSGVO das Bestehen einer automatisierten Entscheidungsfindung im Einzelfall nach Art. 22 DSGVO und, falls eine solche stattfindet, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person mitzuteilen. Auch hier wird jedoch aufgrund der zuvor genannten Einschränkungen eine hinreichende Transparenz und Aufklärung über die Verwendung von Algorithmen nicht hergestellt.

---

[11] *Paal/Hennemann*, in: Paal/Pauly, DS-GVO BDSG, Art. 13 Rn. 31.

[12] BGH, Urt. v. 28.1.2014 – VI ZR 156/13, BGHZ 200, 38 = K&R 2014, 269.

[13] *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 744; *Schmidt-Wudy*, in: Wolff/Brink, BeckOK DatenschutzR, Art. 15 Rn. 78.3.

3.3.3 Nachträgliche Aufklärung

Ist Art. 22 DSGVO ausnahmsweise doch einschlägig, so hat der Verantwortliche neben der Offenlegung der Logik nach Art. 13 Abs. 2 lit. f DSGVO bzw. Art. 14 Abs. 2 lit. g DSGVO weitere Informationspflichten aus Art. 22 Abs. 3 DSGVO zu erfüllen. Danach hat er in den Fällen des Art. 22 Abs. 2 lit. a (Vertrag) oder lit. c (Einwilligung) DSGVO angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Dazu gehört nach ErwG 71 S. 4 DSGVO auch die spezifische Unterrichtung der betroffenen Person inklusive einer Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung. Innerhalb dieser Erläuterung würde es dem Betroffenen also zumindest ermöglicht werden, die Verarbeitung der personenbezogenen Daten beim Verantwortlichen nachzuvollziehen.

4 Unzureichende Transparenz in der DSGVO

Im Ergebnis hat sich gezeigt, dass die Regulierung von Algorithmen und der Schutz von Betroffenen durch die DSGVO nur partiell sichergestellt wird. Bis auf den Grundsatz der Fairness, der alle Algorithmen betrifft, sind nur spezielle Transparenzgebote für Algorithmen erkennbar, die aber auch nur dann eingreifen, wenn diese eine automatisierte Entscheidung im Einzelfall abbilden. Nicht umfasst sind damit reine Vorbereitungshandlungen, die keine Entscheidung nach sich ziehen und Berechnungen, bei denen eine manuelle Verarbeitung eingesetzt wird. Im Ergebnis sind die Regelungen der DSGVO deshalb nicht geeignet, eine umfassende Regulierung der Verwendung von komplexen Algorithmen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Literatur

Boehme-Neßler, Volker: Die Macht der Algorithmen und die Ohnmacht des Rechts – Wie die Digitalisierung das Recht relativiert, NJW 2017, S. 3031-3037.

Ehmann, Eugen/Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung, München 2017.

Gola, Peter (Hrsg.): DS-GVO Datenschutz-Grundverordnung, Kommentar, München 2017.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Martini, Mario: Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, S. 1017-1026.

Pasquale, Frank: The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard 2015.

Plath, Kai-Uwe (Hrsg.): BDSG DSGVO Kommentar, 2. Aufl., Köln 2016.

Schantz, Peter/Wolff, Heinrich Amadeus: Das neue Datenschutzrecht, München 2017.

INTERNATIONALE CYBERSECURITY-REGULIERUNG

Dr. Dennis-Kenji Kipker/Dipl.-Ing. (FH) Sven Müller

DKE – Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
dennis-kenji.kipker@vde.com, sven.mueller@vde.com

Zusammenfassung[1]

Die effektive Gewährleistung von Cybersicherheit ist eine Aufgabe, die genauso wenig wie die sie betreffenden Datenströme an Staatsgrenzen Halt macht. Vor allem im Angesicht der diesbezüglich steigenden Bedrohungslage der vergangenen Jahre haben es sich verschiedene Staaten, aber auch die EU, zum Ziel gemacht, neue politische Strategien und gesetzliche Regularien zur Verbesserung der Cybersicherheit und teils auch des Datenschutzes zu entwickeln. Der vorliegende Beitrag soll hierzu einen Überblick geben und stellt neben den entsprechenden europäischen Vorgaben auch die jüngsten politischen und gesetzlichen Entwicklungen in Deutschland, Russland, China sowie den USA dar und vergleicht diese miteinander. Darüber hinaus wird ein kursorischer Einblick in die Grundlagen der Normung und Standardisierung in diesem Bereich gegeben, soweit es die technisch-organisatorische Implementierung gesetzlich angeordneter Cybersecurity-Maßnahmen anbelangt.

1 Rechtliche Regulierung der Cybersecurity

1.1 Deutschland und Europäische Union

Seit 2015 wird das Thema Cybersicherheit sowohl in der deutschen wie auch in der europäischen Gesetzgebung durch verschiedene Rechtsakte aufgegriffen. Hierzu gehören das deutsche IT-Sicherheitsgesetz (IT-SiG, 2015), die EU-Richtlinie zur Netz- und Informationssicherheit (NIS-RL, 2016) und die für 2018 angekündigte EU Cybersecurity-Verordnung.

1.1.1 Deutsches IT-Sicherheitsgesetz

Das IT-SiG trat am 25.7.2015 mit dem Ziel einer „signifikante[n] Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland“[2] in Kraft. Es ist kein eigenständiges Gesetz, das unmittelbar Verpflichtungen für Bürger und Unternehmen enthält, sondern modifiziert und ergänzt als sog. Artikelgesetz verschiedene, bereits bestehende Einzelgesetze. Somit ist für Private das IT-SiG in erster Linie nur in Form der bereits geltenden Einzelvorschriften, die durch das Gesetz einer Novellierung unterzogen wurden, relevant. Beispiele für solche geänderten Gesetze

[1] Die Verfasser danken *Michael Walkusz* für seine tatkräftige Unterstützung im Rahmen der Erstellung des vorliegenden Beitrages.

[2] BT-Drs. 18/4096, S. 1.

sind unter anderem das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) sowie das Bundeskriminalamtgesetz (BKAG). Die nicht-kodifizierte Regulierung der Cybersicherheit in Deutschland bedingt teilweise eine Unübersichtlichkeit, die gerade für KMU nicht selten mit erheblichen Herausforderungen in der Handhabung effektiver IT-Security-Compliance verbunden ist.

Das IT-SiG lässt zudem die Frage, welche Betreiber und Anlagen im Einzelnen unter die gesetzlichen Vorgaben fallen, weitestgehend offen. Klärung hat hier jedoch die BSI-Kritisverordnung (BSI-KritisV) gebracht, zu deren Erlass das Bundesministerium des Innern (BMI) ausgehend von § 10 Abs. 1 S. 1 BSIG ermächtigt wird. Bewusst hat man diese Form der Konkretisierung des Anwendungsbereiches gewählt, um auf (vor allem technische) Entwicklungen in den betroffenen Branchen schneller reagieren zu können. Die Verordnung als untergesetzliches „Behördenrecht" ist hier flexibler, schneller anpassbar und deshalb im Ergebnis besser als ein formelles Gesetz geeignet, Änderungen im Anwendungsbereich des IT-SiG abzubilden. Inhaltlich basieren die Vorgaben der BSI-KritisV in erheblichen Teilen auf den so genannten „Sektorstudien", die im Auftrag des BSI erarbeitet wurden und neben dem Sektor Gesundheit auch die weiteren KRITIS-typischen Bereiche Energie, Ernährung und Wasser, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Transport und Verkehr, Logistik sowie Medien und Kultur abdecken.

1.1.2 EU-Richtlinie zur Netz- und Informationssicherheit 2016/1148

Auch für die Regelungsstruktur der europäischen IT-Sicherheit gilt – wie schon für das deutsche Recht – dass diese nicht in einem einzelnen Rechtsakt zusammengefasst ist. Die gegenwärtige Rechtslage hier stellt sich sogar noch unübersichtlicher dar als im nationalen Recht, da insbesondere seit der Jahrtausendwende in der Europäischen Union eine Vielzahl von Vorschriften mit einem in unterschiedlicher Granularität gegebenen Cybersecurity-Bezug erlassen wurde.

Besonders hervorzuheben ist in diesem Zusammenhang die EU Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (NIS-RL), die im August 2016 in Kraft getreten ist und die politische Cyber-Sicherheitsstrategie der EU nach schwerwiegenden IT-Sicherheitsvorfällen wie „WannaCry" und „Petya" auf eine klare gesetzliche Grundlage stellt. In dieser Funktion trug die Richtlinie auch bisher entscheidend dazu bei, den Einigungsprozess in der europäischen und transnationalen Cybersecurity-Kooperation deutlich zu beschleunigen. Gleichzeitig soll sie auch als globaler

Ansatz dienen, der gemeinsame Mindestanforderungen für Betreiber wesentlicher und digitaler Dienste bestimmt. Unter letztere zu fassen sind Suchmaschinen, Online-Marktplätze und Cloud-Computing-Anbieter.

Da es sich bei der NIS-RL um einen Gesetzgebungsakt gem. Art. 288 Abs. 3 AEUV handelt, ist für deren Wirksamkeit in den jeweiligen Mitgliedstaaten grds. eine Umsetzung in das nationale Recht notwendig. Für Deutschland ist dies durch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.6.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ geschehen, das im April 2017 den Deutschen Bundestag passiert hat. Durch dieses Gesetz wurden einige der Rechtsvorschriften, die bereits durch das IT-SiG als Artikelgesetz im Juli 2015 neu geschaffen oder geändert wurden, stellenweise erneut angepasst. Insgesamt hielten sich die durch die EU NIS-RL hervorgerufenen Änderungen im nationalen Recht aber – entgegen mancher zuvor geäußerter Vermutung – in einem überschaubaren Rahmen.

1.1.3 EU Cybersecurity-Verordnung (voraussichtlich 2018)

Mit der Veröffentlichung der neuen EU-Cybersicherheitsstrategie im September 2017 definierte die Europäische Union das Politikfeld der IT-Sicherheit noch stärker für sich, indem sie in einem Zuge auch den Entwurf einer Verordnung „über die EU-Cybersicherheitsagentur (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit)“ vorstellte, die gemeinhin auch als „Cybersecurity-Verordnung“ bezeichnet wird und deren Gesetzgebungsverfahren zum Herbst 2018 abgeschlossen sein soll.[3] Mit der neuen Verordnung werden primär zwei Ziele verfolgt, die über die bisherigen europäischen Regulierungsansätze im Bereich Cybersicherheit hinausgehen: So trifft der Rechtsakt Vorgaben, die nicht durch die EU NIS-RL abgedeckt werden, indem er auf Sachverhalte Bezug nimmt, die mehr als nur Kritische Infrastrukturen und die Anbieter von digitalen Diensten betreffen. Zudem sollen mit der künftigen Verordnung Regelungen normiert werden, die europaweit einheitlich zur Anwendung gelangen, da sie in Teilen inhaltlich auch die Regulierung des digitalen Binnenmarktes betreffen. Mit diesem umfassenden Geltungsanspruch der EU, der sich als Resultat der Wahl des Rechtsinstrumentes der Verordnung darstellt, steht den Mitgliedstaaten kein nennenswerter eigener Gestaltungsspielraum bei der Umsetzung der neuen europäischen Cybersicherheitsgesetzgebung zur Verfügung. Denn im Unterschied zur NIS-RL gilt die EU Cybersecurity-Verordnung nach Abschluss des Gesetzgebungsverfahrens grundsätzlich unmittelbar für alle

[3] Hierzu auch *Kipker*, MMR-Aktuell 2017, 395945.

Unternehmen und Behörden in den Mitgliedstaaten, ohne dass es eines weiteren nationalen Umsetzungsaktes bedarf.

Ein weiteres Anliegen der geplanten EU Cybersecurity-Verordnung ist die Einrichtung eines europaweit einheitlichen Zertifizierungsrahmens für die IT-Sicherheit von Produkten und Diensten der Informations- und Kommunikationstechnik. Diese Zertifizierung soll durch eine unabhängige Zertifizierungsstelle durchgeführt werden. Hierdurch werden sowohl die Sicherheit und das Vertrauen in den digitalen Binnenmarkt gestärkt, als auch der gemeinsame europäische Markt weiter harmonisiert. Laut der Begründung der EU-Kommission ist der europäische Zertifizierungsrahmen zur Cybersicherheit zurzeit zu stark fragmentiert, was Marktzugangshürden für Unternehmen zur Folge hat, indem beispielsweise ein Produkt oder eine Dienstleistung, die in einem Mitgliedstaat als sicher anerkannt ist, in einem anderen Mitgliedstaat einer erneuten Überprüfung der IT-Sicherheit bedarf. Dies führt im Ergebnis zu einer erheblichen Erschwernis grenzüberschreitender unternehmerischer Tätigkeit.

Im Zuge der Schaffung des EU-Zertifizierungsrahmens wird die europäische Cybersicherheitsbehörde ENISA als Marktbeobachtungsstelle fungieren und hierbei auch neue Normen zur Cybersicherheit aktiv mitgestalten. Jüngst haben im zurzeit noch laufenden Gesetzgebungsverfahren der EU Cybersecurity-Verordnung der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) sowie der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO) zum Kommissionsentwurf Stellung bezogen. Beide haben dabei auch betont, dass die Einbeziehung der Normung und Standardisierung sowie der entsprechenden Institutionen für den neuen europäischen Zertifizierungsrahmen von unerlässlicher Bedeutung sind. Ein Plenarentscheid zur EU Cybersecurity-Verordnung wird im September 2018 erwartet.

1.2 Russland

1.2.1 Russische Cybersicherheitsdoktrin (2000, 2016)

Mit der ersten „Cyber-Security-Doctrine“ aus dem Jahr 2000,[4] die im Dezember 2016 grundlegend überarbeitet wurde, wurde die Russische Föderation verhältnismäßig früh in Sachen IT-Sicherheit aktiv – jedoch nahm diese erste Fassung der russischen Cyber-Sicherheitsstrategie als politische Blaupause noch nicht explizit auf die durch die Verbreitung des Internets entstehende, zunehmende und spezifische Gefährdungslage vernetzter IT-

[4] Information Security Doctrine of the Russian Federation, approved by President of the Russian Federation Vladimir Putin on September 9, 2000, abrufbar unter: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (abgerufen 15.6.2018).

Systeme Bezug. Die zweite Cyber-Security-Doctrine hingegen, die durch den russischen Präsidenten Vladimir Putin am 5. Dezember 2016 verabschiedet wurde,[5] greift die durch die vernetzte Datenverarbeitung entstehenden technisch-organisatorischen Herausforderungen umfassend auf.

Im Wesentlichen lässt sich sagen, dass der Schwerpunkt der neuen russischen Cyber-Sicherheitsstrategie auf dem Schutz der nationalen Interessen der Russischen Föderation im Cyberspace liegt. Hierbei stehen weniger wirtschaftliche, sondern vor allem politische (Staat und Gesellschaft) und militärische Interessen im Mittelpunkt. Dies wird auch daran deutlich, dass die russische Cyber-Sicherheitsstrategie eng mit der allgemeinen nationalen Sicherheitsstrategie der Russischen Föderation[6] und den Maßnahmen der Verteidigungspolitik verknüpft ist, indem unter anderem vorgeschlagen wird, die Cyber-Sicherheit auch für das russische Militär zu stärken, digitale Waffensysteme kontrollfähig zu halten und die Interessen von Verbündeten der Russischen Föderation zu unterstützen.

1.2.2 Das neue russische Cyber-Sicherheitsgesetz

Als ein zentraler Meilenstein in der praktischen Umsetzung der zweiten Cyber-Sicherheitsstrategie der Russischen Föderation ist das „Federal Law on Security of Critical Russian Federation Information Infrastructure“[7] (im Folgenden als „russisches Cyber-Sicherheitsgesetz“ bezeichnet) anzusehen, das am 26.7.2017 verabschiedet wurde und zum 1.1.2018 in Kraft getreten ist.[8] Dieses neue Gesetz bildet nicht nur den Rahmen zur Absicherung der kritischen Informationsinfrastrukturen des Landes, sondern legt noch weitergehend das Fundament für ein funktionierendes staatliches Informationssicherheitssystem, das sich der Erkennung, Vorbeugung und Beseitigung der Folgen von Cyber-Angriffen gegen die IT-Strukturen der Russischen Föderation verschrieben hat. Die Regelungen des neuen russischen Cyber-Sicherheitsgesetzes schaffen mit dem deutschen IT-SiG und mit der EU NIS-RL inhaltlich teils vergleichbare Vorgaben,[9] indem einerseits verschiedene Rechte und Pflichten für Diensteanbieter bestimmt werden, die andererseits mit einem Ausbau behördlicher Kontroll- und Weisungsrechte zur Überprüfung der neuen gesetzlichen Anforderungen einhergehen.

---

[5] Decree of the President of the Russian Federation No. 646 of December 5, 2016, abrufbar unter: http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2563163 (abgerufen 15.6.2018).

[6] Decree of the President of the Russian Federation No. 683 of December 31, 2015.

[7] No. 187 FZ.

[8] Hierzu detailliert *Kipker*, ZD 2018, S. 296.

[9] Siehe dazu auch schon *Kipker*, ZD-Aktuell 2016, 05261; *Kipker*, ZD-Aktuell 2016, 05363; *Kipker*, MMR-Aktuell 2017, 394677.

Das russische Cyber-Sicherheitsgesetz untergliedert sich in insgesamt 15 Artikel, wobei sich im zweiten Artikel verschiedene Begriffsdefinitionen finden. Zentral ist hier die Bestimmung der Subjekte von kritischen Informationsinfrastrukturen. Hierunter zu fassen sind staatliche Stellen und Institutionen, juristische Personen nach russischem Recht und/oder Einzelunternehmer, die Informations- und Kommunikationssysteme betreiben und im Schwerpunkt in den Sektoren Gesundheit, Wissenschaft, Verkehr, Kommunikation, Energie, Banken und Finanzmarkt, Verteidigung, Bergbau und Chemie tätig sind oder aber im Rahmen ihrer Tätigkeit in Interaktion zu den vorgenannten Sektoren stehen.

Gem. Art. 9 haben die zuvor bestimmten Subjekte der kritischen Informationsinfrastruktur in Russland verschiedene Rechte und Pflichten. Zuallererst nehmen sie am gesetzlich geregelten Informationsaustausch teil, und erhalten die zur Aufrechterhaltung der IT-Sicherheit notwendigen Informationen von der russischen Bundesbehörde für Informationssicherheit. Wie durch das deutsche IT-SiG und durch die EU NIS-RL für die Betreiber von Kritischen Infrastrukturen und von digitalen Diensten auch schon in den §§ 8a ff. BSIG geregelt, trifft die Subjekte kritischer Informationsinfrastrukturen in Russland gleichzeitig die Verpflichtung, die Mittel zur Erkennung, Verhütung und Beseitigung der Folgen von Computerangriffen und zur Reaktion auf Computervorfälle vorzuhalten, sowie Maßnahmen zum Schutz der Betriebsfähigkeit des kritischen Informationsinfrastrukturobjekts zu entwickeln und zu implementieren (Art. 9 ff.). Als entsprechende Maßnahme wird unter anderem die Erstellung von Sicherungskopien genannt; daneben sind verschiedene technische und organisatorische Maßnahmen zu ergreifen. Die umzusetzenden Vorgaben werden in Zusammenarbeit mit der öffentlichen Hand definiert. Ferner informieren die Subjekte kritischer Informationsinfrastruktur die russische Bundesbehörde für Informationssicherheit über Cyber-Sicherheitsvorfälle und unterstützen diese bei der Zustandserkennung, Prävention von und Reaktion auf Cyber-Angriffe.

1.3 China

Im November 2016 wurde in der Volksrepublik China das neue „Cybersecurity Law“ verabschiedet, und darauf basierend auch ein zusätzlicher Maßnahmenkatalog zur technischen Gewährleistung von IT-Sicherheit („Measures on Security Review of Network Products and Services“) vorgestellt. Mit den beiden Regelungen beschreitet das Land neue Wege in Sa-

chen Cybersecurity – und stellt dabei einen ganzheitlichen Ansatz der Informationssicherheit vor, der sowohl die Datensicherheit wie auch den Datenschutz berücksichtigt.[10]

1.3.1 Das Chinese Cybersecurity Law

Das im Jahr 2016 in Kraft getretene Gesetz der Volksrepublik China zur Cybersicherheit gliedert sich in sieben Abschnitte, wobei sich im letzten Abschnitt verschiedene Begriffsdefinitionen finden, die allgemeingültig und mit den Definitionen aus § 2 BSIG vergleichbar auf das gesamte Gesetz zu beziehen sind. Hierbei liegt der Fokus auf der Netzwerksicherheit und dem Datenschutz. So sind nach Art. 76 unter den Begriff des „Netzwerks" alle aus Computern oder sonst datenverarbeitenden Geräten bestehenden technischen Ausrüstungen zu fassen, die bestimmten Regeln der Informationsverarbeitung folgen und zum Sammeln, Speichern, Übertragen, Austausch und zur Verarbeitung von Informationen zuständig sind. „Netzwerksicherheit" umfasst das Ergreifen derjenigen Maßnahmen, um Angriffe, Einbrüche, Beeinflussungen, die Zerstörung, einen rechtswidrigen Gebrauch von Netzwerkressourcen und auch unbeabsichtigte Unfälle zu vermeiden. Hierzu sollen die Netzwerke in einen stabilen und verlässlichen Arbeitsstatus versetzt werden. Als „Betreiber" eines Netzwerks gelten Inhaber, Leiter/Geschäftsführer und Netzwerkdiensteanbieter. „Netzwerkdaten" sind alle Arten elektronischer Daten, die gesammelt, gespeichert, übertragen, verarbeitet und durch Computernetzwerke generiert werden.

Über die Anforderungen reiner IT-Sicherheit hinaus geht Art. 76 Abs. 5, der den Begriff der „personal information" als alle Daten und andere Arten von Informationen, die geeignet sind, eine natürliche Person zu identifizieren, definiert. Deutlich wird mit diesem eindeutigen Bezug zu den personenbezogenen Daten, dass das chinesische Cybersicherheitsgesetz einen ganzheitlichen Ansatz zur Herstellung von Cybersicherheit verfolgt, indem Datenschutz und Datensicherheit, die sowohl in Deutschland als auch in Europa mit dem IT-SiG, der NIS-RL und allgemein dem BDSG-neu bzw. der EU Datenschutz-Grundverordnung (EU DS-GVO) regulatorisch bis auf einige Einzelregelungen eher getrennt voneinander gehalten werden, hier nunmehr ausdrücklich in einem Gesetz mit den für wesentlich gehaltenen Vorgaben zusammen gefasst sind. In Bezug auf Vertraulichkeit, Zweckbindung, Einverständniserklärung, Regulierung der Datenschutzverletzungen und der Betroffenenrechte liegt das chinesische Datenschutzniveau allerdings noch weit unter demjenigen der EU DS-GVO – was sich aber auch als Folge des in China gewählten, gesamtheitlichen Regulierungsansatzes

[10] Zur Entwurfsfassung des Gesetzes siehe *Kipker*, MMR-Aktuell 2015, 370972; zum letztlich verabschiedeten Gesetz *Kipker*, MMR 2017, S. 455.

darstellt, der zwingend einen Ausgleich zwischen IT-Sicherheit und Datenschutz in verschiedenen Vorschriften bedingt.

1.3.2 Maßnahmenkatalog zur Überprüfung der Sicherheit von Netzwerkprodukten und -diensten

Mit dem chinesischen Maßnahmenkatalog zur IT-Sicherheit werden Vorgaben sowohl aus dem National Security Law, Art. 24 und 25, sowie aus dem Cybersicherheitsgesetz, Art. 23 und 35, umgesetzt. Art. 23 des Cybersicherheitsgesetzes regelt die Sicherheitszertifizierung kritischer Netzwerk(sicherheits)produkte, Art. 35 den „national security review" für Netzwerkprodukte und -dienste, die im KRITIS-Sektor eingesetzt werden. Art. 1 des Kataloges schreibt dementsprechend vor, dass dessen primäre Zielsetzung in der Verbesserung der Sicherheit und Kontrollierbarkeit von Netzwerkprodukten und -diensten liegt; in diesem Rahmen ist durch Art. 2 vorgesehen, dass für Schlüsselprodukte, die die nationale Sicherheit und das öffentliche Interesse betreffen, ein „Cybersecurity Review" durchzuführen ist, für den das von der Cyberspace Administration of China (CAC) eingesetzte „Cybersecurity Review Committee" (Art. 5) und das „Cybersecurity Review Expert Committee" (Art. 6) zuständig sind. Zusätzlich können gem. Art. 7 auch Dritte hilfsweise eingesetzt werden.

Der Cybersecurity Review stellt sich ausgehend von Art. 3 als eine Zusammenarbeit zwischen Unternehmen und Behörden dar, wozu Labortests, Betriebsbegehungen, Online-Überwachung und Hintergrundkontrollen gehören. Nach Art. 4 bezieht sich der Review vornehmlich auf die Sicherheit und Kontrollierbarkeit von Produkten, wobei der Ansatz den Hersteller bzw. Anbieter als Risikosphäre einordnet. Genannt werden in diesem Zusammenhang unter anderem Risiken „illegaler Produktkontrolle", Risiken bei der Produktentwicklung, Datenschutzrisiken sowie Missbrauchsrisiken. Koordiniert wird der Review vom „Cybersecurity Review Office", das zugleich auch die Ergebnisse veröffentlichen kann (Artt. 8 und 14). Für den KRITIS-Sektor wird zusätzlich die Zuständigkeit einzelner Fachbehörden bestimmt, Art. 9. In wirtschaftlicher Hinsicht besitzt der Cybersecurity Review auf dem chinesischen Markt eine erhebliche Relevanz, denn Art. 10 des Maßnahmenkataloges bestimmt, dass überprüften Produkten der Vorrang im Einkauf eingeräumt wird – und solche Produkte, die den Review nicht bestanden haben, in China dementsprechend nicht eingesetzt werden sollen.

Der Maßnahmenkatalog zur IT-Sicherheit verdient in Deutschland und Europa besondere Aufmerksamkeit, da durch den darin vorgesehenen Cybersecurity Review auch deutsche Hersteller von IT-Produkten angesprochen werden. Hier wird es in Zukunft vor allem darauf ankommen, welches Vertrauen die ausländischen Hersteller der Arbeit der chinesischen Behörden schenken werden. An dieser Stelle sind somit auch die deutsche und

europäische Außenpolitik sowie die Branchenverbände gefragt, auszuhandeln, welche Kooperations- und Mitwirkungspflichten im Einzelnen noch vertretbar scheinen – und wo die technische Offenbarungspflicht der Hersteller zu weitgreifend wäre, um das Produkt in China noch zu vermarkten.

1.4 USA

Auch in den Vereinigten Staaten existiert zurzeit keine vereinheitlichte bzw. kodifizierte Regelung der IT-Sicherheit, ebenso ist hier die Trennlinie zwischen Datenschutz und Cybersecurity nicht immer deutlich. Zu unterscheiden ist im Rahmen der US-amerikanischen Vorgaben zur IT-Sicherheit zwischen politischen Strategien einerseits und verbindlichen gesetzlichen Anforderungen andererseits, dies sowohl auf Bundesebene wie auch auf Ebene der einzelnen Bundesstaaten.[11]

Im Jahr 2016 veröffentlichte der damalige US-Präsident Obama den Cybersecurity National Security Action Plan (CNAP), der längerfristige Maßnahmen und Strategien zum Schutz gegen Cyberangriffe vorsieht. Zudem erließ er 2013 die Executive Order 13636 „Improving Critical Infrastructure Cybersecurity", die Maßnahmen speziell zum Schutz Kritischer Infrastrukturen enthält. So sollen vor allem der Informationsaustausch zwischen staatlichen Stellen und den Betreibern entsprechender Dienste verbessert und selbstregulative Maßnahmen gefördert werden. Entsprechend dieses Executive Orders publizierte das National Institute of Standards and Technology (NIST) ein „Cybersecurity Framework", das freiwillige Standards, Maßnahmen und Best Practices zur Cyber Security enthält. Darüber hinaus fördert der Cybersecurity Enhancement Act von 2014 die freiwillige Zusammenarbeit von staatlichen und privaten Stellen zur Verbesserung der IT-Sicherheit im Sinne einer public-private partnership (PPP).

Auf föderaler Ebene existiert in den USA eine Reihe von sektorspezifischen Vorschriften zur Cybersicherheit. Beispielhaft zu nennen sind hier der Health Insurance Portability and Accountability Act (HIPAA, 1996) für den Bereich der Gesundheitsdaten, der Financial Services Modernization Act (Gramm-Leach-Bliley Act, 1999) für den Bereich der persönlichen Finanzinformationen, der Federal Information Management Act (FISMA, 2002) für die Datenverarbeitung durch Bundesbehörden, und der Cybersecurity Information Sharing Act (CISA, 2015) zum Austausch IT-sicherheitsbezogener Informationen zwischen Regierung und Unternehmen. Der Federal Trade Commission (FTC) kommt wie auch schon für den US-Datenschutz eine tragende Rolle in der föderalen Cyber-Sicherheitsstrategie

[11] Dazu ausführlich *Fischer/Kipker/Voskamp*, in: Kipker, Handbuch Cybersecurity-Recht, Kap. 16.

der USA zu. Nach dem Federal Trade Commission Act hat die FTC die Aufgabe, unfaire oder betrügerische Marktmethoden zu ermitteln, zu verhindern oder zu sanktionieren. Als solche unfairen Marktmethoden können im Einzelfall insbesondere auch unzureichende Sicherheitsstandards in den Unternehmen eingeordnet werden, was auf fehlende IT-Security-Compliance schließen lässt.

2 Technisch-organisatorische Regulierung der Cybersecurity

Die technisch-organisatorische Implementierung der internationalen gesetzlichen Regelwerke zur Cybersicherheit kann und wird vorwiegend durch die Normung und Standardisierung realisiert. Die Standardisierung, also die Definition der Anforderungen, die ein Produkt oder eine Dienstleistung im Hinblick auf die IT-Sicherheit erfüllen muss, wird dabei in unterschiedlichen nationalen und/oder internationalen Gremien der jeweiligen Normungs- und Standardisierungsorganisationen geleistet. Die Standardisierungsarbeit im Bereich der Cybersecurity ist hochgradig verflochten und komplex, da eine Vielzahl von Branchenverbänden, Industriekonsortien, offenen Interessengruppen oder staatlich anerkannten Normungsorganisationen alle hiermit im Zusammenhang stehenden Grundregeln definiert. Die so entstehenden technischen Normen und Standards bilden die Grundlage von Zertifizierungsverfahren, wie zum Beispiel das Informationssicherheitsmanagementsystem-Zertifikat nach DIN EN ISO/IEC 27001.

2.1 Organisation der technischen Normungsarbeit

Das DIN (Deutsches Institut für Normung) ist die nationale Normungsorganisation Deutschlands und hat die Rechtsform eines eingetragenen Vereins auf gemeinnütziger Grundlage mit Sitz in Berlin. Für die Erarbeitung und Auslegung von Texten elektrotechnischer Normen einschließlich Sicherheitsbestimmungen wurde von DIN und VDE (Verband der Elektrotechnik Elektronik Informationstechnik e.V.) die DKE (Deutsche Kommission Elektronik Informationstechnik in DIN und VDE) als gemeinsames Organ gebildet. Das DIN ist Mitglied in den entsprechenden europäischen und internationalen Normungsorganisationen, zum Beispiel im Europäischen Komitee für Normung (CEN) und der International Organization for Standardization (ISO). Die DKE ist Mitglied in der Normungsorganisation International Electrotechnical Commission (IEC). Auf internationaler Ebene besteht eine Kooperation zwischen ISO, IEC und der International Telecommunication Union (ITU). Das Joint Technical Committee 1 (ISO/IEC JTC 1) ist ein Zusammenschluss aus ISO- und IEC-Experten zur IKT-Standardisierung. Das JTC 1 ist in mehreren Arbeitsgruppen (Sub

Committees, SC) organisiert; für die IT-Sicherheit ist das SC 27 zuständig. Die internationale Standardisierung der IT-Sicherheit ist bei der ITU in der Study Group (SG) 17 „Security“ angesiedelt.

Auf Europäischer Ebene wird die Normungsarbeit durch das eingangs bereits erwähnte CEN, das Europäische Komitee für Elektrotechnische Normung (CENELEC) und durch das Europäische Institut für Telekommunikationsnormen (ETSI) sichergestellt. Letzteres ist historisch bedingt für die europäische Normung im Telekommunikationsbereich zuständig. Das CEN unterhält eine enge Kooperation und Abstimmung mit den internationalen Normungsorganisationen, da mehr als die Hälfte der zurzeit in Entwicklung befindlichen CEN-Normen identisch zu ISO-Normen sind. Das gleiche gilt für CENELEC, denn auch hier sind aktuell mehr als zwei Drittel der derzeit in Entwicklung befindlichen CENELEC-Normen identisch zu IEC-Normen. Die in diesem Zusammenhang bedeutsame Zuordnung und somit die Herkunft einer Norm lässt sich an deren Bezeichnung erkennen:

- DIN – von DIN/DKE auf nationaler Ebene erstellte Norm,
- DIN EN – von CEN/CENELEC erarbeitete Norm, die als deutsche Norm übernommen wurde,
- DIN EN ISO – von ISO aufgestellte Norm, zunächst als europäische und anschließend als deutsche Norm übernommen,
- DIN EN ISO/IEC – von ISO und IEC erarbeitete Norm, zunächst als europäische und anschließend als deutsche Norm übernommen,
- DIN ISO – von ISO aufgestellte Norm, die direkt als deutsche Norm übernommen wurde,
- DIN IEC – von IEC erarbeitete Norm, die direkt als deutsche Norm übernommen wurde,
- DIN ISO/IEC – von ISO und IEC erarbeitete Norm, die direkt als deutsche Norm übernommen wurde,
- DIN ETS – von der ETSI aufgestellte Norm, die als deutsche Norm übernommen wurde, sowie
- DIN VDE – von VDE | DKE arbeitete Norm, die direkt als deutsche Norm übernommen wurde.

Die teils einem gesetzgeberischen Verfahren ähnelnde fachliche Normenarbeit wird von externen Mitarbeitern geleistet, die dabei von hauptamtlichen Bearbeitern der jeweiligen nationalen Normungsorganisation unterstützt werden. Die externen Mitarbeiter sind Fachleute aus den für die Normungsarbeit einschlägigen Kreisen, wie zum Beispiel Anwender, Behörden, Berufs-, Fach- und Hochschulen, Handel, Handwerkswirtschaft, gesetzli-

che Unfallversicherungen, industrielle Hersteller, Prüfinstitute, Sachversicherer, selbstständige Sachverständige, technische Überwacher, Umweltschutzverbände, Verbraucher, Wissenschaft und gesellschaftspolitische Interessensverbände. Die externen Mitarbeiter müssen von den sie entsendenden Stellen für die Arbeit in den Arbeits- und Lenkungsgremien autorisiert und entscheidungsbefugt sein. Daher bildet eine technische Norm stets den Stand der Technik ab.

2.2 Standardisierungsorganisationen

Die Internet Engineering Task Force (IETF) ist eine lose Organisation, in der sich seit 1986 Internetexperten zusammenfinden, um Internetstandards zu entwerfen und weiterzuentwickeln. Im Gegensatz zu den zuvor genannten Normungsorganisationen beruht die IETF nicht auf formaler Mitgliedschaft, sondern verfolgt ein vollständig offenes Konzept. Jede Person kann an Workshops und den mehrmals im Jahr stattfindenden IETF-Meetings teilnehmen. Die IETF hat tragende Protokolle des heutigen Internets standardisiert und ist für die offene Weiterentwicklung des Internets verantwortlich. Alle Dokumente der IETF, einschließlich der Protokolle der Treffen und Diskussionen, sind frei verfügbar, um auf diese Weise eine hohe Nachvollziehbarkeit des Standardisierungsprozesses sicherzustellen. Die IETF erarbeitet und veröffentlicht sogenannte RFCs (Request For Comments).

Beim Institute of Electrical and Electronics Engineers (IEEE) handelt es sich um den größten technischen Berufsverband der Welt. Die Arbeit ist thematisch in verschiedene, so genannte „Societies“ gegliedert. Die Standardisierung findet in der IEEE Standards Association statt. Die IEEE Standards Association (IEEE-SA) verfügt über ein Portfolio von fast 1.300 Industriestandards, zu denen auch gemeinhin bekannte Standards wie zum Beispiel die LAN- und WLAN-Standards 802.3, 802.11 und 802.15 gehören. Zusätzlich werden zurzeit über 600 weitere Standards entwickelt.

Das World Wide Web Consortium (W3C) ist die zentrale Standardisierungsinstanz zur Definition von Web-Standards, wie der Hyper Text Markup Language (HTML) oder der Extensible Markup Language (XML). Das W3C wurde 1994 gegründet und hat mittlerweile fast 500 Mitgliedsorganisationen. Die Standardisierungsorganisation finanziert sich über Mitgliedsbeiträge, Spenden und Forschungsförderung. Ähnlich zur IETF sind sowohl alle durch die W3C entwickelten Standards frei verfügbar, als auch die Teilnahme an der Standardisierungsarbeit für jeden möglich.

Die Trusted Computing Group (TCG) ist eine international tätige, gemeinnützige Organisation, die 2003 als Nachfolger der Trusted Computing Platform Alliance (TCPA) gegründet wurde. Sie hat ihren Sitz in Beaverton,

USA. Zu ihren mehr als 100 Mitgliedern zählen Hersteller von Computersystemen und -komponenten, Softwareentwickler sowie Netzwerk- und Infrastruktursystemfirmen. Die TCG entwickelt und fördert offene Spezifikationen für vertrauenswürdiges Computing. Die Standardisierungsarbeit der ehemaligen TCPA wurde im Jahr 2003 übernommen und wird seither fortgesetzt. Die Mitglieder der TCG entwickeln und fördern offene, herstellerunabhängige Industriestandard-Spezifikationen für plattformübergreifende Trusted Computing-Bausteine und Software-Schnittstellen.

Die gemeinnützige Fast Identity Online (FIDO)-Alliance entwickelt seit 2013 offene Industriestandards zur sicheren Authentifizierung im Internet. Das markenrechtlich geschützt Logo „*FIDO ready*" kennzeichnet Produkte, die nach FIDO-Standards zertifiziert wurden. Der schnell wachsenden FIDO-Alliance gehören inzwischen mehr als 250 Unternehmen und Organisationen an.

Die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) enthalten Empfehlungen und Anforderungen zur Informationssicherheit für Behörden und Unternehmen. Die technischen Richtlinien des BSI (BSI-TR) ergänzen sowohl die technischen Prüfvorschriften des BSI als auch bestehende technische Normen und Standards.

Grundlegend können Dokumente zur Sicherheit nach IEC Guide 120[12] in fünf Kategorien eingeordnet werden:

- Base security standards (Kategorie A) sind Veröffentlichungen, die einen allgemeinen Aspekt der Sicherheit definieren. Diese Sicherheitspublikationen befassen sich mit grundlegenden Konzepten, Prinzipien und Anforderungen hinsichtlich allgemeiner Sicherheitsaspekte, die für eine breite Palette von Produkten und Systemen gelten, zum Beispiel DIN EN ISO/IEC 27001.
- Group security publications (Kategorie B) legen Sicherheitsanforderungen in der jeweiligen Anwendungsdomäne fest. Zu diesem Zweck können diese Dokumente grundlegende Sicherheitsstandards referenzieren oder anpassen. Diese Art von Dokumenten kann auf viele Produkte oder Systeme oder auf Produkt- sowie Systemfamilien anwendbar sein, sodass diese auch als sektorspezifische Sicherheitspublikationen bezeichnet werden, so zum Beispiel IEC 62443-1-1.
- Product security publications (Kategorie C) definieren, wie Base security standards oder Group security publications für einen bestimmten Produkttyp angewendet werden können. Sie legen fest, wie verschiedene Produkte sicher miteinander interagieren und wie sie einheitlich zu steuern und zu verwalten sind. Daher sollten Product security publications

[12] Draft Guide 120 Ed. 1, Security aspects – Guidelines for their inclusion in standards.

ihre Anforderungen so weit wie möglich unter Bezugnahme auf Base security standards und Group security publications definieren, zum Beispiel IEC 62351-3.

- Guidance security publications (Kategorie D) sollten keine Anforderungen enthalten. Sie erläutern, wie Base security standards und Group security publications oder Product security publications umgesetzt werden können. In einigen Fällen werden Guidance security publications jedoch nicht verwendet. Stattdessen findet eine Bereitstellung der notwendigen Leitlinien durch informative Anhänge innerhalb des relevanten Anforderungsstandards statt, zum Beispiel IEC TS 62443-2-2.
- Test security publications (Kategorie E) definieren Möglichkeiten, um festzustellen, ob die Anforderungen von Base security standards und Group security- oder Product security publications korrekt implementiert wurden. Test security publications haben deshalb typischerweise eine spezialisierte Zielgruppe. Sie können Referenzimplementierungen definieren oder identifizieren, die verwendet werden können, um die korrekte Umsetzung durch erfolgreiche Interoperation zu bestimmen, zum Beispiel ISO/IEC 27007.

