Gerrit Hornung · Ralf Müller-Terpitz
Herausgeber

Rechtshandbuch Social Media

Springer

Rechtshandbuch Social Media

Gerrit Hornung • Ralf Müller-Terpitz
(Hrsg.)

Rechtshandbuch Social Media

Springer

Herausgeber
Gerrit Hornung
Inhaber des Lehrstuhls für
Öffentliches Recht,
Informationstechnologierecht
und Rechtsinformatik
Universität Passau
Passau
Deutschland

Ralf Müller-Terpitz
Inhaber des Lehrstuhls für
Öffentliches Recht,
Recht der Wirtschaftsregulierung
und Medien
Universität Mannheim
Mannheim
Deutschland

ISBN 978-3-642-38191-1 ISBN 978-3-642-38192-8 (eBook)
DOI 10.1007/978-3-642-38192-8
Springer Heidelberg NewYork Dordrecht London

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 säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil der Fachverlagsgruppe Springer Science+Business Media
(www.springer.com)

Vorwort

Zehn Jahre nach dem Start des bis heute erfolgreichsten sozialen Netzwerks Facebook spricht alles für die Einschätzung, dass Social Media gekommen sind, um zu bleiben. Die unter diesem Schlagwort zusammengefasste Gruppe von Internetanwendungen und -diensten setzt auf eine aktive Beteiligung der Nutzer – und ist damit extrem erfolgreich. Hierdurch haben sich viele Kommunikationsstrukturen des Internets grundlegend verändert. Diese Veränderungen warfen von Anfang an nicht nur technische, medienwissenschaftliche, wirtschaftliche und politische, sondern auch eine Fülle von rechtlichen Fragen auf.

Dem vorliegenden Rechtshandbuch liegen zwei Überlegungen zugrunde. Zum einen lassen sich Social Media (oder, in anderer Terminologie: Social Web, Soziale Medien, soziale Netzwerke, Web 2.0 etc.) bei allen Randunschärfen als abgrenzbares Phänomen beschreiben, das eine Gesamtdarstellung aus unterschiedlichen rechtswissenschaftlichen Perspektiven ermöglicht. Zum anderen fehlt genau dies, nämlich ein Handbuch, das sowohl dem wissenschaftlich Interessierten als auch dem fundiert arbeitenden Praktiker einen umfassenden und schnellen Zugriff auf die wesentlichen Rechtsfragen ermöglicht und die verschiedenen Lebensbereiche, in denen soziale Netzwerke eine Rolle spielen, miteinander vernetzt. Diese Lücke möchte das Buch schließen.

Wir bedanken uns sehr herzlich bei den Verantwortlichen des Springer-Verlags, vor allem bei Frau Dr. *Brigitte Reschke*, für die spontane Bereitschaft zur Publikation dieses Handbuchs und für die stets unkomplizierte Zusammenarbeit bei seiner Erstellung. Besonderer Dank gebührt daneben Herrn Dr. *Hannes Beyerbach*, der nicht nur einen gehaltvollen Beitrag für den Band verfasst, sondern auch für dessen Gestaltung die redaktionelle Verantwortung übernommen hat. Tatkräftig unterstützt wurde er dabei vom Mannheimer Lehrstuhl-Team, aus dem besonders Frau *Lisa Freihoff*, LL.B., und Frau *Laura Fritsch*, LL.B., lobend hervorzuheben sind.

Rechtsprechung und Literatur konnten in den einzelnen Beiträgen bis zum Frühsommer 2014 berücksichtigt werden. Über Rückmeldungen zur Struktur des Handbuchs und zum Inhalt der einzelnen Beiträge würden wir uns sehr freuen.

Passau/Mannheim, im Juli 2014

Gerrit Hornung
Ralf Müller-Terpitz

Inhaltsverzeichnis

Autorenverzeichnis

Prof. Dr. iur. Frank Bayreuther Inhaber des Lehrstuhls für Bürgerliches Recht und Arbeitsrecht, Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: frank.bayreuther@uni-passau.de

Dr. iur. Hannes Beyerbach Akademischer Rat, Lehrstuhl für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien, Universität Mannheim, Schloss Westflügel, 68131 Mannheim, Deutschland
E-Mail: beyerbach@uni-mannheim.de

Prof. Dr. iur. Peter Bräutigam Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Honorarprofessor für Medien und Internetrecht an der Universität Passau, Noerr LLP, Brienner Str. 28, 80333 München, Deutschland
E-Mail: peter.braeutigam@noerr.de

Prof. Dr. iur. Robert Esser Inhaber des Lehrstuhls für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht sowie Wirtschaftsstrafrecht; Leiter der Forschungsstelle Human Rights in Criminal Proceedings (HRCP), Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: robert.esser@uni-passau.de

Dr. phil. Alexander Godulla Akademischer Rat, Lehrstuhl für Kommunikationswissenschaft, Universität Passau, Innstr. 33a, 94032 Passau, Deutschland
E-Mail: alexander.godulla@uni-passau.de

Prof. Dr. phil. Ralf Hohlfeld Inhaber des Lehrstuhls für Kommunikationswissenschaft, Universität Passau, Innstr. 33a, 94032 Passau, Deutschland
E-Mail: ralf.hohlfeld@uni-passau.de

Prof. Dr. iur. Gerrit Hornung Inhaber des Lehrstuhls für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik, Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: gerrit.hornung@uni-passau.de

Prof. Dr. iur. Ralf Müller-Terpitz Inhaber des Lehrstuhls für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien, Universität Mannheim, Schloss Westflügel, 68131 Mannheim, Deutschland
E-Mail: mueller-terpitz@uni-mannheim.de

Dr. iur. Sönke E. Schulz Geschäftsführender wissenschaftlicher Mitarbeiter, Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Olshausenstraße 40, 24098 Kiel, Deutschland
E-Mail: sschulz@lvstein.uni-kiel.de

Bernhard von Sonnleithner, LL.M. Corporate Counsel, EMEA Privacy, salesforce.com Germany GmbH, Erika-Mann-Str. 63, 80636 München, Deutschland
E-Mail: bvonsonnleithner@salesforce.com

Prof. Dr. iur. Gerald Spindler Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen, Deutschland
E-Mail: lehrstuhl.spindler@jura.uni-goettingen.de

Abkürzungsverzeichnis

a. A.	andere(r) Ansicht
a. a. O.	am angegebenen Ort
a. E.	am Ende
Abb.	Abbildung
ABI.EU	Amtsblatt der Europäischen Union
abl.	ablehnend
ABl.EG	Amtsblatt der Europäischen Gemeinschaft
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Archiv für Presserecht (Zeitschrift)
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AiB	Arbeitsrecht im Betrieb (Zeitschrift)
allg.	allgemein
Alt.	Alternative
Anm.	Anmerkung
AnwK-StPO	AnwaltKommentar, Strafprozessordnung
AnwZert ITR	AnwaltZertifikatOnline IT-Recht (Zeitschrift)
AO	Abgabenordnung
ArbG	Arbeitsgericht, Arbeitgeber
ArbRAktuell	Arbeitsrecht Aktuell (Zeitschrift)
ArbRB	Der Arbeits-Rechts-Berater (Zeitschrift)
ArbR-Hdb.	Handbuch zum Arbeitsrecht
ArbuR	Arbeit und Recht (Zeitschrift)
ArbZG	Arbeitszeitgesetz
arg.	argumentum
Art.	Artikel
AT	Allgemeiner Teil
AuA	Arbeit und Arbeitsrecht (Zeitschrift)
ausf.	ausführlich
AVMD-RL	Richtlinie über audiovisuelle Mediendienste
Az.	Aktenzeichen

BAG	Bundesarbeitsgericht
BAGE	Entscheidungen des Bundesarbeitsgerichts
BayObLG	Bayerisches Oberstes Landesgericht
BayVGH	Bayrischer Verwaltungsgerichtshof
BB	Betriebs-Berater (Zeitschrift)
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BDSG-E	Bundesdatenschutzgesetz (Entwurf)
BeckOK	Beck'scher Online Kommentar
BeckOK-ArbR	Beck'scher Online Kommentar zum Arbeitsrecht
BeckOK-BGB	Beck'scher Online Kommentar zum Bürgerlichen Gesetzbuch
BeckOK-JMStV	Beck'scher Online Kommentar zum Jugendmedienschutz-Staatsvertrag
BeckOK-StGB	Beck'scher Online Kommentar Strafgesetzbuch
BeckOK-StPO	Beck'scher Online-Kommentar Strafprozessordnung
BeckRS	Beck-Rechtsprechung
Bek d. MI	Bekanntmachung des Ministeriums
Beschl.	Beschluss
BetrVG	Betriebsverfassungsgesetz
BfDI	Beauftragter für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen (amtliche Sammlung)
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen (amtliche Sammlung)
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BITV	Barrierefreie Informationstechnik-Verordnung
BKA	Bundeskriminalamt
BKAG	BKA-Gesetz
BK-GG	Bonner Kommentar zum Grundgesetz
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BR-Drs.	Bundesratsdrucksache
BReg	Bundesregierung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BtMG	Betäubungsmittelgesetz
BUrlG	Mindesturlaubsgesetz für Arbeitnehmer
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (amtliche Sammlung)
BVerfG-K	Bundesverfassungsgericht (Kammer)
bzw.	beziehungsweise
CDU	Christlich Demokratische Union

CISG	United Nations Convention on Contracts for the International Sale of Goods
CLSR	Computer Law & Security Review (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
Cri	Computer Law Review International (Zeitschrift)
CSU	Christlich Soziale Union
d. h.	das heißt
DB	Der Betrieb (Zeitschrift)
dgl.	dergleichen
DJT	Deutscher Juristentag
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DRiZ	Deutsche Richterzeitung
DS-GVO-E	EU-Datenschutz-Grundverordnung (Entwurf)
DSRL	Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit
DVBI.	Deutsches Verwaltungsblatt (Zeitschrift)
ECC	European Cybercrime Center
E-Commerce-RL	Richtlinie über den elektronischen Geschäftsverkehr
ECRL	Richtlinie über den elektronischen Geschäftsverkehr
EGMR	Europäischer Gerichtshof für Menschenrechte
Einf.	Einführung
Einl.	Einleitung
EMRK	Europäische Menschenrechtskonvention
ERfKomm	Erfurter Kommentar
ErwG	Erwägungsgrund
et al.	et alii (und andere)
etc.	et cetera (und so weiter)
ETS	Europäisches Institut für Telekommunikationsnormen
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-GRC	EU-Grundrechtecharta
EuGVÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen
EuGVVO	Verordnung über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen
Europol	Europäisches Polizeiamt
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
f.	folgende(r) (Seite, §, Randnummer)
FA	Fachanwalt Arbeitsrecht (Zeitschrift)
FamRZ	Zeitschrift für das gesamte Familienrecht
FAZ	Frankfurter Allgemeine Zeitung
FD-StrafR	Fachdienst Strafrecht

ff.	Folgende (Seiten, Randnummern etc.)
Fn.	Fußnote
FPR	Familie Partnerschaft Recht (Zeitschrift)
FS	Festschrift
GA	Goltdammer's Archiv
GewO	Gewerbeordnung
GewSchG	Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellung
GG	Grundgesetz
ggf.	Gegebenenfalls
GRC	Charta der Grundrechte der EU
GrS	Großer Senat
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRURPrax	Gewerblicher Rechtsschutz und Urheberrecht: Praxis im Immaterialgüter- und Wettbewerbsrecht (Zeitschrift)
h. M.	herrschende Meinung
HFR	Humboldt-Forum-Recht
HGB	Handelsgesetzbuch
HGR	Handbuch der Grundrechte
Hk-GS	Gesamtes Strafrecht Handkommentar
Hrsg.	Herausgeber
Hs	Halbsatz
HStR	Handbuch des Staatsrechts
HumFoR	Humboldt-Forum-Recht
i. E.	im Erscheinen
i. H. v.	in Höhe von
i. R. d.	im Rahmen der/des
i. S.	im Sinne
i. S. d.	im Sinne der/des
i. S. d.	im Sinne der/des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
i. w. S.	im weiteren Sinne
insb.	insbesondere
IP	Internetprotokoll
IPR	Internationales Privatrecht
IPRax	Praxis des Internationalen Privat- und Verfahrensrechts (Zeitschrift)
IT	Informationstechnik
ITRB	Der IT-Rechts-Berater (Zeitschrift)
IuKDG	Informations- und Kommunikationsdienste Gesetz
JA	Juristische Arbeitsblätter (Zeitschrift)
JbArbR	Jahrbuch des Arbeitsrechts
JMStV	Jugendmedienschutz-Staatsvertrag
JMStV	Jugendmedienschutz-Staatsvertrag