3 Fazit

Die in den letzten Jahren zahlreichen und durchaus verschiedenen Ansätze, die global in den unterschiedlichsten Staaten zur Regulierung der Cybersicherheit und bisweilen auch des Datenschutzes verfolgt werden, legen nahe, dass es sich hierbei um ein hochaktuelles Thema handelt, dem eine erhebliche Bedeutung in den innen- wie außenpolitischen Strategien der jeweiligen Regierungen beigemessen wird. Die Konzepte, mit denen der steigenden Bedrohungslage im digitalen Raum begegnet wird, sind dabei unterschiedlich und gehen von punktuellen, themen- und branchenspezifischen Regelungen bis hin zu ganzheitlichen Regulierungsansätzen, die auch Datenschutz- und Zertifizierungsfragen in sektoren- und branchenübergreifender Hinsicht adressieren. Daneben sind es teils auch aktuelle technische Herausforderungen, die die Nationalstaaten zur Förderung der Cybersicherheitsregulierung bewegen, so zum Beispiel für Japan im Bereich des IoT.[13] Cybersicherheit wird man aber letztlich nicht nur als rechtliche, sondern auch als Aufgabe der internationalen Normung und Standardisierung zu betrachten haben:[14] So können einschlägige Normen nicht nur zur

[13] Ein weiteres Beispiel für neue, technikbezogene Gesetzgebungsvorhaben in Asien ist der Entwurf für ein Datenschutzgesetz in Indien, dazu *Kipker*, ZD 2018, S. 253.

[14] Siehe nur *Kipker/Müller*, InTeR 2018, S. 24.

technischen Konkretisierung der rechtlichen Cybersicherheitsanforderungen beitragen, sondern auch die einheitliche Auslegung von (neu erlassenen) Rechtsvorschriften fördern.[15] Nicht zuletzt kann die Standardisierung das Mittel zur Durchführung einer staatenübergreifenden Cybersicherheitszertifizierung sein bzw. diese zumindest erleichtern. Insoweit ist es zu begrüßen, dass die Belange der Normung und Standardisierung voraussichtlich auch in der neuen EU Cybersecurity-Verordnung in angemessener Weise Berücksichtigung finden.

Literatur

Kipker, Dennis-Kenji: Stellungnahme zum Entwurf des People's Republic of China Cybersecurity Law, MMR-Aktuell 2015, 370972.

Kipker, Dennis-Kenji: Unbestimmte Rechtsbegriffe, DuD 2016, S. 610.

Kipker, Dennis-Kenji: Die NIS-RL der EU im Vergleich zum deutschen IT Sicherheitsgesetz, ZD-Aktuell 2016, 05261.

Kipker, Dennis-Kenji: The EU NIS Directive Compared to the IT Security Act – Germany is Well Positioned for the new European Cybersecurity Space, ZD-Aktuell 2016, 05363.

Kipker, Dennis-Kenji: Das neue chinesische Cybersecurity Law – ein ganzheitlicher Ansatz zur Regulierung von Informationssicherheit, MMR 2017, S. 455-460.

Kipker, Dennis-Kenji: Massiver Ausbau der EU-Cyber-Sicherheitskapazitäten – Jahresansprache 2017 des EU-Kommissionspräsidenten Juncker und Veröffentlichung der neuen europäischen Cyber-Sicherheitsstrategie, MMR-Aktuell 2017, 394677.

Kipker, Dennis-Kenji: Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk, MMR-Aktuell 2017, 395945.

Kipker, Dennis-Kenji/Harner, Andreas/Müller, Sven: Der Mensch an der Schnittstelle zur Technik – Praxishilfe in der Umsetzung von Datensicherheit durch den IT-Security Navigator, InTeR 2018, S. 24-29.

Kipker, Dennis-Kenji: Aktuelle Digitalisierungspolitik in Russland: Regulierung von Datenschutz, öffentlicher Sicherheit und Cybersecurity, ZD 2018, S. 296-300.

Kipker, Dennis-Kenji: Pläne für ein Datenschutzgesetz in Indien: Untersuchung des White Paper des Expertenkomitees, ZD 2018, S. 253-255.

Fischer, Matthias/Kipker, Dennis-Kenji/Voskamp, Friederike: Internationaler Rahmen, in: Dennis-Kenji Kipker (Hrsg.), Handbuch Cybersecurity-Recht, Beck-Verlag 2018 (im Erscheinen).

[15] *Kipker*, DuD 2016, S. 610.

ROBOCOP STREIFT DURCH DAS NETZ: GRUNDRECHTSEINGRIFFE DURCH DIE AUTOMATISIERTE UNTERSTÜTZUNG VON POLIZEIARBEIT IM SOCIAL WEB*

Dr. Sebastian J. Golla

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

Zusammenfassung

Dieser Beitrag widmet sich der Frage, ob und inwieweit der Einsatz polizeilicher Software-Anwendungen zur Analyse offen zugänglicher Bereiche Sozialer Netzwerke in Grundrechte der Nutzer eingreift. Im Fokus steht dabei das Recht auf informationelle Selbstbestimmung. Der Beitrag untersucht, nach welchen Kriterien die Intensität eines Eingriffes in dieses Recht zu bewerten ist. Dies ist mitentscheidend für die Frage, ob der Einsatz entsprechender Software-Anwendungen auf die polizeilichen Generalklauseln zur Datenerhebung und -verarbeitung gestützt werden kann.

1 Die Polizei auf „Streife“ im Internet

1.1 (Teil-)Automatisierung polizeilicher Tätigkeiten

Bereits seit dem Aufstieg des Internets zum Massenphänomen in der zweiten Hälfte der 1990er-Jahre ist die Polizei online zu präventiven und repressiven Zwecken aktiv.[1] Im Fokus stehen dabei in den letzten Jahren auch Soziale Netzwerke wie Facebook, Twitter, YouTube oder Telegram.[2] Bisher beobachtet die Polizei Aktivitäten hier im Wesentlichen manuell. Polizeibeamte rufen dabei im Sinne einer „Online-Streife“ beispielsweise Seiten oder Gruppen ab und sichten dort Inhalte. Dabei bedienen sich die Polizisten auch durch die Netzwerke bzw. Websites selbst bereitgestellter Hilfs-

* Der Beitrag entstand im Rahmen der im Zuge der Bekanntmachung „KMU-innovativ: Forschung für die zivile Sicherheit“ des BMBF im Rahmen des Programms „Forschung für die zivile Sicherheit“ der Bundesregierung geförderten Projekte „Visuelle Entscheidungsunterstützung bei der Auswertung von Daten aus sozialen Netzwerken“ (INTEGER) und „Propaganda, Mobilisierung und Radikalisierung zur Gewalt in der virtuellen und realen Welt“ (PANDORA).

1 *Zöller*, GA 2000, S. 563 (567).

2 Vgl. *Schulz/Hoffmann*, DuD 2012, S. 7 (7 f.).

mittel wie Suchfunktionen, um relevante Inhalte aufzufinden und zu ordnen. Bereits diese polizeilichen Aktivitäten mit jedermann zugänglichen Methoden werfen rechtliche Fragen auf.[3]

Neue rechtliche Herausforderungen bringt die automatisierte Auswertung von Online-Inhalten mit eigener polizeilicher Software mit sich. Es zeichnet sich ab, dass die Entwicklung und der Einsatz entsprechender Software-Anwendungen in absehbarer Zeit zunehmen werden. Polizei und Sicherheitsbehörden können durch die automatisierte Analyse und visuelle Aufbereitung von Inhalten aus sozialen Netzwerken sowohl bei ihrer präventiven als auch bei ihrer repressiven Tätigkeit unterstützt werden. Neue Software-Anwendungen können unter anderem für die Polizeiarbeit relevante Interessen- und Nutzergruppen identifizieren, Verknüpfungen zwischen Inhalten der Netzwerke aufzeigen und diese thematisch analysieren. Sie ermöglichen auch vertiefte Recherchen zu einzelnen Personen und den Abgleich von Informationen aus sozialen Netzwerken mit Daten aus dem polizeilichen Bestand.

Dieser Beitrag widmet sich der Frage, ob und inwieweit der Einsatz entsprechender Software-Anwendungen zur Analyse offen zugänglicher Bereiche Sozialer Netzwerke in Grundrechte der Nutzer eingreift. Im Fokus steht dabei das Recht auf informationelle Selbstbestimmung. Der Beitrag untersucht, nach welchen Kriterien die Intensität eines Eingriffes in dieses Recht zu bewerten ist. Dies ist mitentscheidend für die Frage, ob der Einsatz entsprechender Software-Anwendungen auf die polizeilichen Generalklauseln zur Datenerhebung und -verarbeitung gestützt werden kann. Dies

[3] Vgl. zu den Rechtsfragen verdeckter personaler Ermittlungsmaßnahmen von Polizeibeamten in Sozialen Netzwerken *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten"; *Oermann/Staben*, Der Staat 2013, S. 630 (630 ff.); *Rosengarten/Römer*, NJW 2012, S. 1764 (1764 ff.); *Soiné*, NStZ 2014, S. 248 (249 ff.).

ist nur dann der Fall, wenn die Intensität der Grundrechtseingriffe als gering zu bewerten ist.[4] In diesem Fall ist die Polizei nach den Generalklauseln zu der Erhebung und Verarbeitung der für die Erfüllung ihrer Aufgaben notwendigen personenbezogenen Daten ermächtigt.[5]

1.2 Allgemein Zugängliche Daten in sozialen Netzwerken

Die folgende Betrachtung beschränkt sich auf Anwendungen, die mit allgemein zugänglichen Daten aus offenen Bereichen Sozialer Netzwerke arbeiten. Dafür ist vorab zu klären, bis zu welcher Grenze Daten aus sozialen Netzwerken als allgemein zugänglich gelten können. Angelehnt an die Legaldefinition in § 10 Abs. 5 S. 2 BDSG aF lassen sich solche Daten als allgemein zugänglich verstehen, „die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann." Eine rechtliche Beschränkung des Zugangs schließt dabei die allgemeine Zugänglichkeit aus.[6]

Eindeutig allgemein zugänglich sind Informationen aus Profilen, Gruppen oder andere Bereichen von Sozialen Medien, die ohne Anmeldung im Internet frei abrufbar sind und somit geeignet sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[7] Auf der anderen Seite des zu beurteilenden Spektrums stehen Profile und weitere Inhalte, die den Einstellungen des Nutzers entsprechend nur für einen beschränkten Kreis von Personen (z.B. „Freunde") sichtbar sind.[8] Diese sind als nicht allgemein zugänglich anzusehen, da sowohl technisch als auch nach dem Willen des Betroffenen eine klare Einschränkung des Adressatenkreises zu erkennen ist.[9]

---

[4] *Bäcker*, Kriminalpräventionsrecht, S. 258; vgl. auch *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, § 13 Rn. 24.

[5] Art. 31 Abs. 1 und 2 BayPAG; §§ 30 Abs. 1 und 2, 39 Abs. 1 BbgPolG; §§ 18 Abs. 1 S. 2 und 3, 42 Abs. 1 S. 1 ASOG Bln; §§ 28 Abs. 1 – 4, 36a Abs. 1 S. 1 BremPolG; §§ 20 Abs. 2–5, 37 Abs. 1 S. 1 BWPolG; §§ 6, 16 Abs. 1 HambGDatPol; §§ 13 Abs. 1 und 2, 20 Abs. 1 S. 1 HSOG; §§ 27 Abs. 1–4, 36 Abs. 1 S. 1 SOG M-V; §§ 31 Abs. 1–3, 38 Abs. 1 S. 1 Nds-SOG; § 24 Abs. 1 PolG NRW; §§ 26 Abs. 1–4, 33 Abs. 1 RPOG; §§ 26 Abs. 1–3, 30 Abs. 1 S. 1 SPolG; §§ 36 Abs. 1, 43 Abs. 1 S. 1 SächsPolG; §§ 179 Abs. 1 und 2, 188 Abs. 1 S. 1, 189 Abs. 1 S. 1 LVwG Schl.-Holst.; §§ 32 Abs. 1 und 2, 40 Abs. 1 PAG Thüringen; §§ 21 Abs. 1 und 2, 29 Abs. 1 S. 1 BPolG; §§ 8 Abs. 1, 2, 5 und 6, 9, 20g Abs. 1 und 2 BKAG; vgl. zu der besonderen Regelung in § 9 Abs. 1 S. 1, Abs. 3 S. 2 PolG NRW, die letztlich ebenfalls eine Generalklausel zur Datenerhebung ergibt *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, § 13 Rn. 9.

[6] BGH, ZD 2013, S. 502 (505).

[7] *Simitis*, in: Simitis, BDSG, § 28 Rn. 151; *Spindler*, DB 2016, S. 937 (944); *Zilkens/Cavin*, ZD 2013, S. 603 (604).

[8] *Weichert*, in: Kühling/Buchner, DS-GVO, Art. 9 Rn. 82.

[9] So auch *Franck*, in: Gola, DS-GVO, Art. 14 Rn. 14.

Schwierig zu beurteilen ist, ob Profile und andere offenbar von den Betroffenen bereitgestellte Daten als veröffentlicht gelten können, wenn diese nur nach Registrierung und Anmeldung in dem Sozialen Medium eingesehen werden können. Zum Teil wird die öffentliche Zugänglichkeit aufgrund des Erfordernisses einer Anmeldung generell abgelehnt.[10] Sachgerechter erscheint aber eine differenzierte Betrachtung: Soziale Medien sehen unterschiedliche Schwellen für die Anmeldung vor. Wenn eine Registrierung und Anmeldung für jedermann ohne besonderen Aufwand möglich ist, spricht dies dafür, Daten, die nach der Anmeldung eingesehen werden können, als öffentlich zu qualifizieren.[11] Dies gilt stets dann, wenn Registrierung und Anmeldung ausschließlich dazu dienen sollen, Bots und Crawlern den Zugang zu den Medien zu erschweren (technische Zugangsbarriere). Der Anschein der Öffentlichkeit wird auch nicht dadurch beseitigt, dass der Nutzer etwa eine E-Mailadresse hinterlegen muss, damit im Sozialen Netzwerk eine adäquate Zuordnung möglich ist, wenn sonst keine individuellen Anforderungen an den Zugang gestellt werden. Ein soziales Netzwerk – bzw. einer seiner Teilbereiche — ist aber dann nicht als öffentlich anzusehen, wenn die Anmeldung spezifisch zur Überprüfung der Zugehörigkeit zum Adressatenkreis des Contents dient. Bei den populären Netzwerken Facebook und Twitter beispielsweise sind derzeit keine besonderen (technischen) Hürden für eine Anmeldung installiert. Somit ist diese für jedermann ohne besondere Zugangsschwelle möglich. Daher sind die dort netzwerkweit geteilten Inhalte als allgemein zugänglich anzusehen.

2 Eingriff in Grundrechte

Im Folgenden wird die Frage untersucht, ob und inwieweit der Einsatz polizeilicher Software-Anwendungen zur Analyse offen zugänglicher Bereiche Sozialer Netzwerke in Grundrechte der Nutzer eingreift.

2.1 Einschlägige Grundrechte

Dabei konzentriert der Beitrag sich im Wesentlichen auf das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG ist daneben nicht berührt, wenn Anwendungen nur auf offene Teile sozialer Netzwerke und nicht auf zugangsgesicherte Kommunikationsinhalte zielen.[12]

[10] *Wolff*, in: Wolff/Brink, BeckOK DatenschutzR, § 28 Rn. 83; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 58.

[11] Ähnlich *Brenneisen/Staack*, Kriminalistik 2012, S. 627 (629); *Graf*, BeckOK StPO, § 100a Rn. 86; *Zilkens/Cavin*, ZD 2013, S. 603 (604).

[12] Vgl. BVerfGE 120, S. 274 (341); *Rückert*, ZStW 129 2017, S. 302 (309 ff.).

Spätestens seit dem 6. Mai 2018 ist in der grundrechtlichen Betrachtung neben dem Recht auf informationelle Selbstbestimmung auch das Datenschutzgrundrecht aus Art. 8 Abs. 1 GRCh hinzuzuziehen. Mit Geltung der Richtlinie (EU) 2016/680[13] (JIRL) wird der Rechtsrahmen für den polizeilichen Umgang mit personenbezogenen Daten unionsrechtlich harmonisiert.[14] Die JIRL überlässt die Regelung der Befugnisse zur polizeilichen Datenerhebung und -verarbeitung dabei weitgehend den Mitgliedsstaaten.[15] Aufgrund dieses Gestaltungsspielraums bleibt es auch bei der Anwendbarkeit der Grundrechte des Grundgesetzes.[16] Daneben sind aber auch die Unionsgrundrechte zu beachten. Die JIRL stützt sich auf die Kompetenzregelung in Art. 16 AEUV, die auch das Datenschutzgrundrecht regelt.[17] Auch die expansive Rechtsprechung des EuGH zum Anwendungsbereich des europäischen Grundrechtsschutzes spricht für die Anwendung der GRCh.[18]

2.2 Schutzbereich des informationellen Selbstbestimmungsrechts

Das Recht auf informationelle Selbstbestimmung schützt im Ausgangspunkt die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[19] In seinem Volkszählungsurteil folgerte das BVerfG aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Gedanken der Selbstbestimmung, dass jeder Einzelne grundsätzlich selbst darüber entscheiden dürfe, „wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden."[20] Dazu gehöre es auch, dass die Bürger

---

[13] 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, ABl. L 119/89 vom 4.5.2016.

[14] Dazu näher *Bäcker/Hornung*, ZD 2012, S. 147 (151 f.).

[15] Nach Art. 8 Abs. 1 JIRL sehen die Mitgliedstaaten vor, „dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Art. 1 Abs. 1 genannten Zwecken wahrgenommen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt." Nach Abs. 2 der Vorschrift sind im mitgliedsstaatlichen Recht zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung anzugeben; vgl. auch *Bäcker/Hornung*, ZD 2012, S. 147 (149 f.) zu Art. 7 des Kommissionsentwurfes (KOM(2012) 10 endg.).

[16] Vgl. BVerfGE 118, 79 (95 ff.); BVerfGE 129, 78 (103); *Bäcker*, EuR 2015, S. 389 (391).

[17] Art. 16 Abs. 1 AEUV ist wortgleich mit Art. 8 Abs. 1 GRCh.

[18] *Bäcker/Hornung*, ZD 2012, S. 147 (150); *Weinhold/Johannes*, DVBl 2016, S. 1501 (1503 f.) jeweils m.w.N.

[19] BVerfGE 65, 1 (43).

[20] BVerfGE 65, 1 (42).

wissen können müssten, „wer was wann und bei welcher Gelegenheit über sie weiß."[21]

Dieser Schutz knüpft unmittelbar an den Umgang mit jeder Art von personenbezogenen Daten an.[22] Zur Bestimmung des Begriffes „personenbezogene Daten" kann hierbei auf die gesetzliche Definition zurückgegriffen werden. Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen". Hinsichtlich der betreffenden Daten ist es unerheblich, welcher Aussagegehalt ihnen zukommt, solange ein Personenbezug vorhanden ist.[23] Ein „Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten" folgt daraus aber nicht, da der Mensch sich in der sozialen Gemeinschaft entfaltet und auf Kommunikation angewiesen ist.[24] Vor diesem Hintergrund sind auch allgemein zugängliche Daten nur eingeschränkt geschützt.

Im Zusammenhang mit Anwendungen zur Analyse Sozialer Netzwerke fallen grundsätzlich sämtliche Inhalte dieser Netzwerke in den Schutzbereich des informationellen Selbstbestimmungsrechts, die Rückschlüsse auf einzelne identifizierbare Nutzer zulassen.[25] Ob die Nutzer dabei unter Klarnamen oder Pseudonymen agieren, spielt keine Rolle, solange die Möglichkeit besteht, sie mit einem zumutbaren Aufwand persönlich zu identifizieren. Zu den betroffenen personenbezogenen Daten gehören unter anderem Äußerungen, Statusinformationen und weitere geteilte Inhalte von Nutzern Sozialer Netzwerke.

2.3 Eingriffe und ihre Intensität

Grundsätzlich begründet jede Form des Umgangs mit den vom Schutzbereich erfassten Daten einen Eingriff in das informationelle Selbstbestimmungsrecht. Darunter fallen neben der Erhebung und Speicherung der Daten unter anderem ihre Veränderung, Auswertung und Übermittlung.

Eingriffe können dabei von unterschiedlicher Intensität sein. Die Intensität des Eingriffs ist unter anderem für die Frage von Bedeutung, ob dieser unter Anwendung der polizeilichen Generalklauseln zur Datenerhebung und -verarbeitung gerechtfertigt werden kann. Diese können nur Eingriffe von geringfügiger Intensität legitimieren.[26] Die Intensität eines Eingriffs

[21] BVerfGE 65, 1 (43).

[22] BVerfGE 65, 1 (42); vgl. auch *Albers*, Informationelle Selbstbestimmung, S. 280.

[23] Vgl. BVerfGE 65, 1 (45).

[24] BVerfGE 65, 1 (43 f.).

[25] Vgl. *Schulz/Hoffmann*, DuD 2012, S. 7 (9).

[26] *Bäcker*, Kriminalpräventionsrecht, S. 258.

lässt sich nach diversen Kriterien bewerten, die im Folgenden näher beleuchtet werden.

2.3.1 Streubreite, Anzahl der Betroffenen und Anlassbezogenheit

Zunächst ist die Anzahl der betroffenen Personen von Bedeutung.[27] Die potentielle Streubreite des Eingriffs wird auch beim Einsatz polizeilicher Analysetools zu beachten sein. Diese können theoretisch Millionen von Nutzern sozialer Netzwerke betreffen. Schon bei der technischen Ausgestaltung dieser Instrumente wird zu beachten sein, dass sie in quantitativer Hinsicht keine exzessiven Eingriffe ermöglichen dürfen.

Ein weiteres relevantes Kriterium ist, ob und inwiefern die betroffenen Personen für den Eingriff einen Anlass gegeben haben.[28] In Zusammenschau dieser beiden Kriterien weisen nach dem BVerfG „Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – […] grundsätzlich eine hohe Eingriffsintensität auf".[29] Vor diesem Hintergrund kann gerade der Einsatz neuer Technologien, die große Datenmengen nutzen, zu einer Intensivierung des Eingriffs führen.[30] Dies gilt auch für die Erhebung und Verarbeitung allgemein zugänglicher Daten. So hat das BVerfG beispielsweise für die automatisierte Erhebung von Kfz-Kennzeichen im öffentlichen Verkehrsraum und deren Abgleich mit polizeilichen Datenbanken angenommen, dass eine spezifische Ermächtigungsgrundlage erforderlich ist, und hohe Anforderungen an deren Bestimmtheit gestellt.[31]

2.3.2 Art der betroffenen Daten und zu erwartende Folgen

Für die individuelle Intensität des Eingriffs ist weiter maßgeblich, „ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden".[32] Für den besonderen Persönlichkeitsbezug (bzw. die Persönlichkeitsrelevanz) ist zu beachten, ob die betroffenen Informationen besonderen rechtlichen Schutz genießen. Dies kann der Fall sein, wenn sie

---

[27] BVerfGE 115, 320 (347).

[28] BVerfGE 115, 320 (347); vgl. auch BVerfGE 100, 313 (376); BVerfGE 107, 299 (318 ff.).

[29] BVerfGE 115, 320 (354).

[30] Vgl. *Pieroth/Schlink/Kniesel,* Polizei- und Ordnungsrecht, § 14 Rn. 16.

[31] BVerfGE 120, 378 (409 ff.).

[32] BVerfGE 115, 320 (347 f.); vgl. auch BVerfGE 100, 313 (376); BVerfGE 109, 279 (353).

aus einem rechtlich geschützten Vertrauensbereich stammen oder von besonderen Privatheitsgarantien (etwa Art. 10 GG oder Art. 13 GG) erfasst sind.[33] Auch wenn Informationen einen Bezug zu anderen verfassungsrechtlich geschützten Bereichen aufweisen, spricht dies für eine besondere Persönlichkeitsrelevanz. Dies gilt etwa für die rassische und ethnische Herkunft (geschützt durch Art. 3 Abs. 3 GG) oder religiöse Überzeugungen (geschützt durch Art. 140 GG i.V.m. Art. 136 Abs. 3 WRV). Diese beispielhaft genannten und weitere Kategorien sind auch auf einfachgesetzlicher Ebene als besondere Kategorien personenbezogener Daten anerkannt.[34]

Für polizeiliche Analysetools ist daher zu prüfen, ob sie Daten mit besonderem Persönlichkeitsbezug verarbeiten. Dafür müssen die Programme nicht gezielt mit Daten arbeiten, die besonderen grundrechtlichen Schutz genießen. Daten dieser Art können auch beiläufig anfallen. Nutzt die Polizei beispielsweise Software, um Nutzergruppen in rechtsradikalen oder islamistischen Milieus zu identifizieren oder um nach Themen in diesen Milieus zu recherchieren, dann besteht eine hohe Wahrscheinlichkeit, dass sie hierbei auch personenbezogene Daten erfasst, die politische Meinungen oder religiöse Überzeugungen betreffen und damit besonders geschützt sind.

Eine besondere Eingriffsintensität weist die Erhebung und Verarbeitung personenbezogener Daten auch dann auf, wenn sie kumulativ ein umfassendes Bild über die Persönlichkeit oder das Verhalten eines Individuums erzeugt.[35] Das Erstellen von „Persönlichkeitsprofilen“ oder „Persönlichkeitsbildern“ wird dabei auch als „Obergrenze“[36] des Zulässigen betrachtet.[37] Eine „umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger“[38] ist verfassungsrechtlich nicht zulässig.

Als mögliche nachteilige Folgen des Einsatzes von Analysetools kommen für die Betroffenen besonders das Risiko, Gegenstand von Ermittlungsmaßnahmen zu werden, sowie eine mögliche stigmatisierende Wirkung dieser

---

[33] BVerfGE 115, 320 (348); *Gusy*, Polizei- und Ordnungsrecht, Rn. 193.

[34] Vgl. Art. 9 Abs. 1 DSGVO und Art. 10 JIRL.

[35] *Gusy*, Polizei- und Ordnungsrecht, Rn. 193; vgl. auch *Simon/Taeger*, JZ 1982, S. 140 (143), nach denen es der Menschenwürde widerspricht, „den Bürger in seiner ganzen Persönlichkeit zu erfassen oder ihn durch Datensammlungen teilabzubilden“.

[36] *Schaar*, DuD 2001, S. 383; *v. Lewinski*, RDV 2003, S. 122 (123).

[37] Der Begriff des Persönlichkeitsprofils ist allerdings äußerst unscharf und schwer zu operationalisieren; vgl. *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, S. 241 ff.

[38] BVerfGE 115, 320 (351 f.).

Ermittlungen bzw. der Maßnahmen der Datenerhebung selbst in Betracht.[39] Die Intensität des Eingriffs steigt auch dadurch, dass Betroffene weitere einschneidende Maßnahmen auch nur befürchten, ohne dass diese tatsächlich stattfinden müssen. Auf diese Weise können Datenerhebung und -verarbeitung aufgrund von Abschreckungseffekten („chilling effects") eine zusätzliche Eingriffsqualität erhalten.[40]

2.3.3 Offenheit und Unmittelbarkeit der Datenverarbeitung

Das Polizeirecht unterscheidet zwischen der verdeckten und offenen Datenerhebung und -verarbeitung sowie der mittelbaren und unmittelbaren Datenerhebung.[41] Diese Faktoren wirken sich auch auf grundrechtlicher Ebene auf die Intensität eines Eingriffs in das informationelle Selbstbestimmungsrecht aus.

Die Heimlichkeit einer Datenerhebung und -verarbeitung ist ein Umstand, der die Intensität des Eingriffs (gegenüber einer offenen Erhebung und Verarbeitung) erhöht.[42] Die informationelle Selbstbestimmung des Betroffenen ist weniger stark berührt, wenn die Erhebung der Daten für ihn offen und nachvollziehbar erfolgt. Erfolgt sie verdeckt, erschwert es dies dem Betroffenen, Rechtsschutz gegen die Maßnahmen zu erlangen oder diese zu beeinflussen.

Die Erhebung personenbezogener Daten aus sozialen Netzwerken und ihre Weiterverarbeitung durch Analysesoftware werden sich sowohl aus Sicht des Betroffenen als auch aus Sicht der Netzwerkbetreiber regelmäßig als verdeckte Datenerhebung darstellen, da sie diesen verborgen bleiben.[43] Der polizeiliche Charakter der Datenerhebung und -verarbeitung ist für die Betroffenen genauso wenig erkennbar wie die Tatsache, dass überhaupt eine Datenverarbeitung stattfindet.[44] Eine offene Erhebung aus Sicht des Betroffenen läge vor, wenn Polizisten mit Nutzerkonten, die sie als Polizisten kenntlich machen, in sozialen Netzwerken Daten erheben würden.

Auch die mittelbare Erhebung ist gegenüber der unmittelbaren Erhebung, bei der die Betroffenen in die Erhebung aktiv mit einbezogen werden,

---

[39] Vgl. BVerfGE 115, 320 (351).

[40] *Oermann/Staben*, Der Staat 2013, S. 630 (640 ff.); vgl. auch *Gusy*, Polizei- und Ordnungsrecht, Rn. 193.

[41] *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, § 13 Rn. 1.

[42] *Gusy*, Polizei- und Ordnungsrecht, Rn. 173.

[43] Vgl. *Kugelmann*, Polizei- und Ordnungsrecht, S. 167 f.; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, § 13 Rn. 1.

[44] Der verdeckte Charakter liegt hier ähnlich wie bei der „virtuellen Streifenfahrt" bereits in der Natur der Sache; vgl. dazu *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten", S. 140 f.

als intensiverer Eingriff zu werten. Die Erhebung erfolgt auch mittelbar, solange sie über ein Programm erfolgt, das die Inhalte Sozialer Netzwerke über Entwicklerschnittstellen[45] oder deren Web-Oberfläche ausliest. Die Nutzer der Programme treten nicht mit den Betroffenen in Kontakt und beziehen diese weder körperlich noch mental in die Erhebung mit ein, so dass die Datenerhebung nicht von einer Mitwirkung der Betroffenen abhängt. Eine unmittelbare Erhebung wäre erst dann gegeben, wenn Polizisten in den sozialen Netzwerken aktiv partizipieren oder interagieren.

2.3.4 Verarbeitung allgemein zugänglicher Daten

Als mindernder Faktor für die Eingriffsintensität zu berücksichtigen ist insbesondere, wenn lediglich allgemein zugängliche Daten[46] verarbeitet werden.[47] In bestimmten Fällen kann ein Eingriff sogar ganz ausgeschlossen sein, wenn lediglich allgemein zugängliche Daten verarbeitet werden. Nach dem BVerfG ist ein Eingriff bei allgemein zugänglichen Daten erst anzunehmen, wenn die Daten „durch ihre systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhalten, aus dem sich die für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefährdungslage für die Freiheitsrechte oder die Privatheit des Betroffenen ergibt."[48] Dies sei beispielsweise dann der Fall, wenn die Daten mit anderen geschützten Daten verbunden würden und dadurch der Aussagegehalt zunehme.[49] Ein Eingriff liegt jedenfalls dann nicht vor, wenn eine „Online-Streife" sich in allgemein zugänglichen Bereichen von sozialen Netzwerken bewegt, ohne dabei gezielt personenbezogene Daten zu erheben.[50]

Für die Frage des Eingriffs ist mitentscheidend, wann eine für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefährdungslage vorliegt. Es fragt sich, ob eine solche stets anzunehmen ist, „wenn gezielt öffentlich zugängliche Informationen über eine Person zusammengetragen werden".[51] Mit Blick auf die Gefährdungslage, vor der das Recht auf informationelle Selbstbestimmun schützen soll, wird ein beeinträchtigendes Verhalten auch bei der Verarbeitung allgemein zugänglicher Daten dann anzunehmen sein, wenn aus diesen Daten „weitere Informationen erzeugt

[45] Regelmäßig als Application Programming Interface (API) bezeichnet.

[46] Vgl. zu der Frage, welche Daten in Sozialen Netzwerken als allgemein zugänglich gelten können oben 1.2.

[47] Vgl. *Rückert*, ZStW 129 2017, S. 302 (323 f.).

[48] BVerfGE 120, 351 (362); vgl. auch BVerfGE 120, 274 (344 f.).

[49] BVerfGE 120, 351 (362).

[50] *Singelnstein*, NStZ 2012, S 593 (600).

[51] So *Singelnstein*, NStZ 2012, S. 593 (600).

und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können".[52] Sofern sich aus der Verarbeitung der Daten aber nur personenbezogene Informationen ergeben, die nicht über die Summe der von dem Betroffenen an einer konkreten Stelle selbst über ihn veröffentlichten Daten hinausgehen, dürfte kein Grundrechtseingriff vorliegen. Dies bedeutet auch, dass kein Eingriff vorliegen dürfte, solange sich aus einer Verarbeitung keine zusätzlichen Informationen über den Betroffenen, sondern lediglich allgemeine bzw. gruppenspezifische Informationen ableiten lassen.

Für polizeiliche Analysetools, die Daten aus sozialen Netzwerken verarbeiten, bedeutet dies, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung regelmäßig vorliegen wird. Einen Mehrwert für die Polizeiarbeit dürften die Funktionen dieser Tools erst mit sich bringen, wenn sie Inhalte aus Netzwerken auch systematisch erfassen und verarbeiten, um einen neuen Aussagewert zu erzeugen. Darunter fällt auch schon das automatisierte systematische Sortieren von Inhalten zur weiteren manuellen Sichtung.

2.3.5 Anonymisierung der Daten

Auch eine (sofortige) Anonymisierung der Daten kann die Intensität des Eingriffs verringern. In gewissen Fällen können die zuvor genannten Kriterien den Eingriffscharakter einer Maßnahme auch ganz ausschließen. Dies urteilte das BVerfG im Zusammenhang mit der automatisierten Erfassung von Kraftfahrzeugkennzeichen im öffentlichen Verkehrsraum, die mit dem Fahndungsbestand der Polizei abgeglichen wurden.[53] Der Bereich, für den Eingriffe ausgeschlossen werden können, ist allerdings überaus eng. Wenn ein Datenabgleich nicht unverzüglich erfolgt und die personenbezogenen Daten nicht ohne weitere Auswertung sofort und spurenlos gelöscht werden, bleibt es bei einem Eingriff. Jedenfalls bei den Abgleichen, bei denen sich eine Übereinstimmung mit dem Fahndungsbestand ergibt, liegt ein Eingriff vor. Dies ist auch bei jeglicher Form der weiteren Auswertung der erfassten Daten der Fall.

Für den Einsatz von Analyse-Software könnte ein Eingriff nach diesen Kriterien nur dann ausgeschlossen sein, wenn nach der ersten Erfassung personenbezogener Daten ohne jegliche Auswertung eine Aussonderung erfolgte und nur nicht-personenbezogene Informationen verblieben. Auch hier ist es im Ausgangspunkt zweifelhaft, ob sich die Funktionalität solcher

[52] BVerfGE 120, 274 (312).

[53] Ein Eingriff kann danach ausgeschlossen sein, „soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden"; BVerfGE 120, 378 (399).

Anwendungen beibehalten ließe, wenn die Auswertung der Daten nach diesen Kriterien eingeschränkt würde. Eine wirksame Anonymisierung würde eine nicht auf einzelne Personen zurückführbare Reduktion der aus sozialen Netzwerken entnommenen Informationen erfordern. Damit dürften nur noch stark gekürzte oder verfremdete Daten für die weitere Auswertung zur Verfügung stehen. Offen ist, ob diese in ihrem Aussagegehalt für die weitere Polizeiarbeit von Nutzen sein könnten.

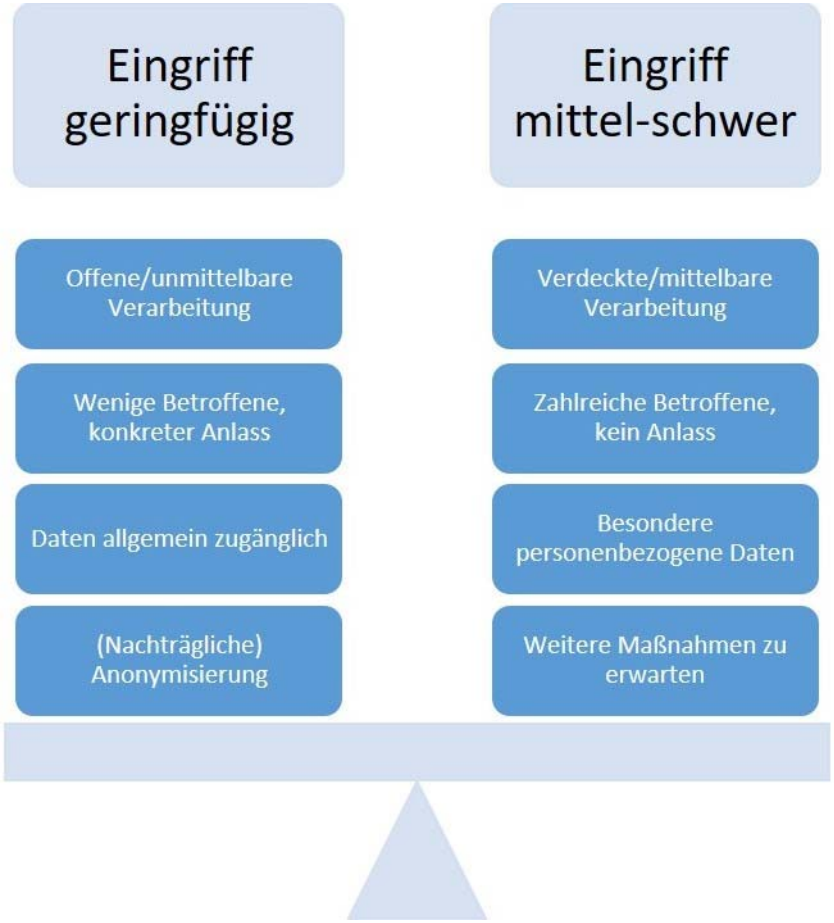

Abb. 1: Kriterien zur Beurteilung der Eingriffsintensität

3 Fazit

Die herkömmlichen „manuellen“ Aktivitäten der Polizei in sozialen Netzwerken wurden überwiegend noch unterhalb der Schwelle eines Eingriffes in das Recht auf informationelle Selbstbestimmung eingeordnet. Diese Schwelle ist aber spätestens mit dem unterstützenden Einsatz von Technologien zur automatisierten Verarbeitung personenbezogener Daten überschritten. Sofern die Funktionen der Software nicht unter Tilgung sämtlicher Personenbezüge der zu Grunde liegenden Informationen einsetzbar sind, begründet ihr Einsatz einen Eingriff und bedarf einer Rechtsgrundlage.

Für die Fragen, von welcher Intensität der Eingriff ist und ob dieser auf die Generalklauseln zur Datenerhebung und -verarbeitung in den Polizeigesetzen gestützt werden kann, sind eine Vielzahl von Kriterien zu beachten (vgl. Abb. 1). Die Intensität des Eingriffs lässt sich im Detail nur anhand der konkreten Funktionalitäten einer Software beurteilen. Schon durch deren technische Gestaltung sollte die Intensität der Eingriffe nach Möglichkeit gemindert werden. Grundlegend lässt sich sagen, dass vertiefte automatisierte Recherchen zu einzelnen Personen – auch ausschließlich auf Grundlage allgemein zugänglicher Daten – aufgrund ihrer erhöhten Persönlichkeitsrelevanz regelmäßig einen mehr als nur geringfügigen Eingriff bedeuten dürften. Eher ereignis- oder gruppenbezogene Analysen, bei denen das Individuum nicht im Mittelpunkt steht, dürften sich bei entsprechenden technischen und organisatorischen Vorkehrungen jedoch auch als geringfügige Eingriffe realisieren lassen.

Literatur

Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden 2005.

Bäcker, Matthias: Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, S. 389-415.

Bäcker, Matthias: Kriminalpräventionsrecht, Tübingen 2015.

Bäcker, Matthias/Hornung, Gerrit: EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa – Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht, ZD 2012, S. 147-152.

Beck'scher Online Kommentar zum Datenschutzrecht, 22. Ed., München 2017.

Beck'scher Online Kommentar zur StPO, 28. Ed., München 2017.

Brenneisen, Hartmut/Staack, Dirk: Die virtuelle Streife in der Welt der Social media, Kriminalistik 2012, S. 627-631.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz- Kompaktkommentar zum BDSG, 5. Aufl., Frankfurt 2016.

Eisenmenger, Florian: Die Grundrechtsrelevanz „virtueller Streifenfahrten", Berlin 2017.

Gola, Peter (Hrsg.): Datenschutz- Grundverordnung (DS-GVO), München 2017.

Golla, Sebastian J.: Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, Berlin 2015.

Gusy, Christoph: Polizei- und Ordnungsrecht, 10. Aufl., Tübingen 2017.

Kugelmann, Dieter: Polizei- und Ordnungsrecht, 2. Aufl., Heidelberg 2012.

Kühling, Jürgen/Buchner, Benedikt: Datenschutz-Grundverordnung (DS-GVO), 2. Aufl., München 2018.

Von Lewinski, Kai: Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, S. 122-132.

Oermann, Markus/Staben, Julian: Mittelbare Grundrechtseingriffe durch Abschreckung? Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online- Ermittlungen in sozialen Netzwerken, Der Staat 2013, S. 630-661.

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael: Polizei- und Ordnungsrecht, 9. Aufl., München 2016.

Rosengarten, Carsten/Römer, Sebastian: „Der virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards, NJW 2012, S. 1764-1767.

Rückert, Christian: Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, ZStW 129 2017, S. 302-333.

Schaar, Peter: Persönlichkeitsprofile im Internet, DuD 2001, S. 383-388.

Schulz, Sönke/Hoffmann, Christian: Staatliche Datenerhebung in Sozialen Netzwerken, DuD 2012, S. 7-13.

Simon, Jürgen/Taeger, Jürgen: Grenzen kriminalpolizeilicher Rasterfahndung, JZ 1982, S. 140-145.

Singelnstein, Tobias: Möglichkeiten und Grenzen neuer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593-606.

Soiné, Michael: Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014, S. 248-251.

Spindler, Gerald: Die neue EU-Datenschutzgrundverordnung, DB 2017, S. 937-947.