JR	Juristische Rundschau (Zeitschrift)
Jura	Juristische Ausbildung (Zeitschrift)
jurisPR-ITR	Juris PraxisReport IT-Recht (Zeitschrift)
JurPC Web-Doc	Internet-Zeitschrift für Rechtsinformatik und Informationsrecht
JuSchG	Jugendschutzgesetz
JZ	Juristen Zeitung (Zeitschrift)
K&R	Kommunikation und Recht
Kap.	Kapitel
KEK	Kommission zur Ermittlung der Konzentration im Medienbereich
KG	Kammergericht
KJM	Kommission für Jugendmedienschutz
KK-StPO	Karlsruher Kommentar zur Strafprozessordnung
KOM	Dokumente der Kommission der EG
KommJur	Zeitschrift Kommunaljurist
krit.	kritisch
KSchG	Kündigungsschutzgesetz
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LAG	Landesarbeitsgericht
LDSG	Landesdatenschutzgesetz
LG	Landgericht
lit.	litera (Buchstabe)
LK-StGB	Leipziger Kommentar Strafgesetzbuch
LR-StPO	Löwe/Rosenberg, Strafprozessordnung
m. Anm.	mit Anmerkung
m. w. N.	mit weiteren Nachweisen
MarkenG	Markengesetz
MMR	MultiMedia und Recht (Zeitschrift)
MMR-Beil.	MultiMedia und Recht Beilage
MschrKrim	Monatsschrift für Kriminologie und Strafrechtsreform (Zeitschrift)
MüKo-BGB	Münchener Kommentar zum Bürgerlichen Gesetzbuch
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NJW-RR	NJW- Rechtsprechungs-Report Zivilrecht
NK-StGB	Nomos Kommentar Strafgesetzbuch
NoeP	Nicht offen ermittelnder Polizeibeamter
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	Neue Zeitschrift für Strafrecht Rechtsprechungsreport
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für VerwaltungsrechtRechtsprechungsreport

NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	Neue Zeitschrift für Arbeitsrecht Rechtsprechungsreport
NZA-RR	Neue Zeitschrift für Arbeits- und Sozialrecht, Rechtsprechungs-Report
o.	oder
o. ä.	oder ähnlich(e)
öAT	Zeitschrift für das öffentliche Arbeits- und Tarifrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PersR	Der Personalrat (Zeitschrift)
PKS	Polizeiliche Kriminalstatistik
PRISM	Prisma
ProPK	Programm Polizeiliche Kriminalprävention
RÄndStV	Rundfunkänderungsstaatsvertrag
RÄStV	Rundfunkänderungsstaatsvertrag
RdA	Recht der Arbeit (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
Red. Ls.	Redaktioneller Leitsatz
RefE	Referentenentwurf
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
RStV	Rundfunkstaatsvertrag
s.	siehe
S.	Satz/Seite
s. a.	siehe auch
s. o.	siehe oben
st. Rspr.	ständige Rechtsprechung
s. u.	siehe unten
SCRIPTed	A Journal of Law, Technology & Society (Zeitschrift)
SK-StGB	Systematischer Kommentar zum Strafgesetzbuch
Slg.	Sammlung
SNS	Social Network Sites
sog.	sogenannten
SPD	Sozialdemokratische Partei Deutschlands
SSW-StGB	Satzger/Schmitt/Widmaier Kommentar zum Strafgesetzbuch
StGB	Strafgesetzbuch
StGB-E	Entwurf zum StGB
StPO	Strafprozessordnung
StraFO	Strafverteidiger Forum
StRÄndG	Strafrechtsänderungsgesetz

StRR	StrafRechtsReport
StV	Strafverteidiger (Zeitschrift)
SZ	Süddeutsche Zeitung
TDDSG	Teledienstdatenschutzgesetz
TDG	Teledienstgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TVG	Tarifvertragsgesetz
TV-L	Tarifvertrag für den Öffentlichen Dienst der Länder
TVöD	Tarifvertrag für den Öffentlichen Dienst
TVöD-BT-V	Tarifvertrag für den Öffentlichen Dienst – Besonderer Teil Verwaltung
Tz.	Textziffer
u. a.	und andere
ULD	Unabhängiges Zentrum für Datenschutz
u. U.	unter Umständen
UGC	User Generated Content
UrhG	Urheberrechtsgesetz
UrhG-E	Entwurf zum Urheberrechtsgesetz
UrhR	Urheberrecht
URL	Uniform Resource Locator
Urt. v.	Urteil vom
US	United States
USA	United States of America
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	von/vom
VE	verdeckter Ermittler
VerfGH	Verfassungsgerichtshof
VersG	Versammlungsgesetz
VerwArch	Verwaltungsarchiv (Zeitschrift)
VG	Verwaltungsgericht
vgl.	vergleiche
VM	Verwaltung und Management (Zeitschrift)
VO	Verordnung
Vorb.	Vorbemerkungen
vs.	versus/gegen
VuR	Verbraucher und Recht (Zeitschrift)
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VwVfG	Verwaltungsverfahrensgesetz
WIPO	World Intellectual Property Organization
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WP	Working Paper
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)

z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZD-Aktuell	Zeitschrift für Datenschutz Aktuell
ZEV	Zeitschrift für Erbrecht und Vermögensnachfolge
ZGE	Zeitschrift für Geistiges Eigentum
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZJS	Zeitschrift für das Juristische Studium
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	Zeitschrift für Urheber- und Medienrecht- Rechtsprechungsdienst
ZWH	Zeitschrift für Wirtschaftsstrafrecht

Kapitel 1
Einführung in das Rechtshandbuch

Gerrit Hornung und Ralf Müller-Terpitz

Inhalt

1.1 Social Media als Phänomen des Alltags und des Rechts

Das Phänomen Social Media ist aus unserem Alltag nicht mehr wegzudenken. Paradigmatisch für seine Bedeutung steht die **Plattform „Facebook"**, die weltweit mehr als eine Milliarde Nutzer vernetzt und im Jahre 2012 durch einen spektakulären Börsengang auf sich aufmerksam gemacht hat. Freilich lassen sich Social Media nicht auf diese Plattform und vergleichbare soziale Netzwerke reduzieren. Sie entwickeln sich bereits seit Jahren in ganz unterschiedlichen Ausprägungen, sei es als privat oder beruflich genutzte Netzwerk- und Multimedia-Plattformen **1**

G. Hornung (✉)
Inhaber des Lehrstuhls für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: gerrit.hornung@uni-passau.de

R. Müller-Terpitz
Inhaber des Lehrstuhls für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien Universität Mannheim, Schloss Westflügel, 68131 Mannheim, Deutschland
E-Mail: mueller-terpitz@uni-mannheim.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_1

(Facebook, Google+, Xing, YouTube etc.), als Personal-Publishing-Plattformen etwa für Blogs, als Wiki-Plattformen oder in Gestalt von Instant Messaging-Diensten (WhatsApp). Infolge ihrer zunehmenden Durchdringungen wichtiger gesellschaftlicher Lebensbereiche wurden und werden sie zwangsläufig auch zum **Gegenstand des Rechts** – sei es in der Rechtspraxis oder in der Rechtswissenschaft.

2 Letztere hat sich diesem Phänomen zwischenzeitlich in Gestalt einiger monographischer Abhandlungen[1] und einer reichhaltigen Aufsatzliteratur genähert. Demgegenüber fehlt es bislang an einer umfassenden wissenschaftlichen Erschließung und Durchdringung der Thematik in Gestalt eines **Rechthandbuchs**, welches ihre verschiedenen tatsächlichen Facetten aus rechtlich unterschiedlichen Perspektiven beleuchtet und miteinander verknüpft. Das vorliegende Werk möchte diese Lücke schließen. Die einzelnen Beiträge decken hierzu jeweils einen speziellen Lebensbereich ab, berühren aber zugleich an nicht wenigen Stellen auch Fragen aus den anderen Bereichen. Dies ist durch Verweise auf die anderen Kapitel des Rechtshandbuchs kenntlich gemacht. Gleichzeitig erlaubt es das Stichwortverzeichnis, zur gesuchten rechtlichen Einzelfrage schnell den einschlägigen Beitrag zu finden.

3 Um den Realbereich der rechtswissenschaftlichen Betrachtung abzustecken, bedarf es freilich einer Grundlegung aus kommunikationswissenschaftlicher Perspektive, die den schillernden und an seinen Rändern unscharfen Begriff der Social Media ausleuchtet und ihn so für eine juristische Analyse fruchtbar macht. Diese „Klammer" um die juristischen Kapitel erlaubt einen ganzheitlichen Zugang zum Phänomen Social Media auch in rechtlicher Hinsicht. Sie zeigt, welche Spezifika Social Media im Gegensatz zu den „klassischen" Medien aufweisen; denn es sind häufig gerade diese Besonderheiten von Social-Media-Anwendungen, aus denen sich die im vorliegenden Werk behandelten speziellen Rechtsfragen ergeben.

1.2 Phänomen der Social Media

4 Dieser Begriffsklärung aus kommunikationswissenschaftlicher Perspektive widmen sich *Ralf Hohlfeld* und *Alexander Godulla* im **2. Kapitel**.[2] Die Autoren zeigen auf, wie sich das ursprünglich monodirektionale Internet zu einem „Web 2.0" weiterentwickelt hat, in welchem aus dem ehemals passiven Konsumenten ein aktiver „Prosument" wurde, der Inhalte nicht nur konsumiert, sondern auch produziert und ins Netz stellt („user generated content"), diese verbreitet (teilt) und mit anderen interagiert.

---

[1] Ohne Anspruch auf Vollständigkeit sind hier etwa zu nennen: J. Kamp, Personenbewertungsportale, 2013; C.M. Köhler, Persönlichkeitsrechte im Social Web – verlorene Grundrechte?, 2011; J. Lacher, Rechtliche Grenzen der Kommunikation über ärztliche Leistungen, 2012; M. Weigl, Meinungsfreiheit contra Persönlichkeitsschutz am Beispiel von Web 2.0-Applikationen, 2011; M. Wieczorek, Persönlichkeitsrecht und Meinungsfreiheit im Internet, 2013.

[2] S. 11 ff.

Diese Wandlung vom Konsumenten zum Prosumenten trägt auch zur Entwicklung neuer **Geschäftsmodelle** bei und wird so zu einem höchst bedeutsamen Innovationsmotor für die wirtschaftliche und gesellschaftliche Entwicklung. Denn das hohe Maß an Interaktion der Nutzer sowie ihre Fähigkeit, selbst Inhalte zu generieren und distributieren, ermöglicht es auch kleinen Unternehmen oder Einzelpersonen, am Wirtschaftskreislauf zu partizipieren und mithin den „Long Tail" von Märkten im Internet zu erschließen. **5**

Daneben zeichnen sich Web 2.0-Angebote durch verschiedene **Komponenten des Identitäts-, Beziehungs- und Informationsmanagements** aus. Ihre Erscheinungsformen – wie etwa Plattformen[3], Blogs[4], Wikis[5] oder Messaging-Dienste[6] – werden sodann näher vorgestellt, bevor die Autoren nachweisen, dass der Social-Media-Konsum im Verhältnis zur allgemeinen Internetnutzung statistisch kaum isoliert messbar ist. **6**

Dennoch zeigen die von *Hohlfeld* und *Godulla* in Bezug genommenen Studien, dass die Bedeutung von Social Media qualitativ wie quantitativ beständig wächst. Auch wenn sich ihre Nutzung zahlenmäßig auf wenige Angebote wie Facebook, Twitter oder WhatsApp konzentriert, sind die dort gepflegten Kontakte nicht nur zu einem wichtigen Mittel des Identitätsmanagements, zum „Sozialkapital im 21. Jahrhundert" geworden, sondern nehmen mittlerweile auch eine wichtige Rolle bei der **Entstehung von Öffentlichkeit** ein. So bewirken soziale Netzwerke, dass Journalisten nicht mehr exklusive „Gatekeeper" öffentlicher Informationen sind. Sie tragen damit ein Stück weit zur Demokratisierung moderner Gesellschaften bei.[7] **7**

1.3 Vertragliche Aspekte der Social Media

Mit dem **3. Kapitel** beginnt der Einstieg in die juristische Analyse des Phänomens der Social Media.[8] Dieser von *Peter Bräutigam* und *Bernhard von Sonnleithner* verantwortete Beitrag widmet sich dem auf soziale Netzwerke anwendbaren Vertragsrecht. Da das BGB für diese modernen Kommunikationsmedien keine speziellen Regelungen bereithält, muss das jeweilige Angebot unter die normierten traditionellen Vertragstypen subsumiert werden. Diese Einordnung hängt vom konkreten Leistungsumfang ab, der bei Social Media nicht immer einfach zu bestimmen ist, zumal bei einigen Angeboten kostenpflichtige Angebotsteile neben kostenlose treten. Insbesondere ist fraglich, ob von einem entgeltlichen Vertrag ausgegangen werden **8**

---

[3] Facebook, YouTube, Google+ etc.
[4] Unter Einschluss sog. Microblogging-Dienste wie z. B. Twitter.
[5] Wie insbesondere Wikipedia.
[6] Wie insbesondere der Dienst WhatsApp.
[7] Besonders deutlich wird dies in Ländern, in denen traditionelle Medien (Rundfunk und Presse) unter staatlicher Kontrolle stehen. Hier haben sich soziale Netzwerke zu alternativen politischen Kommunikations- und Organisationsplattformen entwickelt. Eindrückliches Beispiel hierfür ist der „arabische Frühling".
[8] S. 35 ff.

kann, wenn vom Nutzer keine monetäre Gegenleistung geschuldet wird, sondern dieser mit seinen personenbezogenen Daten „zahlt“, die durch die Anbieter beispielsweise in Form von personalisierter Werbung oder Adresshandel monetarisiert werden.

9 Neben solchen vertragsrechtlichen Zuordnungsfragen sind es vor allem Fragen nach dem anwendbaren Recht und dem **Recht der Allgemeinen Geschäftsbedingungen**, die es im Kontext sozialer Netzwerke zu beachten gilt. Als problematisch erweist sich insoweit nicht selten, ob die für Social Media charakteristische Datenerhebung, -verarbeitung und -nutzung durch den Anbieter auch vertragsrechtlich wirksam mit den Nutzern vereinbart wurde. Daneben ist fraglich, ob Social-Media-Accounts vererbbar sind und – eine für die Praxis besonders bedeutsame Frage – ob **Minderjährige**, eine Hauptnutzergruppe sozialer Netzwerke, die gängigen Social-Media-Verträge selbstständig rechtswirksam abschließen können.

1.4 Datenschutzrechtliche Aspekte der Social Media

10 Mit dem Datenschutzrecht behandelt *Gerrit Hornung* im **4. Kapitel**[9] eine Querschnittsmaterie par excellence, die Bezüge zu allen anderen Kapiteln des Rechtshandbuchs aufweist. Die Interaktionsmöglichkeiten, welche Social Media und das „Web 2.0“ auszeichnen, bauen ganz entscheidend auf der Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf. Neben den (verfassungs-)rechtlichen Grundlagen des Datenschutzes im Grundgesetz und in der Europäischer Menschenrechtskonvention gibt der Beitrag einen Überblick über diejenigen einfachgesetzlichen Regelungen, die bereichsspezifisch datenschutzrechtliche Grundprinzipien (Verbotsprinzip, Zweckbindung, Erforderlichkeit, Datensparsamkeit, Transparenz etc.) umsetzen.

11 Neben dem Problem des Vorliegens personenbezogener Daten ist – umso mehr nach der jüngsten Rechtsprechung des EuGH – rechtlich problematisch, ob deutsches **Datenschutzrecht Anwendung** findet. Social Media mit ihren vielfältigen Datenauswertungen, Erhebungszusammenhängen (z. B. in Gestalt von Cookies für personalisierte Werbung) oder neuartigen Anwendungsformen (z. B. „Social Plug-Ins“) zwingen des Weiteren zu einem genauen Blick auf diejenigen Instanzen, die im Einzelfall Daten erheben und verwenden. Nur so vermag der datenschutzrechtlich Verantwortliche sicher bestimmt zu werden.

12 Neben diesen Fragen geht *Hornung* auch auf die **Zulässigkeit der Datenverarbeitung** im Rahmen von Social-Media-Nutzungsverträgen ein und nimmt dabei die Anbieter, die Zugriffe durch Dritte, aber auch die Verantwortlichkeit der Nutzer selbst in den Blick. Weitere Themenbereiche bilden die Frage der wirksamen Einwilligung durch Minderjährige, technische Lösungsansätze zum Datenschutz, der Umgang mit einem Social-Media-Account nach dem Ableben seines Inhabers sowie ein Ausblick auf die geplante EU-Datenschutz-Grundverordnung.

[9] S. 79 ff.

1.5 Haftungsrechtliche Probleme der Social Media

Das von *Gerald Spindler* verantwortete **5. Kapitel** ist den haftungsrechtlichen Fragen im Zusammenhang mit Social Media gewidmet.[10] Insoweit stellen sich einerseits die „klassischen" zivilrechtlichen Fragen einer deliktischen Haftung oder von Unterlassungs- und Beseitigungsansprüchen analog § 1004 BGB, andererseits aber auch spezielle Fragen zum Urheberrecht. Das allgemeine Zivilrecht wird dabei überlagert durch die speziellen Verantwortlichkeitsprivilegierungen des Telemedienrechts, welche die Haftung in Teilbereichen modifizieren oder gar ausschließen. Daneben zwingen die faktischen Gegebenheiten der Kommunikation im Netz bzw. die technischen Möglichkeiten teilweise zu einer Anpassung der Dogmatik. Dies ist etwa der Fall, wenn bei der Störerhaftung – z. B. für Foreneinträge in sozialen Netzwerken oder für die „Autocomplete"-Funktion von Suchmaschinen – auf die Verletzung zumutbarer Prüfpflichten abgestellt wird. Des Weiteren kann im Urheberrecht eine andere Auslegung des Begriffs der „öffentlichen" Zugänglichmachung im Vergleich zu Offline-Veröffentlichungen angezeigt sein, weil die Gegebenheiten der Online-Welt andere sind. So findet beispielsweise das „Teilen" von Inhalten durch eine Verlinkung auf Plattformen, die nur „Freunden" zugänglich sind, in der analogen Welt keine Entsprechung. **13**

Im Rahmen von Social Media sind darüber hinaus **unterschiedliche Rechtsverhältnisse** zu beachten: So ist nicht nur der Seitenbetreiber als „Anbieter" von den Regelungen des Telemediengesetzes erfasst, sondern oft auch derjenige, der lediglich eine Unterseite (etwa ein Profil auf einer Plattform) bereithält. Nicht immer ist also der „Content-Provider" klar vom Nutzer oder vom „Host-Provider" abgrenzbar. Zugleich kann eine Rechtsverletzung nicht nur im Verhältnis des Nutzers zum Seitenbetreiber von Relevanz sein, sondern auch gegenüber Dritten, die in keinem vertraglichen Verhältnis zum Anbieter stehen. Schwierige Fragen stellen sich zudem in Bezug auf Minderjährige, insbesondere hinsichtlich der für diese sowie ihre Eltern möglicherweise einschlägige Haftungsausschlüsse oder -modifikationen. **14**

1.6 Persönlichkeitsrechtliche Aspekte der Social Media

Eng mit diesen haftungsrechtlichen Fragen verbunden sind persönlichkeitsrechtliche Aspekte der Social Media, denen sich *Ralf Müller-Terpitz* im **6. Kapitel** widmet.[11] Denn über soziale Netzwerke können mit hoher Wirkkraft Persönlichkeitsbeeinträchtigungen gegenüber Dritten, die im Übrigen keine Nutzer dieser Plattformen sein müssen, begangen werden. **15**

[10] S. 131 ff.
[11] S. 163 ff.

16 Vor diesem Hintergrund stellt der Beitrag zunächst **Herleitung und Inhalt des allgemeinen Persönlichkeitsrechts** dar, um sodann auf typische Beeinträchtigungsformen durch Social Media (z. B. in Gestalt von Bewertungsportalen, Online-Prangern etc.) einzugehen. Dem werden die Grundrechtspositionen des Äußernden – insbesondere seine Kommunikationsfreiheiten – gegenübergestellt. Zwischen den widerstreitenden Belangen ist in der Rechtspraxis ein verhältnismäßiger Ausgleich herbeizuführen. Der Beitrag erörtert insoweit typische Abwägungsbelange, die es in Konstellationen sozialer Netzwerke zu berücksichtigen gilt (wie z. B. die weltweite Abrufbarkeit von Inhalten oder die Anonymität des Äußernden). Zum Schluss wird ein Ausblick auf die Frage geworfen, ob durch Instrumente der Selbstregulierung – etwa in Gestalt sog. „Cyber-Courts" – der Problematik von Persönlichkeitsbeeinträchtigungen auf sozialen Plattformen Rechnung getragen werden könnte.