Weinhold, Robert/Johannes, Paul: Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr – Die neue Datenschutz-Richtlinie im Bereich Polizei und Justiz sowie deren Konsequenzen für deutsche Gesetzgebung und Praxis, DVBl 2016, S. 1501-1506.

Zilkens, Martin/Cavin, Adrian: Soziale Netzwerke im Umfeld kommunaler Aufgabenerfüllung – Datenschutzrechtliche Grenzen der Recherche und der eigenen Präsentation, ZD 2013, S. 603-607.

Zöller, Mark Alexander: Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563-577.

PRESSE- UND ÖFFENTLICHKEITSARBEIT UNTER DER DSGVO

Thorsten Feldmann, LL.M.

JBB Rechtsanwälte, Berlin

Zusammenfassung

Die DSGVO (DSGVO) regelt Kommunikationsinhalte. Sie stellt folglich ein Lösungsinstrument des geradezu klassischen Konflikts zwischen dem Datenschutz und der Meinungsfreiheit dar. Wie im Folgenden aufzuzeigen sein wird, hat sich die Rechtslage für die Presse- und Öffentlichkeitsarbeit unter der DSGVO verschärft.

1 Datenschutzrechtlicher Ausgangspunkt

Betreibt man eine Website, auf der Angaben über natürliche lebenden Personen enthalten sind, beispielsweise Name, Geburtsdaten, Fotos o.ä., ist darin ein datenschutzrechtlicher Übermittlungsvorgang zu erblicken. Dies entspricht seit der Entscheidung des EuGH vom 6. November 2003 im Falle Bodil Linquist[1] der ständigen Rechtsprechung auch der deutschen Gerichte. Die juristischen und praktischen Folgen, die diese Feststellung für die Meinungsäußerung im Internet nach sich ziehen, sind erheblich. Vorbehaltlich des Anwendungsbereichs von Medienprivilegien findet demnach das Verbot mit Erlaubnisvorbehalt Anwendung, sodass für jede personenbezogene Veröffentlichung vorab nach einem gesonderten datenschutzrechtlichen Erlaubnistatbestand zu suchen ist, dessen Grenzen bei der Umsetzung der Veröffentlichung natürlich einzuhalten sind. Dies hat sich auch mit dem Inkrafttreten der DSGVO nicht geändert. Art. 6 Abs. 1 DSGVO sieht ausdrücklich vor, dass eine Datenverarbeitung „nur rechtmäßig ist“, wenn die Voraussetzungen eines der von der Norm genannten Erlaubnistatbestände erfüllt sind.

2 Grundrechtskonflikt

Der Konflikt grundrechtlicher Dimension liegt auf der Hand: Der Betroffene hat ein aus Art. 2 Abs. 1 GG ausfließendes Recht auf informationelle Selbstbestimmung, das einen Teilausschnitt seines allgemeinen Persönlichkeitsrechts bildet. Dieses wird zusätzlich abgesichert durch Art. 8 der EU-GRC, wonach der Betroffene Schutz für seine personenbezogenen Daten genießt. Auf der Ebene des einfachen Gesetzesrechts und des sekundären Gemeinschaftsrechts wird dies durch die DSGVO und u.a. das neue

[1] EuGH, Urt. v. 6.11.2003 – Rs C-101/01, MMR 2004, 95 (Bodil Lindquist).

Bundesdatenschutzgesetz (BDSG) weiter ausdifferenziert. Auf der anderen Seite des Konflikts kann der sich Äußernde auf Art. 5 Abs. 1 GG, die Meinung- und Pressefreiheit berufen, die auch durch Art. 11 der EU-GRC verankert ist und darüber hinaus durch Art. 10 EMRK abgesichert wird. Im Falle der Veröffentlichung personenbezogener Daten im Internet treffen diese in diametral in entgegengesetzte Stoßrichtung zielenden Interessen aufeinander.

Setzt man sich auch nur oberflächlich mit der gefestigten Rechtsprechung des Bundesverfassungsgerichts zur Meinungs- und Pressefreiheit gem. Art. 5 Abs. 1 GG auseinander, wird schnell klar, dass der Konflikt zwischen den Äußerungsfreiheiten und dem Datenschutz höchst sensible Bereiche berührt. So lässt sich bereits aus dem Wortlaut von Art. 5 Abs. 1 GG über das Zensurverbot hinaus ableiten, dass man für die Äußerung seiner Meinung keine Erlaubnis und kein berechtigtes Interesse benötigt. Die Meinungsäußerung ist vielmehr auch Ausdruck der eigenen Persönlichkeit, für die aus übergeordneten gesellschaftlichen Gründen ein verfassungsrechtlicher Anreiz bestehen soll. Daraus ergibt sich auch, dass die Ausübung der Meinungsfreiheit nicht durch eine Aufsichtsbehörde überwacht werden darf. Aufgrund einschlägiger Erfahrungen in der deutschen Geschichte steht das Grundgesetz einer staatlichen Regulierung von Äußerungen geradezu feindlich gegenüber. Aus diesem Grunde darf nach der Lüth-Rechtsprechung des Bundesverfassungsgerichts,[2] anders als bei der Eigentumsgarantie des Art. 14 GG, der Inhalt der Meinungsfreiheit nicht zur Disposition des einfachen Gesetzgebers gestellt werden. Die Fragen, welche Äußerudngen in den Schutzbereich des Grundrechts fallen und wann die Grenzen der Meinungsfreiheit im Einzelfall überschritten sind, sind dem einfachen Gesetzgeber grundsätzlich entzogen. In der Regel sind die Grenzen der Meinungsfreiheit durch die Verfassung selbst zu ziehen. Daher muss nach der vom Bundesverfassungsgericht in er Lüth-Entscheidung ins Leben gerufenen Wechselwirkungslehre jedes einfache Gesetz daraufhin überprüft werden, welche Auswirkungen es auf die Ausübung der Meinungsfreiheit insgesamt haben könnte. Dieses Erfordernis ergibt sich aus dem die Demokratie konstituierenden Charakter, der der Meinungsfreiheit zu eigen ist. Bei der Meinungsfreiheit des Art. 5 Abs. 1 GG handelt es sich danach um ein besonderes Grundrecht, das unter einen besonderen Schutz zu stellen ist.

Aus diesen Gründen kann gegenläufigen Interessen einschließlich des allgemeinen Persönlichkeitsrecht und des Datenschutzes im Kollisionsfalle kein automatischer Vorrang gegenüber der Meinungsfreiheit eingeräumt werden. Auch dies hat das Bundesverfassungsgericht schon früh, nämlich

[2] BVerfGE 7, 198 – Lüth.

in der Entscheidung Lebach, ausdrücklich festgestellt.[3] Daraus ergibt sich ein Gebot der Abwägung im Einzelfall, sollte es zu einer derartigen Grundrechtskollision kommen. Bei dem Abwägungsgebot handelt es sich um einen ehernen Grundsatz der Äußerungsfreiheit.

Aus dem besonderen Charakter der Meinungsfreiheit des Art. 5 Abs. 1 GG ergibt sich darüber hinaus, dass gesetzgeberische oder behördliche Chilling Effects durch Sanktionsandrohungen o.ä. strikt zu vermeiden sind.

3 Bisherige datenschutzrechtliche Lösungsmechanismen

Der Konflikt ist nicht neu. Auch das bisherige Datenschutzrecht musste mit ihm umgehen. So sah schon die Datenschutzrichtlinie 95/46/EG in Art. 9 ein Medienprivileg für die „Verarbeitung personenbezogener Daten vor, die „allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt". In der Bundesrepublik Deutschland wurde dies umgesetzt durch die § 41 BDSG und § 57 RfStV. Für den nicht-journalistischen Bereich außerhalb des traditionellen Medienprivilegs half die zivilgerichtliche Rechtsprechung. In seinem Urt. vom 23. Juni 2009[4] setzte der Bundesgerichtshof gleich eine ganze Fülle datenschutzrechtlicher Beschränkungen des damaligen § 29 BDSG außer Kraft, um der nicht-journalistischen Meinungsäußerung das erforderliche Gewicht zu verleihen und um sich gegenüber dem Datenschutzrecht durchzusetzen. Insbesondere die prozeduralen Voraussetzungen einer Datenverarbeitung, namentlich die Glaubhaftmachung eines berechtigten Interesses und die Unterrichtung des Betroffenen, sollten keine Anwendung mehr finden. Stattdessen unterwarf der BGH die Frage der Zulässigkeit der Meinungsäußerung im Internet einer „Gesamtabwägung". Dieser von der Rechtsprechung geschaffene datenschutzrechtliche Lösungsmechanismus stand in Einklang mit den Anforderungen, die Art. 5 Abs. 1 GG an die Meinungsfreiheit beschränkende Gesetze stellt. Die gegen das Urt. des BGH gerichtete Verfassungsbeschwerde hat das Bundesverfassungsgericht nicht zur Entscheidung angenommen.

Vor dem Inkrafttreten der DSGVO bestand nach alledem in der Bundesrepublik Deutschland nicht nur im Anwendungsbereich des Medienprivilegs, sondern auch für die nicht-journalistische Informationsvermittlung im Internet ein austarierter und mit der Meinungsfreiheit in Einklang stehender Lösungsansatz des Grundrechtskonflikts zur Verfügung.

---

[3] BVerfGE 35, 202 – Lebach.

[4] BGH, Urt. v. 23.6.2009 – VI ZR 196/08, K&R 2009, 565.

4 Neuregelungen der DSGVO und des deutschen Rechts

Die DSGVO hat das Rad ein Stück weit zurückgedreht. Der Lösungsvorschlag des gegenwärtigen deutschen Datenschutzrechts lautet: Einseitiger Vorrang des Datenschutzes. Dies wirft Fragen auf.

4.1 Art. 85 DSGVO

Auch die DSGVO sieht in Art. 85 DSGVO ein Medienprivileg vor. Nach dem Wortlaut der Norm in Abs. 1 „bringen" die Mitgliedstaaten den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, „einschließlich" der Verarbeitung zu journalistischen Zwecken, „in Einklang". Gem. Abs. 2 des Art. 85 DSGVO werden für die Verarbeitung, die zu journalistischen Zwecken erfolgt, die wesentlichen Regelungskomplexe der DSGVO, insbesondere die Grundsätze in Kapitel II, die Rechte der Betroffenen in Kapitel III sowie die Regelungen zur Aufsicht in Kapitel VI, komplett ausgeschaltet. Letzten Endes findet damit das Datenschutzrecht auf die journalistische Meinungsäußerung keine Anwendung.

Bereits aus dem Wortlaut des Art. 85 Abs. 1 DSGVO ergibt sich aber, dass die DSGVO nicht nur die journalistische Meinungsäußerung im Blick hat. Sie sieht diese nur als einen Unterfall der Vermittlung von Informationen an. Nach hier vertretener Auffassung sind die Mitgliedstaaten nicht gehindert, auch für den Bereich der nicht-journalistischen Meinungsäußerung Privilegien zu schaffen. Dies wird gestützt durch Erwägungsgrund 153, der vorsieht, dass im Recht der Mitgliedstaaten durch Vorschriften für die freie Meinungsäußerung und Informationsfreiheit „auch" von Journalisten mit dem Datenschutzrecht in Einklang gebracht werden sollen. Des Weiteren verlangt der Erwägungsgrund, dass die Meinungsfreiheit fördernde Begriffe „wie Journalismus" weit ausgelegt werden sollen. Die DSGVO geht vielleicht sogar noch darüber hinaus, wenn man Art. 85 Abs. 1 DSGVO so liest, dass ohne mitgliedstaatliche Regelungen der Datenschutz mit der Meinungsäußerungsfreiheit noch nicht „in Einklang" steht und erst durch Schaffung positiven Rechts durch die Mitgliedstaaten „in Einklang" gebracht wird. Nach anderer Auffassung erschöpft sich der Regelungsbereich von Art. 85 Abs. 1 DSGVO in einer Zuständigkeitszuweisung an die Mitgliedstaaten.[5] Art. 85 Abs. 1 des GVO wäre damit keine Öffnungsklausel.

[5] *Kühling/Martini*, Die DSGVO und das nationale Recht, S. 287. So natürlich auch die Auffassung der Datenschutzkonferenz, Oldenburg November 2017.

4.2 Umsetzung in Deutschland

Seit dem 25. Mai 2018 gilt auch in der Bundesrepublik ein neues Medienprivileg. § 57 RfStV transformiert nahezu wortgleich Art. 85 Abs. 2 DSGVO ins deutsche Recht. Diese Norm gilt allerdings nur für Rundfunk und Telemedien. Sie ersetzt die Regelungen in den Rundfunk- und Mediengesetzen der Länder. Entsprechende Regelungen gibt es in den Landespressegesetzen, zum Beispiel in § 12 LPG NRW oder in § 10 HessLPG. Flächendeckende datenschutzrechtliche Privilegien für nicht-journalistische Angebote gibt es dagegen nicht.

4.3 Folgen

Art. 85 Abs. 2 DSGVO und die deutschen Transformationsgesetze haben für klassische Medien, insbesondere Fernsehsender und Verlage, zur Folge, dass im redaktionellen Bereich des Medienunternehmens mit Art. 6 Abs. 1 DSGVO die zentralen Normen des Datenschutzrecht nicht gilt, dass das Verbot mit Erlaubnisvorbehalt normiert. Des Weiteren entfällt die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Medienunternehmen müssen auch keine Dokumentation gem. Art. 30 DSGVO führen. Die Betroffenenrechte der Art. 12 ff. DSGVO einschließlich des Rechts auf Vergessenwerden gem. Art. 18 DSGVO gibt es für Medien nicht. Schließlich setzen die Medienprivilegien die Regelungen zu den Aufsichtsbehörden, insbesondere auch die Regelungen zu den Befugnissen gem. Art. 58 DSGVO außer Kraft. Im journalistischen Bereich müssen lediglich die Datensicherheit gem. Art. 5 Abs. 1 lit. f und Art. 32 DSGVO eingehalten und die technischen und organisatorischen Maßnahmen gem. Art. 24 DSGVO gewährleistet sein. Verletzungen dieser Normen können auch mit den Sanktionen der Art. 82 und 83 DSGVO belegt werden. Handlungen, die außerhalb der Medien Datenschutzverstöße wären, sind jenseits dessen aber nicht sanktionierbar.

§ 57 RfStV und die Landespressegesetze beschränken sich auf die Verarbeitung zu journalistischen Zwecken. Alle anderen modernen Formen der praktischen Ausübung der Meinungs- und Informationsfreiheit sind nicht erfasst. Komplett von seinem Schutz ausgenommen sind etwa Bewertungsportale, Angebote aus dem Bereich der sozialen Medien von Nicht-Journalisten, wie etwa Blogs, Foren, Podcasts Facebook- und Twitterprofile und vor allem auch der gesamte Bereich der PR und des Lobbyismus einschließlich Websites von Unternehmen, Gewerkschaften, NGOs oder Parteien. Sie alle haben mit dem geltenden Datenschutzrecht zu kämpfen. Die Ausübung ihrer Meinungsfreiheit steht unter dem strengen Vorbehalt der DSGVO. Verstöße können drakonisch sanktioniert werden.

In diesem Zusammenhang ist daran zu erinnern, dass Art. 85 Abs. 1 DSGVO sowie alle Weiteren grundrechtlichen Kommunikationsfreiheiten

sich auf jedwede Meinungsäußerung beziehen, nicht nur auf die professionell-mediale. Das geltende Datenschutzrecht übersieht dies. Nach hier vertretene Auffassung wird es dem durch Art. 85 Abs. 1 DSGVO erteilten Auftrag nicht gerecht. Nach alledem wirkt das Medienprivileg sehr tief. Es ist aber nicht breit genug.

Fraglich ist, inwieweit Regelungen der vor Wirksamwerden der DSGVO am 25. Mai 2018 bestehenden Rechtsordnung zugunsten der Meinungsfreiheit herangezogen werden können. Hier stellt sich vor allem die Frage, ob etwa Art. 5 GG, § 23 Abs. 1 KUG oder § 823 BGB als datenschutzrechtliche Erlaubnisnormen zur Verfügung stehen. Die Datenschutzkonferenz hat sich auf ihrer Sitzung am 9. November 2017 in Oldenburg dagegen positioniert, nämlich so, dass gesetzliche Anpassungen im Sinne des Art. 85 DSGVO konkret und spezifisch sein müssen.[6] Sie müssten sich also auf die jeweiligen Normen und Vorgaben der DSGVO beziehen. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht. Nach dieser Auffassung sind äußerungsfreundliche Normen des Datenschutzrechts spezifisch auf Basis der DSGVO erst zu schaffen.

In diesem Zusammenhang könnte man noch die Frage aufwerfen, ob unmittelbar aus der DSGVO heraus Einschränkungen an ihrem Anwendungsbereich geboten sind, so lange der Schutz personenbezogener Daten noch nicht durch mitgliedstaatliche Regelungen „in Einklang“ mit dem Recht auf freie Meinungsäußerungen und der Informationsfreiheit gebracht wurde (Art. 85 Abs. 1 DSGVO). Eine solche Lösung wird allerdings bislang noch nirgendwo diskutiert. Dogmatischer Ansatz wäre Art. 6 Abs. 1 lit. f DSGVO. Gestützt durch Erwägungsgrund 153, der eine weite Auslegung äußerungsfreundlicher Normen gebietet, ließe sich eine Lösung finden, die sich an die vom Bundesgerichtshof favorisierte Gesamtabwägung im Fall spickmich annähert. Der systematische Boden für eine solche Lösung wäre also bereit.

Allerdings muss beachtet werden, dass das Vorhandensein eines Erlaubnistatbestands für die nicht-journalistische Meinungsäußerung zwar notwendig, aber keinesfalls hinreichend ist, um alle mit der DSGVO verbundenen Fragestellungen und Probleme für die Meinungsäußerung, die private und öffentliche Meinungsbildung und die Informationsfreiheit zufriedenstellend zu lösen. Jenseits des Medienprivilegs schafft die DSGVO wirtschaftliche, technische und administrative Hürden für die elektronische Meinungsäußerung, die gerade keine meinungsfreundliche Umgebung kreiert. Zu nennen sind hier die Nachweispflicht des Art. 5 Abs. 2 DSGVO in

[6] Entschließung der DSK vom 9. November 2018. Abrufbar unter https://www.lfd.niedersachsen.de/download/124346/DSK_Entschliessung__zu_Art._85_DSGVO.pdf (abgerufen am 9.8.2018).

Verbindung mit der Verarbeitungsübersicht gem. Art. 30 DSGVO, das Erfordernis der Darlegung eines berechtigten Interesses im Sinne des Art. 13 Abs. 1 DSGVO, die Benachrichtigungspflicht des Art. 14 DSGVO, der immaterielle Schadensersatz mit Beweislastumkehr gem. Art. 82 DSGVO, die Bußgeldandrohung des Art. 83 DSGVO und vor allem auch die Befugnisse der Behörden in den Art. 57 ff. DSGVO.

Erinnert man sich an die Freiheiten, die Art. 5 Abs. 1 GG auch dem nichtjournalistischen Sprecher verleiht - dies sind vor allem Freiheiten vor gesetzgeberischen Eingriffen und behördlicher Überwachung -, kommt man nicht umhin festzustellen dass das geltende Datenschutzrecht an zentralen Stellen zugunsten der Meinungsfreiheit der Korrektur bedarf. Dies beginnt bereits beim Verbot mit Erlaubnisvorbehalt in Art. 6 Abs. 1 DSGVO. Korrekturen sind aber auch bei der Datenschutzaufsicht, den Sanktionen und zivilrechtlichen Rechtsbehelfen vorzunehmen, von denen ein erheblicher einschüchternder Effekt auf die Ausübung der Meinungsfreiheit ausgeht. Geradezu unlösbar erscheint die Frage des von Art. 5 Abs. 1 GG verhängten Verbots für den einfachen Gesetzgeber, die Meinungsfreiheit durch ein einfaches Gesetz wie das BDSG oder den RfStV durchzuregulieren. Hier hilft nur eine komplette Bereichsausnahme des Datenschutzrechts für die auch private freie Meinungsäußerung.

Literatur

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

DER EUGH ALS LEHRMEISTER: WAS DEUTSCHE GERICHTE BEIM UMGANG MIT DEN MEDIEN VON INTERNATIONALEN GERICHTEN LERNEN KÖNNEN

Dipl.-Jur. Anna K. Bernzen, LL.B.

Universität Mannheim
abernzen@mail.uni-mannheim.de

Zusammenfassung

Journalisten, die aus deutschen Gerichten berichten, sind enge rechtliche Grenzen gesetzt. Mit dem Gesetz zur Erweiterung der Medienöffentlichkeit in Gerichtsverfahren wurden jene Vorgaben jüngst zwar etwas gelockert. Ein Blick auf den Umgang europäischer und internationaler Gerichte mit den Medien zeigt jedoch, dass eine weitere Entspannung möglich wäre. Der vorliegende Beitrag ermittelt, inwiefern der deutsche Gesetzgeber sich hierbei ein Beispiel an den genannten Gerichten nehmen könnte – oder sogar sollte.

1 Einleitung

Diese Bildfolge ist den Fernsehzuschauern bestens bekannt: Gemessenen Schrittes schreiten die Richter in den Sitzungssaal. Im Hintergrund ist das Klicken der Fotokameras zu hören. Sind alle Richter eingezogen, nehmen sie, mehr oder weniger synchron, am Richtertisch Platz. Ein paar Sekunden blicken sie ernst in den Saal, dann wird den Kamerateams bedeutet, die Aufnahmen einzustellen. Doch nicht nur der Auftritt der Richter folgt einer klaren Choreografie. Auch die Arbeit der Medien im Gericht ist streng reglementiert. Dieser Beitrag beginnt damit, die Regeln für die journalistische Arbeit bei Gericht darzustellen. Da sie kürzlich reformiert wurden, wird zwischen bisheriger und neuer Rechtslage unterschieden. Anschließend wird der Rahmen für die Arbeit der Medien an ausgewählten europäischen und internationalen Gerichten aufgezeigt. Zuletzt wird untersucht, inwiefern der Gesetzgeber bei einer denkbaren künftigen Reform von den Erfahrungen dieser Gerichte profitieren kann.

2 Die bisherige Rechtslage in Deutschland

Zentrale Voraussetzung für jede Berichterstattung aus dem Gericht ist, dass die jeweilige Verhandlung öffentlich ist.[1] Jene Voraussetzung gewährleistet der Grundsatz der Öffentlichkeit mündlicher Verhandlungen gem. § 169 Abs. 1 S. 1 GVG. Nach diesem Prinzip darf jeder unbeteiligte Dritte an jeder mündlichen Verhandlung teilnehmen.[2] Dieses Zutritts- und Anwesenheitsrecht steht auch Journalisten zu, die dahingehend zu behandeln sind wie „normale" Bürger.[3]

Eine Grenze setzt der Arbeit der Journalisten allerdings § 169 Abs. 1 S. 2 GVG, der es ihnen verbietet, Bild-Ton- oder Ton-Aufnahmen einer Verhandlung anzufertigen, sofern sie diese Aufnahmen öffentlich vorführen oder ihren Inhalt publizieren wollen. Am BVerfG dürfen jedoch seit 1998 zu Beginn der Verhandlung bis die Anwesenheit der Beteiligten festgestellt wurde und während der öffentlichen Entscheidungsverkündung entsprechende Aufnahmen hergestellt werden (§ 17a Abs. 1 S. 2 BVerfGG). Die Aufnahmen oder ihre Übertragung können im Einzelfall aber untersagt oder unter Auflagen gestellt werden, wenn das zur Wahrung der schutzwürdigen Interessen der Verfahrensbeteiligten oder Dritter bzw. zur Wahrung eines ordnungsgemäßen Verfahrensablaufs nötig ist (§ 17a Abs. 2 BVerfGG).

Bild-Aufnahmen und Wortberichte sind dagegen zwar nicht gesetzlich geregelt.[4] Sie können aber im Einzelfall vom vorsitzenden Richter basierend auf seinen sitzungspolizeilichen Befugnissen nach § 176 GVG oder von der Justizverwaltung auf Basis des Hausrechts untersagt oder eingeschränkt werden.[5] Dass Beschränkungen oft erlassen werden, zeigt eine Vielzahl diesbezüglicher Entscheidungen des BVerfG, das sie in ständiger Rechtsprechung an der Pressefreiheit nach Art. 5 Abs. 1 S. 2 Var. 1 GG misst.[6]

Eine tatsächliche Grenze für die Medien ist die Kapazität des Sitzungssaals. Der Zugang hierzu muss stets nur so weit gewährt werden, wie es

---

1 Zwar kann Journalisten nach § 175 Abs. 2 Nr. 1 GVG auch Zutritt zu nichtöffentlichen Verhandlungen gewährt werden. Praktisch relevanter sind aber öffentliche Verhandlungen.

2 *Mayer*, in: Kissel/Mayer, GVG, § 169 Rn. 1.

3 *Von Coelln*, AfP 2014, S. 193; *Mitsch*, ZRP 2014, S. 137 (138).

4 BT-Drs. IV/178, S. 45.

5 BT-Drs. IV/178, S. 45.

6 BVerfG, Beschl. v. 11.5.1994, 1 BvR 733/94, NJW 1996, 310; Beschl. v. 31.7.2014, 1 BvR 1858/14, NJW 2014, 3013 (3014); Beschl. v. 9.9.2016, 1 BvR 2022/16, NJW 2017, 798; Beschl. v. 17.8.2017, 1 BvR 1741/17, NJW 2017, 3288.

die räumlichen Gegebenheiten zulassen.[7] Zwar darf eine gewisse Anzahl an Plätzen im Zuschauerbereich für Journalisten reserviert werden.[8] Bei öffentlichkeitswirksamen Prozessen reichen jedoch auch diese Plätze oft nicht aus, um allen interessierten Medienvertretern Zutritt zu gewähren – wie sich im Strafprozess gegen die Mitglieder des selbst ernannten „Nationalsozialistischen Untergrunds“[9] zeigte.[10]

3 Die neue Rechtslage in Deutschland

Am 19. April 2018 änderten sich die Arbeitsbedingungen der Journalisten in deutschen Gerichten: Das Gesetz zur Erweiterung der Medienöffentlichkeit in Gerichtsverfahren (EMöGG)[11] trat in Kraft.

3.1 Tonübertragung in einen Medienarbeitsraum

Der dadurch neu eingefügte § 169 Abs. 1 S. 3 GVG ermöglicht es dem Gericht seitdem, die Tonübertragung der mündlichen Verhandlung in einen Medienarbeitsraum zu erlauben. Das wird besonders in den Prozessen relevant, in denen mehr Journalisten Zugang zu Gericht begehren, als Sitzplätze zur Verfügung stehen[12] – das NSU-Verfahren lässt grüßen.[13] Für Journalisten, die vom BVerfG berichten, ist das nichts Neues: Dort gibt es einen solchen Arbeitsraum schon seit einiger Zeit.[14]

Die Einrichtung eines Medienarbeitsraums steht ganz im Ermessen des Gerichts.[15] Bei der Entscheidung hat es einen weiten Beurteilungsspielraum.[16] Es muss dabei insbesondere das öffentliche Informationsbedürfnis

---

[7] Ständige Rechtsprechung, s. nur RG, Urt. v. 3.10.1913, II 809/13, RGSt 47, 322; Urt. v. 4.5.1938, VI 17/38, RGZ 157, 341 (344); BGH, Urt. v. 10.11.1953, 5 StR 445/53, BGHSt 5, 75 (83); Urt. v. 28.6.1984, 4 StR 243/84, NStZ 1984, 470.

[8] Die Gerichte beanstandeten dieses sehr übliche Vorgehen bisher jedenfalls nicht, s. nur BVerfG, Beschl. v. 30.10.2002, 1 BvR 1932/02, NJW 2003, 500; BGH, Beschl. v. 10.1.2006, 1 StR 527/05, NJW 2006, 1220 (1221).

[9] OLG München: laufendes Strafverfahren, 6 St 3/12.

[10] Zum (zuerst missglückten) Verfahren der Platzvergabe *Geuther*, DRiZ 2013, S. 166.

[11] Gesetz v. 18.10.2017, BGBl. I, S. 3546.

[12] *Mayer*, in: Kissel/Mayer, GVG, § 169 Rn. 86a; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, § 169 GVG Rn. 18; *Walther*, BeckOK-StPO, § 169 GVG Rn. 24. Enger *Lückemann*, in: Zöller, ZPO, § 169 GVG Rn. 17: grundsätzlich *nur* in diesen Fällen.

[13] Vgl. *Düwell*, jurisPR-ArbR 41/2017, Anm. 1.

[14] *Mayer*, in: Kissel/Mayer, GVG, § 169 Rn. 86a.

[15] Anders gestaltet es sich nach § 17a Abs. 1 S. 3 BVerfGG am BVerfG, an dem der oder die Vorsitzende die Übertragung gestatten kann.

[16] *Walther*, BeckOK-StPO, § 169 GVG Rn. 25.

auf der einen Seite gegen das allgemeine Persönlichkeitsrecht der Verfahrensbeteiligten, ihren Anspruch auf ein faires Verfahren sowie die Funktionstüchtigkeit der Rechtspflege auf der anderen Seite abwägen. Das Informationsinteresse fällt nach Meinung des Gesetzgebers hierbei besonders schwer ins Gewicht, wenn das Ergebnis der Verhandlung für zahlreiche vergleichbare Fälle relevant wird. Weniger schwer soll es aber wiegen, wenn die Öffentlichkeit den Prozess nur aus Neugier oder Sensationslust verfolgen möchte.[17]

Das Ergebnis der gerichtlichen Abwägung kann auch eine nur teilweise Übertragung der Verhandlung in einen Arbeitsraum sein: Nach § 169 Abs. 1 S. 4 GVG kann das Gericht die Übertragung partiell untersagen, um schutzwürdige Interessen der Beteiligten oder Dritter und den ordnungsgemäßen Ablauf des Verfahrens zu wahren. Die Regelung ist fast wortgleich mit § 17a Abs. 2 BVerfGG und daher ebenso auszulegen. Schutzwürdige Interessen sind demnach bspw. Grundrechte,[18] insbesondere das allgemeine Persönlichkeitsrecht.[19] „Ablauf des Verfahrens" meint den Schutz einer Verhandlung in der gesamten Instanz.[20] Von der Möglichkeit der teilweisen Beschränkung kann das Gericht auch noch während einer laufenden Verhandlung Gebrauch machen, etwa wenn die relevanten Gefahren erst nach seiner ursprünglichen Entscheidung auftreten.[21]

Im Medienarbeitsraum dürfen sich Personen aufhalten, die für Presse, Hörfunk, Fernsehen oder andere Medien berichten. Die offene Formulierung „andere Medien" zeigt, dass er nicht nur klassischen Gerichtsreportern zur Verfügung stehen soll, sondern für „beliebige"[22] Medien geöffnet ist. Weil sich besonders jüngere Bürger über moderne Medien wie Blogs oder soziale Netzwerke informieren, müssen bspw. auch ihre Autoren Zugang erhalten.[23] Dabei kommt es nicht darauf an, dass sie beruflich tätig sind.[24] Den veränderten Informationsgewohnheiten entspricht es, ebenso

[17] BT-Drs. 18/10144, S. 26.

[18] So für § 17a Abs. 2 BVerfGG *von Coelln*, in: Maunz/Schmidt-Bleibtreu/Klein/Bethge, BVerfGG, § 17a Rn. 84.

[19] So für § 17a Abs. 2 BVerfGG BT-Drs. 13/7673, S. 9.

[20] *Albers*, in: Baumbach/Lauterbach/Albers/Hartmann, ZPO, § 169 GVG Rn. 16.

[21] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, § 169 GVG Rn. 19.

[22] *Albers*, in: Baumbach/Lauterbach/Albers/Hartmann, ZPO, § 169 GVG Rn. 13.

[23] *Hirzebruch*, BRJ 2017, S. 5 (8).

[24] So aber *Lückemann*, in: Zöller, ZPO, § 169 GVG Rn. 17.

Personen den Zutritt zu gewähren, die hobbymäßig Bericht erstatten. Probleme bei der Feststellung, wer hierfür in Frage kommt,[25] entstehen dadurch nicht: Am BVerfG wird der Zugang zum Arbeitsraum etwa auch Personen gestattet, die auf eine Website verweisen können, auf der sie regelmäßig publizieren.[26] Auf derartige Anhaltspunkte können in einem Zweifelsfall auch Fachgerichte ihre Entscheidung stützen.

§ 169 Abs. 1 S. 5 GVG regelt zuletzt, dass der in den Arbeitsraum übertragene Ton nicht für Publikationszwecke aufgenommen werden darf, indem er § 169 Abs. 1 S. 2 GVG für entsprechend anwendbar erklärt.[27]

3.2 Tonaufnahmen zu wissenschaftlichen und historischen Zwecken

Gerichtsverfahren von herausragender zeitgeschichtlicher Bedeutung für die Bundesrepublik Deutschland können nach § 169 Abs. 2 GVG nunmehr zu wissenschaftlichen und historischen Zwecken im Ton aufgezeichnet werden, wenn das Gericht dies zulässt. Diese Aufnahmen sollen aber gerade nicht für eine Berichterstattung verwendet werden.[28] Mangels Relevanz für die Arbeit von Journalisten bleibt die Neuerung also außer Betracht.

3.3 Aufnahmen der Entscheidungen oberster Bundesgerichte

Besonders wichtig für die Gerichtsberichterstattung ist der neue § 169 Abs. 3 GVG. Gemäß dieser Vorschrift kann das Gericht für die Entscheidungsverkündung am Bundesgerichtshof (BGH) in besonderen Fällen Bild-Ton- und Ton-Aufnahmen zu Veröffentlichungszwecken zulassen. Durch Änderungen entsprechender Vorschriften der Verfahrensordnungen oder über Verweisungsnormen gilt die Regelung an obersten Bundesgerichten.

Auf Tatbestandsseite wird die Ausnahme dadurch begrenzt, dass die Aufnahmen lediglich in besonderen Fällen zugelassen werden dürfen. Ein Indiz für das Vorliegen eines solchen Falles soll es sein, wenn das Gericht eine Presseerklärung zu dem Verfahren veröffentlichen würde.[29] Generell soll das überregionale Medieninteresse an dem Verfahren berücksichtigt werden.[30] Dieses Tatbestandsmerkmal fehlte im Referentenentwurf noch und wurde, wohl als Reaktion auf Kritik daran, erst in einer späten Phase des

---

[25] Vgl. *Franke*, NJW 2016, S. 2618 (2620); *Schlothauer*, StV 2015, S. 665 (668); *Walther*, BeckOK StPO, § 169 GVG Rn. 26.

[26] *Schlothauer*, StV 2015, S. 665 (668).

[27] Dazu *Hoeren*, NJW 2017, S. 3339: „nur eine Übertragungserlaubnis und kein Veröffentlichungstatbestand".

[28] BT-Drs. 18/10144, S. 19.

[29] BT-Drs. 18/10144, S. 29; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, § 169 GVG Rn. 30.

[30] BT-Drs. 18/10144, S. 29; *Mayer*, in: Kissel/Mayer, GVG, § 169 Rn. 66c.

Gesetzgebungsprozesses eingefügt.[31] Seine Geschichte spricht also für eine enge Auslegung. Darauf deutet auch hin, dass nach Schätzungen des Gesetzgebers nur 50 Verkündungen jährlich für Aufnahmen in Frage kommen.[32] Ob die Gerichte dies in der Praxis so streng handhaben werden, muss sich zeigen. Die Zulassungspraxis des BGH in den ersten Monaten deutet jedenfalls auf eine großzügigere Auslegung hin.[33]

Auf Rechtsfolgenseite steht die Zulassung der Aufzeichnung wiederum im Ermessen des Gerichts. Dabei soll es dieselben Kriterien gegeneinander abwägen wie bei der Entscheidung über eine Tonübertragung in den Medienarbeitsraum.[34] Daneben weist die Gesetzesbegründung auf die „vom Bundesverfassungsgericht aufgestellten Grundsätze“[35] als Maßstab für die Abwägung hin und meint offenbar die erwähnte Rechtsprechung zu den sitzungspolizeilichen Medienverfügungen. Die Begründung nennt für einzelne Verfahrensarten sogar konkrete Positionen, die in die Abwägung einzubeziehen sind: In Strafverfahren seien neben dem Persönlichkeitsrecht des Angeklagten auch seine Sicherheit und Resozialisierung relevant.[36] In Verfahren vor den Arbeitsgerichten könne das Diskretionsinteresse des Arbeitgebers mit Blick auf Betriebs-, Geschäfts- und Erfindungsgeheimnisse gegen Aufnahmen sprechen.[37] Für ihre Zulassung könne in Zivilverfahren dagegen streiten, dass besonders schutzwürdige Belange der Allgemeinheit oder wirtschaftlich bzw. gesellschaftspolitisch bedeutsame Rechtsmaterien betroffen sind.[38]

Wiederum steht es im Ermessen des Gerichts, die Aufnahmen oder deren Übertragung teilweise zu untersagen. Daneben können sie von der Einhaltung von Auflagen abhängig gemacht werden (§ 169 Abs. 3 S. 2 GVG). Das kann, ebenso wie die partielle Untersagung der Tonübertragung in den Arbeitsraum, zur Wahrung schutzwürdiger Interessen der Beteiligten bzw. Dritter und eines ordnungsgemäßen Verfahrensablaufs geschehen. Erneut kann für die Auslegung dieser Begriffe auf das zu § 17a Abs. 2 BVerfGG

[31] *Kreicker*, ZIS 2017, S. 85 (92).

[32] BT-Drs. 18/10144, S. 24 f.

[33] S. seine Übersicht über Termine, in denen Aufnahmen angefertigt werden dürfen, unter www.bundesgerichtshof.de/DE/Presse/Terminhinweise/terminhinweise_node.html;jsessionid=DEE0C19254713C85647F325E5379A201.2_cid368 (abgerufen 12.6.2018).

[34] S. oben unter 3.1).

[35] BT-Drs. 18/10144, S. 29.

[36] BT-Drs. 18/10144, S. 29 f.

[37] BT-Drs. 18/10144, S. 30.

[38] BT-Drs. 18/10144, S. 30.

entwickelte Verständnis zurückgegriffen werden.[39] Eine Auflage könnte also bspw. die zahlenmäßige Begrenzung der Kameras sein.[40]

3.4 Unanfechtbarkeit der Entscheidungen

Nach § 169 Abs. 4 GVG sind die gem. § 169 Abs. 1-3 GVG ergangenen Entscheidungen unanfechtbar.[41] Das beseitigt jedoch nicht die Möglichkeit, Verfassungsbeschwerde beim BVerfG einzulegen.[42]

4 Die Rechts- und Sachlage an den europäischen und internationalen Gerichten

Diese moderate Lockerung der Arbeitsbedingungen für Journalisten an deutschen Gerichten steht im Kontrast zum liberalen Umgang der europäischen und internationalen Gerichte mit den Medien. Im Folgenden werden drei verschiedene Modelle dargestellt. Gemeinsam ist allen drei Gerichten, dass zwar die Öffentlichkeit ihrer Verhandlungen ausdrücklich in den relevanten EU- und völkerrechtlichen Regelwerken festgelegt ist. Der Umgang mit den Medien findet dagegen, anders als in Deutschland, an keinem der Gerichte eine explizite rechtliche Grundlage.

4.1 Die Rechts- und Sachlage am Europäischen Gerichtshof

Verhandlungen am Europäischen Gerichtshof (EuGH) sind gem. Art. 47 UAbs. 2 GRCh öffentlich. Wie in Deutschland können Journalisten somit grundsätzlich allen Prozessen beiwohnen. Am EuGH wird außerdem aber oft ein Pressesaal für akkreditierte Pressevertreter eingerichtet.[43] Welche Verfahren dorthin per Video übertragen werden, ist von der Nachfrage der Journalisten abhängig. Sie können die Aufnahmen, die fest installierte Kameras in den Sitzungssälen anfertigen, dort während der gesamten mündlichen Verhandlung auf zwei großen Bildschirmen verfolgen und währenddessen mittels fest installierter Telefon- und Internetanschlüsse an ihren Gerichtsberichten arbeiten.[44]

Journalisten, die für ihre Beiträge außerdem Bild und Ton aus dem Gericht benötigen, erhalten diese über den EU-eigenen Informationsservice

[39] S. oben unter 3.1.

[40] *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, § 169 GVG Rn. 31.

[41] Ein Unterschied ergibt sich auch hier im Vergleich mit dem BVerfG: Gegen Anordnungen des oder der Vorsitzenden kann der Senat angerufen werden (§ 17a Abs. 4 BVerfGG).

[42] *Walther*, BeckOK StPO, § 169 GVG Rn. 21.

[43] Curia.europa.eu/jcms/jcms/Jo2_7054/en/ (abgerufen 12.6.2018).

[44] Email des Pressesprechers des EuGH *Ost* v. 18.4.2018.