1.7 Strafrechtliche Aspekte der Social Media

17 Auch das Strafrecht stellen Social Media vor neue Herausforderungen. Vor diesem Hintergrund geht *Robert Esser* im **7. Kapitel**[12] auf materiell-rechtliche und prozessuale Fragen ein, die sich aus einer Verlagerung von Kriminalität in Social Media, insbesondere Netzwerkplattformen, ergeben. Neben dem Schutz des Urheber- und Markenrechts stehen dabei Delikte im Fokus, die sich durch kommunikative Handlungen (Beleidigungen, Verletzungen der Privat- und Intimsphäre, „Cyberstalking", „Cybermobbing", Volksverhetzung etc.) auszeichnen. Insoweit können gängige Rechtsfiguren – wie etwa die beleidigungsfreien Räume – nicht unmodifiziert angewandt werden. Daneben ist es insbesondere das Sexualstrafrecht (Streaming illegaler pornographischer Inhalte etc.), welches durch das Internet im Allgemeinen und Social Media im Besonderen vor Herausforderungen gestellt wird. In diesem Rahmen geht der Beitrag auf neuere Entwicklungen durch das Unionsrecht, aber auch auf Reformvorschläge einzelner Bundesländer zur Verschärfung bestehender Regelungen (etwa zum „Posing" von Kindern) ein.

18 Weitere **netzwerktypische Begehungsformen** wie beispielsweise zu Schäden führende Facebook-Parties, Flashmobs oder verbrauchertäuschende Produktbewertungen (Rezensionen) werden ebenfalls eingehend gewürdigt, bevor sich *Esser* **strafprozessualen Fragen** rund um die Social Media zuwendet. Letztere werden in zwei Richtungen untersucht: Zum einen wird danach gefragt, wie in Social Media ermittelt und auf welche Kommunikationsdaten (z. B. aus einer Facebook-Kommunikation) auf der Grundlage des geltenden Strafprozessrechts zugegriffen werden darf. Zum anderen wird erörtert, in welcher Weise Social Media zur Ermittlung im Strafverfahren eingesetzt werden dürfen, etwa durch offene Fahndungsseiten der Polizei oder verdeckte Ermittler im Netz bzw. sog. „nicht offen ermittelnde Polizeibeamte".

[12] S. 203 ff.

1.8 Arbeitsrechtliche Aspekte der Social Media

Auf die arbeitsrechtlichen Aspekte der Social Media geht *Frank Bayreuther* im **8. Kapitel** ein.[13] Auch im Arbeitsleben haben diese zu einer Dynamisierung der Kommunikation geführt, woraus vielfältige rechtliche Fragen resultieren. So können Social Media arbeitsrechtlich aus zwei Perspektiven relevant werden: Zum einen ist fraglich, ob Arbeitnehmer zur Teilnahme an Social Media verpflichtet werden können und wie sich die durch Online-Kommunikation bewirkte ständige Verfügbarkeit auf ihre Arbeitszeit auswirkt. Zum anderen stellt sich die Frage, in welchem Umfang die Nutzung von Social Media während der Arbeitszeit gestattet ist bzw. vom Arbeitgeber verboten werden darf und wie sich eine außerdienstliche Nutzung möglicherweise auf das Arbeitsverhältnis auswirkt. Immer öfter hat die arbeitsgerichtliche Rechtsprechung in diesem Kontext über Beleidigungen des Arbeitgebers durch den Arbeitnehmer zu entscheiden, welche Letzterer in insbesondere in sozialen Netzwerken kommuniziert. Dies erfordert eine Abwägung seiner Meinungsfreiheit mit den Wirtschaftsgrundrechten und dem Unternehmerpersönlichkeitsrecht des Arbeitgebers. Entsprechende Wertungen sind von Relevanz, wenn der Arbeitnehmer in Social Media über Missständen in seinem Unternehmen berichtet (sog. „Whistleblowing“). **19**

Schließlich kann der Arbeitgeber Social Media auch zur **Überwachung** seiner Arbeitnehmer nutzen. Zudem bieten ihm soziale Netzwerke die Möglichkeit, sich bereits vor der Einstellung über das Privatleben und den Charakter eines Bewerbers zu informieren. Solche „Ermittlungsmethoden“ des Arbeitgebers werfen u. a. Fragen zum Arbeitnehmerdatenschutz auf. **20**

1.9 Medien- und internetrechtliche Anforderungen an Social Media

Im **9. Kapitel** sortiert *Hannes Beyerbach* Social Media in das Regelungsregime des Rundfunk- und Telemedienrechts ein.[14] Insoweit erörtert er zunächst die Frage, ob es sich bei Social Media um „Rundfunk“ handelt. Diese Analyse kommt zu einem differenzierten Ergebnis, da der (weite) verfassungsrechtliche Rundfunkbegriff i. S. d. Art. 5 Abs. 1 S. 2 GG nicht mit dem (engen) einfachrechtlichen i. S. d. § 2 Abs. 1 RStV identisch ist. **21**

Gesetzliche Anforderungen an Social Media ergeben sich – auch wenn sie den einfachrechtlichen Rundfunkbegriff nicht erfüllen – sowohl aus dem **Rundfunkstaatsvertrag** als auch aus dem **Telemediengesetz**. Die Vorgaben des Rundfunkstaatsvertrags richten sich an unterschiedliche Kategorien von Telemedien, was im Hinblick auf Social Media zu Abgrenzungsproblemen führt. Insbesondere der Begriff der „journalistisch-redaktionellen Gestaltung“ wirft neue Fragen auf; er ist für die Impressumspflicht und die Pflicht zur Veröffentlichung von Gegendarstellungen von Relevanz. **22**

---

[13] S. 323 ff.
[14] S. 361 ff.

23 Neben die rechtlichen Anforderungen an Social Media als solche treten im Rundfunkrecht noch Vorschriften zum Online-Engagement der **öffentlich-rechtlichen Rundfunkanstalten**. Diese – zumeist begrenzenden – Regelungen sind das Ergebnis eines langjährigen Streits über die Frage, was öffentlich-rechtliche Rundfunkveranstalter im Internet anbieten dürfen und was nicht. Hiervon betroffen ist auch die Frage, inwieweit sich der öffentlich-rechtliche Rundfunk Social Media zur Erfüllung seines Rundfunkauftrags bedienen darf.

1.10 Einsatz von Social Media durch die öffentliche Verwaltung

24 Social-Media-Applikationen haben schließlich auch – worauf *Sönke E. Schulz* im **10. und letzten Kapitel** des vorliegenden Rechtshandbuchs eingeht – Einzug in die Praxis der öffentlichen Verwaltung gehalten.[15] Zwar existieren nur vereinzelt spezielle Social-Media-Angebote von Behörden. Allerdings gehen diese vermehrt dazu über, die in großer Zahl von Bürgern genutzten Anwendungen (namentlich Facebook) auch für ihre Zwecke zu verwenden. So werden Social Media für die Öffentlichkeitsarbeit, aber auch zur Recherche oder gar zur strafrechtlichen Fahndung eingesetzt. Dies wirft die Frage nach der Zulässigkeit eines solchen Einsatzes von Social Media durch die öffentliche Verwaltung auf. Insbesondere die datenschutzrechtliche Zulässigkeit und die Einhaltung der Vorgaben des Telemedienrechts sind hierbei von Relevanz, wobei sich im Ergebnis ähnliche Fragen stellen wie bei Privaten. Die allgemeinen Haftungsgrundsätze für Telemedien werden nach Auffassung von *Schulz* allerdings durch allgemeine öffentlich-rechtliche Vorgaben – wie etwa die grundrechtliche Schutzpflicht oder das Diskriminierungsverbot – sowie durch die Vorgaben für staatliche Informationstätigkeit überlagert. Diese Modifikationen verbindet der Autor zu konkreten Handlungsempfehlungen für den Social-Media-Einsatz durch Behörden und Mandatsträger. Die klassischen Haftungsfragen des 5. Kapitels stellen sich von daher in anderem Gewande.

25 Erörtert wird daneben die Frage, inwiefern sich ein (scheinbar) privater Einsatz von Social Media durch Beamte und Angestellte der Verwaltung auf ihr Dienstverhältnis auszuwirken vermag. Diese Frage weist Parallelen zum Arbeitsrecht auf. Auch hierfür werden **Handlungsempfehlungen** („Social-Media-Guidelines“) vorgeschlagen.

1.11 Fazit und Ausblick

26 Wie der vorstehende Überblick zeigt, thematisiert das Rechtshandbuch eine Vielzahl relevanter und hoch aktueller Rechtsfragen, die sich aus dem privaten, beruflichen, aber auch öffentlichen Einsatz von Social Media ergeben. Die Beiträge verdeutlichen

[15] S. 429 ff.

dabei einerseits, dass der Lebenssachverhalt Social Media als Teil der „virtuellen Welt“ typische Fragen des sog. Online- bzw. Internet-Rechts tangiert. Das Phänomen Social Media – dies folgt aus dem Rechtshandbuch in einer Gesamtschau – weist allerdings auch **rechtliche Besonderheiten** auf, welche gerade für soziale Netzwerke mit ihren Interaktionsmöglichkeiten kennzeichnend sind. Hierzu gehören neben den vertrags-, haftungs- und datenschutzrechtliche Fragen, die sich insbesondere aus häufig bestehenden Dreiecks- oder Mehrpersonenverhältnis ergeben, auch solche zum Minderjährigenschutz, zum Umgang mit Inhalten verstorbener Nutzer, zur medienrechtlichen Einordnung sozialer Netzwerke sowie zu ihrem Einsatz für private oder behördliche Ermittlungszwecke oder generell zur Erledigung von Aufgaben durch juristische Personen des öffentlich-rechtlichen Rechts.

Ziel des Rechtshandbuchs ist es, diese besonderen Charakteristika von Social Me- **27**
dia rechtlich zu beleuchten und damit sowohl einen Beitrag zur wissenschaftlichen Durchdringung zu leisten als auch dem Praktiker den schnellen Zugriff auf Einzelfragen zu ermöglichen. Sollte trotz der verschiedenen rechtlichen Blickwinkel eine (Rechts-)Frage vermisst werden, sind Herausgeber und Autoren für entsprechende Ergänzungsvorschläge ebenso dankbar wie für sonstige konstruktive Hinweise.

Kapitel 2
Das Phänomen der Sozialen Medien

Ralf Hohlfeld und Alexander Godulla

Inhalt

2.1 Sozialer Charakter sozialer Medien

Soziale Medien beschreiben zunächst den schlichten Umstand, dass das Internet immer weiter in die Gesellschaft hineinwächst[1]. Ähnelten die Angebote der ersten Generation des Internets noch stark der Kommunikationsstruktur der traditionellen Massenmedien, entwickelten sich in der vergangenen Dekade unzählige Kanäle, **1**

[1] Vgl. Schmidt (2009).

R. Hohlfeld (✉) · A. Godulla
Inhaber des Lehrstuhls für Kommunikationswissenschaft, Universität Passau,
Innstr. 33a, 94032 Passau, Deutschland
E-Mail: ralf.hohlfeld@uni-passau.de

A. Godulla
Akademischer Rat, Lehrstuhl für Kommunikationswissenschaft, Universität Passau,
Innstr. 33a, 94032 Passau, Deutschland
E-Mail: alexander.godulla@uni-passau.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_2

Dienste und Plattformen, die den Netzwerkcharakter des Internets zur Anregung, Entwicklung und Stabilisierung sozialer Beziehungen nutzen. Internetauftritte werden dabei so gestaltet, dass ihre Gestalt von den Partizipationsmöglichkeiten der Nutzer mitbestimmt wird[2]. „Während der Informationsfluss in klassischen Internetangeboten weitgehend einseitig verläuft, erlaubt das Web 2.0 oder Social Web seinen Nutzern eine aktive Beteiligung mit geringen Einstiegshürden“[3]. Kommunikationstheoretisch betrachtet bestehen Soziale Medien aus den in unterschiedlichen Kombinationen verknüpften formalen Kategorien Kommunikation (der Verständigung dienender inhaltlicher Bedeutungsprozess[4], Interaktion (formaler Akt des In-Beziehung-Treten zwischen Nutzern[5], Partizipation (Teilhabe, die aus Initiation und Reaktion besteht) und Kollaboration (mit dem Zweck sozialer Sinnstiftung).

2 Treibende Kraft sozialer Medien ist der **Netzwerkgedanke**, der kleinere interpersonale Sozialbeziehungen mit größeren Sozialgebilden (Gruppen) verknüpft und vielfältige gesellschaftliche Effekte bewirken kann. Technisch gesehen ist das Metamedium Internet schon immer ein soziales Medium, denn durch die kommunikative Verbindung zwischen Nutzern entstehen automatisch Grundformen von Sozialität. Es bedurfte aber spezifischer Entwicklungsbedingungen, um im Zuge des Gebrauchs und der Aneignung echte soziale Formen auszubilden[6].

3 Soziale Medien im Internet sind eng verknüpft mit dem Begriff **Web 2.0**. Zwar bezweifeln Vordenker des Internets, dass sich Soziale Netzwerke, Weblogs und Wikis fundamental von den länger entwickelten Formen E-Mail, Chats, Homepages, Newsgroups und Foren unterscheiden, um die herum sich schon früh Communities gebildet hatten. So meint der Miterfinder des World Wide Web *Tim Berners-Lee*: „Wer sagt, im Web 2.0 gehe es um Blogs und Wikis, der meint Kommunikation von Mensch zu Mensch. Aber genau das sollte das Internet von Anfang an sein.“[7] Die dazu notwenigen Prinzipien haben zweifelsfrei schon früher existiert, jedoch wurden sie seinerzeit noch nicht genutzt. *Hamann* (2008) weist darauf hin, dass das Internet die Gesellschaft und deren Kommunikation nicht nur verändern kann, sondern dies seit seiner Umformung zum Web 2.0 – „Die nächste Generation Internet“[8] – auch tatsächlich tut.

4 In diesem Sinne ist zu unterscheiden zwischen dem **Potenzial** eines neuen sozialen Mediums und seinem tatsächlichen **Gebrauch**. Auch wenn bestimmte Techniken der interpersonalen Vernetzung in der digitalen Sphäre (Plattformen zum Austauschon von Daten, Upload- und Download-Funktionen, Verknüpfungen von Adressbüchern) schon früh vorhanden waren, so hat sich der soziale Gebrauch, etwa Sozialbeziehungen zu knüpfen, zu verstärken oder abzusichern, erst langsam entwickelt. Kommunikation und Vernetzung sind inhärente Merkmale des Internets;

---

[2] Vgl. Münker (2010).
[3] Leiner, Hohlfeld und Quiring (2010).
[4] Vgl. Maletzke (1998).
[5] Vgl. Pürer (2003).
[6] Vgl. Busemann, Fisch und Frees (2012).
[7] Berners-Lee zitiert in Hamann (2008).
[8] Meckel/Stanoevska-Slabeva (2008).

dass aber die Etablierung sozialer Beziehungen zum dominierenden Movens des Internets werden würde, war zur Jahrtausendwende noch nicht absehbar. Und doch haben sich, obwohl Foren und Communities schon seit der Frühphase des World Wide Web Formen von sozialer Kommunikation konstituiert hatten, die Gebrauchsweisen und Praktiken erst ab 2004 auszuformen begonnen, wie in Abschn. 2 gezeigt werden soll.

Zu den **Gebrauchsweisen** zählt, dass soziale Informations- und Unterhaltungs- **5**
plattformen von den Nutzern als komplementäre Alternativen zu den konventionellen Angeboten traditioneller Medien betrachtet und funktionalisiert werden.[9] Die Formate der aktuellen Internetöffentlichkeit sozial zu gebrauchen, bedeutet: Austausch statt bloßer Zurschaustellung, Kommentieren statt Konsumieren, Identitätsmanagement statt Selbstmarketing. In den weltumspannenden Zyklus des Austauschs werden per Link Hinweise auf Fundstücke aus dem Internet genauso eingespeist wie selbstproduzierte digitale Inhalte, die in allen multimedialen Aggregatzuständen verfügbar gemacht werden.

Die **sozialen Praktiken** des Teilens, Empfehlens und Filterns, die den Social Netwok Sites wie Facebook zum Durchbruch verholfen haben, sind nicht nur zur Hauptwährung sozialer Medien, sondern gleichsam des gesamten Internets geworden. Als Facebook 2009 den Like-Button einführte, wurde nicht nur eine neue Metrik für Marktteilnehmer, sondern für die gesamte soziale Kommunikation etabliert. Mit diesen Formen des Social Sharing können Nutzer nun von der Selektions- und Filterleistung anderer Nutzer profitieren.[10] **6**

Als **Merkmale** sozialer Medien lassen sich folgende **Praktiken** zusammenfas- **7**
sen: Es sind auf der Basis von so genannter Social Software operierende Dienste, die auf Austausch angelegt sind, stets gemeinschaftlich genutzt werden, die Möglichkeiten des Empfehlens und Bewertens enthalten, Schnittstellen und Verknüpfungen zu anderen Nutzern bilden und dadurch soziale Beziehungen konstituieren. Thematisch bzw. inhaltlich sind soziale Medien offen, formal umfassen sie alle Darstellungsformen, alle Medienformate und alle multimedialen Formen wie Text, Bild, Bewegtbild und Audio.

Wenn man vom konkreten Anbieter ausgeht, lassen sich Soziale Medien auf **8**
den ersten Blick typologisch nur schwer unterscheiden, da die besonders nutzungsstarken und kommerziell Erfolg versprechenden Plattformen wechselnde Allianzen eingehen, um letztlich unter einer Marke möglichst alle sozialen Dienste anbieten zu können. Soziale Medien sind flüchtig und beständig gleichermaßen. Hinsichtlich des beschriebenen Charakters des Sozialen werden sie lange überdauern, die **Netzwerkstruktur** digitaler Kommunikation dürfte sich evolutionär bewährt haben wie die Verbreitung des Schriftguts durch den maschinellen Buchdruck vor mehr als fünfeinhalb Jahrhunderten. Jedoch werden soziale Medien ihre Gestalt immer wieder verändern; Soziale Netzwerke wie Facebook im Jahr 2014 sind eine Momentaufnahme der Mediengeschichte.

[9] Vgl. Münker (2010).
[10] Vgl. Schmidt 2009; Busemann und Frees und Fisch (2012).

2.2 Übergang vom Internet zum Web 2.0

9 Zunächst ist das Internet noch weit davon entfernt, sich zum heute bekannten Web 2.0 mit seinen zahlreichen sozialen Implikationen zu entwickeln. Die technische Basis seiner Evolution bildet zunächst der **Computer**, dessen mechanisch operierende Vorläufer bereits im 18. Jahrhundert nachweisbar sind. Wesentliche Evolutionsschritte sind die Erfindung der Lochkarte als Speichermedium (1805) sowie der Bau des ersten programmgesteuerten Rechenautomaten durch *Konrad Zuse* (1941), ehe 1946 an der Universität von Pennsylvania eine erste elektronische Großrechenanlage in Betrieb geht. Rasant steigende Speicherkapazitäten bei gleichzeitiger Miniaturisierung der Technik lassen spätestens in den neunziger Jahren des letzten Jahrhunderts Computer entstehen, die sich zusehends für den Heimgebrauch eignen und die Grundlage für die beginnende Konvergenz aller Digitalmedien hin zum Plattformmedium Computer bilden. Anfang 2002 wird die Summe der mittlerweile weltweit verkauften Computer auf etwa eine Milliarde geschätzt.[11]

10 Die Etablierung dieser technischen Infrastruktur geht einher mit dem Aufbau des **Internets**, das in den 1960er- und 1970er-Jahren zunächst als Netzwerk zur Kommunikation mit E-Mails genutzt wird. Primär werden diese Kommunikationsformen in den Anfangstagen von staatlichen Institutionen und Universitäten genutzt.[12] Es bildet zugleich die Grundlage für den Aufbau des World Wide Web, dessen System von elektronischen Hypertext-Dokumenten („Websites“) nach klar definierten Regeln über sogenannte Hyperlinks miteinander verbunden sind. Dort als Digitalcode hinterlegte Elemente (Text, Foto, Video, Audio etc.) und Programme werden von Webbrowsern decodiert und in rezipierbare Inhalte transformiert.

11 Die daraus resultierenden **Kommunikationsinhalte** waren zunächst statischer Natur und wurden in ähnlicher Weise linear rezipiert – vom Sender zum Empfänger. Dies sollte sich zu Beginn dieses Jahrtausends ändern, als Nutzern allmählich die Möglichkeit zur kollaborativen Partizipation am Erstellen von Online-Inhalten geboten wurde. Charakterisiert wird diese Neudefinition der Kommunikationsmodi auch als „das lebendige Web, das Hypernet, das Mitmach-Web, das Schreib-Lese-Web“[13], wohinter sich nichts anderes als der mittlerweile geläufige Begriff vom Web 2.0 verbirgt.

12 Als Urheber des Begriffs hat *Tim O'Reilly* folgende **Definition** entwickelt: „Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them“.[14] Ein wesentlicher Faktor hinter dem Erfolg des Web 2.0 ist demnach das Phänomen der **Emergenz:** Netzwerkeffekte

[11] Vgl. detailliert Stockmann (2004).
[12] Vgl. Seufert und Gundlach (2012).
[13] Tapscott und Williams (2009).
[14] O'Reilly (2006).

verhelfen Anwendern zu einer besseren Nutzungserlebnis, wenn mehr Anwender das gleiche Produkt nutzen.