„Europe by Satellite“ (EbS).[45] Bitten die Medien den EuGH um Aufnahmen eines Verfahrens oder besteht aus anderen Gründen erkennbar ein großes Interesse hieran, fertigt ein meist zweiköpfiges Kamerateam des Gerichtshofs entsprechende Aufzeichnungen an. Aufgenommen werden allerdings nur die Urteilsverkündung sowie die Verlesung des Schlussantrags des Generalanwalts. Während der Verhandlung wird allenfalls der Aufruf der Sache aufgezeichnet. Sodann schneidet das Kamerateam die Aufnahmen und übermittelt sie per EbS an die Journalisten. Im Einzelfall stellt der EuGH den interessierten Medien die Aufnahmen auch über den Filehosting-Dienst WeTransfer zur Verfügung.[46]

4.2 Die Rechts- und Sachlage am Internationalen Gerichtshof

Verhandlungen am Internationalen Gerichtshof (IGH) sind gem. Art. 46 IGHSt öffentlich. Weil die Plätze im Sitzungssaal aber bevorzugt an Vertreter beteiligter Staaten sowie Diplomaten vergeben werden,[47] kommt dem Pressesaal eine besondere Bedeutung zu. Dort können akkreditierte Journalisten auf einem großen Bildschirm die Videoübertragung der gesamten Verhandlung verfolgen. Der IGH geht aber noch weiter als der EuGH: Die Medienvertreter können sich die internen Aufnahmen über entsprechende Anschlüsse im Pressesaal zugleich für Berichterstattungszwecke herunterladen.[48]

Zusätzlich besteht für Medien mit Onlinepräsenz die Möglichkeit, einen Livestream der Verhandlung auf der Internetseite einzubetten: Die internen Aufnahmen der Verhandlungen werden zeitgleich auf der Webseite des IGH[49] und auf „UN Web TV“[50] übertragen und im Anschluss in eine Multimedia-Galerie auf der Website des IGH eingestellt. Aufgezeichnet werden Bild und Ton im Gericht von einem meist dreiköpfigen audiovisuellen Team. Im Gerichtssaal stehen ihm hierfür sechs fest installierte Kameras sowie diverse fest installierte und bewegliche Mikrofone zur Verfügung. Weil der Livestream zeitgleich übertragen wird, bleiben alle Aufnahmen unbearbeitet.[51]

---

[45] Curia.europa.eu/jcms/jcms/Jo2_7056/en/ (abgerufen 12.6.2018).

[46] Email des Pressesprechers des EuGH *Ost* v. 18.4.2018.

[47] Www.icj-cij.org/en/media-services (abgerufen 12.6.2018).

[48] Email des Information Department des IGH v. 23.4.2018.

[49] Www.icj-cij.org/en/multimedia-index (abgerufen 12.6.2018).

[50] Webtv.un.org (abgerufen 12.6.2018).

[51] Email *des Information Department des IGH* v. 23.4.2018.

Zusätzlich zu den vom Gericht gestellten Aufnahmen dürfen die Fotografen und Kamerateams der Medien sowohl am ersten Tag der ersten mündlichen Stellungnahmen jeder Partei als auch bei der Urteilsverkündung eigene Aufnahmen anfertigen. Etwa eine Viertelstunde vor Beginn der Verhandlung werden sie in den Gerichtssaal geführt und können dort bspw. die anwesenden Delegationen aufnehmen. Eine Minute vor dem Beginn müssen sie sich auf der rechten Seite des Saals positionieren und dürfen von dort den Einzug der Richter und die ersten fünf Minuten der Verhandlung aufzeichnen.[52]

4.3 Die Rechts- und Sachlage am Internationalen Seegerichtshof

Auch Verhandlungen am Internationalen Seegerichtshof (ISGH) sind nach Art. 26 II ISGHSt öffentlich. Dort gibt es – vermutlich aufgrund des oft geringeren öffentlichen Interesses und entsprechend kleineren Medienaufkommens – keinen Pressesaal, in den die Verhandlungen übertragen werden.[53] Wie der IGH zeichnet der ISGH seine Verhandlungen aber auf, um sie als Livestream auf seiner Webseite zu übertragen und sie in ein Onlinearchiv[54] einzustellen.[55] Zuständig für die Aufnahmen sind jene drei Mitarbeiter, die auch die übrige Technologie des Gerichts verantworten. Sie fertigen mithilfe von vier fest installierten Kameras und Mikrofonen Aufnahmen an, die sodann unbearbeitet gestreamt werden. Diese Aufnahmen können bei Bedarf den Medien zur Verfügung gestellt werden.[56]

Hinzu kommt, dass die Medien selbst die ganze Verhandlung am ISGH aufzeichnen dürfen. Sie können im Gerichtssaal sowohl Bild-Ton- als auch Ton-Aufnahmen anfertigen, solange sie die Arbeit des ISGH dabei nicht stören. So werden sie bspw. angehalten, leise zu arbeiten und möglichst wenig umherzulaufen. Kamerateams aus den am Verfahren beteiligten Staaten nehmen diese Möglichkeit durchaus wahr.[57]

5 Die Vorbildfunktion der europäischen und internationalen Gerichte

EuGH, IGH und ISGH bieten drei Alternativen zur gegenwärtigen Rechtslage in Deutschland. Überwiegend ist ihr Umgang mit der Medienöffentlichkeit im Vergleich großzügiger, teils regulieren sie die Arbeit der Medien

[52] Email des Information Department des IGH v. 23.4.2018.

[53] Email der Pressesprecherin des ISGH *Ritter* v. 16.5.2018.

[54] Www.itlos.org/cases/webcast/ (abgerufen 12.6.2018).

[55] Www.itlos.org/en/press-media/media-services/ (abgerufen 12.6.2018).

[56] Email der Pressesprecherin des ISGH *Ritter* v. 16.5.2018.

[57] Email der Pressesprecherin des ISGH *Ritter* v. 16.5.2018.

aber auch stärker. Im Folgenden ist daher zu überlegen, inwiefern die Rechtslage in Deutschland an die Praxis der europäischen und internationalen Gerichte angepasst werden könnte und sollte.

5.1 Verbesserungen des Medienarbeitsraums

Positiv ist die Einrichtung der Pressesäle am EuGH und IGH zu bewerten. Sie unterstützt die Journalisten dabei, die Allgemeinheit über die Arbeit des Gerichts zu informieren. Diese Information ist heute der vorrangige Zweck des Öffentlichkeitsgrundsatzes.[58]

Zur Information der Allgemeinheit trägt einerseits die technische Ausstattung der Säle insbesondere mit einem Internetzugang bei. Die Wortberichterstattung in Echtzeit aus dem Gericht, etwa auf Twitter, wird bspw. als aus Zeitgründen oft inhaltlich unzutreffend kritisiert.[59] Auch für Autoren von Zeitungsartikeln, Fernseh- oder Radiobeiträgen, die schon kurz nach dem Prozess erscheinen, ist die Zeit für gründliche Recherchen jedoch regelmäßig zu knapp. Hätten Journalisten im Medienarbeitsraum einen stabilen Zugang zum Internet, könnten sie während der Verhandlung die nötigen Internetrecherchen durchführen und offene Fragen per Email klären.[60] Auf diese Weise könnten sachliche Fehler in Gerichtsberichten vermieden werden. Die Allgemeinheit würde dadurch über die Arbeit der Judikative besser informiert und dieser Zweck des Öffentlichkeitsgrundsatzes demnach in größerem Umfang verwirklicht.

Des Weiteren sollte auch in Deutschland die Übertragung von Ton *und* Bild in den Medienarbeitsraum zugelassen werden. Eine reine Tonübertragung führt dazu, dass den Journalisten insbesondere die Mimik und Gestik der Beteiligten entgehen.[61] Dadurch wird ihnen aber ein wichtiger Teil der Eindrücke genommen, die sie für die Berichterstattung benötigen.[62] Hinzu kommt, dass es nicht immer möglich ist, den Redner anhand seiner Stimme zutreffend zu identifizieren.[63] Diese beiden Fehlerquellen könnte die Videoübertragung eliminieren. Auch auf diese Weise könnte eine bessere Information der Allgemeinheit erreicht werden. Beschränkt der Gesetzgeber sich dagegen weiter auf Tonübertragungen, könnte die Einrichtung des Me-

---

[58] *Von Coelln*, Zur Medienöffentlichkeit der Dritten Gewalt, S. 196 f. m.w.N.

[59] *Graf*, bei: Libor, AfP 2014, S. 224 (227).

[60] Vgl. *Rath*, DRiZ 2014, S. 8 (9).

[61] Das beabsichtigte der Gesetzgeber auch genau so, s. BT-Drs. 18/10144, S. 27.

[62] *Hoeren*, NJW 2018, S. 3339 (3340); *Rittig*, NJ 2016, S. 265 (268).

[63] *Von Coelln*, AfP 2016, S. 491 (493); *Hirzebruch*, BRJ 2017, S. 5 (8); *Koch/Wallimann*, MDR 2018, S. 241 (243).

dienarbeitsraums in der Praxis ohne Relevanz bleiben. Die Berichterstattung aus dem Gerichtssaal wäre schließlich aus den genannten Gründen attraktiver als die aus dem Arbeitsraum.[64]

5.2 Aufnahmen durch das Gericht, aber nicht ausschließlich

Ambivalent ist die an allen drei Gerichtshöfen praktizierte Aufnahme der Verhandlungen mit hauseigenen Kameras zu bewerten.

Mit Blick auf den Informationszweck der Gerichtsöffentlichkeit ist einerseits positiv zu bewerten, dass sie die Aufzeichnung allen Journalisten für deren Berichterstattung zur Verfügung stellen. Mit diesen Aufnahmen können auch die Medien, die selbst keine Aufnahmen angefertigt haben, ihre Gerichtsberichte illustrieren. So kann zum Beispiel ein lokaler Fernsehsender, der aus finanziellen Gründen kein Kamerateam zum EuGH schicken würde, anschaulich über ein europarechtliches Urteil berichten. Weil Aufnahmen die Gerichtsberichte für Zuschauer attraktiver machen, werden die darin enthaltenen Informationen auf die Weise weiterverbreitet als ohne Aufnahmen.[65] In quantitativer Hinsicht kann der Informationszweck der Öffentlichkeit daher besser erfüllt werden.

Dass IGH und ISGH ihre Prozesse zusätzlich per Livestream übertragen und in Archive auf ihren Webseiten einstellen, ermöglicht es außerdem auch Journalisten, die nicht im Gericht anwesend sind, über die Prozesse zu berichten. Dank der Übertragung im Internet können sie die Verhandlungen jedenfalls am Bildschirm mitverfolgen und sind demnach nicht auf Berichte aus zweiter Hand angewiesen. Da diese Berichte von Zuschauern aus der Verhandlung subjektiv gefärbt sein können, ist der unmittelbare Eindruck ihnen vorzuziehen. Er schafft die Voraussetzungen für eine objektivere Berichterstattung und kann daher in qualitativer Hinsicht den Informationszweck besser erfüllen.

Problematisch ist mit Blick auf die Grundrechte der Journalisten dagegen, wenn wie am EuGH nur das Gericht Aufnahmen anfertigen darf. Die Pressefreiheit schützt das Recht der Journalisten, sich über Vorgänge in einer

[64] *Von Coelln*, AfP 2016, S. 491 (493).

[65] Vgl. *Bamberger*, ZUM 2001, S. 373 (378).

öffentlichen Gerichtsverhandlung zu informieren sowie darüber zu berichten.[66] Der grundrechtliche Schutz beginnt mit der Beschaffung der Informationen und endet mit deren Verbreitung.[67] Das Fotografieren im Gericht ist hiervon nach ständiger Rechtsprechung des BVerfG erfasst.[68] Für die Rundfunkfreiheit nach Art. 5 Abs. 1 S. 1 Alt. 2 GG meint das BVerfG dagegen offenbar, ihr Schutzbereich sei nur eröffnet, soweit die Informationsquelle „Gerichtsverhandlung" für den Rundfunk allgemeinzugänglich sei.[69] Rundfunkaufnahmen in der Verhandlung wären, anders als für Aufnahmen im Umfeld der Verhandlung in ständiger Rechtsprechung anerkannt,[70] aufgrund des Verbots in § 169 Abs. 1 S. 2 GVG danach nicht grundrechtlich geschützt. Eine solche Beschränkung auf allgemeinzugängliche Quellen fordert der Wortlaut der Rundfunkfreiheit allerdings nicht.[71] Dagegen spricht auch ein Umkehrschluss aus ihrer expliziten Normierung für die Informationsfreiheit in Art. 5 Abs. 1 S. 1 Alt. 1 GG.[72] Vor allem bedeutet sie aber nicht nur einen Widerspruch zum Schutz der Bild-Aufnahmen durch die Pressefreiheit, sondern auch zum Schutz der Bild-Ton- sowie der Ton-Aufnahmen im Umfeld der mündlichen Verhandlung durch die Rundfunkfreiheit. Für sie alle kommt es auf die Allgemeinzugänglichkeit schließlich nicht an.

Subsumiert man demnach alle Aufnahmen unter die Medienfreiheiten, stellt die Übertragung der Aufnahmetätigkeit auf das Gericht eine Verletzung dieser Grundrechte dar. Faktisch folgt daraus nämlich ein absolutes Aufnahmeverbot für Journalisten. Dadurch wird die mediale Informationsbeschaffung unverhältnismäßig stark eingeschränkt. Nötig wäre anstelle einer absoluten Lösung eine differenzierte Ausgestaltung des Rechtsrahmens für Aufnahmen bei Gericht, die den Unterschieden zwischen Verfahrensarten, Instanzen und Medienformen Rechnung trägt. Dass die Interessenlagen voneinander abweichen können, hat auch der Gesetzgeber des EMöGG

---

[66] BVerfG, Beschl. v. 6.2.1979, 2 BvR 154/78, BVerfGE 50, 234 (240); Beschl. v. 14.7.1994, 1 BvR 1595/92, BVerfGE 91, 125 (134).

[67] Ständige Rechtsprechung, s. nur BVerfG, Beschl. v. 6.10.1959, 1 BvL 118/53, BVerfGE 10, 118 (121); Urt. v. 27.2.2007, 1 BvR 538/06, BVerfGE 117, 244 (259); Beschl. v. 10. 12.2010, 1 BvR 1739/04, NJW 2011, 1859 (1860); Beschl. v. 10.12.2010, 1 BvR 2020/04, NJW 2011, 1863.

[68] S. oben unter 2.

[69] BVerfG, Urt. v. 24.1.2001, 1 BvR 2623/95, BVerfGE 103, 44 (62).

[70] BVerfG, Beschl. v. 14.7.1994, 1 BvR 1595/92, BVerfGE 91, 125 (135); Beschl. v. 30.3.2012, 1 BvR 711/12, NJW 2012, 2178; Beschl. v. 31.7.2014, 1 BvR 1858/14, NJW 2014, 3013 (3014); Beschl. 9.9.2016, 1 BvR 2022/16, NJW 2017, 798.

[71] *Von Coelln*, AfP 2014, S. 193 (194); *ders.*, Zur Medienöffentlichkeit der Dritten Gewalt, S. 395.

[72] *Von Coelln*, Zur Medienöffentlichkeit der Dritten Gewalt, S. 395.

erkannt und für die nach § 169 Abs. 3 S. 1 GVG nötige Abwägung auf die je nach Verfahrensart divergierenden Positionen hingewiesen.[73]

5.3 Erweiterung der Aufnahmemöglichkeiten für die Medien

Welche Aufnahmen den Medien konkret gestattet werden sollten, kann vorliegend nicht abschließend erörtert werden. Dafür ist vielmehr eine umfassende Abwägung der tangierten Rechte und schutzwürdigen Interessen erforderlich.[74] Dabei können jedoch die positiven Erfahrungen am IGH und ISGH berücksichtigt werden. Für viele befürchtete Nebenwirkungen von Aufnahmen fehlen in Deutschland noch empirische Belege; es handelt sich vielmehr um eine „gefühlte Selbstverständlichkeit".[75] Ein Blick auf die europäischen und internationalen Gerichte kann helfen, die Vermutungen auf ihre Plausibilität zu überprüfen. Dort darf die mündliche Verhandlung (jedenfalls teilweise) von den Medien aufgenommen werden. Dass dabei etwa die Wahrheitsfindung in großem Umfang gefährdet würde – eines der Argumente, die hierzulande oft gegen Aufnahmen angeführt werden –,[76] ist nicht ersichtlich. Das deutet darauf hin, dass auch Aufnahmen an deutschen Gerichten nicht so gravierende negative Konsequenzen haben könnten, wie aktuell befürchtet wird.

Auch für die konkrete Ausgestaltung der neuen Rahmenbedingungen kann der Umgang mit den Medien am IGH und am ISGH Anhaltspunkte liefern. Am IGH dürfen die Medien ihre Aufnahmen nur an ausgewählten Verhandlungstagen und an diesen Tagen auch nur in einem begrenzten Zeitraum anfertigen. Eine derartige zeitliche Beschränkung könnte in Deutschland ebenfalls eingeführt werden. Für das Umfeld der mündlichen Verhandlung billigte das BVerfG bspw. in der Vergangenheit eine Medienverfügung, die Aufnahmen nur am ersten Verhandlungstag gestattete,[77] und eine Verfügung, die den Medien vor der Verhandlung im Grundsatz nur zehn Minuten für ihre Aufnahmen zugestand.[78] Ähnliche Vorgaben könnten für die Verhandlung gemacht werden. Begrenzte man die Aufnahmen so auf bestimmte Phasen, könnten sie jedenfalls in allen übrigen Phasen keinerlei negativen Auswirkungen haben.

---

[73] S. dazu 3.3.

[74] Eine Aufzählung der potentiell tangierten Rechte und Interessen findet sich bei *Bernzen*, Medienrecht im Medienumbruch, S. 205 ff.

[75] So etwa *von Coelln*, AfP 2014, S. 193 (201); *ders.*, bei: *Libor*, AfP 2014, S. 224 (225) für die negativen Auswirkungen auf die Wahrheitsfindung.

[76] S. *Mayer*, in: Kissel/Mayer, GVG, § 169 Rn. 90 m.w.N.

[77] BVerfG, Beschl. v. 18.1.2003, 1 BvQ 2/03, NJW 2003, 2671.

[78] BVerfG, Beschl. v. 17.8.2017, 1 BvR 1741/17, NJW 2017, 3288.

Zudem wird den Medien am IGH kurz vor Beginn der Verhandlung ein fester Standort zugewiesen. Am ISGH werden die Kamerateams in ähnlicher Weise dazu angehalten, sich im Gerichtssaal nicht allzu viel umherzubewegen. Räumliche Vorgaben jener Art könnten auch in Deutschland gemacht werden. Am BVerfG etwa sind die Aufnahmen so anzufertigen, dass das Blickfeld der Richter nach allen Seiten frei ist.[79] Am BGH dürfen die Kameraleute sich während der Aufnahme der Entscheidungsverkündung nicht im Saal umher bewegen.[80] Für das Umfeld der Verhandlung schlug das BVerfG Vorschriften dieser Art ebenfalls immer wieder vor.[81] Ein fester Standort für Kameras und Kameraleute könnte daher an allen deutschen Gerichten vorgeschrieben werden. Jedenfalls Störungen für den äußeren Verfahrensablauf ließen sich so eliminieren.

6 Fazit

Die moderaten Änderungen, die sich für die Arbeit der Journalisten bei Gericht durch das EMöGG ergeben haben, sind zu begrüßen. Der deutsche Gesetzgeber sollte hierbei allerdings nicht stehenbleiben. Der Umgang der europäischen und internationalen Gerichte, die Journalisten bei ihrer Arbeit allesamt stärker unterstützen, kann ihm Anhaltspunkte dafür liefern, dass und wie die Gerichtsberichterstattung auch in Deutschland künftig weniger streng geregelt werden könnte.

[79] Siehe zum Beispiel die Akkreditierungsbedingungen zur Urteilsverkündung in der Frage „Streikrecht für Beamte“ unter www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2018/bvg18-035.html?cms_layoutVariant=StandardAkkreditierung (abgerufen 12.6.2018).

[80] So seine Akkreditierungsbefindungen, abrufbar unter www.bundesgerichtshof.de/DE/Presse/Akkreditierung/akkreditierung_node.html (abgerufen 12.6.2018).

[81] BVerfG, Beschl. v. 11.11.1992, 1 BvR 1595/92, 1 BvR 1606/92, BVerfGE 87, 334 (340); Beschl. v. 14.7.1994, 1 BvR 1595/92, BVerfGE 91, 125 (138 f.); Beschl. v. 19.12.2007, 1 BvR 620/07, BVerfGE 119, 309 (326).

Literatur

Bamberger, Christian: Medienöffentlichkeit im Lichte der Rundfunkfreiheit, ZUM 2001, S. 373-378.

Baumbach, Adolf/Lauterbach, Wolfgang/Albers, Jan/Hartmann, Peter (Hrsg.): Zivilprozessordnung, 76. Aufl., München 2018.

Bernzen, Anna K.: Keine Angst vor Football-Spielern, oder: Warum die Regeln für die Berichterstattung aus dem Gericht überarbeitet werden müssen, in: Louisa Specht/Anne Lauber-Rönsberg/Maximilian Becker (Hrsg.), Medienrecht im Medienumbruch, Tagungsband der Tagung „Junge Wissenschaft – Kolloquium zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht", Köln 2017, S. 205-224.

Von Coelln, Christian: Mehr Medienöffentlichkeit vor Gericht? Zum Entwurf eines Gesetzes über die Erweiterung der Medienöffentlichkeit in Gerichtsverfahren (EMöGG), AfP 2016, S. 491-495.

Von Coelln, Christian: Justiz und Medien. Rechtliche Anforderungen an das Verhältnis zwischen der Justiz und den Medien, insbesondere an die Berichterstattung über Gerichtsverfahren, AfP 2014, S. 193-202.

Von Coelln, Christian: Zur Medienöffentlichkeit der Dritten Gewalt. Rechtliche Aspekte des Zugangs der Medien zur Rechtsprechung im Verfassungsstaat des Grundgesetzes, Tübingen 2005.

Düwell, Franz Josef: Die Erweiterung der Medienöffentlichkeit in Gerichtsverfahren durch das EMöGG, jurisPR-ArbR 41/2017 Anm. 1.

Franke, Ulrich: Öffentlichkeit im Strafverfahren, NJW 2016, S. 2618-2621.

Geuther, Gudula: Schwierige Lehren, DRiZ 2013, S. 166.

Graf, Jürgen-Peter (Hrsg.): BeckOK StPO mit RiStBV und MiStra, München, Stand: 1.1.2018.

Hirzebruch, Christian: Erweiterung der Medienöffentlichkeit in Gerichtsverfahren, BRJ 2017, S. 5-10.

Hoeren, Thomas: Medienöffentlichkeit im Gericht – die Änderungen des GVG, NJW 2017, S. 3339-3341.

Kissel, Otto Rudolf/Mayer, Herbert (Hrsg.): Gerichtsverfassungsgesetz, 9. Aufl., München 2018.

Koch, Raphael/Wallimann, Matthias: Das Gesetz zur Erweiterung der Medienöffentlichkeit in Gerichtsverfahren, MDR 2018, S. 241-245.

Kreicker, Helmut: Medienübertragungen von Gerichtsverhandlungen im Lichte der EMRK, ZIS 2017, S. 85-105.

Libor, Christine: Kameras im Gerichtssaal? Zur Zulässigkeit verschiedener Formen der Berichterstattung über Gerichtsverfahren. 115. Tagung des Studienkreises für Presserecht und Pressefreiheit e.V. am 9./10.5.2014 in Köln, AfP 2014, S. 224-229.

Maunz, Theodor/Schmidt-Bleibtreu, Bruno/Klein, Franz/Bethge, Herbert (Hrsg.): Bundesverfassungsgerichtsgesetz, München, Stand: September 2017.

Meyer-Goßner, Lutz/Schmitt, Bertram: Strafprozessordnung, 61. Aufl., München 2018.

Mitsch, Wolfgang: Medienpräsenz und Persönlichkeitsschutz in der öffentlichen Hauptverhandlung, ZRP 2014, S. 137-140.

Rath, Christian: Der Laptop des Journalisten im Gerichtssaal, DRiZ 2014, S. 8-9.

Rittig, Steffen: Mehr Medienöffentlichkeit in Gerichtsverfahren? – Zu den Reformüberlegungen zu § 169 GVG, NJ 2016, S. 265-269.

Schlothauer, Reinhold: Strafverfahren und Öffentlichkeit, StV 2015, S. 665-668.

Zöller, Richard (Begr.): ZPO: Zivilprozessordnung, 32. Aufl., Köln 2018.

LOCATION BASED ADVERTISING - EINE ANALYSE AUS DATENSCHUTZ- UND WETTBEWERBSRECHTLICHER SICHT

RAin Kathrin Schürmann

SWD Rechtsanwälte
schuermann@swd-rechtsanwaelte.de

Zusammenfassung

Der Anteil ortsbezogener (Location Based) Services ist in den letzten Jahren rasant angestiegen und wird vor allem vom stationären Handel als wichtiges Marketinginstrument angesehen, um Kunden direkt am Point of Sale anzusprechen. Jeder dritte Smartphone Nutzer teilt seinen Standort mit, um ortsbezogene Dienste zu nutzen. Wo finde ich ein bestimmtes Geschäft, Restaurant oder den nächsten Friseur? Location Based Services ermöglichen eine unmittelbare Antwort auf all diese täglichen Fragen und Bedürfnisse der Nutzer. Genau diese Möglichkeit, den Nutzer über sein persönlichstes Gerät (das Smartphone) jederzeit an seinem Standort anzusprechen und mit relevanten Informationen, Services und Angeboten zu bespielen, macht die Nutzung von Standortdaten für das Marketing von Unternehmen so attraktiv. Seit dem 25. Mai 2018 gilt die EU-Datenschutzgrundverordnung. Mit ihr finden viele Fragen im Zusammenhang mit Online- und Mobile-Werbung und damit auch dem Location Based Advertising eine neue Beantwortung. Das Location Based Advertising, also Werbung unter Nutzung von Angaben über den Standort des Users, stellt dabei eine besonders sensible Art der Werbung dar. Die Standortdaten können – insbesondere in Verbindung mit anderen personenbezogenen Daten - besonders viel zur Bestimmbarkeit, Individualisierung oder Profilbildung des Einzelnen beitragen. Die Verarbeitung von Standortdaten unterliegt daher besonders hohen Hürden und Risiken. Auch das Wettbewerbsrecht kann unter den Aspekten der unzumutbaren Belästigung und der Behinderung von Wettbewerbern zur Hürde für das Location Based Marketing werden. Dieser Beitrag soll einen Überblick über die wichtigsten Anforderungen der DSGVO und des Wettbewerbsrechts in Bezug auf das Location Based Advertising geben.

1 Location Based Advertising

Location Based Marketing ist ein Advertising Konzept, welches auf ortsbezogene Werbung setzt. Hierbei wird der aktuelle Aufenthaltsort eines Smartphone-Nutzers ermittelt, um ihm dann Angebote und Aktionen in der Nähe anzuzeigen. Meist erfolgt dies durch eine entsprechende App, die der Nutzer auf seinem Smartphone installiert hat. Wenn sich der Nutzer dann in einem bestimmten Bereich befindet, können ihm über die App gezielt Angebote in seiner Nähe unterbreitet werden. Zusammenfassend kann somit Location Based Advertising als eine Marketingmethode beschrieben werden, die die Standortinformationen des Users nutzt, um diesen am Point of Sale und Point of Interest mit relevanten Informationen zu versorgen.

Aus technischer Sicht gibt es dabei unterschiedliche Möglichkeiten, wie die Standorte der Nutzer erfasst und in welcher Form Nutzer beispielsweise am Point-of-Sale mit ortsbezogener Werbung angesprochen werden. Bei der direkten Ansprache liegen sicherlich die Push-Nachrichten vorn, bei der Bestimmung des Standortes kommen GPS, Wifi, RFID, NFC, Bluetooth (Beacons) sowie Informationen wie mobile Funkzelle, IP-Adresse und Netzwerkdaten zum Einsatz, je nachdem, wie genau der Standort des Nutzers erfasst werden soll.

Beispiele für den Einsatz von Location Based Marketing sind etwa Geo-Fencing und Tracking. Beim Geo-Fencing werden virtuelle Grenzen („Zäune“) innerhalb eines bestimmten Gebietes gezogen. Überschreitet ein Smartphone Nutzer diese Grenzen, so registriert das System den Ein- und Austritt in den registrierten Bereich und lässt bspw. regionale Angebote in Form von Nachrichten zukommen. Verfügt der Kunde über entsprechende Apps, so kann durch die Kombination mit den Standortdaten ein ganzes Gerüst an Informationen über das Kaufverhalten erstellt werden.

Aber es ist auch eine noch gezieltere Kundenansprache möglich. Beim Tracking der Standortdaten wird von der Zustimmung zur „Nutzung des Standortes“ Gebrauch gemacht, die viele Apps vom Kunden vor der Nutzung einholen. Wird dabei ein ungefähr umrissener Weg zur Arbeit deutlich, so kann das gezielte Versenden von Angeboten über Kaffeespezialitäten in der unmittelbaren Nähe vom Kunden als Mehrwert empfunden werden. Bei all diesen Vorteilen für Werbetreibende sind aber die Grenzen des Datenschutzrechts und Wettbewerbsrechts zu beachten.

2 Das Datenschutzrecht

Voraussetzung für die Anwendbarkeit der DSGVO ist zunächst die Verarbeitung personenbezogener Daten (vgl. Art. 2 Abs. 1 DSGVO).

2.1 Personenbezogene Daten

Liegen „personenbezogene Daten“ vor, ist der sachliche Schutzbereich der Datenschutzgrundverordnung eröffnet. Daten sind „personenbezogen“, wenn sie mindestens eine Information über eine identifizierte Person enthalten, ohne dass die Information selbst die Identifikation herbeiführen muss.[1] Ist die betroffene Person nicht benannt, so genügt eine Identifizierbarkeit der Person. Eine Möglichkeit der Identifizierbarkeit besteht gem. Art. 4 Nr. 1 DSGVO in der Zuordnung zu Standortdaten. Da Identifizierbarkeit genügt, muss durch die Zusammenführung nicht etwa der Name

[1] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 3.

der betroffenen Person bekannt werden.[2] Liegen beispielsweise genügend Standortdaten vor, so kann dies auch allein für die Identifizierbarkeit einer Person genügen.

Die DSGVO nimmt dabei keinen ausdrücklichen Bezug auf das Location Based Advertising. Allerding ist dieses – zumindest bei einer umfassenden Nutzung – eng verbunden mit dem Konzept des Profilings, sodass sich die rechtlichen Anforderungen an das Location Based Advertising auch aus den Anforderungen an das Profiling ergeben. Das Profiling setzt die Bildung von Nutzerprofilen voraus, die viele Informationen enthalten, die zur Identifizierbarkeit einer Person beitragen können. Mittels Standorten können dabei sehr aufschlussreiche Informationen über Wohnort, Arbeitsplatz, regelmäßig zurückgelegte Strecken und Vorlieben erhoben werden, die die Profilbildung erleichtern. Die Anforderungen an das Location Based Advertising sind daher zunächst an den Anforderungen des Profilings zu messen.

2.2 Profiling

Mittels Profiling werden personenbezogene Daten für eine automatisierte Bewertung persönlicher Aspekte einer natürlichen Person genutzt. Bewertet werden kann dabei auch der Aufenthaltsort einer natürlichen Person und ein Ortswechsel.[3] Damit fällt die Nutzung standortbasierter Werbung zunächst unter den Begriff des Profiling und eröffnet dabei die besonderen Anforderungen der DSGVO hieran. Dabei kann jedoch nicht davon ausgegangen werden, dass gem. Art. 22 DSGVO personalisierte, auch standortbezogene, Werbung den Betroffenen „erheblich beeinträchtigt“ und daher verboten ist. Eine solche Folge kann nur dann angenommen werden, wenn die Entscheidung rechtliche oder erhebliche Auswirkungen auf die Persönlichkeitsentfaltung des Einzelnen, etwa auf wirtschaftlicher oder persönlicher Ebene hat.[4] Dies ist in der Regel bei Location Based Advertising nicht der Fall. Art. 22 Abs. 2 DSGVO bestimmt zudem, dass personalisierte Werbung unter den dort genannten Voraussetzungen (Erforderlichkeit für die Erfüllung eines Vertrages, gesetzliche Erlaubnis, Einwilligung) zulässig ist. Die Zulässigkeit für standortbasierte Werbung richtet sich damit nach den allgemeinen Rechtmäßigkeitsanforderungen für Datenverarbeitungen nach der DSGVO.

2.3 Rechtmäßigkeit der Datenverarbeitung nach der DSGVO

Die Eröffnung des Anwendungsbereiches der DSGVO führt grundsätzlich dazu, dass die Verarbeitung personenbezogener Daten verboten ist, jedoch

---

[2] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 34; *Ernst*, in: Paal/Pauly, DS-GVO, Art. 4 Rn. 40-47.

[3] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 34.

[4] *Martini*, in: Paal/Pauly, DS-GVO, Art. 22 Rn. 26.

durch bestimmte Erlaubnistatbestände rechtmäßig werden kann (sog. Verbot mit Erlaubnisvorbehalt). Die wichtigsten Erlaubnistatbestände enthält dabei Art. 6 Abs. 1 DSGVO. Hervorzuheben sind dabei vor allem die Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO und die Interessenabwägung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO. Neben Einwilligung und Interessenabwägung kommen gem. Art. 6 Abs. 1 S. 1 lit. c DSGVO auch gesetzliche Regelungen als Erlaubnistatbestände für Datenverarbeitungen in Betracht, sowie die Erforderlichkeit der Datenverarbeitung für die Durchführung eines Vertrages gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO.

Die Einwilligung erfordert eine „eindeutig bestätigende Handlung" als vorherige Zustimmung in die Datenverarbeitung durch den Betroffenen.[5] Gem. der Transparenz- und Informationsvorschriften der DSGVO muss es sich dabei um eine „informierte Einwilligung" handeln (vgl. Art. 4 Nr. 11 DSGVO). Das heißt, dass der Betroffene in einer „leicht verständlichen Sprache" verstehen muss, in was er einwilligt. Darüber hinaus muss über den Verantwortlichen, den Zweck und die Dauer der Datenverarbeitung sowie über seine Betroffenenrechte, vor allem sein Widerrufsrecht, aufgeklärt werden (vgl. Art. 12 und 13 DSGVO).[6] Die Einholung der Einwilligung darf dabei nicht unfreiwillig erfolgen (vgl. Art. 7 Abs. 4 DSGVO). Bezüglich der Form der Einwilligung genügt eine unmissverständliche Handlung. Diese kann mündlich, schriftlich oder elektronisch erfolgen. Auch ein Mausklick kann damit ausreichend sein.[7] Willigt der Betroffene in standortbasierte Werbung ein, so ist die Datenverarbeitung nur dann zulässig, wenn die Einwilligungserklärung diese Anforderungen erfüllt. Zahlreiche Apps (wie Wetter-Apps oder Karten-Apps) verlangen vor Beginn der Nutzung der App die Einwilligung in die Nutzung von Standortdaten. Werden solche Daten für Werbezwecke genutzt, ist insbesondere auf die transparente Kommunikation dieses Zusammenhangs zu achten.

Die Interessenabwägung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO verlangt, dass die Rechte und Interessen der betroffenen Personen mit den Interessen des Unternehmens abgewogen werden müssen. Die DSGVO erkennt dabei die Direktwerbung ausdrücklich als berechtigtes Unternehmensinteresse an (vgl. Erwägungsgrund 47 der DSGVO). Dabei verlangt Art. 6 Abs. 1 S. 1 lit. f DSGVO, dass die Verarbeitung für die Wahrung der Interessen des werbenden Unternehmens erforderlich ist. An die Erforderlichkeit sind jedoch keine strengen Maßstäbe im Sinne echter Verhältnismä-

[5] *Frenzel*, in: Paal/Pauly, DS-GVO, Art. 6 Rn. 11.

[6] *Paal/Hennemann*, in: Paal/Pauly, DS-GVO, Art. 12 Rn. 33-35; *Paal/Hennemann*, in: Paal/Pauly, DS-GVO, Art. 13 Rn. 1.

[7] *Albers/Veit*, BeckOK DatenschutzR, Stand 1.5.2018, DS-GVO, Art. 6 Rn. 24.

ßigkeit zu stellen. Es genügt, wenn das Erforderlichkeitskriterium als Ausgangspunkt für die Abwägung der Rechte und Interessen der Beteiligten herangezogen werden kann.[8] Dabei ist für standortbasierte Werbung einerseits deren hohe Effizienz, andererseits aber der besonders sensible Charakter von Standortdaten zu berücksichtigen. Um die Abwägung im Sinne der Unternehmen zu gestalten, müssen diese bestimmte Maßnahmen ergreifen, um die Rechte und Interessen der betroffenen Personen zu schützen. Die wichtigste Voraussetzung ist dabei die Pseudonymisierung der Daten.

Werden Standortdaten zu Werbezwecken verwendet, ist nach der Art ihrer Verwendung zu differenzieren. Danach richtet sich welcher Erlaubnistatbestand der DSGVO greift. Sind Standortdaten zur Durchführung eines Vertrages erforderlich (bspw. Navigations-App oder Lauftracker) so genügt gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO, dass die betroffene Person Vertragspartei dieses Vertrages ist. Dagegen ist eine Einwilligung erforderlich, wenn der Vertragszweck auch ohne den aktuellen Standort des Betroffenen erfüllt werden kann (z.B. bei einer Wetter-App, da auch davon ausgegangen werden kann, dass der Betroffene selbst den Ort aus einer Liste auswählt, an dem er sich befindet, ohne dass die App diesen Ort automatisch finden muss). Liegt weder eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO noch die Erforderlichkeit für eine Vertragsdurchführung gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO vor, ist eine Interessenabwägung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO wie oben beschrieben notwendig.

2.4 Pseudonymisierung

Besteht die Erforderlichkeit einer solchen Interessenabwägung, sollten Verantwortliche unbedingt auf die Einhaltung der Grundsätze der Pseudonymisierung achten, um die Interessenabwägung zu ihren Gunsten zu beeinflussen. Gem. Art. 4 Nr. 5 DSGVO handelt es sich bei der Pseudonymisierung von Daten um die Verarbeitung von personenbezogenen Daten in einer Weise, die die Zuordnung zu einer identifizierbaren Person ohne Hinzuziehung zusätzlicher Informationen nicht mehr ermöglicht. Damit es nicht zu einer Zuordnung zur Identität der betroffenen Person kommt, müssen die (weiteren) Daten, die eine solche Zuordnung ermöglichen, gesondert aufbewahrt werden. Besondere technische und organisatorische Maßnahmen müssen die Zusammenführung mit anderen Daten verhindern, um die Zuweisung zu einer Person zu vermeiden.[9] Kann unter Berücksichtigung aller dem Verantwortlichen oder einer anderen Person zur

[8] *Albers/Veit*, BeckOK DatenschutzR, Stand 1.5.2018, DS-GVO, Art. 6 Rn. 24.

[9] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 36.

Verfügung stehenden Mittel davon ausgegangen werden, dass eine Identifikation der Person wahrscheinlich erfolgen kann, handelt es sich um den Tatbestand der Pseudonymisierung, der Personenbezug bleibt erhalten und die DSGVO bleibt anwendbar.[10] Wird der Personenbezug etwa durch Löschung der Identifikationsmerkmale dagegen aufgehoben, liegt der Tatbestand der Anonymisierung vor und die DSGVO ist nicht mehr anwendbar.[11]

Im Falle der Verarbeitung von Standortdaten für Zwecke des Location Based Advertising ist die Pseudonymisierung deshalb von großer Bedeutung, weil im Falle einer Interessenabwägung die berechtigten Unternehmensinteressen dem Interesse des Einzelnen am Schutz besonders wichtiger Daten gegenüberstehen. Ohne Pseudonymisierung könnte ein Überwiegen der Unternehmensinteressen gegenüber dem Schutz vor Bekanntwerden der eigenen Standortdaten kaum gerechtfertigt werden.

Neben der Pseudonymisierung ist durch weitere Vorsichtsmaßnahmen, gegebenenfalls auch in den technischen Voreinstellungen (Privacy by Design), darauf zu achten, dass die mittels Standortdaten erhobenen Daten eine gewisse Unschärfe aufweisen und keine Zusammenführung mit besonders sensiblen Informationen ermöglichen. So dürfen etwa keine Bewegungsprofile erstellt werden oder Daten erhoben werden, die Rückschlüsse auf bestimmte Krankheiten (Arztpraxen) oder Glaubenszugehörigkeiten (Kirchen) ermöglichen.

Werden Signale demnach um ein Haus gestreut und wird auf diese Weise der Standort einer Person eingegrenzt und für interessenbasierte Werbung genutzt, so kann wegen der gewahrten Unschärfe grundsätzlich von einem Überwiegen der Unternehmensinteressen gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO ausgegangen werden. Kommt es dagegen umgekehrt zu einer Zusammenführung dieser Standortdaten mit anderen Daten, die eine Individualisierung des Einzelnen ermöglichen, so überwiegen die Interessen des Betroffenen und die Interessenabwägung fällt zu seinen Gunsten aus. Standortbasierte Werbung auf dieser Grundlage wäre dann ein Verstoß gegen die DSGVO. Erforderlich wäre eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO.

2.5 Neueste Entwicklungen

Allerdings ist aktuell fraglich, ob standortbasierte Werbung in Deutschland überhaupt auf eine Interessenabwägung im Sinne des Art. 6 Abs. 1 S. 1 lit. f

[10] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 39.

[11] *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 39 f.

DSGVO gestützt werden kann oder ob immer eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO notwendig ist.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichten am 25.4.2018 eine Stellungnahme, in der im Zusammenhang mit der Nutzung von Cookies erklärt wurde, dass beim Einsatz von Tracking-Mechanismen im Internet in jedem Fall eine informierte Einwilligung des Nutzers eingeholt werden muss.[12] Dies kann generell auch auf den Einsatz von Technologien zur Standortbestimmung übertragen werden.

Gegen die Auslegung des DSK spricht, dass die DSGVO in Erwägungsgrund 47 und in Artikel 21 die Direktwerbung als berechtigtes Interesse ausdrücklich anerkennt und damit nahelegt, dass sie zum Gegenstand einer Interessenabwägung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO gemacht werden kann. Die unbedingte Erforderlichkeit einer Einwilligung für Tracking- und Profiling-Maßnahmen würde dieser gesetzgeberischen Wertung widersprechen. Für eine sachgerechte Differenzierung sind wohl auf die Art der Trackingmaßnahme und die berechtigten Erwartungen der betroffenen Personen abzustellen.