Das **wissenschaftliche Verständnis** hält mit dieser Entwicklung in vielerlei Hinsicht zunächst nicht Schritt. Sozialwissenschaftler, aber auch Juristen und Politiker begriffen die entstehende Struktur der sich allmählich vernetzenden Computer lange Zeit als eine Art Fortsetzung der bereits etablierten medial vermittelten Kommunikation mit anderen Mitteln. Doch im World Wide Web werden eigentlich dezentrale Computernetze in theoretisch unbegrenztem Umfang miteinander verknüpft, so dass rasch ein dynamisch wachsendes System mit einer eigenen Funktionslogik entsteht.[15] **13**

Wie *Schmidt* (2009) nachweist, fällt die **Bewertung** dieser Erstellung und Konsumierung nutzergenerierter Inhalte jedoch ambivalent aus. Neben Warnungen vor unerwünschten Eingriffen in die Privatsphäre und einem der Qualität nicht immer zuträglichen Konkurrieren von Experten und Laien um die Meinungshoheit werde zugleich das kreative **Potential** eines partizipativen Medienkonsums hervorgehoben. Vor diesem Hintergrund hat sich das Betreiben von sozialen Plattformen, auf denen Anwender Inhalte selbstständig veröffentlichen und teilen, zu einem florierenden Geschäftsmodell entwickelt. **14**

Selbst ausgesprochene Partikularinteressen lassen sich in diesem Kontext im Web 2.0 in funktionierende **Geschäftsmodelle** transformieren: „Durch Datenmanagement und Nutzerbeteiligung erschließen Web-2.0-Unternehmen den ‚Long Tail', den ‚langen Schwanz' von Märkten: Im Internet ist es auf effiziente Weise möglich, die Nachfrage kleiner Kundengruppen zu befriedigen oder ein Netz vieler kleiner Händler zu organisieren".[16] Gleichzeitig lässt sich eine einst bestehende Dichotomie zwischen Produzierenden auf der einen Seite und Rezipierenden auf der anderen Seite vor diesem Hintergrund nicht mehr aufrechterhalten. Die Digitalisierung aller Inhalte gestattet es Mediennutzern, sich an den jederzeit sichtbaren Präferenzen anderer zu orientieren (etwa in Gestalt der Zahl von „Likes" bei Facebook) oder sich (teil-)automatisiert passende Inhalte empfehlen zu lassen (wie dies Musikstreaming-Dienste wie Spotify anbieten). **15**

Vor diesem Hintergrund hat das Web 2.0 längst damit begonnen, nach und nach in alle Lebensbereiche vorzudringen. Vom „**Internet der Dinge**" ist die Rede, so wie es *Mark Weiser* 1991 in einem wegweisenden Text skizziert hat.[17] An die Stelle des mit dem Web 2.0 kommunizierenden Computers treten zusehends intelligente Gegenstände, die Teilfunktionen des stationären PCs substituieren.[18] Gleichzeitig nimmt die Bedeutung mobiler Endgeräte wie Smartphones und Tablets stetig zu, was die Nutzung von Web 2.0-Anwendungen von jedem Ort gestattet, der durch Satelliten- oder WLAN-Verbindungen ans World Wide Web koppelbar ist. **16**

[15] Lang und Bekavac (2004).
[16] Neuberger (2009).
[17] Weiser (1991).
[18] Vgl. Fleisch und Mattern (2005).

17 Der Rezipient kann vor diesem Hintergrund jederzeit mit neuen Nutzungsszenarien und -situationen experimentieren.[19] Die dahinter stehende Logik lässt sich unter der Formel „The Right Information, at the Right Time, in the Right Place“[20] zusammenfassen. Für das Web 2.0 typisch ist dabei der ständige Rollenwechsel: Beispielsweise lässt sich unterwegs mit Hilfe eines Smartphones ebenso ein YouTube-Video konsumieren, wie es unter ähnlichen Bedingungen mit Hilfe der eingebauten Produktionstechnik (Kamera und Mikrofon) produziert werden kann. Das Spektrum an Interaktionsmöglichkeiten steigt so theoretisch unbegrenzt an: „Nutzer gestalten Inhalte, schaffen sich ihre eigenen Räume und Tools und tauschen sich aus.“[21]

18 Im Web 2.0 wird damit jener Mechanismus wirksam, den *Alvin Toffler* 1980 bei der Charakterisierung neuer Geschäftsmodelle beschrieb: Verbraucher eines Produkts („consumer“) sind gleichzeitig als dessen Produzenten tätig („producer“), was sie zu **Prosumenten** macht.[22] Da sie im Zuge dieses Prozesses unwillkürlich ihre Präferenzen offenbaren, generieren sie im Web 2.0 fortwährend personalisierte Informationen. Diese stellen ein wertvolles Gut dar, das vom Anbieter der vermeintlich kostenlosen Plattform monetarisiert wird.[23] Bei der wissenschaftlichen Betrachtung öffentlicher Kommunikation gewinnt dieser Ansatz derzeit kontinuierlich an Relevanz.[24]

19 Das Resultat dieser Entwicklung ist die Etablierung einer ganzen Reihe von **Social-Web-Praktiken**, die sich vorrangig auf drei Bereiche richten. So dient das Identitätsmanagement der Darstellung ausgewählter Eigenschaften, durch die sich eine Person je nach Kontext unterschiedlich charakterisiert (z. B. privat genutzter Facebook-Account, geschäftlich genutzter Xing-Account). Das Beziehungsmanagement vernetzt die hier versammelten Identitätsmerkmale mit den virtuellen Repräsentationen anderer Nutzer. Als letzte Kategorie rückt das Informationsmanagement ins Blickfeld: Hier werden Informationen nicht nur ausgewählt und strukturiert, sondern darüber hinaus auch durch Relevanzzuschreibung (sei es durch automatisch auswertbares Anklicken, sei es durch „Liken“ etc.) für andere Nutzer mit Bedeutsamkeit versehen. Die Handlungskomponenten von Social-Web-Praktiken lassen sich daher in folgende Systematik überführen:[25]

[19] Vgl. Höflich und Hartmann (2007).
[20] Wolf und Hohlfeld (2012).
[21] Ahlers (2008).
[22] Vgl. Toffler (1980).
[23] Vgl. dazu detailliert Rn. 51 ff.
[24] Vgl. Knieper aud Tonndorf und Wolf (2011).
[25] Schmidt (2009).

Handlungskomponente	Tätigkeiten	Beispiele
Identitätsmanagement	Zugänglich-Machen von Aspekten der eigenen Person	Ausfüllen einer Profilseite; Erstellen eines eigenen Podcasts; Hochladen eines selbst erstellten Videos
Beziehungsmanagement	Pflege bestehender und Knüpfen neuer Relationen	Eintrag auf der Pinnwand eines Kontakts; Aussprechen oder Annehmen von Kontaktgesuchen; Verlinken von Weblogeinträgen
Informationsmanagement	Selektieren, Filtern, Bewerten und Verwalten von Informationen	Taggen einer Website; Bewerten eines Videos durch Punktevergabe; Abonnieren eines RSS-Feeds

Die hier vorgestellten Praktiken finden im Umfeld diverse Gattungen und Angebote statt, deren Ausdifferenzierung nun in Anschluss an *Schmidt* (2009) teilweise vorgestellt werden soll und deren Nutzen im Kapitel 6 beschrieben werden. **20**

2.3 Angebote im Web 2.0

2.3.1 Plattformen

Obwohl sich die **Angebotsvielfalt sozialer Medien** in den letzten Jahren kontinuierlich vergrößert hat, sind die Präferenzen der derzeit 54,2 Mio. deutschen Internetnutzer laut der Projektgruppe ARD/ZDF-Multimedia weitgehend stabil. So führen „die mehr oder weniger zielgerichtete Suche nach Angeboten und Informationen sowie die Kommunikation über E-Mail“[26] seit 1997 die Liste der meistgenutzten Anwendungen unverändert an. Wesentliche Gewinner im mittlerweile fast drei Stunden umfassenden Zeitbudget für Online-Anwendungen sind demnach Onlinecommunitys wie Facebook, die von 39 % der Internetnutzer wenigstens ein Mal pro Woche frequentiert werden.[27] **21**

Plattformen haben sich damit als Kommunikationsinfrastruktur auf breiter Basis etabliert. Netzwerkplattformen oder auch Social Network Sites (SNS) haben dabei in den vergangenen Jahren in Deutschland einen massiven Konzentrationsprozess durchlaufen. Facebook hat hier stetig seinen Marktanteil auf Kosten von Mitbewerbern wie SchülerVZ oder StudiVZ ausgebaut. So sind neun von zehn Nutzern sozialer Communitys mittlerweile bei Facebook angemeldet.[28] **22**

[26] Van Eimeren und Frees (2013).
[27] Van Eimeren und Frees (2013).
[28] Vgl. Busemann (2013).

23 Folgende **Merkmale** lassen sich Netzwerkplattformen zuschreiben:[29]

- Es handelt sich um einen **geschlossenen Raum**, dessen Nutzung ohne die Erstellung eines persönlichen Profils nur sehr eingeschränkt möglich ist. Es entsteht also eine langfristige Beziehung zwischen dem Anbieter der Netzwerkplattform und dem Inhaber des persönlichen Profils, da dessen Pflege und Weiterentwicklung Zeit kostet. Da in aller Regel keine Kompatibilität der Profile über die Grenzen verschiedener Plattformen hinweg besteht, hat das Profil nur innerhalb des geschlossenen Systems einen Wert. Dieser wird beispielsweise von Google dadurch gesteigert, dass unter dem Schlagwort „Einmal anmelden. Alle Google Produkte nutzen“[30] über einen Account Zugang zu verschiedenen Plattformen und Diensten gewährt wird. So ist beispielsweise der Datenaustausch zwischen dem sozialen Netzwerk Google+ und der Videoplattform YouTube möglich. Für den Nutzer wird es so zusehends unattraktiv, sich anderen Plattformen zuzuwenden.
- **Soziale Beziehungen** zwischen Nutzern werden explizit sichtbar gemacht, indem über Freundschafts- bzw. Kontaktanfragen Verbindungen zwischen Personen und Institutionen bestätigt werden. Dies wiederum macht es möglich, die Daten eines Accounts mit dessen sozialem Umfeld zu synchronisieren. Für den Plattformbetreiber werden so statistische Rückschlüsse auf potentielle Interessen des Nutzers möglich.
- Mit Hilfe des explizit gemachten Netzwerks von Freunden und Kontakten wird auf der Plattform navigiert, da die Relevanz von empfohlenen Inhalten basierend auf dem Verhalten registrierter Kontakte erhöht oder vermindert wird. Der Nutzer ist so Teil einer kollektiven Anwendungserfahrung, die mit der Zahl vorhandener Kontakte an Qualität gewinnt. Es ist daher attraktiv, reale soziale Beziehungen in die virtuelle Welt zu überführen, um in dem so entstehenden Bezugsraum über vorhandene und neu generierte Inhalte zu interagieren.