Kann dieser vernünftigerweise mit dem Tracking rechnen, so genügt eine Interessenabwägung. Geht die Art und Weise des Trackings jedoch über die berechtigten Erwartungen hinaus, so ist eine Einwilligung erforderlich. Ähnlich argumentiert die Gesellschaft für Datenschutz und Datensicherheit e.V.[13] Letzteres dürfte insbesondere bei Zusammenführung der Standortdaten mit anderen Daten der Fall sein, die eine Individualisierung ermöglichen, da ein solch erheblicher Eingriff in die Privatsphäre des Einzelnen nicht mehr erwartet werden kann und von seiner Einwilligung abgedeckt sein muss.

Für das Jahr 2019 wird mit dem Inkrafttreten der ePrivacy-Verordnung gerechnet. Diese soll als lex specialis den Datenschutz für Fälle der elektronischen Kommunikation regeln.[14] Da auch diese Verordnung die Verarbeitung von Standortdaten regelt, kann es in Zukunft zu Rechtsunsicherheit kommen. Standortdaten könnten dann jeweils einer unterschiedlichen

---

[12] Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf.

[13] Zulässigkeit des Trackings nach der DSGVO – Die GDD bezieht Stellung zur Position der Datenschutzkonferenz, abrufbar unter: https://www.gdd.de/aktuelles/startseite/zulaessigkeit-des-tracking-nach-der-ds-gvo.

[14] *Selmayr/Ehmann*, in: Ehmann/Selmayr, DS-GVO, Einführung Rn. 109.

Behandlung unterliegen, abhängig davon, ob sie im Rahmen elektronischer Kommunikation oder anderweitig verarbeitet werden.

3 Location Based Advertising und Wettbewerbsrecht

3.1 Unzumutbare Belästigung

Bei standortbasierter Werbung sind nicht nur die Anforderungen des Datenschutzrechts, sondern auch diejenigen des Wettbewerbsrechts zu beachten.

Werden Push-Mitteilungen versendet, wie es bei Benutzung vieler Apps üblich ist, die auf Standortdaten zurückgreifen, sind die Push-Mitteilungen wie elektronische Post (E-Mails) gem. § 7 Abs. 2 Nr. 3 UWG zu behandeln. Gem. Art. 2 S. 2 lit. h der ePrivacy-Richtlinie (Richtlinie für elektronische Kommunikation 2002/58/EG) ist elektronische Post jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton – oder Bildnachricht, die im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird. Im Unterschied zu E-Mails und SMS lassen sich Push-Nachrichten grundsätzlich nicht ohne weiteres zurückstellen um später gelesen zu werden. Vielmehr ist primärer Erscheinungsort der Home-Screen des Nutzers, der Schwerpunkt liegt auf einem Moment der Überraschung. Trotz dieser teleologischen Bedenken spricht aber eine funktionale Betrachtung für die Gleichbehandlung von Push-Nachrichten mit E-Mails und SMS. Denn Push-Nachrichten werden über das Internet versandt und auf einem Empfangsgerät oder Server derart gespeichert, dass sie zu einem späteren Zeitpunkt eingesehen und gelesen werden können.[15] Demgemäß sind werbliche Push-Nachrichten gem. § 7 Abs. 2 Nr. 3 UWG nur dann zulässig, wenn der Nutzer vorher eingewilligt hat. Die Einwilligung muss dabei ausdrücklich erfolgen, freiwillig sein und auf der Grundlage ausreichender Informationen über den Werbenden und den Zweck der Werbung erfolgen. Sie muss sich auf den konkreten Fall beziehen und in vollständiger Kenntnis der Sachlage erfolgen. Ein Durchschnittsverbraucher muss erkennen, dass er sein Einverständnis in den Empfang (standortbasierter) Push-Mitteilungen gibt.[16] Bei der Verwendung vieler Apps werden diese Anforderungen oftmals nicht erfüllt. Vielmehr liegen standardisierte Texte vor, die nicht klar erkennen lassen, dass eine Einwilligung für den Versand von standortbasierten werblichen Push-Mitteilungen eingeholt wird. Hier ist eine Anpassung, v.a. in App-Stores und Betriebssystemen von Smartpho-

[15] *Schürmann/Günther*, Werbung über mobile Push-Dienste als unzumutbare Belästigung? Wettbewerbsrechtliche Einordnung von Push-Nachrichten, MMR 2015, S. 419.

[16] *Köhler*, in: Köhler/Bornkamm/Feddersen, UWG, § 7 Rn. 149h.

nes, erforderlich. Für Unternehmen heißt es aufgrund der technischen Gegebenheiten derzeit noch häufig einen Work-Around, bspw. durch Info-Screens zu nutzen, um überhaupt die Möglichkeit zu haben, die rechtlichen Anforderungen zu erfüllen.

3.2 Behinderung von Mitbewerbern

Zudem kann bei standortbasierter Werbung das Verbot des § 4 Nr. 4 UWG betroffen sein, wenn die Werbung direkten Bezug zu Mitbewerbern aufweist. § 4 Nr. 4 UWG verbietet eine Behinderung von Mitbewerbern. Im Falle von Werbung ist dies vor allem dann der Fall, wenn sie nur den Zweck hat den Mitbewerber in seiner wettbewerblichen Entfaltung zu hindern.[17] Im Internet ist eine solche unlautere Behinderung dann anzunehmen, wenn durch Störmaßnahmen der Zugang zu einer Website des Mitbewerbers vereitelt, erschwert oder verzögert wird.[18] Vergleicht man dies mit standortbasierter Werbung so darf jedenfalls durch Push-Mitteilungen nicht die Speicherkapazität des Nutzers derart beansprucht werden, dass Mitbewerber keine Möglichkeit auf Versenden eigener Push-Nachrichten erhalten (z.B. durch Spamming). Zugleich darf Werbung nicht von einer Intensität sein, dass die Verbreitung oder Rezeption von Werbung des Mitbewerbers verhindert wird. Dies ist bspw. der Fall, wenn der Kunde vor dem Eingang des Konkurrenten durch direkte Ansprache derart abgefangen wird, dass er die Werbung und Angebote des Kontrahenten nicht mehr wahrnehmen kann.[19] Grenzwertig sind daher die Fälle, bei denen ein Kunde im Ladengeschäft eines Konkurrenten per standortbasierter Push-Mitteilung angesprochen wird, um ihn mit Angeboten in das eigene Geschäft zu locken. Dagegen muss ein Wettbewerber es hinnehmen, dass die Werbung eines Mitbewerbers die eigene Werbung beeinträchtigt, etwa weil sie im selben räumlichen Umfeld stattfindet (Geo-Fencing).[20] Demgemäß darf auch standortbasierte Werbung dazu dienen mittels Push-Mitteilungen die Aufmerksamkeit von Angeboten von Mitbewerbern im lokalen Umfeld abzulenken, solange darin keine gezielte Behinderung von Mitbewerbern liegt.

4 Fazit

Wollen Unternehmen sich absichern, so sollten sie sowohl aus datenschutzrechtlicher als auch aus wettbewerbsrechtlicher Sicht die Einwilligung des Kunden für den Fall standortbasierter Werbung einholen. Diese muss in jedem Fall auf der Grundlage transparenter Information über den

[17] *Köhler*, in: Köhler/Bornkamm, UWG, § 4 Rn. 4.71.

[18] *Köhler*, in: Köhler/Bornkamm, UWG, § 4 Rn. 4.73.

[19] *Omsels*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 4 Rn. 76.

[20] *Omsels*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 4 Rn. 69.

Zeck der Einwilligung und freiwillig erfolgen. In Zukunft gilt es für die Rechtsprechung die genauen Anforderungen an die Rechtmäßigkeit von Location Based Marketing zu klären. Insbesondere das Verhältnis von Location Based Marketing und Profiling sollte von der Rechtsprechung festgelegt werden. Zudem ist eine klare Entscheidungslinie bezüglich der Erforderlichkeit von Einwilligungen im Zusammenhang mit Location Based Advertising und auch übrigen Tracking-Technologien erforderlich. Die Stellungnahme der Datenschutzkonferenz ist in der Praxis nicht zu Unrecht auf Unverständnis gestoßen. Auch das Verhältnis von (geplanter) ePrivacy-Verordnung und DSGVO bezüglich der Verarbeitung von Standortdaten muss geklärt werden. Die ungleiche Behandlung derselben Daten stellt eine nicht tragbare Rechtsunsicherheit dar.

Insgesamt sollte bei der Nutzung von Location Based Marketing ein gesundes Mittelmaß gewahrt werden. Aus Sicht der Nutzer kann der Mehrwert durch standortspezifische Angebote schnell verloren gehen, wenn der Kunde sich „verfolgt“ fühlt. Die Grenzen des Wettbewerbsrechts über unzumutbare Belästigung sollten daher als Richtschnur für den verhältnismäßigen Einsatz von Location Based Marketing dienen.

Literatur

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.): BeckOK Datenschutzrecht, 24. Ed., Stand 1.5.2018, München 2018.

Ehmann, Eugen/Sehlmayr, Martin: DS-GVO Kommentar, München 2017.

Gola, Peter (Hrsg.): DS-GVO Kommentar, München 2017.

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke: Gesetz gegen den unlauteren Wettbewerb, 4. Aufl., München 2016.

Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn: Gesetz gegen den unlauteren Wettbewerb, 36. Aufl., München 2018.

Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutzgrundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Schürmann, Kathrin/Günther, Lucas: Werbung über mobile Push-Dienste als unzumutbare Belästigung? Wettbewerbsrechtliche Einordnung von Push-Nachrichten, MMR 2015, S. 419-423.

WERBUNG AUF ONLINE-PLATTFORMEN: INFLUENCER MARKETING

Hans-Christian Gräfe

Ruhr-Universität Bochum

Zusammenfassung

Der Beitrag soll eine überblicksartige Darstellung der rechtlichen Bewertung des sog. Influencer Marketing geben. Dabei stehen die Fragen im Vordergrund, woher die Verpflichtung zur Trennung von Inhalt und Werbung bzw. zur Kennzeichnung von Werbung kommt (2.) und welche Probleme sich für werbende Beiträge von Bloggern daraus ergeben (3.). Abschließend wird auf die Frage eingegangen, ob sich aus der Diskussion um das Influencer Marketing im Hinblick auf die zunehmende Medienkonvergenz mehr ziehen lässt als eine bloße Anleitung zur Vermeidung von Schleichwerbung (4.).

1 Der Hype um Influencer im Marketing

Influencer Marketing ist derzeit ein hochgejubelter Begriff unter Werbefachleuten. Kaum eine Marketingkonferenz kommt ohne Beiträge zu dem Thema aus. Die Idee dahinter ist, dass bekannte Blogger mit ihrer Reichweite auf Online-Plattformen Produkte oder Dienstleistungen eines Unternehmens anpreisen. Es handelt sich also um eine Spielart des Online-Marketings. Die Besonderheit dabei ist, dass durch Analyse der Follower der Blogger bestimmte Zielgruppen ganz direkt erreicht werden können und die Blogger je nach ihrem bestimmten Themenfeld bei den Followern eine besondere Vertrauenswürdigkeit besitzen. Deshalb wird ihnen zugetraut, ihre Follower durch Empfehlungen beeinflussen zu können, das macht sie zu sog. Influencern.

Dass Unternehmen in ihren Marketingstrategien auf Influencer zurückgreifen, hat vor allem zwei Gründe: Den mit dem Medienwandel einhergehenden Wandel des Medienkonsums und der (wohl) nachgewiesenen Wirksamkeit von Influencer Werbung. Die Ziele, die die Unternehmen verfolgen, sind die klassischen Ziele des Marketings: Abverkauf, Steigerung der Bekanntheit oder die Verbesserung des Images einer Marke.

1.1 Wandel des Medienkonsums

Die Medienlandschaft hat sich den letzten 15 Jahren verändert. Neben die klassischen Medien Presse, Radio und Fernsehen ist das Internet getreten. Dies sorgte zunächst dafür, dass Presse und Rundfunk Konkurrenz durch neue Inhalteanbieter bekamen. Anfangs hat das die klassischen Medien aber nicht dazu veranlasst, ihr Geschäft ins Internet auszubreiten. Erst als

die Anzeigenverkäufe und Werbeeinahmen dorthin abwanderten und die Abonnements zurückgingen, begann ein flächendeckendes Umdenken. Inzwischen stellen Rundfunk und Presse ihre Angebote durchgängig auch online zur Verfügung. Das für die Medienfinanzierung größte Problem stellen aus Sicht der Medienhäuser dort inzwischen sog. AdBlocker dar.[1]

Viele Medienkonsumenten beziehen Inhalte inzwischen aber nicht mehr direkt über die Online-Angebote der Medienanbieter, sondern nutzen Informationsvermittler wie die sozialen Netzwerke. Dort können sie sich ihren eigenen Newsfeed aus klassischen Medienangeboten, Uploads von Freunden und Bekannten und den Beiträgen von Bloggern zusammenstellen. Das enorme Potential sozialer Netzwerke als Werbeplattform haben daher auch die Unternehmen erkannt.

1.2 Wahrnehmung und Wirkung

Dass sich die Medienkonsumenten nicht mehr ausschließlich über Presse und Rundfunk mit Inhalten versorgen, sondern multimediale Angebote und vor allem die Online-Plattformen nutzen, ist an sich aber noch nicht der ausschlaggebende Grund für die Bedeutung des Influencer Marketings. Die Unternehmen können – trotz Adblockern – direkt auf den Plattformen Werbung schalten und so eine große Anzahl von Konsumenten erreichen. Der Grund, dass 2/3 der online werbenden Unternehmen auf Influencer zurückgreifen,[2] liegt in deren starker Präsenz bei den höchstumworbenen Zielgruppen und dem besonderen Vertrauen,[3] das die Zielgruppe wohl in die Influencer hat. Ihnen wird eine besondere Expertise und damit Glaubwürdigkeit in bestimmten Themengebieten zugestanden, sodass die Empfehlung eines Influencers den Absatz erhöhen kann. Meistens handelt es sich dabei um die Themengebiete Ernährung und Fitness, Mode und Beauty, Gaming, Technik oder Reisen. Unternehmen nutzen die Influencer aber auch beim Marketing für einfache Alltagsprodukte wie Waschmittel.

---

[1] Eine Übersicht über den unendlichen Rechtsstreit findet sich unter https://www.telemedicus.info/tag/Adblock+Plus.

[2] Statista: 2/3 der befragten Unternehmen hatten 2017 ein Budget für Influencer-Marketing vorgesehen, abrufbar unter https://de.statista.com/statistik/daten/studie/686090/umfrage/geplante-investitionen-in-influencer-marketing/.

[3] Studie im Auftrag von BVDW und INFLURY, Bedeutung von Influencer Marketing in Deutschland 2017: 68 % deutscher Online-User sind über Social Media auf ein Produkt aufmerksam geworden; 15 % davon über Influencer; abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/studien/171128_IM-Studie_final-draft-bvdw_low.pdf.

Die hohen Budgets der Werbeindustrie machen sich wiederum bei Qualität und Quantität der Influencer Beiträge bemerkbar.[4] Längst gibt es eigene Influencer Awards[5] und Blogger, die sich hauptsächlich damit beschäftigen, wie es ist als Influencer zu arbeiten und zu leben.[6] Da eine derartige Karriere augenscheinlich sehr attraktiv zu sein scheint, stellt sich für viele junge Blogger die Frage: Wie werde ich Influencer? Auch dazu gibt es inzwischen jede Menge mehr oder weniger seriöse Beiträge und Webseiten, die auflisten, ab welcher Followerzahl bei welchem Netzwerk mit welchem Preis für ein bezahltes Posting geplant werden kann.[7] Das Sonderproblem, ob und ab wann Eigenwerbung auf dem Weg zum Influencer selbst wieder werbe- und wettbewerbsrechtliche Probleme aufwirft, soll hier nur am Rande behandelt werden.[8] Im Folgenden soll es darum gehen, wie Werbung in Form von Influencer Beiträgen rechtlich korrekt gestaltet sein muss.

2 Wann muss gekennzeichnet werden?

Der Grundsatz im Medienrecht lautet, dass Werbung vom redaktionellen Teil sichtbar getrennt sein muss. Eine gesonderte Kennzeichnung zur Verdeutlichung der Trennung muss immer dann erfolgen, wenn ein Medium sowohl einen (redaktionell gestalteten) Inhaltsteil als auch Werbung bzw. kommerzielle Kommunikation enthält. Seine Grundlage findet das sog. Trennungsgebot in der Informationsfreiheit des Art. 5 Abs. 1 S. 1 GG. Die Informationsfreiheit wird als Grundvoraussetzung für eine demokratische Willensbildung angesehen. Damit die Bürger sich ihre politische Meinung frei bilden können, müssen sie (objektive) Informationen des Inhaltsteiles von subjektiven Aussagen werbungstreibender Unternehmen unterscheiden können. Es soll die Medien vor einer zu großen Einflussnahme der werbenden Unternehmen auf die Berichterstattung schützen und so deren publizistische Glaubwürdigkeit erhalten. Denn die privaten Medien genießen die sog. Tendenzfreiheit der Berichterstattung, dürfen also ihre Inhalte aus einer gewissen (politischen) Perspektive präsentieren, und auch das Schal-

---

4 Der Jahresumsatz der Bloggerin Caro Daur soll 1.000.000€ betragen; *Henning-Bodewig*, WRP 2017, S. 1415 mit Verweis auf http://www.manager-magazin.de/unternehmen/karriere/caro-daur-die-instagram-influencerin-im-interview-a-1155194.html.

5 "Place to B Influencer Award" der „BILD"; vgl. https://www.wuv.de/medien/place_to_b_influencer_award_bild_adelt_social_media_stars.

6 Z.B. https://www.blogger-bazaar.com.

7 https://www.influencerdb.net/.

8 Dazu aber *Borsch*, MMR 2018, S. 127 f.

ten von Werbung und die Werbung selbst ist in den Schutzbereich der Medienfreiheit[9] des Art. 5 Abs. 1 S. 2 GG einbezogen und damit von der Tendenzfreiheit umfasst. Dies könnte dazu führen, dass der Einfluss bestimmter Werbender auf den Inhalt zu groß wird, was das Trennungsgebot verhindern soll. Schleichwerbung zu verhindern ist also das Wesen des Trennungsgebots.[10]

2.1 Einfachgesetzlicher Ansatz im Medienrecht

Der Trennungsgrundsatz gilt für alle klassischen Medien und findet seine Ausprägung in den jeweiligen Spezialgesetzen.

2.1.1 Trennungsgrundsatz im Presserecht

Presserecht ist Landesrecht. Das Trennungsgebot ist in den jeweiligen Pressegesetzen allerdings identisch geregelt, z.B. in § 10 PresseG NRW. Danach hat der Verleger eines periodischen Druckwerks oder der Verantwortliche i.S.d. Presserechts eine Veröffentlichung, für die er ein Entgelt erhalten, gefordert oder sich versprechen lassen hat, soweit sie nicht schon durch Anordnung und Gestaltung allgemein als Anzeige zu erkennen ist, deutlich mit dem Wort „Anzeige" zu bezeichnen.

Ergänzend kommt noch die Selbstverpflichtung der meisten Presseunternehmen aus dem Pressekodex in Betracht. Ziffer 7 des Pressekodex legt fest: *„Die Verantwortung der Presse gegenüber der Öffentlichkeit gebietet, dass redaktionelle Veröffentlichungen nicht durch private oder geschäftliche Interessen Dritter oder durch persönliche wirtschaftliche Interessen der Journalistinnen und Journalisten beeinflusst werden. Verleger und Redakteure wehren derartige Versuche ab und achten auf eine klare Trennung zwischen redaktionellem Text und Veröffentlichungen zu werblichen Zwecken. Bei Veröffentlichungen, die ein Eigeninteresse des Verlages betreffen, muss dieses erkennbar sein."*

Für die Presse ist weithin anerkannt, dass Werbung einerseits vom redaktionellen Teil getrennt und als solche gekennzeichnet sein muss. Zumeist sind Zeitungsanzeigen daher durch grafische Elemente wie Kästen oder Ordnungslinien vom redaktionellen Teil abgegrenzt und zusätzlich als „Werbung" oder „Anzeige" gekennzeichnet. Mit dem Problem eines sog. Advertorials, also der redaktionellen Aufmachung einer Werbeanzeige, hat sich der BGH in seinem Urt. vom 6. Februar 2014[11] beschäftigt. Das strikte

---

[9] Gerade in den sozialen Netzwerken, die für das Influencer Marketing erst die Grundlage bilden, zeigt sich die zunehmende Medienkonvergenz. Daher spricht viel dafür, stärker von einem einheitlichen Mediengrundrecht auszugehen, als die Freiheit des Rundfunks, der Presse und des Filmes aus Art. 5 Abs. 1. S 2 GG jeweils gesondert zu betrachten; ähnlich auch *Fechner*, Medienrecht, 12. Kap. Rn. 8; *Sporn*, Beihefter 2 zu K&R 2013, S. 1 (8).

[10] *Paschke/Berlit/Meyer*, Medienrecht, 22. Abschn. Rn. 3, m.V.a. BVerfG, NJW 2005, 3201 f.

[11] BGH, Urt. v. 6.2.2014 – I ZR 2/11 – GOOD NEWS II.

Gebot der Kenntlichmachung von Werbung werde verletzt, wenn unter dem Deckmantel eines redaktionellen Artikels Wirtschaftswerbung betrieben und der präzise Begriff „Anzeige" vermieden werde. Es käme nicht darauf an, ob die in Rede stehenden Teile tatsächlich redaktionell recherchiert und gestaltet worden seien, sondern dass der Verlag für die Veröffentlichung ein Entgelt erhalten habe.

2.1.2 Trennungsgrundsatz im Rundfunkrecht

Rundfunkrecht ist ebenfalls Landesrecht. Doch auch in diesem Bereich gelten die einheitlichen Reglungen des Rundfunkstaatsvertrages (RStV). Im 13. Rundfunkänderungsstaatsvertrag (RÄStV) haben die Länder die europarechtlichen Vorgaben der Richtlinie 2010/13/EU (AVMD-RL 2010) umgesetzt. Seitdem ist durch die Einführung sog. Produktplatzierung eine Kombination von Werbung und Programm in gewissem Maße zulässig.[12] Nichtsdestotrotz normiert § 7 Abs. 3 RStV für alle sonstigen Fälle eindeutig eine Trennung von Inhalt und Werbung und deren Kennzeichnung: *„Werbung und Teleshopping müssen als solche klar erkennbar sein. Sie müssen im Fernsehen durch optische Mittel, im Hörfunk durch akustische Mittel eindeutig von anderen Programmteilen getrennt sein. In der Werbung und im Teleshopping dürfen keine unterschwelligen Techniken eingesetzt werden."* Zumeist wird das Trennungsgebot im Fernsehen und Radio durch sog. Werbetrenner umgesetzt. Das sind akustische oder grafisch Signale, die zwischen Werbung und Programm gesetzt werden. Prominentestes Beispiel sind die Mainzelmännchen des ZDF. Im Radio erscheint oftmals ein kurzer Jingle oder einfach die Ansage „Werbung" oder „Reklame". Auch der sog. split screen setzt Trennung und Kennzeichnung im Fernsehen derart um, dass um das Programm ein optisch abgegrenzter Rahmen oder Balken gelegt wird, innerhalb dessen die Werbung erfolgt. Im Balken selbst steht das Wort Werbung.

Das Ziel der Neureglung zur Einführung von Produktplatzierung stellt Erwägungsgrund 81 zur AVMD RL 2010 klar: „Der Trennungsgrundsatz sollte auf Fernsehwerbung und Teleshopping beschränkt werden und die Produktplatzierung sollte unter bestimmten Voraussetzungen erlaubt werden – sofern ein Mitgliedstaat nicht etwas anderes beschließt. Produktplatzierung, die den Charakter von Schleichwerbung hat, sollte jedoch verboten bleiben. Der Einsatz neuer Werbetechniken sollte durch den Trennungsgrundsatz nicht ausgeschlossen werden." Das bedeutet im Ergebnis, dass zwar an der Trennung grundsätzlich festgehalten werden, aber bei Produktplatzierung tatsächlich eine Abkehr vom strikten Trennungsgrundsatz möglich sein soll. Für weitere Verwirrung mag der Nachsatz zum Einsatz

[12] Zur Umsetzung vgl. *Holzgraefe*, MMR 2011, S. 221 (221).

neuer Werbetechniken sorgen, der als Türöffner für eine Abwendung vom strikten Trennungsgrundsatz missverstanden werden kann.

2.1.3 Trennungsgrundsatz im Telemedienrecht

Telemedien – also Webseiten oder Teile davon – sind primär im Telemediengesetz (TMG) geregelt. § 6 Abs. 1 Nr. 1 TMG, der Art. 6 der Richtlinie 2003/31/EG (E-Commerce-RL) umsetzt, normiert, dass kommerzielle Kommunikation auf einer Webseite klar als solche zu erkennen sein muss. Das Telemediengesetz wird durch landesrechtliche Bestimmungen über den Inhalt von Telemedien ergänzt.[13] Vorschriften über Werbung, Sponsoring und fernsehähnliche Telemedien finden sich in § 58 RStV. Nach der allgemeinen Regelung des § 58 Abs. 1 RStV muss Werbung als solche klar erkennbar und vom übrigen Inhalt der Angebote eindeutig getrennt sein. § 58 Abs. 3 i.V.m. §§ 7, 8 RStV befasst sich hingegen speziell mit audiovisuellen Mediendiensten auf Abruf (sog. Video on demand). Für sie sollen die gleichen werberechtlichen Regeln gelten wie für den Rundfunk. Das heißt im Ergebnis, dass für Video on demand die gleiche flexiblere Handhabung der Trennung gelten soll wie inzwischen für das Fernsehen. Erklärbar ist dies damit, dass bei der Einführung der Regelung an die Mediatheken der Rundfunkanstalten gedacht wurde[14] – zunächst nicht an die sich heute bei dem Begriff Video on demand wohl eher aufdrängenden Videoplattformen wie YouTube, Vimeo etc.

Festzuhalten ist, dass das TMG eine Kennzeichnung von kommerzieller Kommunikation normiert, wohingegen der für Telemedien einschlägige sechste Abschnitt des RStV grds. eine Trennung von Inhalt und Werbung vorsieht.

2.1.4 Begrifflichkeiten

In den bisher dargestellten Normen fallen leichte Unterschiede in den Begrifflichkeiten auf. So wird teilweise von Trennung, teilweise von Kennzeichnung oder klarer Erkennbarkeit gesprochen.[15] Auch wird zwischen Werbung und kommerzieller Kommunikation unterschieden. Da eine genaue Unterscheidung der Begrifflichkeiten im Folgenden noch eine Rolle spielen wird, lohnt ein Blick auf die vorhandenen Legaldefinitionen:

---

[13] *Fechner*, Medienrecht, 12. Kap. Rn. 70.

[14] Vgl. Erwägungsrund 27 zur Richtlinie 2010/13/EU (AVMD RL 2010).

[15] § 10 PresseG: Erkennbarkeit und Bezeichnung als „Anzeige"; § 58 Abs. 1 RStV: Erkennbarkeit und Trennung; § 58 Abs. 3 i.V.m. § 7 Abs. 3 RStV: Erkennbar- und Unterscheidbarkeit sowie optische und akustische Abgrenzung; § 58 Abs. 3 i.V.m. § 7 Abs. 4 RStV: Bei Teilbelegung des Bildes Trennung und Kennzeichnung; § 58 Abs. 3 i.V.m. § 7 Abs. 5 RStV: Dauerhafte Kennzeichnung bei Dauerwerbesendungen; § 58 Abs. 3 i.V.m. § 7 Abs. 7, 8 RStV: Hinweis zu Beginn bei Produktplatzierung; § 6 Abs. 1 Nr. 1 TMG: Erkennbarkeit.

2.1.4.1 Werbung und kommerzielle Kommunikation

Werbung ist in § 2 Abs. 2 Nr. 7 RStV legaldefiniert. Werbung ist „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs, die im Rundfunk von einem öffentlich-rechtlichen oder einem privaten Veranstalter oder einer natürlichen Person entweder gegen Entgelt oder eine ähnliche Gegenleistung oder als Eigenwerbung gesendet wird, mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, gegen Entgelt zu fördern."

Kommerzielle Kommunikation ist nicht im RStV, sondern in § 2 Nr. 5 TMG geregelt als „jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt (…)."

Die Begriffe „Werbung" und „kommerzielle Kommunikation" ähneln sich zwar sehr, aber kommerzielle Kommunikation ist etwas weiter gefasst.[16] Neben der Produktwerbung und konkreten Verkaufsangeboten ist ebenfalls die der Absatzförderung dienende Aufmerksamkeitswerbung erfasst.[17] Auch alle Formen der Selbstdarstellung, die eine wirtschaftlich tätige Person vornimmt, fallen darunter.[18] Dieser Selbstdarstellung dienen auch die Posts professioneller Influencer, jedenfalls dann, wenn sie das Erscheinungsbild ihres eigenen Blogs dadurch verbessern, dass sie auf für die Zielgruppe relevante Unternehmensseiten verlinken.[19]

2.1.4.2 Schleichwerbung, Produktplatzierung und Dauerwerbesendung

Schleichwerbung gem. § 2 Abs. 2 Nr. 8, § 7 Abs. 7 RStV ist „die Erwähnung oder Darstellung von Waren, Dienstleistungen, Namen, Marken oder Tätigkeiten eines Herstellers von Waren oder eines Erbringers von Dienstleistungen in Sendungen, wenn sie vom Veranstalter absichtlich zu Werbezwecken vorgesehen ist und mangels Kennzeichnung die Allgemeinheit hinsichtlich des eigentlichen Zweckes dieser Erwähnung oder Darstellung irreführen kann. Eine Erwähnung oder Darstellung gilt insbesondere dann als zu Werbezwecken beabsichtigt, wenn sie gegen Entgelt oder eine ähnliche Gegenleistung erfolgt."

---

[16] *Laoutoumai/Dahmen*, K&R 2017, S. 29 (32); *Pries*, in: Gersdorf/Paal, TMG, § 6 Rn. 3.

[17] *Köhler/Bornkamm*, UWG, § 6 Rn. 62.

[18] *Martini*, in: Gersdorf/Paal, TMG, § 2 Rn. 27.

[19] Vgl. LG Berlin, Urt. v. 24.5.2018 – 52 O 101/18.

Produktplatzierung gem. § 2 Abs. 2 Nr. 11, § 7 Abs. 7 i.V.m. § 15 RStV „ist die gekennzeichnete Erwähnung oder Darstellung von Waren, Dienstleistungen, Namen, Marken, Tätigkeiten eines Herstellers von Waren oder eines Erbringers von Dienstleistungen in Sendungen gegen Entgelt oder eine ähnliche Gegenleistung mit dem Ziel der Absatzförderung. Die kostenlose Bereitstellung von Waren oder Dienstleistungen ist Produktplatzierung, sofern die betreffende Ware oder Dienstleistung von bedeutendem Wert ist." Die Schwelle des bedeutenden Wertes wird von den Landesmedienanstalten mit 1.000€ festgelegt.

Es handelt sich also immer dann um Produktplatzierung und nicht um Schleichwerbung, wenn die Darstellung ausreichend als Produktplatzierung gekennzeichnet ist. Nach Rundfunkstaatsvertrag ist dabei entscheidend, dass die Produktplatzierung deutlich am Anfang des Beitrages erfolgt.

Eine Legaldefinition der Dauerwerbesendung findet sich in § 7 Abs. 5 RStV: *„[…], wenn der Werbecharakter erkennbar* im *Vordergrund steht und die Werbung einen wesentlichen Bestandteil der Sendung* darstellt.*"* Wie bei der Produktplatzierung muss der Hinweis Dauerwerbesendung am Anfang erfolgen, aber die ganze Sendung über eingeblendet werden.

2.1.4.3 Sponsoring

Sponsoring gem. § 2 Abs. 2 Nr. 9, § 8 RStV meint „jeden Beitrag einer natürlichen oder juristischen Person oder einer Personenvereinigung, die an Rundfunktätigkeiten oder an der Produktion audiovisueller Werke nicht beteiligt ist, zur direkten oder indirekten Finanzierung einer Sendung, um den Namen, die Marke, das Erscheinungsbild der Person oder Personenvereinigung, ihre Tätigkeit oder ihre Leistungen zu fördern."

In der oben bereits erwähnten BGH-Entscheidung GOOD NEWS II ging es ebenfalls um den Begriff „Sponsored by". Im Printbereich genüge dieser nicht der strengen Kennzeichnungspflicht als *Anzeige* oder *Werbung*. Obwohl der Begriff also rundfunkrechtlich geprägt ist, ist er zivilgerichtlich als eine nicht ausreichende Werbekennzeichnung (für den Pressebereich) vorbelastet.[20]

2.2 Problem Videoplattformen

Streitig ist es derzeit wohl, ob Videoplattformen wie YouTube in den Anwendungsbereich von § 58 Abs. 3 RStV fallen. Laut Erwägungsgrund 27 AVMD-RL *„sollten für Fernsehprogramme oder einzelne Fernsehsendungen, die zusätzlich als audiovisuelle Mediendienste auf Abruf von demselben* Mediendiensteanbieter *angeboten werden, die Anforderungen dieser Richtlinie mit der Erfüllung*

[20] Kritisch hierzu *Laoutoumai/Heins,* MMR 2018, S. 106 (108).

der Anforderungen für die Fernsehausstrahlung*, d. h. die lineare Übertragung, als erfüllt gelten. Wenn jedoch verschiedene Arten von Diensten, bei denen es sich um eindeutig unterscheidbare Dienste handelt, parallel angeboten werden, so sollte diese Richtlinie auf jeden dieser Dienste Anwendung finden."* Das bedeutet, dass YouTube Videos, die von Rundfunkanbietern zusätzlich zur Ausstrahlung im Rundfunk auf eine Videoplattform gestellt werden, vom § 58 Abs. 3 RStV und dessen Privilegierung erfasst sein müssen. Das betrifft dann sowohl die YouTube Kanäle – gleich wie die Mediatheken – der großen Rundfunkanbieter wie ARD und ZDF oder ProSieben und RTL, als auch die nicht als Rundfunk eingestuften weiteren Kanäle der YouTuber oder Twitcher mit Rundfunklizenz.[21] Im Umkehrschluss sind Videos von Bloggern, die ihre Beiträge nur auf YouTube zum jederzeitigen Abruf bereitstellen, nicht als Video on demand i.S.d § 58 Abs. 3 RStV einzustufen.[22] Für die Influencer Blogs auf YouTube gilt stattdessen die allgemeine – aber strengere – Regel des § 58 Abs. 1 RStV und des – durch die Verwendung des Begriffes kommerzielle Kommunikation in seinem Anwendungsbereich weiteren – § 6 Abs. 1 TMG. In der Evaluierung der AVMD-RL 2010 für die AVMD-RL 2016 unterscheidet die Europäische Kommission denn auch zwischen Video-on-demand-Diensten i.S.d. AVMD-RL 2010 und Videoplattformen im Internet.[23] Für reine YouTube Werbekanäle – wie z.B. die meisten Unternehmenskanäle – hat der EuGH Anfang des Jahres ebenfalls festgestellt, dass es sich nicht um audiovisuelle Mediendienste auf Abruf i.S.d. AVMD-RL 2010 handeln würde. Die Videos hätten rein kommerziellen Charakter, der Hauptzweck des YouTube Kanales sei nicht die Bereitstellung eines Programmes und die Videos seien auch sonst nicht einer Sendung als Werbung beigefügt. Damit seien sie vom Geltungsbereich der AVMD-RL 2010 nicht erfasst.[24]

Schon tatbestandlich nicht in den Anwendungsbereich von § 58 Abs. 3 RStV fallen die kurzen Videosequenzen bei Instagram – sog. Stories – oder SnapChat. Denn diese Videos bleiben nur eine begrenzte Zeit bestehen und sind somit nicht auf Abruf verfügbar.

---

[21] Twitch Streams, Gronkh bekommt Rundfunklizenz, abrufbar unter https://www.heise.de/newsticker/meldung/Twitch-Streams-Gronkh-bekommt-eine-Rundfunklizenz-3941102.html.

[22] Auf die Professionalität der Kanäle abstellend wohl a.A.: *Heins*, Produktplatzierung auf Videoportalen, S. 65.

[23] http://www.consilium.europa.eu/en/press/press-releases/2018/06/13/audiovisual-media-services-agreement-on-a-new-directive-to-boost-competitiveness-and-promote-european-content/.

[24] EuGH, Urt. v. 21.2.2018 – C-132/17.

2.3 Ergänzender lauterkeitsrechtlicher Schutz

Zusätzlich zu den medienrechtlichen Vorschriften finden die allgemeinen Vorschriften des Lauterkeitsrechts Anwendung. Der für das gesamte Medienrecht geltende Grundsatz der Trennung von Inhalt und Werbung ist zudem im § 5a Abs. 6 UWG ausdrücklich generalisiert.[25] Danach stellt ein Nicht-Kenntlichmachen von kommerziellen Inhalten eine unlautere Handlung dar. Außerdem stellt die Tarnung von Werbung als redaktioneller Inhalt einen Verstoß gegen Nr. 11 der sog. „Black List", dem Anhang zu § 3 Abs. 3 UWG, dar.

Festzuhalten bleibt, dass Influencer Beiträge trotz aller Zuordnungsverwirrung in jedem Fall Telemedien bzw. Teile von Telemedien sind. Wenn sie werblichen Inhalt haben, sind sie nach dem TMG oder lauterkeitsrechtlichen Vorschriften kennzeichnungspflichtig. Hauptangriffspunkt der bisherigen Verfahren um Influencer Beiträge ist deshalb die fehlerhafte oder gänzlich fehlende Kennzeichnung werblichen Charakters gewesen.[26] Noch keine Einigkeit herrscht hingegen bei der Frage, wie bzw. mit welchen Begriffen konkret die Kennzeichnung zu erfolgen hat. Die für die Praxis bedeutsame Frage lautet also: Wie kennzeichne ich einen Influencer Beitrag?

3 Wie muss gekennzeichnet werden?

Klare Regelungen und Beispiele für die Kennzeichnung werbender Beiträge existieren für die alten Medien Presse und Rundfunk.[27] Darauf kann zumindest vergleichend zurückgegriffen werden, auch wenn die Zivilgerichtliche nicht an die Maßstäbe gebunden sind, die bspw. die Landesanstalten für Medien als Rundfunkaufsicht aufgestellt haben.[28] Die im Rahmen des Lauterkeitsrechts beachtlichen presserechtlichen Vorschriften finden in der strengen Auslegung des BGH[29] dabei schon eher Eingang in die Rechtsprechung. In jedem Fall kann auf eine Wertung online wie offline zurückgegriffen werden:

---

[25] *Fechner*, Medienrecht, 6. Kap. Rn. 74.

[26] *Laoutoumai/Heins*, MMR 2018, S. 106 (108), Anm. zu LG Hagen, Urt. v. 13.9.2017 – 23 O 30/17; mit Verweis auf OLG Celle, Urt. v. 8.6.2017 – 13 U 53/17; KG Berlin, Beschl. v. 11.10.2017 – 5 W 221/17.

[27] Kennzeichnung als Anzeige oder Werbung in der Presse; Werbetrenner (z.B. Mainzelmännchen) fürs Fernsehen, ebenso split screen gem. § 7 Abs. 4 RStV, Dauerwerbesendung gem. § 7 Abs. 5 RStV, Produktplatzierung gem. § 7 Abs. 7 RStV oder Sponsoring gem. § 8 RStV.

[28] *Troge*, GRUR-Prax 2018, S. 87 (88).

[29] S. Fn. 11.

Erreicht die Überblendung von Inhalt mit Werbung eine zu hohe Intensität oder findet eine Vermengung von Inhalt und Werbung statt, so handelt es sich ohne Kenntlichmachung um unzulässige Schleichwerbung.[30]

3.1 Grundsätze und Normen

Der Grundsatz der Werbekennzeichnung gem. § 6 Abs. 1 Nr. 1 TMG und §§ 3 und 5a Abs. 6 UWG i.V.m. § 2 S. 1 Nr. 5 TMG lautet, dass für den Verbraucher klar erkennbar sein muss, ob und dass es sich um kommerzielle Kommunikation handelt. Auf die einzelnen Prüfungsmerkmale soll hier nicht genauer eingegangen werden.[31] Die Verbraucher sollen in der Lage sein, auf den ersten Blick zu erkennen, ob es sich beispielsweise um einen Unternehmensblog, also reine kommerzielle Kommunikation, oder um Werbung auf einer Webseite handelt, die auch nicht-kommerzielle Inhalte anbietet. Abzustellen ist dabei auf die Sicht des jeweils angesprochenen Verkehrskreises. Wenn danach eine Kennzeichnung zur sofortigen Erkennbarkeit der kommerziellen Kommunikation vonnöten ist, dann ist die Wahl der richtigen Begriffe und des richtigen Ortes bzw. die Art und Weise der Kenntlichmachung entscheidend.

3.2 Bekanntgewordene Entscheidungen

Innerhalb des letzten Jahres sind insb. vier Gerichtsentscheidungen bekanntgeworden, die sich mit Werbekennzeichnung beim Influencer Marketing beschäftigen. Ihnen gemein ist, dass sie allesamt Zivilrechtsstreitigkeiten gewesen sind. Kläger war jeweils ein Wettbewerbsverein, also kein anderer Influencer. Dass es trotz der großen Bedeutung des Influencer Marketing nicht zu mehr streitigen Entscheidungen gekommen ist, lässt vermuten, dass es zu einigen gütlichen Einigungen gekommen ist.