24 In enger Beziehung dazu stehen **Multimedia-Plattformen**, die Inhalte wie Video (YouTube, Vimeo), Fotos (Flickr, 500px) oder Audio (last.fm, spotify) in aller Regel über eine permanente Internetverbindung zur Verfügung stellen. Die Nutzung erfolgt dabei in einem sozialen Kontext, da für den Zugang ähnlich wie bei Netzwerkplattformen oft eine Registrierung notwendig ist. Diese verknüpft ein explizit gemachtes Nutzungsverhalten kontinuierlich mit dem personalisierten Account, so dass basierend auf selbstlernenden Algorithmen Rückschlüsse auf zu erwartende Nutzungswünsche und -präferenzen möglich werden. Erneut bietet es für die User Experience Vorteile, in eine explizit gemachte Beziehung zu anderen Anwendern zu treten, da deren Verhalten in Empfehlungen überführt wird. Das Bereitstellen eigener Inhalte ist häufig, aber je nach Plattform nicht immer möglich.

[29] Vgl. Schmidt (2009) in Anschluss an Boyd und Ellison (2007) und Richter und Koch (2008).
[30] Google (2014).

2.3.2 *Personal Publishing*

Im klassischen Verständnis von Öffentlichkeit war der über Medien zugängliche gesellschaftliche Diskurs einer kleinen Gruppe **professioneller Kommunikatoren** vorbehalten, die zumeist als Journalisten idealerweise im öffentlichen Interesse tätig wurden. Die „Herstellung und Bereitstellung von Themen zur öffentlichen Kommunikation“[31] war damit eine hochgradig professionalisierte Kommunikationsleistung, die Laienakteuren nur in sehr begrenztem Maße möglich war. Durch die sozialen Praktiken des Web 2.0 lässt sich diese Monopolisierung nunmehr schon seit einigen Jahren nicht mehr aufrechterhalten.[32] Die Zahl der in der Öffentlichkeitsarena tätigen Kommunikatoren ist vielmehr rasant angewachsen, da jeder Person mit Zugang zu technischen Produktionsmitteln wie Computern oder mobilen Endgeräten eine digitale Präsentationsarchitektur zur Verfügung gestellt wird. **25**

Das in diesem Kontext bedeutsamste soziale Medium ist das sogenannte **Weblog**. Der Begriff ging als Hybrid aus den Termini „Web“ und „Logbuch“ hervor und lässt sich erstmals im Jahr 1997 nachweisen.[33] Mittlerweile weitgehend durch die Kurform „Blog“ abgelöst, umschreibt der Begriff eine öffentlich auf einer Website geführte Publikation, die von einer oder mehreren Personen mit Inhalten jeder beliebiger Form (sogenanntem Content) gefüllt wird. Dabei kommen also auch multimediale Varianten wie Audio- und Videoinhalte (Podcasts bzw. Vodcasts) in Frage. Der Kostenaufwand ist dank freier Software wie WordPress relativ gering und korrespondiert mit vergleichsweise basalen Kompetenzen im Programmierbereich. **26**

Sechs wesentliche Merkmale lassen sich Weblogs zuschreiben:[34] **27**

- Die Kommunikation ist **individualisiert**. Einzelne Akteure können daher autonom über den gesamten Publikationsprozess entscheiden und sind dabei nicht mehr in die Restriktionen komplexerer Steuerungsroutinen eingebunden.
- Die Medienkommunikation ist **reflexiv**. Auf eine vorhandene Themenagenda wird also häufig reagiert, indem Themen übernommen oder Kommentare getätigt werden.
- Die Webkommunikation ist **verlinkt** und **vernetzt**. Längst ist die Rede von der Vernetzung aller Blogs zur Blogosphäre, also zu einer interdependent agierenden Kommunikationsstruktur der wechselseitigen Bezugnahme.
- Medienkommunikation wird **gefiltert** und **selektiert**. Die Thematisierungsleistungen anderer Kommunikatoren werden also je nach Präferenz des Blogs aus der Masse herausgehoben oder aber ignoriert.
- Alle Beteiligten treten in **Interaktion** zueinander. Es ist jederzeit möglich, vorhandene Blogeinträge von Nutzerseite zu kommentieren oder auch über soziale Netzwerke zu verbreiten. Dialogsituationen sind damit zumindest zeitversetzt möglich.

---

[31] Rühl (1980).
[32] Vgl. Hohlfeld und Strobel (2012).
[33] Schmidt (2006).
[34] Vgl. Bucher und Büffel (2005).

- Die Dichotomie Rezipient vs. Produzent bzw. Profi vs. Laie besteht nicht mehr. Mit der Demokratisierung der Kommunikationsmittel geht ein **Grenzverlust** zwischen diesen Sphären einher, der mit dem traditionellen Journalismus sowohl konkurriert, als ihn auch komplementiert.

28 Einer ähnlichen Logik folgen sogenannte **Microblogging-Dienste** wie Twitter, die ihren Nutzern die Versendung von Kurznachrichten in beliebig große Gruppen ermöglichen. Hier überstieg die weltweite Zahl der aktiven Accounts im Jahr 2012 die Grenze von 200 Mio.[35] Ähnlich wie bei komplexeren Bloganwendungen können auch hier Verlinkungen auf Artikel oder Multimedia-Plattformen versendet werden, was die Vernetzung zwischen sozialen Medien verschiedener Gattungen weiter vorantreibt.

2.3.3 Wikis

29 *Wikis* (von hawaiisch für „schnell“) sind über Hypertext verbundene Systeme von Webseiten, die von Nutzern nicht nur gelesen, sondern auch direkt im Browser editiert werden können. In einem **kollaborativen Prozess** entsteht so eine Sammlung von Informationen zu einem bestimmten Themengebiet. Das weltweit populärste Beispiel für ein *Wiki* ist die Online-Enzyklopädie Wikipedia, deren Mutterseite derzeit auf Platz 6 aller meistbesuchten Internetseiten steht.[36] Da sich der individuelle Profit bei diesem Einsatz sozialer Software nicht in einer materiellen Gratifikation oder einem klar definierbaren Vorteil niederschlägt, ist in der Betrachtung von Wikis mitunter vom „Rätsel der Kooperation“ die Rede.[37]

30 Tatsächlich ist die **Motivation** für die Partizipation an Wikis nicht hinreichend erklärt: „Individuelle Motive kommen zunächst einmal kaum in Frage, da in aller Regel die Autoren von Artikeln nicht persönlich benannt werden. Oft tauchen sie nur unter einer ‚IP-Nummer‘ (einer Internetadresse, aus der sich nicht auf die Identität schließen lässt) oder unter einem ‚Nickname‘ auf“.[38] Dennoch haben sich die hinter Wikis stehenden Softwarelösungen auf breiter Basis im sozialen Netz verbreitet, so dass heute eine Vielzahl themengebundener Projekte zu einem breiten Inhaltsspektrum besteht.

2.3.4 Instant Messaging

31 Insbesondere durch die fortschreitende Verbreitung von Smartphones hat **Instant Messaging** in den letzten Jahren enorme Zuwächse erfahren. Es handelt sich dabei

[35] Vgl. Pingdom (2013).
[36] Vgl. Alexa – The Web Information Company (2014).
[37] Vgl. Stegbauer (2009).
[38] Stegbauer (2009).

um Programme, die Anwender in Echtzeit über einen oder auch mehrere Kommunikationskanäle miteinander verbinden. Ähnlich wie auf Plattformen können die Nutzer Kontaktlisten pflegen und andere Personen dort wahlweise hinzufügen oder aber ihnen die Autorisierung verweigern. Dabei wird Kontakten auch in Echtzeit angezeigt, welche ihrer Kontaktpersonen derzeit eingeloggt und erreichbar sind. Plattformanbietern wie Facebook erwächst so im Kampf um Aufmerksamkeit eine ernstzunehmende Konkurrenz. So werden derzeit mehr als 50 Mrd. Kurznachrichten pro Tag über den Messagingservice WhatsApp versandt. Die Zahl der aktiven Nutzer beträgt 430 Mio.[39] Der Erfolg von WhatsApp hängt eng mit einem plattformübergreifenden Konzept zusammen. Es gestattet es den Nutzern, Inhalte über die Grenzen der Betriebssysteme mobiler Endgeräte hinweg zu teilen – beispielsweise zwischen iPhones (iOS) und dem derzeit am weitesten verbreiteten mobilen Betriebssystem Android. Da Facebook die Gefahren einer solchen Konkurrenz erkannt hat, kaufte es im Februar 2014 kurzerhand den Dienst für die erstaunliche hohe Summe von 19 Mrd. US$.

2.4 Nutzung sozialer Medien

Soziale Netzwerke haben in den Jahren zwischen 2004 und 2014 einen rasanten **32**
Bedeutungszuwachs erfahren; sie sind heute kein Nischenphänomen mehr, sondern haben insbesondere bei den so genannten Digital Natives, den Jahrgängen und Kohorten, die mit dem Internet ausgewachsen sind, einen Sonderstatus erlangt: Diese finden ihren Zugang zum Internet häufig direkt über Netzwerke wie Facebook. *Mende*, *Oehmichen* und *Schröter* (2013) sprechen davon, dass Facebook inzwischen auch „das „All-in-one-Medium" für die junge Generation geworden" ist. „Man hat hier nicht nur seinen persönlichen Freundeskreis, sondern Facebook entwickelt sich immer mehr auch zum Info- und Unterhaltungsportal" (ebd.). Durch den sozialen Charakter der Netzwerke gelangen viele Nutzer erst über das Teilen und Empfehlen von Hinweisen aus Facebook heraus ins Internet. „Facebook ist für seine Nutzer deshalb eine Art Tor zur Welt".[40] Mit der forcierten Integration publikumsattraktiver Applikationen (etwa Spiele, Chroniken, Newsfeeds) beschritt Facebook seit 2007 sukzessive einen Weg, der darin enden soll, dass dieses Netzwerk schlechthin zum „Betriebssystem des Internet" werden soll, was *van Eimeren* und *Frees* (2013) zufolge schon für einen Teil seiner Nutzer Realität geworden sei. Eine zukunftsweisende Frage wird sein, ob Facebook wie andere geschlossene Systeme oder so genannter „Walled Gardens" wie Google und Apple die Onlinenutzung seiner Mitglieder auf das geschlossene System begrenzen kann. Noch scheint das empirisch nicht der Fall zu sein, denn „nur" 16 % der Nutzer privater sozialer Netzwerke stimmten im Rahmen der ARD-ZDF-Onlinestudie 2013 der Aussage zu, alles Wichtige „innerhalb ihrer Community zu finden und das Internet außerhalb der Community nicht mehr so

[39] Vgl. Gantt (2014).
[40] Busemann, Fisch und Frees (2012).

wichtig zu empfinden".[41] Aber auch die Mehrheit der Netzwerknutzer, die weiterhin das Bedürfnis hat, sich flanierend im offenen Internet zu bewegen, weist mit Blick auf traditionelle Medien weniger eine konkurrierende oder substituierende als eine komplementäre Nutzungsweise auf. Die rasch gestiegene Nutzung sozialer Medien hat sich nicht in signifikanter Weise auf die Nutzung etablierter Medien ausgewirkt.