3.2.1 OLG Celle

Der bloße #ad unter bzw. neben einem Beitrag genügt nicht zur Kennzeichnung kommerzieller Kommunikation in Social Media, insbesondere wenn er sich an zweiter Stelle von sechs Hashtags befindet Dies entschied das OLG Celle im wohl aufsehenerregendsten, weil ersten Urteil zur Kennzeichnung von Influencer Beiträgen.[32] Ein Verstecken der Werbekennzeichnung in einer „Hashtagwolke“ genüge nicht. Dass der Beitrag jedenfalls kennzeichnungspflichtig sei, machte das OLG daran fest, dass er sich von

[30] Zur Tarnung von Werbeaussagen *Sosnitza*, in: Ohly/Sosnitza, UWG, § 5a Rn. 99.

[31] Vgl. hierzu aber insb. *Mallick/Weller*, WRP 2018, S. 155 (157 ff).

[32] OLG Celle, Urt. v. 8.6.2017 – 13 U 53/17; *Gerecke*, GRUR-Prax 2017, S. 446.

den anderen Beiträgen des Bloggers kaum unterscheide, aber Werbung enthalte. Auf den ersten Blick sei der werbende Charakter daher nicht zu erkennen.[33]

3.2.2 LG Hagen

Das LG Hagen legte fest, dass eine kommerzielle Kommunikation mit einer Kennzeichnung als *„Werbung"* oder *„Anzeige"* zu erfolgen habe.[34] Im dortigen Fall hatte die Bloggerin sog. affilliate links verwendet und keinerlei Werbekennzeichnung vorgenommen. Affilliate links sind Verlinkungen, die direkt auf die Unternehmenswebseite führen und den Verlinkenden über einen Rabattcode o.Ä. am Umsatz beteiligen können.

3.2.3 KG Berlin

Die Hashtags #sponsoredby und #ad genügen laut KG Berlin nicht zur Kennzeichnung werbender Beiträge in sozialen Medien.[35] Im ersten Fall verwies das KG auf die BGH-Entscheidung GOOD NEWS II, im zweiten Fall auf das OLG Celle. Durch diese Hashtags werde nicht deutlich genug auf den kommerziellen Zweck der Beiträge hingewiesen. Eine Werbekennzeichnung würde auch nicht entfallen, weil sich die kommerzielle Kommunikation schon aus den Umständen ergebe. Trotz der verwendeten Hashtags müsse ein Verbraucher die Beiträge erst einer genaueren Analyse unterziehen, um herauszufinden, ob es sich um Werbung oder normale Bloginhalte handele. Auf den ersten Blick erkennbar sei die Werbung jedenfalls nicht.

3.2.4 LG Berlin

Das LG Berlin hat entschieden, dass eine Werbekennzeichnung auch bei privat erworbenen Produkten erfolgen muss, wenn „die Art der Präsentation der Waren und der Verlinkung auf die Instagram-Auftritte der jeweiligen Unternehmen objektiv der Förderung des Absatzes der […] Unternehmen dient und damit deren kommerziellen Zwecken."[36] Das LG Berlin verweist dabei auf den Leitsatz der Entscheidung des KG Berlin, wonach derjenige geschäftlich handele, der sprechende Links auf Unternehmensseiten setze. Die Besonderheit im Fall vor dem LG ist aber gewesen, dass die Influencerin Rechnungen für die von ihr getragenen Modeartikel vorgelegt hatte. Dem LG war dies egal, weil die Influencerin in ihrem gesamten Blog

---

[33] Zu den Tatbestandsmerkmalen und Haftungsfragen vgl. *Reinholz/Schirmbacher*, K&R 2017, S. 753 (754).

[34] LG Hagen, Urt. v. 13.9.2017 – 23 O 30/17; *Laoutoumai/Heins*, MMR 2018, S. 106.

[35] KG Berlin, Beschl. v. 11.10.2017 – 5 W 221/17.

[36] LG Berlin, Urt. v. 24.5.2018 – 52 O 101/18; vgl. https://www.beckmannundnorda.de/serendipity/index.php?/archives/3859-LG-Berlin-Nicht-unbedeutender-Instragram-Influencer-muss-Posts-als-Werbung-kennzeichnen-geschaeftliche-Handlung-auch-bei-Praesentation-privat-erworbener-Produkte.html.

die Unternehmen durch Verlinkung auf deren Shop bewerben würde und so das Ziel hätte „die geschäftlichen Entscheidungen des Verbrauchers in Bezug auf diese Produkte zu beeinflussen." Das LG gewichtete außerdem, dass die Influencerin eine Projektmanagerin für ihren Blog beschäftige und Einkünfte daraus erziele, mithin ihr Blog als Unternehmen anzusehen sei und nicht als ein Privataccount. Inzwischen kennzeichnet die Influencerin sämtliche ihrer Beiträge zu Beginn mit „Werbung #unbezahlt"[37] und ihre Instagram Stories mit der Kennzeichnung „Dauerwerbesendung" (sog. Overlabeling).

3.3 Praktische Leitfäden

Die Entscheidungen haben Eingang in praktische Leitfäden für Blogger gefunden. Unter anderem sind hier die FAQ der Medienanstalten[38] zu nennen sowie der Leitfaden zur Kenntlichmachung von Werbung auf Instagram der Wettbewerbszentrale.[39] Die FAQ der Landesmedienanstalten orientieren sich stark an den rundfunkrechtlichen Normen und führen insofern zu einer Selbstbindung der Verwaltung, dass bei ihrer Beachtung kein aufsichtsrechtliches Verfahren eingeleitet werden soll[40] – falls die jeweilige Landesmedienanstalt dafür überhaupt zuständig ist. Beim Leitfaden der Wettbewerbszentrale hingegen handelt es sich um ein reines Privatgutachten.

Hier soll nur auf die Punkte eingegangen werden, die die Voraussetzungen aus den Entscheidungen erweitern bzw. ändern.

3.3.1 FAQ Landesmedienanstalten

Laut den FAQ sollen kostenlos von Unternehmen zur Verfügung gestellte Produkte ab einer Wertgrenze von 1.000 EUR als Produktplatzierung gekennzeichnet werden. Dabei genüge die Einblendung „Werbung" immer dann, wenn das Produkt dargestellt werde. Diese Empfehlung entspricht nicht gerade der klassischen Ausformung des Trennungsgrundsatz als Werbetrenner wie bei den Mainzelmännchen. Fairerweise muss gesagt werden, dass die FAQ ohne Differenzierung – fälschlicherweise – auf § 58 Abs. 3 RStV rekurrieren.

Was affilliate links angeht, geben die FAQ hingegen übermäßig strenge Ratschläge. Affiliate links seien immer Werbung. Der Werbehinweis solle „direkt im unmittelbaren Umfeld der Links" stehen und erklären, „wie ein

[37] Z.B. https://www.instagram.com/p/Bj-NyjQnX0G/?taken-by=vrenifrost.

[38] Abrufbar unter https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Richtlinien_Leitfaeden/FAQ-Flyer_Kennzeichnung_Werbung_Social_Media.pdf.

[39] Abrufbar unter https://www.wettbewerbszentrale.de/media/getlivedoc.aspx?id=35905.

[40] *Fuchs/Hahn*, MMR 2016, S. 503 (505).

affiliate link funktioniere“ und darauf hinweisen, dass eine Umsatzbeteiligung erfolge, wenn der User das Produkt über diesen Link bestellt. Dies geht über die vom LG Hagen geforderte bloße Kenntlichmachung als Werbelink weit hinaus und erscheint wenig praktikabel.

Das LG Berlin hat sich in seinem Urteil explizit gegen die in den FAQ der Medienanstalten geäußerte Auffassung entschieden, dass Postings mit kostenlos zur Verfügung gestellten Produkte nicht als Werbung gekennzeichnet werden müssten. Dies gelte nicht bei einer für Personen mit einer so hohen Followerzahl, wenn in Postings auf den Unternehmensshop verlinkt werde.[41]

3.3.2 Leitfaden Wettbewerbszentrale

Der Leitfaden betont die Kombination aus deutlicher Platzierung der Kennzeichnung und klarer, wörtlicher Bezeichnung. Durchschnittsnutzer der jeweiligen Plattform müssten ohne Zweifel von einem Werbehinweis ausgehen dürfen. Dabei solle der Hinweis immer am Anfang des jeweiligen Beitrages stehen, damit er noch vor dem Lesen wahrgenommen werden kann. Unproblematisch sei es bei der Kennzeichnung durch die Begriffe „Werbung“ oder „Anzeige“, die empfohlen wird, die Hashtagschreibweise zu wählen, also #Werbung oder #Anzeige. #Collaboration genüge hingegen nicht. Sollten plattformseitig frames angeboten werden – wie „Paid partnership“ auf Instagram – könne „eine derart klare Platzierung an prominenter Stelle eine kommerzielle Kommunikation auf den ersten Blick sichtbar werden lassen“.

3.4 Beurteilungsmaßstab/System

Aus den genannten Entscheidungen, Leitfäden und der Diskussion in der Literatur[42] lässt sich inzwischen ein gewisser Maßstab ableiten. Die Verwendung der Begriffe „Werbung“ und „Anzeige“ genügt jedenfalls dann, wenn sie direkt am Anfang des Beitrages stehen und deutlich sichtbar sind. Ein Verstecken unter mehreren Hashtags lässt die klare Kennzeichnung aber entfallen. Die Bezeichnungen „Sponsored by“, „gesponsert“, „Ads“ oder „Powered by“ genügen nicht als Werbekennzeichnung.[43]

Keine Kennzeichnung muss erfolgen, wenn es sich offensichtlich um einen Unternehmensblog oder Werbekanal handelt. Vorsicht ist aber dann

[41] So vorher auch schon *Gerecke*, GRUR 2018, S. 153 (155).

[42] Eine schöne Zusammenfassung (aber noch ohne das Urt. des LG Berlin) findet sich unter https://blog.socialhub.io/influencer-marketing-werbekennzeichnung/#kein-anschein-der-neutralitaet-wann-liegt-schleichwerbung-vor.

[43] Kritisch hierzu unter Verweis auf Englisch als Sprache des Internets *Laoutoumai/Heins*, MMR 2018, S. 106 (108).

geboten, wenn derartige Werbe-*„Inhalte“* als „Infomercials“ oder „Storymercials“ auf andere Blogs geladen werden oder der Blog den Anschein eines Privatprofiles erweckt. Wurde ein Produkt selbst erworben oder kostenlos überlassen und sachlich bewertet, muss keine Werbekennzeichnung erfolgen. Es handelt sich dann um neue Art der Wirtschaftsberichterstattung. Wurde ein Produkt allerdings kostenlos überlassen oder selbst erworben und hat der Influencer eine genügend große Followerzahl (im Fall vor dem LG Berlin waren es 50.000) und verlinkt in mehreren Posts auf die Unternehmenswebseiten, so müssen die Posts als Werbung gekennzeichnet werden. Auch hier ist also Vorsicht geboten, wenn der ganze Blog den Anschein eines Werbeprofiles aufweist.

Fraglich erscheint, ob die plattformseitigen Rahmen wie z.B. „paid partnership“ auf Instagram genügen. Dies wird von Teilen der Literatur abgelehnt.[44] Insbesondere wenn Begriffe wie „Sponsored by“ den Rahmen bilden, findet sich dafür auch eine Anknüpfung in Gesetz und Rechtsprechung. Die wohl für die Praxis entscheidende Frage lautet nun, inwiefern das skizzierte System einerseits abmahnsicher, andererseits aber flexibel genug ist, um auf neue Entwicklungen in Social Media übertragen werden zu können.

4 Ist Kennzeichnung gleich Trennung?

Die medienrechtlich interessantere Frage ist aber eigentlich: Entspricht eine den unter 3.1.4 genannten Anforderungen genügende Werbekennzeichnung auch dem Trennungsgebot? Ist Trennung und Kennzeichnung also im Ergebnis synonym zu verstehen oder müssten die unterschiedlichen Sachverhalte – z.B. YouTube-Videos oder Instagram Posts – unterschiedlich bewertet werden?[45] Zwar wird in der Literatur wie im Gesetz zwischen Trennung und Kennzeichnung unterschieden,[46] in der Praxis ist aber nicht klar, welche Anforderungen jeweils erfüllt werden müssen. Ein Ansatzpunkt, Trennung und Kennzeichnung synonym zu verstehen, könnte im letzten Satz des Erwägungsgrundes der 27 AVMD-RL 2010 gesehen werden: *„Der Einsatz neuer Werbetechniken sollte durch den Trennungsgrundsatz nicht ausgeschlossen werden.“* Hieraus könnte abgeleitet werden,

[44] *Mallick/Weller*, WRP 2018, S. 155 (159).

[45] Verf. beschäftigt sich mit dieser Frage in einer Seminararbeit i.R.d. Zusatzausbildung im Informations-, Telekommunikations- und Medienrechts an der WWU Münster.

[46] Statt vieler *Holznagel*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 3 Rn. 156 f.

dass eine strikte Trennung beim Influencer Marketing als *„neuer Werbetechnik“* nicht mehr vonnöten sei. Doch dies ist abzulehnen, da es sich bestenfalls um eine neue Werbemethode handelt.[47]

Bei einer Unterscheidung von bloßer Kennzeichnung und strikter Trennung ergibt sich die Überlegung, welcher der beiden Ansätze am sinnvollsten erscheint.

4.1 Fortführung Trennung oder übertragbare Kennzeichnungsregeln

Im Folgenden soll kurz dargestellt werden, was für einen strikten Trennungsgrundsatz beim Influencer Marketing sprechen würde und was für ein wie oben dargestelltes Kennzeichnungssystem. Hierfür ist aber zunächst ein Blick auf den Medienkonsum der Zielgruppe notwendig.

4.1.1 Derzeitiger Medienkonsum und Medienkonvergenz

Der Konsum klassischer Medien ist unter jungen Leuten stark rückläufig und der Medienkonsum on demand nimmt stetig zu.[48] Wenn das Fernsehen gesamtgesellschaftlich noch als Leitmedium gilt, so trifft das auf die unter 30-Jährigen schlicht nicht mehr zu. Dies erkennen immer häufiger auch die Gerichte an: *„In den letzten Jahren habe sich in sichtbarer Weise die Mediennutzung verändert. Die Idee der Veranstaltung eines Rundfunkprogramms werde zunehmend belanglos, wie sich an der sehr großen Resonanz von sog. Youtube-Kanälen zeige. Zunehmend werde der eigene Medienkonsum “on demand” gesteuert.“*[49] Diese Situation führt dazu, dass eine Generation herangewachsen ist, die die klassische Trennung von Werbung und Programm nicht derart verinnerlicht hat wie vorherige Generationen.[50]

Im Hinblick auf die Informationsfreiheit des Art. 5 Abs. 1 S. 1, 2. Hs. GG, die – wie in der Einführung dargestellt – Grund für Trennung und Kennzeichnung ist, muss diese fehlende Differenzierung zwischen Werbung und Inhalt in jedem Falle Berücksichtigung finden. Es kommt noch im besonderen Maße hinzu, dass gerade Jugendliche und junge Leute die Zielgruppe der Influencer sind.[51]

4.1.2 Starre Trennung v. flexible Kennzeichnung

Für eine Fortführung des klassischen strengen Trennungsgrundsatz wie in der Presse oder früher im Rundfunk spricht zunächst der Art. 5 Abs. 1 S. 1, 2. Hs. GG. Eine saubere Trennung durch Verwendung von Einrahmungen,

---

[47] Vgl. allgemein zu Native Advertising *Wiebe/Kreutz*, WRP 2015, S. 1053 (1053 ff).

[48] *Gajo*, GmbHR 2017, Rn. 332.

[49] OLG Hamburg, Urt. v. 1.3.2018 –3 U 167/15, Rn. 11.

[50] Zur Diskussion um ein Internet-Verbraucherleitbild vgl. *Wiebe/Kreutz*, WRP 2015, S. 1179 (1181).

[51] So auch LG Hagen, Urt. v. 29.11.2017 – 23 O 45/17.

Linien, akustischen Signalen ist die einfachste Lösung dem Sinn der Informationsfreiheit tatsächlich gerecht zu werden. Praktisch wäre dies auch in jedem Fall umsetzbar, da die Influencer werbende Beiträge selbst so gestalten könnten und technisch nicht auf die Plattformen angewiesen sind. Das wäre problemlos möglich sowohl bei Bild-, als auch bei Videobeiträgen.

Zudem sorgt eine strenge Trennung für die größte Rechtssicherheit, da die werbenden Beiträge auf diese Art in jedem Fall schon bei Betrachten des Blogs, also nicht des einzelnen Postings, als Werbung zu erkennen wären. Das Dilemma, dass die Vorinstanz die Werbung für offensichtlich erkennbar hält und die nächste Instanz das Gegenteil annimmt,[52] entfällt so.

Die negative Informationsfreiheit gem. Art. 5 Abs. 1 S. 1, Var. 1 GG spricht ebenfalls für eine Beibehaltung eines strikten Trennungsgrundsatzes. Denn sie schützt insoweit vor Werbung, als sie das Recht beinhaltet eine Information nicht zur Kenntnis nehmen zu müssen, also in Ruhe gelassen zu werden. Zumindest dann, wenn die Werbung unausweichlich ist, ist sie betroffen.[53] In der Rechtsprechung hat dieser Gedanke – soweit ersichtlich – bisher keine Rolle gespielt, auch wenn der EuGH einen Schutz vor übermäßiger Werbung anerkannt hat.[54]

Für ein Kennzeichnungssystem spricht vor allem dessen Anpassbarkeit auf neue technologische Möglichkeiten und dessen Flexibilität, was die Ausgestaltung neuer Werbemöglichkeiten angeht. Dies ist auch im Sinne der AVMD-RL, die mehr Werbung zulassen möchte. Auf wessen Lobby Druck sei dahingestellt.

Gegen ein bloßes Kennzeichnungssystem spricht die Rechtsunsicherheit, wie sie wohl gerade derzeit noch vorherrscht. Allerdings geht es bei den zuletzt aufgekommenen Fragen und Unsicherheiten meist nur um Detailregelungen. Ein Problem, was sich durch die bloße Kennzeichnung wohl nur schwer wird regeln lassen, ist, wann kommerzieller Charakter offensichtlich erkennbar ist. Denn die meisten Influencer Blogs sind inzwischen dermaßen professionell gestaltet, dass die Inhalts- und Werbepostings nicht mehr voneinander zu unterscheiden sind.

4.2 Kurzfazit

Die Privilegierung von Rundfunkanbietern, die ehemals starre Trennung von Inhalt und Werbung zugunsten von mehr Werbung aufweichen zu lassen, gilt nur für ebendiese. Bei anderen Multimediadiensteanbietern ohne

[52] Wie beim LG Hannover und OLG Celle geschehen.

[53] *Fechner*, Medienrecht, 6. Kap. Rn. 44.

[54] EuGH, Urt. v. 23.10.2003, C-245/01 – RTL Television.

organisatorische Verknüpfung zu Rundfunk müsste es bei einer eindeutigen Trennung von Inhalt und Werbung bleiben. Viele Influencer werden dem nicht gerecht, auch wenn inzwischen zumindest bekannt zu sein scheint, dass eine Kennzeichnung von Werbung in jedem Fall erfolgen muss. Nur ist Kennzeichnung eben nicht automatisch gleich Trennung oder wenigstens auf den ersten Blick erkennbar.

Eine strenge Beibehaltung des klassischen Trennungsprinzips wie im RStV und in den Pressegesetzen geregelt, würde daher für Rechtsklarheit sorgen. Werbetrenner, akustische und optische Abgrenzung bis hin zu split screens würden dem genügen. Damit würde auch den Anforderungen aus dem TMG nach klarer Erkennbarkeit genüge getan werden.

Da sich Influencer Blogs zwischen den beiden Polen reiner kommerzieller Kommunikation (wie z.B. die YouTube Werbekanäle der Unternehmen selbst) und wohl noch privaten Blogs bewegen, lässt sich die Frage nötiger Werbekennzeichnung für sie nicht pauschal beantworten. Festzuhalten ist aber, dass weder ein absoluter Verzicht auf Kennzeichnung noch ein Overlabeling jedes Postings als Werbung der Königsweg für rechtskonformes Influencer Marketing sein kann.

Literatur

Borsch, Uwe: Der angemaßte Influencer – Markenpiraterie 2.0, Aspekte und Möglichkeiten der Abwehr aufgezwungener Werbung, MMR 2018, S. 127-129.

Fechner, Frank: Medienrecht, 18. Aufl., Tübingen 2017.

Fuchs, Thomas/Hahn, Caroline: Erkennbarkeit und Kennzeichnung von Werbung im Internet – Rechtliche Einordnung und Vorschläge für Werbefragen in sozialen Medien, MMR 2016, S. 503-507.

Gajo, Marianne: Studie zur Entwicklung der Sportindustrie, GmbHR 2017, S. 332-333.

Gerecke, Martin: Kennzeichnung von werblichen Beiträgen im Online-Marketing, GRUR 2018, S. 153-159.

Gersdorf, Hubertus/Paal, Boris (Hrsg.): BeckOK Informations- und Medienrecht, 20. Ed., München 2018.

Henning-Bodewig, Frauke: Influencer-Marketing – der „Wilde Westen des Werbens“?, WRP 2017, S. 1415-1421.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, 46. EL, München 2018.

Holzgraefe, Moritz: Bühne frei für Product Placement – Werden die neuen Werberichtlinien der Landesmedienanstalten dem RStV gerecht?, MMR 2011, S. 221-226.

Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn: Gesetz gegen den unlauteren Wettbewerb, 36. Aufl., München 2018.

Laoutoumai, Sebastian: Kennzeichnungspflichten und Werbeverbote im Influencer Marketing, MMR 2018, S. 106-109.

Laoutoumai, Sebastian/Dahmen, Anna: Influencer Marketing – Neue Stars, alte Pflichten?!, K&R 2017, S. 29-33.

Mallick, Rani/Weller, David: Aktuelle Entwicklungen im Influencer Marketing – Ein Blick aus der Praxis, WRP 2018, S. 155-161.

Ohly, Ansgar/Sosnitza, Olaf: Gesetz gegen den unlauteren Wettbewerb, 7. Aufl., München 2016.

Paschke, Marian/Berlit, Wolfgang/Meyer, Claus (Hrsg.): Hamburger Kommentar Gesamtes Medienrecht, 3. Aufl., Baden-Baden 2016.

Reinholz, Fabian/Schirmbacher, Martin: Anforderungen an die Kennzeichnung von Influencer-Werbung, K&R 2017, S. 753-758.

Sporn, Stefan: Ein Grundrecht der Medienfreiheit – Gleiches Recht für alle!?, Beihefter 2 zu K&R 2013, S. 1-9.

Troge, Thorsten: Herausforderung Influencer-Marketing, GRUR-Prax 2018, S. 87-89.

Wiebe, Andreas/Kreutz, Oliver: Native Advertising – Alter Wein in neuen Schläuchen?, WRP 2015, S. 1053-1060 und WRP 2015, S. 1179-1187.

KARTELLRECHTLICHE GRENZEN DES INFORMATIONSAUSTAUSCHS

RA Sebastian Louven

Interdisziplinäres Zentrum für Recht der Organisationsgesellschaft (ZRI)
Carl von Ossietzky Universität Oldenburg
sebastian.louven@uni-oldenburg.de

Zusammenfassung

Moderne Geschäftsmodelle leben von modernen Kooperationsformen. Hierzu gehören mehr denn je datengetriebene Geschäftsmodelle, Plattformen, sowie zunehmend automatisierende Systeme. Allen ist gemein, dass sie die wettbewerblichen Entfaltungsmöglichkeiten der beteiligten Unternehmen beschleunigen und vereinfachen – aber ebenso ein hohes Risiko wettbewerbswidriger Abstimmungen in sich bergen. Denn der Austausch von Informationen ist aus wettbewerbsrechtlicher Sicht nicht völlig unbedenklich. Dieser Beitrag stellt in einem ersten Abschnitt die kartellrechtlichen Grundlagen des Verbots abgestimmter Verhaltensweisen sowie die bisherige Rechtsprechung zu Marktinformationssystemen dar. Im zweiten Schritt sollen moderne Geschäftsmodelle untersucht werden, bei denen wettbewerbsrelevante Abstimmungen oder Kooperationen naheliegen könnten.

1 Abstimmung durch Informationsaustausch

1.1 Verbot von Wettbewerbsbeschränkungen

Das allgemeine Verbot wettbewerbsbeschränkender Maßnahmen findet sich in Art. 101 Abs. 1 AEUV sowie der regelungstechnisch gleichlautenden Vorschrift § 1 GWB im deutschen Recht. Danach sind Vereinbarungen, Beschlüsse und abgestimmte Verhaltensweisen verboten, die eine Beschränkung des Wettbewerbs bezwecken oder bewirken. Bewirkt eine der genannten Maßnahmen lediglich eine Wettbewerbsbeschränkung, so wird nach den insofern gleichlaufenden Mitteilungen der Kartellbehörden von einem Eingreifen abgesehen, wenn die jeweiligen Marktanteile auf dem betroffenen Markt unterhalb der Schwelle von 10 % bzw. 15 % bei mehreren betroffenen Märkten liegen.[1] Diese Bagatellschwellen gelten jedoch nicht, wenn eine Maßnahme die Beschränkung des Wettbewerbs bezweckt. Dies

[1] Kommission, Bekanntmachung über Vereinbarungen von geringer Bedeutung, die im Sinne des Art. 101 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union den Wettbewerb nicht spürbar beschränken - De-minimis-Bekanntmachung, 30.8.2014; in der Regelung insofern gleichlautend, dogmatisch jedoch an der Festlegung des Aufgreifermessens orientiert: BKartA, Bekanntmachung Nr. 18/2007 des Bundeskartellamtes über die Nichtverfolgung von Kooperationsabreden mit geringer wettbewerbsbeschränkender Bedeutung - Bagatellbekanntmachung, 13.3.2007.

ist dann anzunehmen, wenn eine Maßnahme bereits „ihrem Wesen nach“ als wettbewerbsbeschränkend anzusehen ist.[2]

1.2 Abgestimmte Verhaltensweisen – Hub-and-Spoke-Konstellation

Besondere Herausforderungen stellen sich in der Praxis durch das Tatbestandsmerkmal der abgestimmten Verhaltensweisen. Die anderen beiden Kollusionsformen der Vereinbarung und des Beschlusses sind regelmäßig objektiv unmittelbar nachweisbar. Abgestimmte Verhaltensweisen jedoch knüpfen nicht an eine vorhergehende unmittelbare Willensäußerung an. Vielmehr bestehen sie an sich bereits in der Vollziehung des wettbewerbsbeschränkenden Verhaltens. Abgestimmte Verhaltensweisen sind dabei als Vorstufe zu Vereinbarungen und Beschlüssen zu sehen. Hierzu hat sich in der europäischen Rechtsprechung die Formel etabliert, dass es sich hierbei um eine Koordinierung zwischen Unternehmen handelt, die zwar noch nicht bis zum Abschluss eines Vertrags im eigentlichen Sinne gediehen ist, jedoch bewusst „eine praktische Zusammenarbeit an die Stelle des mit Risiken verbundenen Wettbewerbs treten lässt“.[3] Diese praktische Zusammenarbeit lässt sich auch als Abstimmung zusammenfassen, wobei diese unmittelbar wie auch mittelbar erfolgen kann.[4]

Für den Bereich des Informationsaustauschs wird nach der europäischen Rechtsprechung regelmäßig vermutet, dass eine unmittelbare Abstimmung zum einen zu ihrer Berücksichtigung durch die beteiligten Unternehmen führt und zum anderen hiermit kausal eine Wettbewerbsbeschränkung verbunden ist.[5] Den beteiligten Unternehmen wird damit also der Gegenbeweis aufgelastet, dass ein behördlich festgestellter Informationsaustausch zum einen nicht zu einer verbotenen Abstimmung und zum anderen nicht zu einer Wettbewerbsbeschränkung geführt hat. Der EuGH sieht in diesen Vermutungen einen „integralen Bestandteil des anwendbaren Gemeinschaftsrechts“, sodass trotz erheblicher Zweifel für das deutsche Kartell-

---

[2] Kommission, Leitlinien zur Anwendbarkeit von Art. 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit - Horizontalleitlinien, 14.1.2011, Rz. 72.

[3] EuGH, Urt. v. 4.6.2009 – C 8/08 (T-Mobile Netherlands), Rn. 26; EuGH, Urt. v. 14.7.1972 – C 48/69 (Imperial Chemical Industries/Kommission), Rn. 64; EuGH, Urt. v. 16.9.2013 – T-380/10 (Wabco Europe) Rn. 37; EuGH, Urt. v. 16.9.2013 – T-386/10 (Dornbracht), Rn. 123.

[4] *Grave/Nyberg*, in: Loewenheim/Meessen/Riesenkampff/Kersting/Meyer-Lindemann, Kartellrecht, Art. 101 AEUV, Rn. 230 ff.

[5] EuGH, Urt. v. 4.6.2009 – C 8/08 (T-Mobile Netherlands), ECLI:EU:C:2009:343, EuZW 2009, 505, Rz. 51; zuletzt noch EuGH, Urt. v. 21.1.2016 – C-74/14 (Eturas), ECLI:EU:C:2016:42, NZKart 2016, 133, Rz. 26 ff.; *Emmerich*, in: Immenga/Mestmäcker, Wettbewerbsrecht, Art. 101 AEUV, Rn. 83 ff.

Ordnungswidrigkeitenrecht[6] bis zu einer endgültigen Klärung von einer Anwendung dieser Grundsätze ausgegangen werden kann. Jedenfalls kann festgehalten werden, dass sich aus dem Verbot wettbewerbsbeschränkender Abstimmungen eine Compliance-Belastung ergibt, die sich nicht lediglich auf Vereinbarungen oder Beschlüsse bezieht, sondern auch andere Kooperationsformen mit Branchenbegleitern.

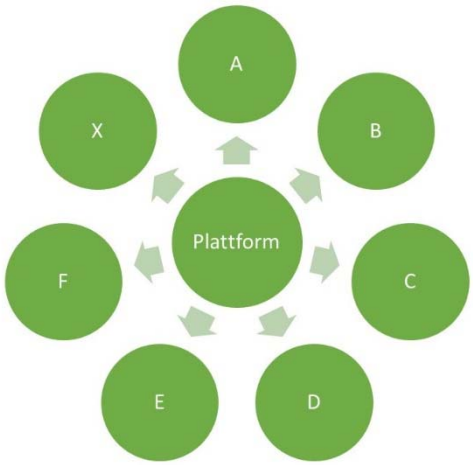

Abb. 1: Schematische Darstellung einer sternförmigen Vertriebsstruktur

Exemplarisch für eine mittelbare Abstimmung ist das sogenannte Hub-and-Spoke-Kartell.[7] Hierbei erfolgt kein unmittelbarer Kontakt zwischen den teilnehmenden Unternehmen, sondern es findet eine Abstimmung über einen in der Mitte des Geschehens stehenden Vermittler statt. Dieser Vermittler unterhält Verbindungen zu teilnehmenden Unternehmen, die sich schematisch in Form einer Radnabe (Hub) und von diesen ausgehenden Speichen (Spoke) darstellen lassen. Aufgrund dieser Verbindungen kann der Vermittler die angeschlossenen Unternehmen koordinieren. Die Verbindungen zwischen dem Vermittler und den einzelnen beteiligten Unternehmen können sowohl als vertikalen Vereinbarung ausgestaltet sein, als auch in Form einer lediglich faktischen Einflussmöglichkeit bestehen. Ausschlaggebend für die Annahme einer wettbewerbsbeschränkenden Abstimmung ist nämlich bereits die faktische Koordinierungsmöglichkeit. Entsprechend hoch sind die Prüfanforderungen der beteiligten Unternehmen in der Kartellrechts-Compliance. Denn wollen diese sich dem möglichen Risiko kartellrechtlicher Haftung entziehen, müssen sie ihre Kooperationen und ihr Verhalten auch auf derartige Koordinierungsmöglichkeiten hin untersuchen.

---

6 *Grave/Nyberg*, in: Loewenheim/Meessen/Riesenkampff/Kersting/Meyer-Lindemann, Kartellrecht, Art. 101 AEUV, Rn. 231.

7 *Hainz/Benditz*, EuZW 2012, S. 686 (686).

1.3 Verbotene Fühlungnahme und bewusstes Parallelverhalten

Problematisch hat sich im letzten Jahren jedoch auch gezeigt, dass vielfach im weitesten Sinne Kooperationen zwischen Unternehmen mittels digitaler Hilfsmittel der Information Bearbeitung vollzogen werden. Dies birgt zum einen zwar das Risiko, dass auch Abstimmungen oder wettbewerbswidrige Vereinbarungen nicht nur quantitativ, sondern auch qualitativ mehr Bedeutung. Zum anderen geht mit der zunehmenden kartellrechtlichen Aufmerksamkeit, die diese technischen Entwicklungen auf sich lenken, die Befürchtung betroffener Unternehmen einher, nicht mehr trennscharf zwischen verbotenen Abstimmungen und erlaubtem Marktverhalten unterscheiden zu können.

Grundlegende Prinzipien in diesem Zusammenhang sind zum einen das sogenannte Selbstständigkeitspostulat und zum anderen das hieraus entwickelte Verbot der Fühlungnahme. Ersteres ist als das wettbewerbsimmanente Auftreten von Unternehmen am Markt zu verstehen, das grundsätzlich ohne eine wettbewerbliche Einflussnahme von oder mit anderen Unternehmen stattzufinden hat. Stattdessen haben Unternehmen ihre wettbewerblichen Geschicke in den Markt grundsätzlich selbst zu bestimmen.[8] Eine Fühlungnahme kann hiernach darin liegen, dass Unternehmen entweder direkt andere Unternehmen informieren mit dem Ziel oder der Wirkung der Beeinflussung des Wettbewerbs, oder der Beeinflussung anderer Unternehmen zur Ausschaltung des Wettbewerbs. In diesen Fällen tritt an die Stelle des an sich bestehenden Wettbewerbsrisikos eine Vorhersehbarkeit für die Unternehmen.[9] Auf der anderen Seite sind Unternehmen nicht gehindert, moderne Datenverarbeitungsmethoden und-Technologien nutzen, hierdurch autonom Wettbewerbsvorteile zu spielen. Die Kommission spricht hierbei von einem Beobachten der Konkurrenten mit wachen Sinnen,[10] so das für die neuen Technologien davon ausgegangen werden kann, dass diese jedenfalls dann unbedenklich sind, wenn sie lediglich eine Verschärfung der unternehmerischen Sinne darstellen.

2 Neue Kooperationsmöglichkeiten

Die verschiedenen neuen Kooperationsmöglichkeiten zeichnen sich sämtlich durch das Merkmal einer externen Autonomie aus. Dies beschreibt den

---

[8] *Emmerich*, in: Immenga/Mestmäcker, Wettbewerbsrecht, Art. 101 AEUV, Rn. 89.

[9] So zuletzt auch: EuGH, Urt. v. 21.1.2016 – C-74/14 (Eturas), ECLI:EU:C:2016:42, NZKart 2016, 133; vgl. *Emmerich*, in: Immenga/Mestmäcker, Wettbewerbsrecht, Art. 101 AEUV, m.w.N. in Fn. 254.

[10] Kommission, Leitlinien zur Anwendbarkeit von Art. 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit - Horizontalleitlinien, 14.1.2011, Rz. 61.

Umstand, dass mittels des genutzten Angebots marktrelevante Entscheidungen getroffen werden. Dabei lassen sich die dargestellten herkömmlichen Grundsätze übertragen. Jedoch verlangt dies zudem eine Erörterung der tatsächlichen Umstände der Kooperation.

2.1 Digitale Plattformen

Als digitale Plattformen lassen sich vor allem Angebote des sogenannten Web 2.0 beschreiben. Es handelt sich um einen bislang nicht genau definierten Begriff. Das Bundeskartellamt beschreibt digitale Plattformen als Geschäftsmodelle mit Angeboten gegenüber mehreren Nutzergruppen, zwischen denen indirekte Netzwerkeffekte bestehen. Indirekte Netzwerkeffekte beschreiben die Auswirkungen individueller Entscheidungen der Teilnehmer einer Nutzergruppe auf die Entscheidungsmöglichkeiten der Teilnehmer einer anderen Nutzergruppe. Diese können sowohl einseitig, asymmetrisch als auch mehrseitig vorliegen. Bei einseitigen Netzwerkeffekten wirken sich lediglich die Entscheidungen einer Nutzergruppe auf die andere aus, ohne dass ein entsprechend gegenläufiger Effekt besteht. Besteht ein gegenläufiger negativer indirekter Netzwerkeffekt, lässt sich von asymmetrischen indirekten Netzwerkeffekten sprechen.

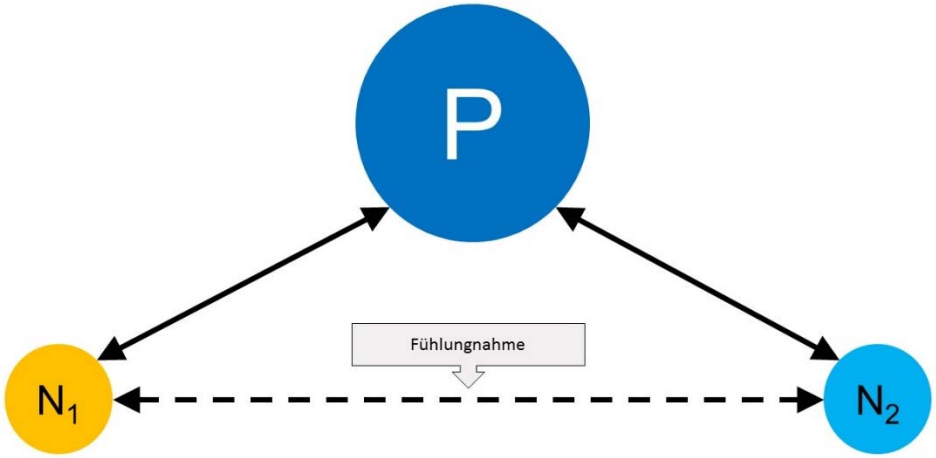

Abb. 2: Schematische Darstellung der Fühlungnahme mittels einer Plattform

Jedoch erscheint für die Zwecke dieser Untersuchung eine Definition ausschließlich über indirekte Netzwerkeffekte nicht abschließend. Vielmehr kann ein Plattformangebot auch bei direkten Netzwerkeffekten bestehen, also wenn sich die Entscheidungen einzelner Individuen auf die Entscheidungen der Teilnehmer derselben Nutzergruppe auswirken. In diesem Fall vermittelt die Plattform die gleichlaufenden Interessen einer Nutzergruppe. Zu den Plattformen können deshalb auch Cloud-Geschäftsmodelle zählen. Maßgeblich ist dabei der zentrale Betrieb.

Wird eine digitale Plattform eingesetzt, um zwischen verschiedenen Unternehmen zu vermitteln, kann über diese Vermittlung auch eine Koordination stattfinden. Hierfür können die etablierten Grundsätze der Hub-and-Spoke-Konstellation übertragen werden. Kartellrechtswidrige Abstimmungen können dabei mittels der Einflussnahmemöglichkeiten über sternförmige Vertragsstrukturen erfolgen. So könnten Betreiber von Vertriebsplattformen technische Voreinstellungen aufnehmen, mittels derer die freie Preisgestaltung teilnehmender Unternehmen unterbunden wird.[11] Nehmen die beteiligten Unternehmen diese Änderung oder ähnliche Preisanpassungs- oder Erhöhungsschreiben passiv an, kann nach der Eturas-Rechtsprechung des EuGH hierin die Mitwirkung an einer Abstimmung gesehen werden. Ebenso wird eine Abstimmung durch Cloud-Anbieter zu sehen sein, wenn diese über Updates Informationen an ihre Kunden senden. Handelt es sich hierbei um Informationen, die ein Abweichen vom selbstständigen Auftreten im Wettbewerb ermöglichen, ist nach den etablierten Grundsätzen der Rechtsprechung von einer Fühlungnahme auszugehen. Der fehlende unmittelbare Kontakt zwischen den einzelnen Plattform-Teilnehmern ist dabei unerheblich.

2.2 Verteilte Systeme und Blockchain-Technologie

Eine weitere technische Neuerung mit bislang scheinbar unklarer kartellrechtlicher Bewertungslage sind allgemein verteilte Systeme und im Besonderen die sogenannte Blockchain-Technologie. Hierbei handelt es sich stark verkürzt nicht um Plattformen im oben dargestellten Sinn, da es regelmäßig keinen speichenartig in der Mitte stehenden Vermittler gibt, der über seine Einflussmöglichkeiten das wettbewerbliche Verhalten der angeschlossenen Unternehmen koordinieren kann. Dennoch kann nach technischem Verständnis auch über diese Technologien eine Abstimmung im Sinne des Verbots aus Art. 101 Abs. 1 AEUV bzw. § 1 GWB erfolgen.

2.2.1 Technische Hintergründe

Verteilte Systeme stellen allgemeinhin betrachtet moderne Formen einer intensiveren Zusammenarbeit dar. Dabei lässt sich dies am besten über den Unterschied zwischen einer Server- und demgegenüber einer Peer-to-Peer-Infrastruktur (P2P) erklären. Das erste Modell zeichnet sich im Wesentlichen durch eine zentrale Bereitstellung und Steuerung eines bestimmten Angebots aus. So werden Inhalte oder Kommunikation nicht über eine dedizierte Verbindung zwischen den Austauschenden geteilt. Stattdessen erfolgt das Routing und die genaue Zuteilung über eine zentrale Infrastruktur eines Betreibers. In infrastrukturtechnischer Hinsicht kann damit eine

[11] EuGH, Urt. v. 21.1.2016 – C-74/14 (Eturas), ECLI:EU:C:2016:42, NZKart 2016, 133.

zentrale Koordination von Informationen weiterhin durch das Betreiber-Unternehmen erfolgen.

Bei einer P2P-Infrastruktur gibt es keinen unmittelbaren Vermittler. Stattdessen wird in technischer Hinsicht die Art und Weise der Kooperation oder des Austauschs vorgeschrieben. Der Begriff „Verteilte Systeme" beschreibt dabei anders als bei herkömmlichen P2P-Systemen nicht lediglich die leitungsbezogene direkte Austauschbeziehung zwischen den einzelnen Teilnehmern. Darüber hinaus werden wesentliche Ressourcen des betreffenden Systems dezentral betrieben oder gespeichert. Dies kann wiederum auch für wettbewerblich relevante Informationen der Fall sein.

Vor diesem technischen Hintergrund stellt sich die sogenannte Public Blockchain als Erweiterung dar. Hierbei handelt es sich um ein System miteinander technisch dezentral verknüpfter Teilnehmer, die über ein vorgegebenes System und nach vorgegebenen Regeln miteinander kommunizieren. Als Public Blockchain stellt sich dies dann dar, wenn keine zentrale Instanz zur Entscheidung berufen ist. Auch hierbei entfällt also ein Vermittler. Allerdings wird dessen Funktion in technischer Hinsicht abstrahiert. So werden Informationen mittels der Blockchain-Technologie über ein Konsensverfahren verifiziert und in einzelnen Blöcken abgesichert hinterlegt. Damit kann jeder Teilnehmer einer spezifischen Blockchain Koordinierungspartner für eine Vielzahl an Informationsaustauschen sein.

Die Private Blockchain dagegen stellt wiederum ein von einer zentralen Instanz bereitgestelltes oder betriebenes System dar, das nicht für Jedermann offen zugänglich ist. Stattdessen bestimmt ein Unternehmen die Vorgaben von Informationsaustauschen. Dies ähnelt wiederum einer herkömmlichen Plattform-Infrastruktur, wobei lediglich eine andere Technologie verwendet wird.

2.2.2 Koordinierung

Die dargestellten neuen technologischen Entwicklungen entbinden zunächst nicht von einer kartellrechtlichen Bewertung. Gleichzeitig wie sie zu einer Erweiterung tatsächlicher Handlungsmöglichkeiten im Wettbewerb führen, bedeutet dies die daraus folgende Untersuchung der neuen Kooperations- und Koordinierungsmöglichkeiten. Dabei lässt sich zunächst für die Private Blockchain festhalten, dass hier eine kartellrechtliche Haftung beteiligter Unternehmen nach den herkömmlichen Grundsätzen der Hub-and-Spoke-Konstellation und der Eturas-Rechtsprechung herleiten lässt. Denn die zentrale Instanz erhält durch die Vorgaben der weiteren Abläufe eine ähnliche Einfluss- und Koordinierungsmöglichkeit, um die erforderliche Abstimmung über die Bande vorzunehmen.

Anders stellt sich dies jedoch allgemein für verteilte Systeme und Public Blockchain dar, gleichfalls wenn bei einer Private Blockchain die angeschlossenen Unternehmen selbstständig die zur Verfügung gestellte Technologie zu wettbewerbswidrigen Informationsaustauschen nutzen. Zwar entfällt hierbei der bei Plattform-Konstellationen typische Vermittler. Allerdings bedeutet dies nicht, dass keine indirekte Abstimmung mehr vorliegen kann. Stattdessen können sich die beteiligten Unternehmen die Mechanismen der jeweiligen Blockchain zunutze machen und dabei weiterhin auch mittelbar ihr Verhalten abstimmen. Statt eines Abstimmungsmittlers steht den über die Blockchain angeschlossenen Unternehmen nämlich ein komplexer Konsensmechanismus zur Verfügung, mittels dessen jede auf der Blockchain zur Verfügung gestellte Information von den anderen Teilnehmern verifiziert wird. Dies führt zum einen dazu, dass eingestellte Informationen in faktischer Hinsicht allen beteiligten Unternehmen zur Verfügung stehen. Zum anderen wird ihre Authentizität über den Konsensmechanismus sichergestellt. Letzteres ist geeignet, ein gegenseitiges Vertrauen sicherzustellen, das sich schließlich auch in wettbewerblicher Hinsicht als relevant erweisen kann. Wenn nämlich ein über die Blockchain abgesichertes Vertrauen in den Bestand der jeweiligen Information besteht, kommt dies der sternförmigen Koordinierung im Sinne einer Hub-and-Spoke-Konstellation gleich. Die vorher faktische oder rechtliche Koordinierung durch ein Unternehmen wird auf einer technisch-logischen Ebene abstrahiert.

2.3 Algorithmen und autonome Systeme

2.3.1 Einsatzmöglichkeiten von Algorithmen

Algorithmen stellen eine wesentliche Grundlage heutige Entscheidungsfindung dar. Auch in Blockchain-Technologien werden algorithmische Regeln verwendet. Sie stellen Anwendungen dar, die Aufgaben nach vorgegebenen Mustern ausführen. In der Praxis können Algorithmen vor allem zur Automatisierung bisher durch andere technische Vorgänge oder menschliches Verhalten abgebildete Maßnahmen herangezogen werden. Dabei können sie einerseits autonom durch ein Unternehmen verwendet werden. Dies ist im Zusammenhang mit dem Kooperationsverbot unbedenklich. Lediglich eine kartellrechtliche Untersuchung unter dem Gesichtspunkt des Marktmachtmissbrauchs kommt in Betracht, zum Beispiel wenn ein marktbeherrschendes Unternehmen Algorithmen zu Preisanpassungen aufgrund seiner wettbewerblichen Handlungsspielräume nutzt.[12]

[12] *Künstner/Franz*, K&R 2018, S. 688.

2.3.2 Koordinierung durch Algorithmen

Werden Algorithmen zur wettbewerblichen Verhaltenskoordinierung mehrerer Unternehmen verwendet, so gelten auch hier die herkömmlichen Grundsätze der Hub-and-Spoke-Konstellation.[13] Allerdings gibt es keinen Hub in Form eines Unternehmens. Ebenso wie bei der Blockchain-Technologie erfolgt eine externe Koordinierung auf einer logischen Ebene.

3 Abhilfemaßnahmen

Für die kartellrechtliche Praxis ergeben sich hier verschiedene Problemstellungen.[14] Zum einen ist noch ungeklärt, inwiefern Unterlassungsverfügungen sich in Konstellationen vollziehen lassen, bei denen technisch notwendigerweise auch ohne eine kartellrechtlich relevante Beteiligung die Mitwirkung anderer die Technologie nutzender Unternehmen erforderlich ist. Bei der Blockchain zum Beispiel könnte eine Beseitigung ausgetauschter Informationen nicht in Betracht kommen, wenn dabei auch Unternehmen mitwirken müssten, die an dem eigentlichen Informationsaustauch nicht beteiligt waren. Auch in praktischer Hinsicht könnte sich das Bedürfnis nach einer möglichst ausgewogenen Compliance-Lösung ergeben.

So wie die dargestellten Technologien ein wettbewerblich nicht gerechtfertigtes Vertrauen zwischen den Unternehmen herstellen und damit den Geheimniswettbewerb aushebeln, könnte die Lösung darin liegen, genau dieses Vertrauen zu verhindern.[15] Die Unternehmen wären dann weiterhin dem allgemeinen Geheimniswettbewerb ausgesetzt. Da in bestimmten Situationen, wie zum Beispiel bei der bilateralen Vertragsabwickelung oder dem Austausch sicherheitsrelevanter Spezifikationen, die Preisgabe von Informationen erforderlich ist, könnten diese Situationen in technischer Hinsicht in die jeweilige Technologie implementiert werden. So könnte es bei der Blockchain einen Konsensmechanismus über den lediglich bilateralen Informationsaustausch und die allgemeine Verhinderung eines allgemeinen Austauschs geben. Algorithmen oder autonome Systeme könnten so

[13] *Dohrn/Huck*, DB 2018, S. 173.

[14] *Ylinen*, NZKart 2018, S. 19; *Künstner/Franz*, K&R 2018, S. 688; *Göhsl*, WuW 2018, S. 121; *Dohrn/Huck*, DB 2018, S. 173.

[15] *Louven/Saive*, NZKart 2018, im Erscheinen; *Vezzoso*, Competition by Design, SSRN v. 29.11.2017.

ausgestaltet werden, dass sie lediglich in den engen erlaubten Grenzen koordinieren, die in der Rechtsprechung oder Behördenpraxis entwickelt werden.[16] Die Entscheidungspraxis würde also algorithmisiert.

Literatur

Dohrn, Daniel/Huck, Linda: Der Algorithmus als „Kartellgehilfe"? – Kartellrechtliche Compliance im Zeitalter der Digitalisierung, DB 2018, S. 173–179.

Göhsl, Jan-Frederick: Algorithm Pricing and Article 101 TFEU, WuW 2018, S. 121–125.

Hainz, Josef/Benditz, Robert: Indirekter Informationsaustausch in Hub and Spoke-Konstellationen – Der Teufel steckt im Detail, EuZW 2012, S. 686–690.

Immenga, Ulrich/Mestmäcker, Ernst-Joachim (Hrsg.): Wettbewerbsrecht, Kommentar zum Europäischen Kartellrecht, 5. Aufl., München 2012.

Künstner, Kim/Franz, Benjamin: Preisalgorithmen und Dynamic Pricing: Eine neue Kategorie kartellrechtswidriger Abstimmungen?, K&R 2018, S. 688–693.

Loewenheim, Ulrich/Meessen, Karl Matthias/Riesenkampff, Alexander/Kersting, Christian/Meyer-Lindemann, Hans Jürgen (Hrsg.): Kartellrecht, Kommentar, 3. Aufl., München 2016.

Louven, Sebastian/Saive, David: Antitrust by Design – Das Verbot wettbewerbsbeschränkender Abstimmungen und der Konsensmechanismus der Blockchain, NZKart 2018, im Erscheinen.

Vezzoso, Simonetta: Competition by Design, SSRN v. 29.11.2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2986440 (abgerufen am 2.7.2018).

Ylinen, Johannes: Digital Pricing und Kartellrecht, NZKart 2018, S. 19–22.

[16] BKartA, Fallbericht v. 29.5.2018 - B9-175/17, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2018/B9-175-17.pdf?__blob=publicationFile&v=4 (abgerufen am 29.6.2018).

GERMAN SUPREME COURT ON LICENSING AGREEMENTS: A NEW UNDERSTANDING OF THE LEGAL NATURE OF LICENSING CONTRACTS

Dr. Anselm Brandi-Dohrn, maître en droit, CLP

Von BOETTICHER Rechtsanwaelte PartG mbB, Berlin
abrandi-dohrn@boetticher.com

Summary

The German Supreme Court – developing a new view on the legal nature of license grants as not being merely contractual rights but rights similar to a right in rem – has decided that sublicenses shall remain unaffected by the termination of the underlying principal license. This has been held true even in cases where the principal license had been rightfully terminated by the licensor for breach of the licensee. In any license agreement which is either subject to German law or relates to the territory of Germany (even if only in part, e.g. a license for the territory of the entire EU) the consequences of this new jurisprudence will have to be considered.

1 The traditional Approach of German Courts

German law, in the tradition of Roman legal thinking, has structured its contract law provisions in chapters, starting with provisions relating to all types of contracts, followed by several chapters dealing with specific types of contracts – like contracts for sale, for rent, for services etc. Notwithstanding the enormous commercial relevance of licensing for the German economy, the German Civil Code ("BGB") does not provide for a specific chapter for licensing contracts. Even though it would have been possible to subject licensing agreements to the contract type of legal lease ("Rechtspacht"), the German Supreme Court ("BGH") – following older decisions by the Reichsgericht – has always held that a licensing contract is a contract *sui generis*, that means it does not belong to the standard types of contracts set forth in the BGB but a solution has to refer rather to the general rules of contract law.

This approach gave the courts a lot of liberty in assessing and resolving legal issues relating to license agreements – an approach which in my opinion is preferable over the more rigid approach of the civil law contract types as practice has developed a broad variety of licensing agreements with totally different economic background, economic impact for the contract partners and distribution of risks.

The freedom the courts enjoy in this respect has, however, resulted in recent years in a series of decisions which query the contractual nature as such of licensing contracts. As the German economy is strongly relying on IP and licensing, licensing contracts in an export-oriented country like Germany are an important tool of international trade. It is, therefore, of highest importance to understand the differences in the German approach to licensing contracts to avoid fundamental misconceptions when negotiating or executing an international licensing contract.

2 Is a License Contract a Contract or a right in rem?

2.1 The Nemo dat quod non habet rule

A first fundamental principle of contract law is that a contract results in rights and obligations exclusively for the contractual partners – except if the contractual parties in their contract grant rights to a third party (contract in favor of third parties – Vertrag zu Gunsten Dritter). A second fundamental principle dating back to the Roman empire is that nobody can grant more rights to someone else than he has himself (*Nemo* dat *quod* non *habet* – rule: *nemo plus juris transferre potest quam ipse habet*).

When it comes to chains of licenses – licensor grants a license, the licensee then grants a sublicense to the sub-licensee –, these principles result in the sublicensee being dependent upon the continuing existence of the principal license: If the principal license agreement is invalid or is terminated, the licensee loses its right of use and therefore cannot continue to convey a right of use to the sublicensee. The sublicensee – even if acting in good faith and not being in breach with its obligations under the sublicense agreement – is not entitled to use the IP it has licensed. Clearly, it has a claim for damages against the faulty licensee – but such claim may either be utterly worthless (for the licensee being insolvent) or may not repair its losses entirely as the right of use might be of crucial importance to him.

2.2 BGH „Reifen Progressiv“, „Take Five“, „M2 Trade“

Starting in 2009, the German Supreme Court in a first series of decisions started to nibble away these basic principles in case of licensing contracts – with the explicit assumption that under normal circumstances the faultless sublicensee should not bear the risk of contractual breaches relating to the principal license agreement. Even if all these decisions relate exclusively to trademarks and copyrights (as well works of art and software licenses) – and there hasn't been any decision of the patent law senate yet – the Supreme Court has stated that it has aligned its position with the patent law senate. Therefore – and notwithstanding very critical voices from scholars

in patent law – we must assume that this position is applicable to any type of IP right in Germany.

2.2.1 BGH „Reifen Progressiv“[1]

In the “Reifen Progressiv” case the claimant had developed a software called “Reifen Progressiv”. It had granted an exclusive license to a company A (= licensee) enabling it to market and modify the software. Company A then granted non-exclusive licenses to third parties, including a company B (= sublicensee) to use the software. When company A went bankrupt, the claimant revoked the principal license (pursuant to sect. 41 German Copyright Act, allowing for withdrawal of an exclusive license in case the licensee doesn’t make use of such license). The claimant then sued company B for copyright infringement as its sublicense agreement couldn’t entitle it any more to a derivated right of use.

The court held that „a non-exclusive right of use derived from an exclusive right of use shall not expire if the exclusive right of use terminates due to an effective recall based upon non-exercise (Section 41 UrhG).“ While the Supreme Court already voiced its fairness argument to protect the sublicensee, for the licensor not too much was lost – after having terminated the exclusive license, it was free to grant further non-exclusive or another exclusive license to continue to exploit its copyright (such later licenses having to respect, however, the existing non-exclusive licenses).

2.2.2 BGH „Take Five“[2]

Take Five is a world-famous jazz tune composed by Paul Desmond. A Californian publishing house (claimant) held the exclusive and worldwide rights of use since the 1960ies. In a first subpublishing agreement it granted an exclusive sublicense for Europe to company A, which in turn granted a sub-sub-license (equally exclusive) for Austria and Germany to company B, the later defendant. In a settlement agreement the Californian claimant agreed with company A (i) to terminate the main sublicense agreement and (ii) that such agreement would terminate as well any and all sub-sub-license agreements company A had agreed to – including the one with company B, covering Germany and Austria.

In the Take Five decision the Supreme Court expands its Reifen Progressiv-findings to a general principle: „The expiry of the main license in general does not result in the expiry of the sublicense if the main licensee has granted the sublicensee an exclusive right of use against participation in the license revenues and the main license expires for other reasons (here:

[1] BGH, dec. of 26.3.2009 – I ZR 153/06, GRUR 2009, 946 – Reifen Progressiv.

[2] BGH, dec. of 19.7.2012 – I ZR 24/11, GRUR 2012, 914 – Take Five.

amicable cancellation of the main license agreement) – not only in case of a recall due to non-exercise."

The rationale for this finding is (i) that under normal circumstances the sublicensee is more worthy of protection than the licensor (he could have abstained from granting a license – or agreeing to an amicable settlement to the detriment of the sublicensee) and (ii) that the legal principle of protection of the licensee against transfer of the IP right to a new owner ("Sukzessionsschutz") has to be understood to protect the (sub-)licensee also against any activities affecting the principal license agreement.

2.2.3 BGH „M2 Trade"[3]

In the same-day „M2 Trade" decision the Supreme Court has marked a (preliminary?) final position: The prior decisions always comprised a small loop hole, as the Supreme Court pointed out that only in „general" it deemed the sublicensee to be worthy of protection and hence upheld the sublicense agreement after termination of the principal license.

"M2 Trade" might have been a case allowing the Supreme Court to delineate its new jurisprudence and point out cases where the sublicensee would not be worthy of protection – and thus avoid unforeseen and unwanted consequences of its new jurisprudence.

"M2 Trade" is a software based on a standard software program which the later claimant had adapted to the needs of the "M-Group". The claimant had licensed this software to one of the group companies ("M-NetCom") for further sublicensing within the entire M-group. When the licensee M-NetCom ceased to pay its license fees, the claimant rightfully terminated the principal license agreement for breach of contract and raised an action against another company of the M-group which continued to use the software. Here the sublicensee – as affiliate – was closely linked to the licensee and the licensee was clearly not worth protecting; the Supreme Court, however, held that even in this arrangement the sublicensee should be protected and upheld the sublicense.

2.3 The - Unforeseen - Consequences for Licensing Contracts

Most other legal systems in the world continue to interpret licensing contracts as regular contracts, which results in a sublicense grant to automatically terminate in case the principal license grant is terminated. In the understanding of the German Supreme Court, however, a license grant has to a certain extent an *erga omnes* quality, it carves out a part of the IP, which carved out part then may lead a "legal life" of its own.

[3] BGH, dec. of 19.7.2012 – I ZR 70/10, I ZR 24/11, GRUR 2012, 916 – M2 Trade.

Scholars have already severely criticized the new jurisprudence and have proposed alternative solutions to protect the respective participants in a licensing chain: *McGuire/Kunzmann*[4] favor a step-in right of the licensor into the sublicense agreement if the principal license is terminated, applying by analogy § 565 BGB (a stipulation whereby the landlord becomes a party to a subrental agreement in case the principal agreement is terminated). The drawback of this proposal is that the licensor may find itself subject to sublicense terms which it is unable to fulfill (e.g. obligations of the licensor of a pharmaceutical patent to provide certain additional data or regulatory approvals held by the former licensee). *Karl/Melullis* have proposed exactly the opposite solution – the sublicensee steps into the principal license agreement in lieu of the licensee.[5] This solution, however, cannot rely on any provision of German civil law – and it may unfairly favor the sublicensee who may find itself granted a much broader license or terms more advantageous that it had negotiated originally with the licensee. However, when negotiating a license agreement, an explicit contractual clause providing for such step-in rights might be an acceptable compromise.

In my opinion, the Supreme Court would have resolved better the cases before him by relying on the standard approach of the law of contracts and rather interpreting the respective contracts as allowing implicitly for the survival of the sublicense upon termination of the principal license – a solution which English[6] and Swiss[7] courts have already endorsed. This way is, however, not viable in cases like "Take Five" where the contract explicitly provided for termination of any sublicenses.

The new jurisprudence has an enormous impact on contract drafting, as well on a national and international level.

a) A licensor granting an exclusive license and allowing sublicensing might find himself in an awkward situation when he wants to terminate the principal license agreement: If the licensee in turn has granted an exclusive sublicense (e.g. for a specific country where licensee is not able to market the licensed products itself), this sublicense would remain valid after termination of the principal license, thus blocking the licensor from

---

4 *McGuire/Kunzmann*, GRUR 2014, p. 28 (30 ss).

5 *Karl/Melullis*, GRUR 2016, p. 755 (762).

6 High Ct., dec. of 13.2.2013 – EWHC 228 (Ch.) – VLM Holdings Ltd. v. Ravensworth Digital Services Ltd. (license agreement interpreted that sublicense survived termination of principal license).

7 Swiss Supr. Ct., dec. of 15.9.2016 – 4A_317/2016, (sub D. 2.5): while a license is merely a contract, it may be interpreted as allowing the granting of sublicenses in the form of an usufruct in rem (dinglicher Nießbrauch), which usufruct would survive the termination of the principal license.

exploiting his IP in such country. Economically, the licensor thus may lose its IP even if he has terminated rightfully the license grant.

Presently, there is only one safe way to protect the interest of the licensor: The principal license must exclude the right of licensee to further sublicense. In case of an exclusive license such stipulation is even more important as courts have held that an exclusive license normally must be interpreted as entitling the licensee to grant sublicenses.[8] In several cases, such a limitation will not be acceptable to the licensee; in this case the only viable compromise would be to subject sublicensing to the prior agreement of licensor who in turn engages to agree to such sublicense if the sublicensing agreement explicitly provides for automatic termination in case of termination of the principal agreement. Any clause falling short of requiring the explicit consent of the licensor will not protect licensor's interest – namely a clause in the principal license merely obliging the licensee to provide for automatic termination of the sublicense agreement in case of termination of the principal license is not sufficient: If licensee breaches his obligation by granting an unconditioned sublicense, this sublicense would stay in place if the licensor decides to terminate the principal license for breach.

b) On a second level, the question remains whether the licensor would at least be entitled to collect the sublicense fees which the sublicensee continues to pay under its valid sublicense to the licensee. Clearly, it would seem unfair if the licensee – who doesn't have a right of use any more after termination of the principal license – could retain the proceeds of the sublicense. As the licensor is the owner of the IP, such proceeds should rightfully belong to him – but the licensor does not have any contract with the sublicensee under which licensor would be entitled to claim such royalty payments. The Supreme Court saw this inherent unfairness of its new jurisprudence and pointed out that under the German Civil Code (BGB) there is a claim which licensor could rely on – the principle of "unfair enrichment" (§ 812 BGB). Thus, licensor can claim the proceeds from licensee, as licensee is unfairly taking advantage of licensor's IP to collect royalties from sublicensee.

This solution does not work, however, if the licensee is insolvent – which will be the principal reason for licensee not to pay the license fees and for licensor to terminate the principal license. In such case, the appointed receiver is entitled to collect the sublicense fees and distribute them evenly among the creditors – which means that in most cases the licensor will only receive a small percentage of the license fees it would be entitled to. To date

[8] BGH, dec. of 7.11.1952, GRUR 1953, 114 (118) – Reinigungsverfahren.

there hasn't been any court decision addressing this issue or proposing alternative solutions which would better protect the licensor.

c) Last but not least, notably the "M2 Trade" case indicates a way to a further, rather disturbing, negotiation strategy which the Supreme Court most likely did not consider either. If a sublicense remains valid even in cases of intra-group licensing, then the following scheme might be pursued by licensee: Assume that licensee has not been able to negotiate a license fee acceptable to licensee. Licensee then could set up a financially weak new company belonging to licensee who would take out the license, allowing (at least) for intra-group sublicensing – a construct which today is quite common for various reasons, notably to minimize tax exposure. Licensee then grants a sublicense (with a sublicensing fee equaling the license fee which licensee would have found acceptable) to the other group companies; then licensee immediately stops any payments, thus triggering the termination of the principal license. The licensor then would continue to receive (pursuant to § 812 BGB) the sublicense payments, but these would only amount to the sums which the licensee prior hadn't been able to negotiate with licensor. Under Civil law, licensor would continue to have a claim for damages against the licensee for breach of contract, and this claim would cover the agreed license fees – but licensor couldn't risk claiming such higher amount as licensee then might go bankrupt and licensor wouldn't even receive the lower sublicense fees. In consequence, the position of a shrewd licensee is substantially better under the new jurisprudence.

2.4 When is this Jurisprudence applicable in Romania?

This jurisprudence wouldn't be of much interest in the context of a German-Romanian workshop if the jurisprudence were limited to German licensing contracts. On an international level, however, it is not so clear that this jurisprudence doesn't also affect licensing contracts which at first sight don't have much connection to Germany:

Most conflict of law principles – including the Romanian – refer to the law chosen by the parties as the law applicable to contractual rights and obligations. However, several countries (e.g. Germany) subject the validity of a license with respect to third parties to the law of the country of protection.

This means that in all instances where either

- the license agreement is subject to German law, or
- the validity of a (sub-)license in Germany is concerned

German law might be applicable. If, e.g. a Romanian licensor grants an exclusive license to a UK company for the entire territory of the European

Union, then a sublicense which the UK company later grants to a German sublicensee will be subject to the above jurisprudence.

3 "Real" and "not so real" Licenses?

The traditional understanding is that there is only one type of licensing contract. The content and scope of the rights of use granted to the licensee may vary, but regardless of the degree of limitations such a contract contains, it still remains a licensing agreement and the principles which the law and jurisprudence have attributed to this type of contract apply equally to all license grants.

3.1 The new Distinction between "license" and "permission"

New jurisprudence of the German Supreme Court indicates, however, that contracts granting rights of use may come in (at least) two different categories – notably the "classic" license has to be differentiated from a mere "permission" (schuldrechtliche Gestattung). The latter quite often appears in the context of an author granting rights of use on the internet (e.g. by uploading a photo onto his facebook profile this person allows all facebook users to download (= copy) this photo onto their client computer),[9] but recently this concept has been extended to rights of use granted by the owner of a company name and/or trademark.[10]

The Supreme Court has deduced several consequences from this differentiation:

- Only a real license is opposable to an eventual new owner of the licensed IP right (so-called "Sukzessionsschutz"), whereas the permission creates rights only against the contractual partner.
- Consequently, while the rights of use under a real license may be transferred to another party, this is not possible in case of a contractual permission, where any transfer of the contract requires the consent of the grantor.
- While a licensor under German law assumes (at least) full liability for the existence of the right at the time the license is granted, a person granting a mere permission is not liable for any deficiency in title with respect to the IP rights the permission relates to.

[9] BGH, dec. of 19.10.2011 – I ZR 140/10, GRUR 2012, 602 – Vorschaubilder II: A person uploading photos onto the internet declares its consent to all uses which are common for internet users.

[10] BGH, dec. of 27.3.2013 – I ZR 93/12, GRUR 2013, 1150 – Baumann; BGH, dec. of 21.10.2015 – I ZR 173/14, ZIP 2016, 40 (43) – EcoSoil.

- On the other hand, only in a real license agreement the principle applies that any acts of use of the licensee that lead to the acquisition of additional rights (e.g. a trademark right which results from the actual use in commerce of such trademark) are exclusively to the benefit of the licensor – which means that upon termination of the license, any such rights will be deemed accrued with the licensor. In contrast, in a permission contract, the person making use of such permission would acquire rights of its own which it may oppose even to the owner of the IP right granted when the permission is terminated.[11]
- Following general principles on the burden of proof, the licensee must prove that a real license agreement had been agreed upon and not merely a permission. The Supreme Court has decided that such evidence can only be given by some written deed.[12] As German law in no place requires the written form for license agreements, the Supreme Court couldn't require a proper written form, but admitted also other written evidence like a protocol of a meeting of all affected parties.

3.2 The Practical Consequences

In the area of copyright law, the distinction between a "real" license agreement and a mere permission can be based upon § 29 par. 2 German Copyright Act, which provides that as well rights of use (= real licenses) may be granted as "contractual permissions" – and most probably the Supreme Court intended to extend this principle to other forms of IP rights. However, even in copyright law § 29 par. 2 in the past hadn't played any substantial role as the understanding was that people granting rights of use in general want to agree to a real license, not only a simple permission.[13]

In the light of the new jurisprudence this presumption will have to be reconsidered, as in all cases of non-written agreements the parties then would be presumed to have agreed to an invalid real license agreement. It is, however, another principle in German jurisprudence that contracts should in doubt be interpreted in a way that they remain a valid and binding agreement.

However, notably within groups of companies, IP rights quite often are granted only implicitly – as an affiliate company belongs to the same group of companies one simply supposes that it shall (and therefore is entitled)

[11] Namely with respect to trademarks this may result in the awkward situation that the former owner of a company name having allowed use of such name to another company may find itself enjoined from using this company name after terminating the permission contract.

[12] BGH, dec. of 21.10.2015 – I ZR 173/14, ZIP 2016, 40 (43) – EcoSoil.

[13] *Nordemann*, in: Fromm/Nordemann, Urheberrecht, § 29 note 24.

to use e.g. the same company name. The above cases show what this may mean in case such affiliate either becomes insolvent or is sold off following a divestment decision: Without a written license agreement such company may be entitled to continue to use trademarks and/or company names even if it does not belong to the group anymore. This notably may be an awkward situation if the affiliate has been bought by a competitor.

Literature

Karl, Christian/Melullis, Klaus-Jürgen: Grenzen des Sukzessionsschutzes bei patentrechtlichen Unterlizenzen, GRUR 2016, S. 755-763.

Nordemann, Axel/Nordemann Jan Bernd (Hrsg.): Urheberrecht: Kommentar zum Urheberrechtsgesetz, zum Verlagsgesetz und zum Urheberrechtswahrnehmungsgesetz, 11. Aufl., Stuttgart 2014.

McGuire, Mary-Rose/Kunzmann, Jens: Sukzessionsschutz und Fortbestand der Unterlizenz nach „M2Trade“ und „Take Five“ – ein Lösungsvorschlag, GRUR 2014, S. 28-35.

ELEKTRONISCHE VERTRÄGE IM RUMÄNISCHEN RECHT

RAin Michaela Braun-Noviello

Rechtsanwaltskanzlei Braun-Noviello, Heidelberg

1 Einführung

Der rumänische IT-Markt erfuhr in den letzten sechs Jahren eine rasche Entwicklung. Der Gesamtumsatz der rumänischen IT-Unternehmen erreichte 2017 fünf Milliarden EUR, wobei das IT-Segment (inkl. Kommunikationstechnologie) im Gesamtkontext der Nationalwirtschaft 6 % von BIP übersteigt.[1] Die Anzahlt der IT Unternehmen auf der Nationalebene ist in der Zeitspanne 2011-2017 von 9.823 auf ca. 17.000 gestiegen.

Beginnend mit Februar 2018 sind Angestellte von IT-Unternehmen, deren effektive Tätigkeit im IT-Bereich („in Informatik spezialisierte Angestellte") liegt, von der Einkommensteuer für das Einkommen aus dieser Tätigkeit befreit.[2] Diese Steuerbefreiung betrifft auch Angestellte ohne Studienabschluss, die aber Studenten einer Fachuniversität sind und deren berufliche Tätigkeit im Bereich der kreativen Software-Entwicklung liegt. Somit versucht der rumänische Gesetzgeber durch steuerliche Begünstigungen die Entwicklung von Software in Rumänien als Basis einer Informationsgesellschaft zu fördern.

Bezüglich der Entwicklung des E-Commerce in Rumänien ist festzuhalten, dass nach den offiziellen Statistiken des Nationalinstituts für Statistik, der Online-Einkaufswert 2017 ca. 2,8 Milliarden EUR und somit 40 % mehr als 2016 erreichte.[3]

Dem letzten UNO-Bericht (UN Department of Economic and Social Affairs) gem. ist die Bevölkerung Rumäniens von 19,4 Millionen im Jahr 2016 auf 19,1 Millionen im Jahr 2017 gesunken. Davon sind 11 Millionen Internetnutzer mit einer mobilen Internetnutzung von 85 %.

Der Online-Einkaufswert in Höhe von 2,8 Milliarden EUR bezieht sich lediglich auf E-Tail (körperliche Sachen, die online bestellt worden sind) ohne Dienstleistungen und Zahlungen oder Buchungen von Reisen, Flügen, Eventstickets usw. zu berücksichtigen.

---

1 ZF Business Hi-Tech - www.zf.ro.

2 Idem, Ordinul comun nr. 1168/2017, Monitorul Oficial, Partea I, nr. 52 din 18 ianuarie 2018.

3 www.insse.ro; www.gpec.ro.

Die Steigerung des Einkaufsumsatzes um 40 % von einem Jahr auf das andere ist eine der größten Entwicklungen auf der europäischen Ebene. Auch wenn der Wert im E-Commerce im Zusammenhang des rumänischen Retail-Marktes lediglich 5,6 % erreicht hat und somit im Vergleich zu den ökonomisch starken EU-Ländern noch sehr niedrig ist, zeigt diese Steigerung das riesige Potenzial auf dem rumänischen E-Commerce Markt sehr deutlich.

2 Gesetzgebung

Derzeit gibt es in Rumänien gesetzliche Regelungen (Gesetze, Regierungsverordnungen, Ministerverordnungen, Anwendungsnormen) in folgenden IT-Bereichen: E-Commerce; Urheberrecht; Elektronische Dokumente; Elektronische Zahlungen; Online-Werbung; Schutz des Privatlebens und Datenschutz; Kriminalität im Internet; Elektronische Kommunikation; Videodienstleistungen im Internet.

- Die wichtigsten, gesetzlichen Vorschriften im IT-Recht sind:
- Das Gesetz über den elektronischen Handel Nr. 365/2002
- Die Regierungsverordnung Nr. 130/2000 über den Verbraucherschutz
- Das Gesetz Nr. 193/2000 bezüglich der rechtswidrigen Klausen in den Verbraucherverträgen
- Das Gesetz Nr. 329/2006 über das Urheberrecht
- Das Gesetz Nr. 455/2001 über die elektronische Signatur
- Das Gesetz Nr. 589/2004 über die elektronische Tätigkeit der Notare
- Das Gesetz Nr. 135/2007 über die elektronische Archivierung von Dokumenten
- Das Gesetz Nr. 148/2012 über die Speicherung von elektronischen Handelsoperationen
- Das Gesetz Nr. 127/2011 über die elektronische Währung
- Das Gesetz Nr. 158/2008 über die irreführende und unerlaubte Werbung im Internet
- Das Gesetz Nr. 148/2000 über die Werbung
- Das Gesetz Nr. 82/2012 über die Aufnahme und Speicherung von Daten durch Dienstleiter und Verarbeitung von personenbezogenen Daten

Eine gesonderte, gesetzliche Verankerung der IT-EDV-Verträge gibt es derzeit nicht. Abhängig vom Gegenstand und Zweck des jeweiligen Vertrags wird in der Regel allgemeines Kaufrecht (Sachkauf), Werkvertragsrecht oder Nutzungsrecht (Mietrecht) angewendet. Eine Unterordnung der

Softwareüberlassungsverträge unter der Kategorie der Lizenzverträge oder deren Einstufung als Verträge sui generis wurde in der Fachliteratur auch oft diskutiert, durch die Rechtsprechung dennoch nicht einheitlich angenommen. Auch der Gesetzgeber hat in das neue Bürgerliche Gesetzbuch (NCC) keine neuen Vertragsarten definiert, so dass die jeweilige Natur der verschiedenen elektronischen Verträge sich abhängig von deren Inhalt nach den klassischen Vertragsarten richtet.

Durch die rasante Entwicklung des IT-Marktes und besonders durch das Outsourcing großer IT-Unternehmen nach Rumänien nahm die Bedeutung der IT-Verträge in der Praxis sehr stark zu und die Rechtsdienstleister haben sich entsprechend anpassen müssen und sich im Bereich des IT-Vertragsrechts spezialisiert.

3 E-Commerce

Im Bereich des E-Commerce hat Rumänien die EU-Richtlinie 2000/31/EG in das Gesetz Nr. 365/2002 übernommen und fast vollständig abgeschrieben.

Es bleibt nun abzuwarten, wie der rumänische Gesetzgeber die neue Geoblocking-Verordnung der EU, die am 22.3.2018 in Kraft getreten ist, in das Nationalrecht umsetzen wird.

Gem. Art. 2 des rumänischen Gesetzes über E-Commerce ist das Ziel dieser Norm die Festlegung der Voraussetzungen und des Rahmens für die Sicherstellung des freien Verkehrs der Dienste der Informationsgesellschaft. Art. 1 Nr. 1 dieses Gesetzes definiert den elektronischen Handel als „jene Dienstleistung, die auf dem elektronischen Wege erfolgt und folgende Kriterien erfüllt:

- die Erlangung eines materiellen Vorteils wird bezweckt, der üblicherweise dem Anbieter durch die Leistung des Empfängers zuwächst;
- Anbieter und Empfänger befinden sich nicht zur gleichen Zeit am gleichen Ort;
- die Übermittlung von Informationen erfolgt auf Verlangen des Empfängers.

Das neue rumänische Bürgerliche Gesetzbuch (NCC) sieht in Art. 1166 vor, dass der Vertrag eine Willensübereinstimmung zwischen zwei oder mehreren Parteien ist, mit dem Ziel, ein Rechtsverhältnis zu schaffen, ändern oder beenden. Diese geforderte Willensübereinstimmung bedeutet eine Kommunikation zwischen den Parteien, also die Äußerung ihres Willens. Die Art dieser Willensäußerung bestimmt die Vertragsform. Art. 1179 Abs. 2 NCC sieht vor, dass, in den Fällen, in denen das Gesetz

eine bestimmte Form des Vertrags vorsieht, ist diese unter der für die Nichteinhaltung der vorgeschriebenen Form vorgesehenen Sanktion einzuhalten."

Art. 1240-1245 NCC beinhalten spezielle Regelungen bezüglich unterschiedlicher Vertragsformen, darunter wird auch die elektronische Form ausdrücklich vorgesehen.

Anstatt eines verbalen oder auf dem Papier festgehaltenen Konsenses wird ein Vertrag in elektronischer Form durch Übermittlung von Nachrichten auf einem elektronischen Support abgeschlossen.

Aus diesem Grund besteht zwischen dem elektronischen Vertrag und dem mündlich oder schriftlich abgeschlossenen Vertrag mit dem gleichen Inhalt kein Unterschied bezüglich der Rechtsnatur. Sodann sind in elektronischer Form abgeschlossene Verträge keine Verträge sui generis.

3.1 Unterteilung der elektronischen Verträge

Eine von der klassischen abweichenden Unterteilung der elektronischen Verträge erfolgt nach folgenden Kriterien:

- Qualität der Vertragsparteien,
- Entfernung der Vertragsparteien und
- Erfüllungsmodalität.

3.1.1 Das Kriterium der Qualität der Vertragsparteien.

- Kaufmann – engl. „business" – abgekürzt B
- Verbraucher – engl. „consumers" – abgekürzt C
- Körperschaft öffentlichen Rechts – engl. ,,government" – abgekürzt G

Unter Anwendung dieses Kriteriums ergibt sich folgende Unterteilung der elektronischen Verträge:

- „business to business" oder im Internetjargon B2B, wobei der erste Buchstabe immer diejenige Partei bezeichnet, die die Vertragsinitiative hat.
- „business to consumers" oder B2C mit der Variante B2B2C, die zu bedeuten hat, dass der Produkthersteller die Ware über einen kaufmännischen Vermittler (Vertrieb) an den Verbraucher liefert.
- „government to business" oder G2B, wobei es sich um öffentliche Auftragsvergabe handelt.

Diese Unterteilung erlangt eine besondere Bedeutung im Bereich des Verbraucherschutzes.

3.1.2 Das Kriterium der Entfernung zwischen den Vertragsparteien

Mit „Entfernung" wird die juristische Entfernung gemeint, also die Zeitdauer, die dafür notwendig ist, dass die Willenserklärung einer Partei bei der anderen Vertragspartei ankommt. Aus dieser Perspektive lassen sich die elektronischen Verträge in zwei Kategorien teilen:

- zwischen Anwesenden (Chat-Dienste)
- zwischen Abwesenden – die Willenserklärung einer Partei gelangt zur Kenntnis der anderen Partei mit einem gewissen Zeitunterschied.

Diese Unterteilung ist für die Problematik der Annahme eines zeitlich begrenzten Angebots von großer, praktischer Bedeutung.

3.1.3 Das Kriterium der Erfüllungsmodalität

Die Erfüllungsmodalität der elektronischen Verträge hängt im Wesentlichen von der Natur des Vertragsgegenstandes ab. Alle Güter, die (durch Digitalisierung) eine materielle Form annehmen können sind durch ein Kommunikationsnetz in elektronischer Form übertragbar. Beispielsweise kann ein Phonogram in digitalisierter Form vom PC des Verkäufers auf den PC des Käufers übersendet und dort heruntergeladen werden. Das Phonogramm kann aber auch auf einem materiellen Support (CD) verkauft werden und die Vertragserfüllung kann in diesem Fall nicht auf dem elektronischen Weg erfolgen. Da der Gegenstand des Vertrags ein körperliches Gut ist, kann die Lieferung nur außerhalb des virtuellen Raumes erfolgen. Unter Anwendung dieses Kriteriums gibt es Verträge:

- mit online Ausführung
- mit offline Ausführung.

Bei dieser Unterteilung wird lediglich der Gegenstand der vertraglichen Hauptflicht als Kriterium herangezogen. Neben- oder korrelative Pflichtenwie z.B. Preiszahlung werden auch bei dem elektronischen Vertrag mit offline Ausführung weiterhin auf dem elektronischen Weg erfüllt.

In der Praxis wird sehr oft eine gemischte Erfüllungsform eines Vertrags auftreten, die zu einer Anpassung der jeweiligen, elektronischen Verträge und somit zu einer besonderen, am elektronischen Markt angepassten Vertragsgestaltung führt. Dennoch behält der jeweilige elektronische Vertrag seine klassische Natur und wird nicht zu einem Vertrag sui generis.

3.2 Besonderheiten der elektronischen Verträge

3.2.1 Einschränkung der Verhandlungsfreiheit

Eine Besonderheit der elektronischen Verträge besteht darin, dass der Anbieter einen Standardvertrag zur Annahme durch unbestimmte oder nach im Vertrag genannten Kriterien bestimmte Personen im virtuellen Raum vorschlägt. Der Empfänger kann in der Regel das Angebot annehmen oder

ablehnen. Der elektronische Vertrag ist somit in der Regel ein Adhäsionsvertrag. Damit ist die klassische Vorvertragsphase der Verhandlungen im Fall der elektronischen Verträge ausgeschlossen. Die vorvertragliche Phase wird bei den elektronischen Verträgen durch die Werbung ersetzt. Dazu werde ich in einem gesonderten Kapitel mehr ausführen.

3.2.2 Vertragsform

Für diejenigen Vertragsarten, wofür das Gesetz eine bestimmte Form ad validitatem, ad probationem oder wegen der Wirkung erga omnes vorsieht, stellt sich die Frage, wie die elektronischen Verträge diese Voraussetzungen erfüllen können.

Die Übereinkommen der Vereinten Nationen über die Verwendung elektronischer Mitteilungen bei internationalen Verträgen sehen unter anderem vor, dass die Rechtswirkung, Gültigkeit und Verbindlichkeit von elektronischen Informationsübersendungen und Verträgen nicht deswegen aberkannt werden dürfen, weil sie in elektronischer Form erfolgt sind (Art. 5 MLEC; Art. 8 CUECIC).[4]

Außerdem verpflichtet auf der europäischen Ebene Art. 9 der EU-Richtlinie 2000/31/EG die Mitgliedstaaten zur Gewährleistung der Gültigkeit und Anwendbarkeit der elektronischen Verträge durch entsprechende Anpassung des Nationalrechtes. Gem. dieser Norm kann der elektronische Vertragsabschluss – also die elektronische Form des Vertrags – nicht zu Aberkennung seiner Gültigkeit wegen Nichteinhaltung der Formvorschriften führen.

Im rumänischen Recht ist die rechtliche Wirkung der auf dem elektronischen Weg abgeschlossenen Verträge im Art. 7 Abs. 1 des Gesetzes Nr. 365/2002 verankert: „die durch elektronische Mittel abgeschlossenen Verträge entfalten alle Wirkungen, die das Gesetz den Verträgen anerkennt, solange die Gültigkeitsvoraussetzungen eingehalten worden sind."

Als Schlussfolgerung ist hier festzuhalten, dass ein auf dem elektronischen Weg abgeschlossener Vertrag, wofür das Gesetz keine zwingende Form für seine Gültigkeit vorsieht, ohne Einhaltung weiterer Voraussetzungen gültig abgeschlossen worden ist.

3.2.3 Nachweis des elektronischen Vertragsabschlusses

Das elektronische Schriftstück und der Nachweis des elektronischen Vertrags werden mangels materieller Form besonderen Schwierigkeiten im Be-

[4] *Tudorache,* Contractul incheiat prin mijloace electronice in reglementarea din Noul Cod Civil, S. 19-20.

weisverfahren ausgesetzt. Außerdem kann der Nachweis eines elektronischen Vertrags durch die gesetzlich vorgesehenen Beweisregeln in den verschiedenen Rechtssystemen erschwert sein.

Im rumänischen Recht unterliegt der Nachweis der elektronischen Verträge und der daraus resultierenden Pflichten dem allgemeinen Verfahrensrecht und dem Gesetz Nr. 455/2001 über die elektronische Signatur.

Ein gesondertes Kapitel über die Beweismittel wurde in der neuen Zivilprozessordnung aufgenommen. Demnach unterliegt der Beweiswert eines elektronischen Schriftstückes der Äquivalenzprüfung bezüglich des Schriftstückes in Papierform und der elektronischen Signatur mit der eigenhändigen Unterschrift. Diese Prozedere führt in der Praxis nicht selten zu Beweisschwierigkeiten. In diesem Kontext gebührt der elektronischen Signatur, die auf der europäischen Ebene eine einheitliche Basis für den wirksamen Abschluss von elektronischen Verträgen schafft, eine wichtige Rolle.

Bis dato haben die meisten EU-Länder die Richtlinie 1999/93/CE über die elektronische Signatur in nationales Recht umgesetzt. Art. 5 Abs. 1 dieser Richtlinie sieht die rechtliche Gleichbehandlung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift. Bezüglich der einfachen, elektronischen Signatur verlangt Art. 5 der Richtlinie, dass die Mitgliedsstaaten deren Zulässigkeit als Beweismittel im Verfahren gewährleisten.

Das Gesetz Nr. 455/2001 beinhaltet eine Aufzählung der Gültigkeitsvoraussetzungen einer elektronischen Signatur, damit sie den gleichen Beweiswert erlangt, wie die handschriftliche Unterschrift auf einem Schriftstück in Papierform. Dabei wird danach unterschieden, ob die Partei, der das elektronische Schriftstück entgegengehalten wird, es anerkennt oder bestreitet. Demnach wird ein elektronisches, anerkanntes Schriftstück auch ohne qualifizierte Signatur den vollen Beweis erbringen, während das nicht anerkannte Schriftstück auch beim Vorhandensein einer qualifizierten oder akkreditierten elektronischen Signatur der Echtheitsprüfung unterworfen werden kann.

3.3 Willensübereinstimmung (Zustimmung zum Standardvertrag)

3.3.1 Vorvertragliche Phase

Im rumänischen Recht ist die Werbung im Allgemeinen durch das Gesetz Nr. 148/2000 über die Werbung und das Gesetz Nr. 158/2008 über die irreführende und unerlaubte Werbung geregelt.

In der Regel wirbt jeder Anbieter von Diensten auf dem elektronischen Markt online mittels einer Webseite, worauf die angebotene Ware und Dienstleistungen in der Absicht, Verträge mit den potenziellen Interessen-

ten abzuschließen, beschrieben werden. Die Online-Vermarktung von Produkten und Dienstleistungen ermöglicht den Anbietern im technischen Sinne ihre Identität zu verbergen und vertragliche Beziehungen zu begründen, ohne den Vertragspartner „kennenzulernen".

Zur Vermeidung rechtsmissbräuchlichen Verhaltens im elektronischen Handel übernahm das Gesetz Nr. 365/2002 alle durch die EU-Richtlinie 2000/31/EG vorgesehenen Pflichten der Online-Anbieter bezüglich der Veröffentlichung von Mindestangaben zur unentgeltlichen und permanenten Feststellung und Prüfung ihrer Identität, also die folgenden allgemeinen Informationen:

a) Name oder Bezeichnung des Anbieters,

b) Wohnsitz oder Gesellschaftssitz des Anbieters,

c) Telefon- und Faxnummer, E-Mail-Adresse und andere Kontaktdaten des Anbieters,

d) Handelsregisternummer oder andere, ähnliche Identifikationsmerkmale,

e) Identifikationsdaten der Aufsichtsbehörde, falls die Tätigkeit des Anbieters einer behördlichen Genehmigung unterliegt,

f) Beruflicher Titel und Name des Staates, in dem der Titel verliehen wurde oder die Berufskammer (Organisation) des Anbieters und ihren Sitz, Angabe der Berufsregeln des Staates, in dem der Anbieter seinen Sitz hat sowie der Zugangsvoraussetzungen, falls der Anbieter eine genehmigungs- oder aufsichtspflichtige Tätigkeit entfaltet,

g) die Preise für die angebotene Ware oder Dienstleistungen unter Berücksichtigung der Handelsbedingungen auf dem Markt und unter Hinweis auf die Steuerpflicht oder Befreiung von Mehrwertsteuer und Angabe des Steuersatzes,

h) Hinweise bezüglich der Verpflichtung zur Übernahme der Lieferkosten sowie deren Wert,

i) jede weitere Information, die gesetzlich dem Anbieter als Pflichtangabe auferlegt wurde.

Ferner ist der Anbieter gem. Art. 8 Abs. 1 des Gesetzes Nr. 365/2002 verpflichtet, dem Adressaten noch in der vorvertraglichen Phase mindestens folgende Informationen, die klar, deutlich und verständlich zu formulieren sind, zur Verfügung zu stellen:

- die rechtstechnischen Schritte zum Abschluss des Vertrags,
- ob der abgeschlossene Vertrag vom Anbieter zugänglich gespeichert wird,

- die dem Empfänger zur Verfügung stehenden Mittel zwecks Identifizierung und Berichtigung von Fehlern bei der Eingabe seiner Daten,
- die Vertragssprache,
- die Verhaltensregelungen (Kodex) des Anbieters sowie die notwendigen Zugangsdaten für die elektronische Prüfung dieser Verhaltensregelungen,
- alle weiteren gesetzlich vorgesehenen Pflichtangaben.

Diese Informationspflichten betreffen die Vertragsanbahnung. Die Sanktion für die Nichteinhaltung dieser vorvertraglichen Pflichten ist die relative Nichtigkeit des Vertrags, also die Nichtigerklärung des Vertrags auf Antrag des Empfängers.

Wenn man die Webseiten vieler rumänischer Online-Anbieter besucht, stellt man fest, dass diese Mindestpflichtangaben in der Regel nicht eingehalten werden. Das Vorhandensein eines Impressums ist eine Seltenheit. Daher besteht m.E. in diesem Bereich ein akuter Handlungsbedarf betreffend die Sanktionierung dieser Mängel.

3.3.2 Rechtliche Behandlung der elektronischen Verbraucherverträge

Die rechtliche Behandlung der elektronischen Verbraucherverträge ist in der Regierungsverordnung Nr. 130/2000 über den Verbraucherschutz gesetzlich verankert. In Bezug auf Verbraucherverträge gelten besondere Vorschriften zum Verbraucherschutz.

Gem. Art. 3 Abs. 1 der Regierungsverordnung Nr. 130/2000 muss der gewerbliche Anbieter den Verbraucher noch vor dem Abschluss des Fernvertrags über folgende Aspekte klar, vollständig, brauchbar und verständlich informieren:

a) die Identität des Gewerbetreibenden, seine vollständigen Kontaktdaten und seine Steuernummer, für den Fall, dass der Verbraucher mit der Zahlung in Vorleistung tritt;
b) die wichtigsten Eigenschaften des Produktes oder Dienstes;
c) den Preis der angebotenen Produkte und Dienstleistungen inkl. Gebühren und Steuern;
d) die Kosten für die Lieferung;
e) die Lieferungs-, Ausführungs- und Zahlungsmodalitäten;
f) das Widerrufsrecht und dessen Ausübung und Frist;
g) Gültigkeitsdauer des Angebotes;
h) Mindestdauer der angebotenen Dienstleistung für die Verträge über wiederkehrende Leistungen;

i) die Erfüllungsfrist.

Zusätzlich zu diesen Informationen muss der Gewerbetreibende nach der neuen EU-Richtlinie über den Verbraucherschutz weitere Angaben bezüglich eventueller Pflichten des Verbrauchers zur Zahlung der Kosten für die Rücksendung der Ware infolge eines Widerrufs machen, Informationen über die konkrete Vorgehensweise bei Widerruf. Informationen über die Gewährleistungsrechte für die digitalen Produkte und über die alternative Schlichtung von Streitigkeiten zur Verfügung stellen.

Für die vorvertragliche Phase bei den elektronischen Verbraucherverträgen sieht das Gesetz Nr. 193/2000 vor, dass die Formulierung der Vertragsklausel einfach und verständlich sein muss, damit für das Verständnis des Vertragsinhaltes keine Fachkenntnisse benötigt werden.[5] Im Zweifel bezüglich der Bedeutung einer Vertragsklausel ist diese immer zugunsten des Verbrauchers auszulegen.

Da die Vertragsklauseln der elektronischen Verträge mit den Verbrauchern nicht im Vorfeld des Vertragsabschlusses verhandelt werden, sind sie als rechtsmissbräuchlich und somit als unwirksam einzustufen, wenn sie alleine oder in Verbindung mit anderen Klauseln den Verbraucher unverhältnismäßig bezüglich seiner Pflichten und unter Berücksichtigung des „Treu und Glauben"-Grundsatzes benachteiligen.

3.3.3 Angebotsannahme

Gem. Art. 9 Abs. 1 und 2 des Gesetzes Nr. 365/2002 kann die Annahme des Online-Angebotes ausdrücklich oder stillschweigend erfolgen.

Die ausdrückliche Annahme des Vertragsangebotes erfolgt in der Regel bei den „Click-wrap"-Verträgen durch Click auf das Feld „Einverstanden" oder „Annehmen" – „i agree". Der Oberste Gerichtshof Rumäniens hat eine ausdrückliche Annahme eines „Click-wrap"-Standardvertrags über den Erwerb eines Internet-Domains durch die Zahlung des verlangten Preises an den Anbieter angesehen.[6]

Die stillschweigende Annahme des Vertragsangebotes erfolgt durch das vollständige Lesen der Informationen und allgemeinen Vertragsbedingungen des Anbieters über Verbindung mit einem Hyperlink – „browse-wrap"-Verträge. Damit der elektronische Vertrag wirksam abgeschlossen werden kann, müssen diese Informationen und allgemeinen Vertragsbedingungen als Teil des elektronischen Vertrags für den Empfänger leicht sichtbar und

---

[5] *Bleoanca*, Contractul in forma electronica – Teza de Doctorat coordonator Prof. Univ. Dr. C. Barsan, S. 47.

[6] *Silaghi*, Aspecte juridice privind formarea contractelor electronice, www.academia.edu, S. 31.

lesbar sein. Wenn aber diese Informationen oder allgemeinen Vertragsbedingungen spezielle, von den Standardklauseln abweichende Klausel beinhalten, muss die Annahme doch ausdrücklich erfolgen.[7]

Nach dem Gesetz Nr. 365/2002 können „Browse-wrap"-Verträge nicht durch das einfache Klicken der Option „Weiter" nach Zustimmung zu den allgemeinen Vertragsbedingungen wirksam abgeschlossen werden, sondern nur mit Beginn der Vertragsausführung, wenn der Vertrag eine sofortige Ausführung ermöglicht oder der Anbieter dies verlangt.

Die elektronischen Verträge können in der Regel nur als einseitige Standardverträge – Adhäsionsverträge - abgeschlossen werden. Verhandlungen über die Vertragsklausel und die Abgabe eines Gegenangebotes sind nur bei den elektronischen Verträgen möglich, die per elektronische Post (E-Mail) abgeschlossen werden.

3.4 Schwierigkeiten in der Praxis

Trotz Vereinheitlichung und Vereinfachung der Gesetzgebung im Bereich des E-Commerce entstehen für manche Anbieter, meistens bezüglich der elektronischen Verbraucherverträge, unüberwindbare Schwierigkeiten in der Praxis. Als Beispiel sei ein deutsches Unternehmen gegeben, das ein Direktinvestment in Deutschland vermarkten möchte. Gegenstand des Direktinvestments sind Baum-Plantagen in Rumänien, wo das Rechtssystem die rechtliche Trennung der Plantage vom Grund erlaubt und wonach die Plantage gemäß ihres Zwecks und der Absicht der Parteien als bewegliche Sache durch den Willen der Parteien erklärt werden kann. Empfänger des Investment-Angebotes sind im Wesentlichen deutsche Verbraucher. Diese Verbraucher werden beim Erwerb der mit dem Grund verbundenen Bäume die gekaufte Sache nicht erhalten, so dass es einen Beginn des Widerrufsrechts gar nicht gibt, es sei denn, die Anleger fahren (da ein Direktinvestment regelmäßig als Geldanlage gedacht ist) nach Rumänien, um die gekauften Bäume zu besichtigen und dass diese Inaugenscheinnahme als „Erhalt der Ware" bezeichnet wird. Dies wird natürlich selten der Fall sein, da die Empfänger von Online-Diensten gerade die Vereinfachung des Online-Erwerbs und die damit verbundene Zeitersparnis suchen.

Unter solchen Umständen kann ein Unternehmen sein Geschäftsrisiko nicht abschätzen und müsste seine unternehmerische Geschäftsidee wegen der rechtlichen Hindernisse aufgeben.

---

[7] *Silaghi*, Aspecte juridice privind formarea contractelor electronice, www.academia.edu, S. 32.

4 Schlussbemerkungen

Die elektronischen Verträge gewinnen mit der raschen Entwicklung des IT-Marktes immer mehr an Bedeutung und bewirken Änderungsbedarf auch in anderen Rechtsbereichen. Von diesem Wachstum am meisten beeinflusst ist der notarielle Bereich, in dem bereits zahlreiche Regelungen zu den elektronischen notariellen Akten – Beglaubigungen, Beurkundungen, Ausstellung von Duplikaten und Ausfertigungen von elektronischen Verträgen, Speicherung und Archivierung von elektronischen Dokumenten – und deren Gültigkeitsvoraussetzungen verabschiedet worden sind.

Ein weiterer von den Entwicklungen des IT-Marktes abhängiger Rechtsbereich ist der Datenschutz. Die Angst, dass unsere Daten rechtswidrig gespeichert und weiterverkauft werden und dadurch unser Leben, unser Konsumverhalten und nicht zuletzt unsere Meinung unkontrollierbar von außen bestimmt und manipuliert werden können, hindert die meisten von uns daran, den Nutzen und die Vorteile des elektronischen Handels vollständig in Anspruch zu nehmen.

Nun ist es Sache des Gesetzgebers, unsere Rechte und Freiheiten durch effektive und effiziente Gesetze zu schützen. Ob die neue EU-Verordnung 679/2016 über den Datenschutz dieser Aufforderungen genügt, wird sich demnächst zeigen.

Literatur

Tudorache, Mihaela: Contractul incheiat prin mijloace electronice in reglementarea noului Cod Civil, Bucuresti 2013.

Predoiu, Catalin: Comertul prin internet. Studiu economic si juridic. Juridica Nr. 10/2000, S. 377-385.

Bleoanca, Alexandru: Contractul in forma electronica, Teza de doctorat coordonata de Prof. Univ. Dr. Corneliu Barsan, 2010.

Bucur, Cristina-Mihaela: Comertul electronic, Bucuresti 2009.

CHANCEN FÜR LÄNDLICHE RÄUME AUFGRUND DER WIFI4EU-VERORDNUNG

Dr. Matthias Baumgärtel

EWE TEL GmbH
matthias.baumgaertel@ewe.de

Zusammenfassung

Die Verordnung zur Förderung der Internetanbindung in Kommunen, auch WiFi4EU-Verordnung genannt, beruht auf einem Kommissionsvorschlag vom 14. September 2016 und hat die Förderung kostenloser öffentlicher WLAN-Hotspots in Städten und Gemeinden in der gesamten EU zum Schließen von Versorgungslücken als Ziel. Im Rahmen des bis 2020 laufenden Programms mit einem Volumen von 120 Mio. EURO sollen bis zu 8.000 Gemeinden und öffentliche Einrichtungen mit einem kostenlosem WLAN-Zugang versorgt werden. Vorrang haben dabei die Orte, an denen bisher kein kostenloser privater oder öffentlicher WLAN-Hotspot vorhanden ist. Der Antrag auf Förderung muss über eine spezielle Online-Plattform gestellt werden. Anschließend werden die Projekte nach dem Windhundverfahren ausgewählt.

Die Finanzierung der WLAN-Hotspots wird in Form von Gutscheinen ("Voucher") in Höhe von EUR 15.000 an die öffentlichen Stellen vergeben. Der Voucher deckt die Installationskosten für den Aufbau der Internetzugangspunkte ab. Die öffentliche Stelle bezahlt die Netzanbindung und sorgt für die Instandhaltung der Anlage für eine Laufzeit von mindestens drei Jahren. Dabei steht es der Gemeinde frei, ein Telekommunikationsunternehmen seiner Wahl mit der Installation und dem Betrieb des WLAN-Zugangs zu betrauen.

Den ersten Aufruf vom 15. Mai 2018 hat die für digitale Wirtschaft und Gesellschaft zuständige EU-Kommissarin Mariya Gabriel am 14.6.2018 für ungültig erklärt, da aufgrund eines Problems in der Software keine gleichen Bedingungen für die Teilnahme an dem Aufruf sichergestellt werden konnte. Das Anmeldeportal wurde geschlossen, der Zeitpunkt der Wiederaufnahme und Wiederholung des ersten Aufrufs ist noch nicht bekannt.

1 Gegenstand des Förderprogramms WiFi4EU

WiFi4EU ist ein Förderprogramm der Europäischen Union. Nach der im September 2016 vorgelegten Initiative der EU-Kommission sollen bis 2020 die wichtigsten öffentlichen Orte in europäischen Städten und insbesondere Dörfern mit einem freien und superschnellen Internetzugang ausgestattet werden. Nach langen Verhandlungen im europäischen Parlament und im Rat über die Ausstattung und Umfang des Förderprogramms ist am 25. Oktober 2017 eine Verordnung[1] erlassen worden und am 4. November 2017 in Kraft getreten. Die Verordnung gibt den rechtlichen Rahmen für

[1] Verordnung (EU) 2017/1953 vom 25. Oktober 2017 zur Änderung der VO (EU) Nr. 13/1316 und (EU) Nr. 283/2014 im Hinblick auf die Förderung der Internetanbindung in Kommunen.

die finanzielle Unterstützung des Projekts WiFi4EU vor, bereitgestellt werden die Mittel über die EU-Generaldirektion Connect.

Das Förderprogramm hat eine Laufzeit von 2018 – 2020 und umfasst ein Volumen von 120 Mio. Euro. Das Portal www.wifi4eu.eu ist in allen Landessprachen der EU abrufbar. Allerdings ist das Portal untermittelbar nach dem ersten Aufruf am 15. Mai 2018 geschlossen worden und wird erst wieder in Betrieb genommen, sobald die technischen Störungen behoben sind.[2]

2 Ziel der Förderinitiative WiFi4EU

Ziel der EU-Förderinitiative WiFi4EU ist, die Anbindung an schnelles Internet durch drahtlose Internetzugänge, sogenannte WLAN-Hotspots, im öffentlichen Raum zu unterstützen. Dadurch sollen Versorgungslücken geschlossen und insbesondere kleine Unternehmen und der Tourismus gefördert werden, aber die Initiative soll allen Bürgern zugutekommen. Mithilfe der Fördermittel sollen EU-weit und in den teilnehmenden EWR-Ländern (Norwegen und Island) bis zu 8.000 Gemeinden, in denen bislang keine schnelle Internetversorgung vorhanden ist, auf Marktplätzen oder anderen zentralen Orten Hotspots installiert werden. Dabei soll ein europaweites WLAN-Netz geschaffen werden, bei dem jeder Nutzer sich einmalig registriert und anschließend ohne weitere Anmeldung über alle lokalen WiFi4EU-Hotspots EU-weit kostenlos und werbefrei surfen kann. Das Motto lautet: „Einmal registrieren – überall surfen."[3]

3 Verfahren der Förderung

3.1 Antragsberechtigung

Der erste Aufruf erfolgte am 15 Mai 2018 und dabei sollten 1.183 Gutscheine (Vouchers) im Wert von 15 Mio. Euro vergeben werden. Das Programm erzeugte ein enormes Interesse bei den Kommunen, die EU hatte auch entsprechende Informationsveranstaltungen durchgeführt. In weniger als zwei Monaten haben mehr als 18.000 Gemeinden ihr Interesse bekundet. Ein erster Aufruf zur Einreichung von Bewerbungen wurde am 15. Mai 2018 gestartet. Innerhalb von Sekunden hatten sich bereits mehr als 5.000 Kommunen beworben und innerhalb weniger Stunden waren es bereits 11.000,[4] der 1. Aufruf war damit deutlich überzeichnet, obwohl hier nur

[2] http://europa.eu/rapid/press-release_STATEMENT-18-4158_en.htm (abgerufen am 20. 6.2018).

[3] https://breitbandbuero.de/wissenwertes/foerderprogramme/wifi4eu (abgerufen am 8.3. 2018).

[4] https://wifi4eu.blog/ vom 19. Juni 2018 (abgerufen am 20.6.2018).

Gemeinden (oder entsprechende kommunale Verwaltungen) sowie Gemeindeverbände einen Antrag stellen konnten.

„Gemeindeverbände" können mehrere Gemeinden registrieren und müssen den endgültigen Antrag für jede Gemeinde in ihrer Registrierung einzeln online einreichen. Gemeindeverbände haben keinen Anspruch auf einen Gutschein. Jeder Gutschein wird an eine einzelne Gemeinde als Begünstigte vergeben. Während der gesamten Laufzeit der Initiative kann jede Gemeinde nur einen einzigen Gutschein einsetzen. Daher dürfen Gemeinden, die im Rahmen eines der fünf Aufrufe für einen Gutschein ausgewählt wurden, bei weiteren Aufrufen nicht mehr mitmachen, wohingegen sich Gemeinden, die einen Antrag gestellt, aber keinen Gutschein erhalten haben, sich in einer späteren Runde wieder bewerben können.

Der 2. und 3. Aufruf in Höhe von insgesamt 45 Mio. Euro sind im Zeitraum Ende 2018 bis Mitte 2019 geplant und dabei sollen auch öffentliche Einrichtungen wie Universitäten, Bibliotheken, Museen, Krankenhäuser und Rathäuser antragsberechtigt sein. Der Zeitplan sieht schließlich zwei weitere Aufrufe bis 2020 vor, bei denen die restlichen 60 Mio. Euro vergeben werden sollen.

Die Gutscheine sollen innerhalb der EU ausgeglichen verteilt werden, so sollen pro Mitgliedsland bei entsprechender Nachfrage mindestens 15 und maximal 95 Gutscheine (bzw. max. 8 % der für den ersten Aufruf zur Verfügung stehenden Mittel) vergeben werden.

3.2 Elektronisches Antragsverfahren

Die Gemeinden können sich jederzeit unter dem Portal www.wifi4eu.eu registrieren, indem sie ein einfaches Formular ausfüllen. Für die Registrierung benötigt die Gemeinde ein EU-Login-Benutzerkonto "ECAS".

Das WiFi4EU-Webportal gibt außerdem Telekommunikationsanbietern oder WLAN-Dienstleister die Möglichkeit, sich anzumelden und anzugeben, in welchen Regionen sie WLAN-Hotspots errichten können, so dass die Gemeinden diese Liste bei ihrer eigenen Auftragsvergabe zur Einlösung der Gutscheine zurate ziehen können.

Die Gemeinden müssen bei der Registrierung Basisdaten eingeben, z.B. die Kontaktdaten ihres gesetzlichen Vertreters (z.B. Bürgermeister mit der Ernennungsurkunde) und die Kontaktdaten des Mitarbeiters, dem die Verantwortung für die Registrierung und Bewerbung übertragen wurde.

Bei der Registrierung als Gemeinde sind folgende Angaben erforderlich, die jedoch nicht öffentlich gemacht werden:

- Land und Art der anzumeldenden Organisation (Gemeinde oder Gemeindeverband);

- Informationen über die Gemeinde, wie Name und offizielle Anschrift;
- Angaben zum gesetzlichen Vertreter mit Name und E-Mail-Adresse;
- Angaben zu der Kontaktperson, falls diese nicht mit dem gesetzlichen Vertreter identisch ist mit.

Das Registrierungsverfahren ist einfach gestaltet, jede Gemeinde kann sich in der Sprache ihrer Wahl anmelden. Die Gemeinden brauchen bei der Registrierung weder Informationen über ein technisches Projekt noch eine Dokumentation über das einzurichtende WiFi-Netz übermitteln. Auch wird kein Kostenvoranschlag eines Anbieters benötigt, um den Gutschein beantragen zu können.

Bei den geplanten fünf Aufrufen bis 2020 können die angemeldeten Gemeinden über dasselbe Portal die Gutscheine für die WiFi-Hotspots beantragen. Der Antrag kann einfach durch Anklicken der entsprechenden Schaltfläche eingereicht werden. Die Auswahl der Gemeinden erfolgt nach dem Windhundrennenprinzip, d.h. die Gutscheine werden in der Reihenfolge der Beantragung vergeben (Datum und der Uhrzeit der Antragstellung).

3.3 Voraussetzungen der Förderung eines Hotspots

Gefördert werden ausschließlich Gebiete, wo bis dato am Platz kein öffentlich zugängliches kostenloses WiFi oder WLAN-Netz vorhanden ist, jedoch ein Zentrum des öffentlichen Lebens in der Gemeinde darstellt. Mit diesem Duplizierungsverbot sollen bestehende öffentliche oder private Hotspots, sofern frei zugänglich, vor einem Überbau geschützt werden.

Das WiFi-Netz muss Nutzern ein hochwertiges Interneterlebnis ermöglichen. Die Gemeinden sollen daher das Angebot mit der höchsten auf dem Massenmarkt verfügbaren Geschwindigkeit in ihrem Umkreis auswählen, in jedem Fall müssen mindestens stabile 30 Mbit/s erreicht werden, wobei die Bandbreite der Backhaul-Leitung mindestens der Verbindung entsprechen sollte, die die Gemeinde für ihren internen Bandbreitenbedarf nutzt. Solange stets ein hochwertiges Interneterlebnis gewährleistet bleibt und die Bedingungen des Programms erfüllt werden, kann die Gemeinde entscheiden, ob sie den Anschluss an das WiFi4EU-Netz beschränkt oder mit anderen Diensten/Netzen teilt.

Voraussetzung ist ferner, dass ein kostenloser und diskriminierungsfreier Zugang gewährt wird. Es darf keine zeitliche Limitierung geben, d. h. der Internetzugangsanbieter darf fremde Kunden nicht anders behandeln als seine eigenen. Die Vorschaltung von Werbung, die für die Gemeinde eine Einnahmequelle darstellt oder den Endnutzer verpflichtet, ein Produkt oder eine Dienstleistung zu erwerben, um Zugang zum Netz zu erhalten, ist

nicht erlaubt.[5] Der Hotspot muss mit der Landingpage WiFi4EU-Kennzeichnung (WiFi4EU-SSID) beginnen, später kann dies mit dem Gemeindenamen verbunden werden.

Der Internetzugang an dem geförderten Hotspot muss mindestens drei Jahre lang betrieben werden. Die Gemeinden können ihren Internetanbieter frei wählen, der mit dem WiFi-Infrastrukturinstallateur identisch sein kann, aber nicht sein muss. Da gemäß der Haushaltsordnung die rückwirkende Gewährung einer Finanzhilfe verboten ist, ist ein Gutschein für bereits abgeschlossene Maßnahmen nicht zulässig.

3.4 Gegenstand der Hot-Spot-Förderung

Der Wert eines WiFi4EU-Gutscheins beläuft sich auf max. 15.000 Euro und deckt die Geräte- und Installationskosten von WiFi-Hotspots (Access-Points) ab, die den Anforderungen entsprechen müssen, die in der Ausschreibung und in der mit den ausgewählten Gemeinden zu unterzeichnenden Finanzhilfevereinbarung festgelegt sind. Die ausgewählte Gemeinde trägt für mindestens drei Jahre die Kosten für die Internetverbindung sowie die Wartungs- und Betriebskosten der Geräte. Bei der Auftragsvergabe für die Errichtung des Hotspots oder für den Internetzugang ist das nationale Vergaberecht mit den entsprechenden Schwellenwerten zu beachten.

Die Kosten im Zusammenhang mit dem Ausschreibungsverfahren (wie Planungskosten), die Einrichtung der erforderlichen Backhaul-Leitung (z.B. Tiefbaukosten für den Ausbau des Netzes) oder zusätzliche Geräte, die nicht speziell mit den WiFi-Hotspots in Verbindung stehen (Ladestationen, Straßenmobiliar usw.), müssen ebenfalls von der Gemeinde übernommen werden.

Die Gemeinde muss dafür sorgen, dass innerhalb von anderthalb Jahren nach Erhalt des Gutscheins die Installation abgeschlossen ist und der WiFi-Hotspot den Betrieb aufnimmt. In diesem Zeitraum kann die Gemeinde also ihr Projekt festlegen und ein TK-Unternehmen oder WiFi-Installationsunternehmen auswählen, das den Hotspot einrichten kann.

Die Gemeinde beauftragt ggf. nach einem durchgeführten Vergabeverfahren für öffentliche Aufträge ein Unternehmen seiner Wahl mit der Installation der Hotspotgeräte. Die EU-Kommission wird per Fernüberwachung

[5] In Erwägungsgrund 4 der Verordnung (EU) 2017/1953 wird ausgeführt, dass die mithilfe der WiFi4EU-Hotspots erbrachte Dienstleistung kostenlos sein sollte, d.h. sie sollte in den ersten drei Betriebsjahren ohne entsprechendes Entgelt, sei es durch direkte Zahlung oder auf andere Art und Weise geleistet (z.B. durch Werbung oder der Übermittlung personenbezogener Daten für gewerbliche Zwecke) bereitgestellt werden.

die korrekte Umsetzung des Hotspots überprüfen, aber nicht in die vertraglichen Beziehungen der Gemeinde zu seinem TK-Anbieter eingreifen.

Der TK-Anbieter kann dann den Gutschein bei der Europäischen Kommission einlösen und alle noch ausstehenden Beträge, die nicht durch den Gutschein gedeckt sind, müssen durch die Gemeinde direkt beglichen werden.

3.5 Sicherheitsvoraussetzungen und technische Anforderungen für die WiFi4EU-Netze

In der Anfangsphase werden die öffentlichen WiFi4EU-Hotspots nicht verschlüsselt sein müssen. In dieser Phase fällt die Registrierung und Authentifizierung von Nutzern und damit die mögliche Erfassung und Verarbeitung personenbezogener Daten in die Zuständigkeit jeder einzelnen Gemeinde und ihres beauftragten Internetdienstanbieters.

In einer zweiten Phase ab 2019 wird es eine einheitliche Authentifizierungsplattform mit zusätzlichen Sicherheitsmerkmalen geben, die es den Nutzern ermöglicht, sich nur ein einziges Mal anzumelden (E-Mailadresse oder Mobilfunknummer) und dann zwischen allen WiFi4EU-Hotspots zu surfen, ohne ihre Zugangsdaten erneut eingeben zu müssen. Dann wird ein reibungsloses Roaming zwischen WiFi4EU-Hotspots in verschiedenen Gebieten der EU möglich sein muss.

Die Sicherheitsfunktionen werden dann Teil der technischen Spezifikationen der Geräte und in der Finanzhilfevereinbarung aufgeführt. Letztendlich sind die Gemeinden für den Zugang und die Verwaltung des einzelnen WiFi4-EU-Netzes auf lokaler Ebene zuständig und legen die Sicherheitseinstellungen im Einklang mit dem EU-Recht und dem nationalen Recht fest.

4 WiFi4EU – Verstoß gegen Datenschutz?

Fraglich ist, ob die auf dem WiFi4EU-Portal vorgenommene Erfassung und Speicherung von personenbezogenen Daten mit den geltenden nationalen und EU-Rechtsvorschriften, insbesondere der Verordnung (EG) Nr. 45 /2001, im Einklang steht.

Am 11.10.2017 hat der Kieler Bürgerrechtler Patrick Breyer (Piratenpartei) gegen die geplante Zwangsregistrierung postwendend Beschwerde beim EU-Datenschutzbeauftragten Giovanni Buttarelli eingelegt. Nach Breyers Ansicht liegt „kein berechtigtes Interesse an der Identifizierung von

Nutzern kostenloser Internetzugänge“ vor. Die Beschwerde wurde als offener Brief im Internet veröffentlicht.[6] Als Argumente führt Breyer an, dass in Deutschland durch die kürzlich abgeschaffte Störerhaftung sehr viele WLAN-Zugänge mittlerweile identifizierungsfrei benutzbar seien und der Betreiber nach der E-Commerce-Richtlinie zudem nicht für durchgeleitete Datenströme hafte. Patrick Breyer führt in dem offenen Brief ferner aus, dass auch Telefonzellen anonym nutzbar seien, einen staatlichen Identifizierungszwang für WLAN-Anbieter gebe es nicht. Zugleich erinnerte er daran, dass der Europäische Menschengerichtshof die unter anderem die 2004 in Deutschland eingeführte und inzwischen verschärfte Identifizierungspflicht von Prepaid-Karten für Mobilgeräte prüfe.[7]

Über die Beschwerde ist bislang noch nicht entschieden worden, ein Verstoß gegen die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 DSGVO oder den konkretisierenden Vorschriften nach Art. 25-29 DSGVO ist nicht festzustellen. Es werden ausschließlich personenbezogene Daten, die für die Teilnahme an der WiFi4EU-Initiative und deren Verwaltung durch die Europäische Kommission benötigt werden, erfasst und nur dann gespeichert, wenn dies für Kontroll- und Prüfungszwecke erforderlich ist. Durch Verifizierung mittels Handynummer soll geklärt werden, ob der jeweilige Nutzer für das offene WLAN autorisiert ist und dabei dürfen personenbezogene Daten nur dann verarbeitet werden, wenn dies nationale Gesetze erlauben.

Die Europäische Kommission kann die Daten auf Grundlage des Grundsatzes des berechtigten Informationsinteresses anderen EU-Organen und -Einrichtungen, den Mitgliedstaaten (einschließlich ihrer regionalen oder lokalen Behörden) oder den für Kontrollen oder Inspektionen nach europäischem Recht zuständigen Dienststellen (z.B. Europäischer Rechnungshof, OLAF, Ombudsmann usw.) übermitteln.[8] Derzeit wird nach einem externen Dienstleister gesucht, der ein Authentifizierungssystem aufbauen und betreiben soll.

5 Risiko der Störerhaftung für Gemeinden?

Nach langem Ringen wurde in Deutschland am 30.6.2017 das dritte Gesetz zur Änderung des Telemediengesetzes (3. TMG-ÄndG) beschlossen, dass

[6] http://www.daten-speicherung.de/index.php/beschwerde-gegen-wifi4eu-wegen-geplantem-wlan-identifizierungszwang-eingereicht (abgerufen am 25.6.2018).

[7] Application no. 50001/12 Patrick Breyer and Jonas Breyer against Germany, wobei in Europa immer weniger Länder den Kauf anonymer Prepaid-SIM-Karten zulassen.

[8] Einzelheiten siehe WiFi4EU-Datenschutzerklärung.

die Störerhaftung für WLAN-Betreiber rechtssicher abschaffen soll.[9] Das Gesetz sollte Unsicherheiten begegnen, welche aus der Mc Fadden/Sony Music Entscheidung resultieren, in dem es klarstellt, dass WLAN-Anbieter nicht verpflichtet sind, die Nutzer zu registrieren, die Eingabe eines Passwortes verlangen oder das WLAN-Angebot einzustellen. Nach § 4 S. 1 TMG bleibt der WLAN-Betreiber allerdings verpflichtet, Nutzer zu sperren, wenn Dritte eine Verletzung ihrer Rechte beanstanden. In der Literatur wird angezweifelt, ob mit dem 3. TMG-ÄndG Rechtssicherheit hergestellt worden ist.[10]

Inzwischen liegt die Entscheidung des OLG München vom 15.3.2018 in dem Berufungsverfahren Mc Fadden/Sony Music.[11] Danach besteht nach der Neufassung des TMG keine Störerhaftung mehr für offene WLAN-Hotspots. Die Änderung des TMG ist europarechtskonform, eine Haftung der Gemeinden für den Betrieb der WiFi4EU-Hotspots besteht daher nicht.

6 Unterbrechung des Förderprogramms im Juni 2018

Am 14. Juni 2018 hat die für digitale Wirtschaft und Gesellschaft zuständige Kommissarin Mariya Gabriel eine Erklärung veröffentlicht, in dem Sie die erste Ausschreibung für die WiFi4EU-Gutscheine, welche am 15. Mai 2018 erfolgt ist, für ungültig erklärt.[12]

Dies wird damit begründet, dass ein Problem in der Software des externen Dienstleisters dazu geführt hat, dass sich einige Antragsteller (Städte und Gemeinden) schon vor dem offiziellen Beginn der Ausschreibung bewerben konnten, während andere nach der Eröffnung der Ausschreibung an einer Bewerbung gehindert wurden. Aufgrund dieses technischen Fehlers konnten die Antragsteller nicht zu gleichen Bedingungen an dem Aufruf teilnehmen. Um weiterhin einen fairen und transparenten Prozess der Gutscheinvergabe zu gewährleisten, hat die Kommisssarin folglich den Aufruf abgebrochen.

Die Entscheidung, die zu viel Spot[13] geführt hat, war richtig, denn die Kommission ist den Grundsätzen der Fairness, Transparenz und Zuverlässigkeit verpflichtet. Da dieses technische Problem alle Gemeinden daran

[9] Siehe Begründung RegE, BT-Drs. 18/12202, S. 1; *Sesing/Baumann*, MMR 2017, S. 583 ff.

[10] *Spindler*, MMR 2018, S. 47 (51); *Volkmann*, K&R 2018, S. 361.

[11] OLG München, Urt. v. 15.3.2018 – 6 U 1741/17 (nicht rechtskräftig).

[12] http://europa.eu/rapid/press-release_STATEMENT-18-4158_en.htm (abgerufen am 20. 6.2017).

[13] Nordwest-Zeitung vom 8. Juni 2018, S. 3: „peinlicher Fehler stoppt Projekt".

hinderte, sich gleichberechtigt anzumelden, musste der erste Aufruf storniert werden. Es bleibt zu hoffen, dass der Aufruf schnellstmöglich nachgeholt werden kann.

Literatur

Sesing, Andreas/Baumann, Jonas S.: Sperranspruch statt Störerhaftung? MMR 2017, S. 583-589.

Spindler, Gerald: Haftung ohne Ende?, MMR 2018, S. 48-52.

Volkmann, Christian: Aktuelle Entwicklungen in der Providerhaftung im Jahr 2017, K&R 2018, S. 361-367.