33 Anfang 2014 hat allein das soziale Netzwerk Facebook mehr als 1,2 Mrd. angemeldete Accounts; Facebook wird damit von rund 15 % der Weltbevölkerung genutzt. Die Social Media-Videoplattform Youtube hat eine monatliche Nutzerschaft, die ebenfalls über einer Milliarde Personen liegt. Rechnet man – ohne Doppelnutzung – die User anderer großer Social Media Plattformen wie renren.com in China oder VKontakte in Russland hinzu, dürfte die **weltweite regelmäßige Nutzung** von Social Media bei rund zwei Mrd. Menschen absolut und damit zwischen 25 und 30 % liegen.

34 Seit Facebook seine Aktivitäten auf die **mobile Nutzung** des Netzwerks konzentriert hat, ist die Facebook-App im Jahr 2013 zur meistgeladenen und -genutzten Applikation geworden. Auch im Bereich stationärer Computernutzung bildet Facebook häufig die Startseite. Mit der starken Verbreitung von Smartphones und Tablet-Computern steigt nicht nur die Nutzung des Internets[42], sondern speziell die mobile Nutzung sozialer Medien rasant an (BITKOM 1983). Bei den 14–29-Jährigen greifen schon 74 % der Nutzer sozialer Netzwerke von unterwegs auf soziale Medien zu.

35 Das Internet wurde 2013 in Deutschland von 54,2 Mio. Personen ab 14 Jahren genutzt, was einer **Reichweite** von 77,2 %[43] und einer Verzehnfachung seit 1997 entspricht.[44] Knapp 80 % der Internetnutzer haben sich zumindest in einem sozialen Online-Netzwerk offiziell angemeldet, gut zwei Drittel der Internetnutzer nutzen soziale Medien aktiv.[45] Damit dürfte die Zahl der deutschen Social Media-Nutzer zum Zeitpunkt der Veröffentlichung bei über 40 Mio. liegen, hinzu kommt eine „Dunkelziffer" der unter 14-Jährigen, die unterdessen in großer Zahl sehr aktiv soziale Dienste wie „Whatsapp" nutzen, ein Dienst, der unterdessen für 19 Mrd. Dollar von Facebook gekauft wurde.

36 Da sich die allgemeine Internetnutzung und die Social Media-Nutzung infolge der wechselseitigen Durchlässigkeit kaum analytisch trennen lassen, gibt es wenig belastbare Zahlen für die **Dauer** der täglichen Social Media-Nutzung. Nach Schätzungen von *Weinberg*, *Pahrmann* und *Ladwig* (2012), die sich auf Zahlen von BITKOM (2013) berufen, entfällt in Deutschland ein Viertel des Onlinekonsums, der bei 169 min täglich liegt, auf soziale Netzwerke. Das entspricht einer täglichen Social-Network-Nutzungsdauer von durchschnittlich über 40 min. Da hier aber auch die Nichtnutzer der sozialen Dienste eingerechnet sind, liegt die tatsächliche

[41] Busemann (2013).
[42] Vgl. van Eimeren und Frees (2013).
[43] Van Eimeren und Frees (2013).
[44] Mende, Oehmichen und Schröter (2013).
[45] BITKOM (2013).

Nutzungsdauer der Social-Media-User bei über einer Stunde. Auch die ARD-ZDF-Onlinestudie kam 2013 zu dem Ergebnis, dass die durchschnittliche Nutzungsdauer pro Tag bei 63 min liegt, die 14–29-Jährigen verbringen sogar durchschnittlich 87 min mit ihren bevorzugten privaten sozialen Netzwerken.[46] Zieht man die Perspektive der Lebensstile hinzu, so werden private Soziale Netzwerke bevorzugt von den „Jungen Wilden" (87 %) und den „Zielstrebigen Trendsettern" (73 %) genutzt.

37 Eine große Mehrheit (etwa 85 %) der (erwachsenen) aktiven Netzwerknutzer in Deutschland besitzt ein **Facebookprofil**, alle anderen Netzwerke wie Stayfriends, Google+ und XING bilden hier unter aufmerksamkeitsökonomischer Perspektive nur den Longtail dieses Marktes. Der deutsche Branchenverband BITKOM (2013) gibt an, dass rechnerisch jeder Internetnutzer bei 2,5 Netzwerken angemeldet ist (ebd.). Zwei von fünf Internetnutzern sind mindestens einmal pro Woche in einem sozialen Netzwerk aktiv, bei den Jüngeren sind es sogar drei von Vieren.[47] Bei den aktiven Nutzern sozialer Netzwerke ist die Nutzung stark habitualisiert: 69 % der Mitglieder nutzen soziale Netzwerke täglich, bei den Jüngeren sind es gar 89 %.

38 Die absoluten Zahlen für die Nutzung sozialer Medien in Deutschland liegen unterdessen im zweistelligen Millionenbereich. Im Jahr 2010 hatte Facebook 5,75 Mio. aktive Nutzer, drei Jahre später waren es fünfmal so viele. Gleichwohl ist ein exponentielles **Wachstum** in der Zukunft unwahrscheinlich. Da Facebook die automatische Erfassung von Nutzerzahlen im Herbst 2013 unterbunden hat, müssen die Zahlen geschätzt werden; *allfacebook* (2014) zufolge hatte Facebook Anfang 2014 ca. 26 bis 27 Mio. Nutzer, die zumindest monatlich aktiv waren, 19 Mio. Nutzer waren sogar täglich aktiv. Nimmt man statt der aktiven Benutzer die Zahl der Besucher (inkl. Mehrfachbesuchen) zum Maßstab, lag Facebook 2013 bei knapp 40 Mio., Google+ bei 6,7 Mio. und XING bei 5,2 Mio.

39 Vergleicht man die Nutzung aller möglichen Social Media-Anwendungen, dann liegen **Private Netzwerke** und **Communitys** deutlich vorne. 41 % der Onliner in Deutschland nutzen diese mindestens einmal wöchentlich, bei Wikipedia und den Videoportalen (vor allem Youtube) sind es je 32 %, bei beruflichen Netzwerken wie XING und bei Weblogs sind es je vier Prozent, bei Twitter nur zwei Prozent.[48] Das Wachstum der Sozialen Netzwerke verläuft dabei rasant: 46 % der Onliner hatten 2013 ein Profil bei einer privaten Community, 2007 waren es nur 15 %.[49]

40 Dagegen stagniert die Nutzung **beruflicher Netzwerke** wie XING und LinkedIn auf bescheidenem Niveau: 2007 wie 2013 hatten je zehn Prozent aller Onlinenutzer ein Profil in einem solchen Netzwerk, das sie zumindest selten genutzt hatten. Nur in der Gruppe der 30–49-Jährigen liegt die Nutzung signifikant höher, bei den über 50-Jährigen gibt es mit nur zwei Prozent keine nennenswerte Nutzung beruflicher sozialer Netzwerke.

[46] Busemann (2013).
[47] Van Eimeren und Frees (2013).
[48] ARD-ZDF-Onlinestudie (2013).
[49] Busemann (2013).

41 Die Bedeutung des **Microblogs Twitter**, die in Deutschland bislang bescheiden war, nimmt hingegen seit 2013 deutlich zu. Unterdessen nutzen sieben Prozent der Onlinenutzer Twitter, im Jahre 2010 waren es nur drei Prozent. Besonders stark wird Twitter von den 14–29-Jährigen genutzt (14 %), besonders schwach ist die Nutzung bei den über 50-Jährigen. Nur ein Drittel der Twitteruser gehört zu den aktiven Nutzern, verfasst also selbst Tweets. Im Jahr 2013 waren das insgesamt 1,2 Mio. Deutsche. Fast ebenso hoch ist mit 29 % der Anteil derer, die Twitterkanäle von Fernsehsendern benutzen. In diesem Zusammenhang ist auch die so genannte *Second Screen*-Nutzung aufschlussreich. Mehr als 20 % der Onlinenutzer in Deutschland nutzen das Internet mit seinen Social Media-Anwendungen gelegentlich unter direktem Bezug zu einer parallel genutzten Fernsehsendung. Aus diesem Nutzungsmuster wird ein vergleichsweise großes Potenzial für die Entwicklung und Etablierung von Social TV-Formaten abgeleitet. Die zeitgleiche Nutzung von TV und Internet ohne jeden inhaltlichen Bezug liegt bei 38 %, bei den 14–29-Jährigen ist die zumindest gelegentliche Parallelnutzung mit 58 % schon weit verbreitet.

42 Die **Sättigung der Bevölkerung** mit sozialen Medien wird in absehbarer Zeit erreicht werden; eine Deckelung der Internetnutzung wird ca. 2018 in Deutschland bei 85 % erwartet[50], so dass künftig letztlich kaum mehr als von 75 % der Gesamtbevölkerung soziale Medien zumindest gelegentlich genutzt werden. Anders als das Fernsehen werden soziale Medien zwar eine starke, aber wegen der erforderlichen *Computer Literacy* (Digitale Kompetenz) auf überschaubare Zeit keine flächendeckende Verbreitung in der Bevölkerung erfahren. Erst wenn die Kohorte der heute 14–29-Jährigen, von denen 2013 rund 95 % bei Facebook angemeldet waren, in die Jahre kommt, dürfte aus Sicht der Mediennutzungsforschung theoretisch noch eine weitere Anhebung möglich sein.

2.5 Nutzen sozialer Medien

43 Unter dem Nutzen sozialer Medien ist in erster Linie die **funktionale Aneignung** der sozialen Praktiken durch den Nutzer zu verstehen. Darunter sind konkrete Handlungsweisen zu fassen, die kommunikativen und sozialen Zielen dienen. Wie in Kap. 2 gezeigt, unterscheidet *Schmidt* (2009) beim Nutzen und den Zielen des Gebrauchs sozialer Medien zwischen den Handlungskomponenten Identitätsmanagement, Beziehungsmanagement und Informationsmanagement. Das Social Web ermöglicht also die Entwicklung digitaler Identitäten (Identitätsmanagement), die Bildung von sozialem Kapital (Beziehungsmanagement) und die Teilhabe an der kollektiven Informationsverteilung und Wissensentstehung (Informationsmanagement). Der Aufbau digitaler Identitäten und die Bildung sozialen Kapitals lassen sich auch gemeinsam unter den Begriff Reputationsmanagement[51] subsumieren.

[50] Van Eimeren und Frees (2013).
[51] Schulzki-Haddouti und Lorenz-Meyer (2008).

Soziale Netzwerke und das Feedback, das Nutzer aus diesen Netzwerken erhal- **44**
ten, „stellen wichtige Ressourcen bei der Konstruktion der eigenen Identität dar".[52] Das **Identitätsmanagement** mit dem Nutzen des Aufbaus einer digitalen Identität lässt sich in Zusammenhang mit dem gesellschaftlichen Wertewandel hin zu postmateriellen Bedürfnissen wie Selbstverwirklichung und Individualisierung bringen. Die Teilhabe an sozialen Medien, deren Zugang offen und deren Beherrschung nicht sehr voraussetzungsreich ist, versetzt Menschen in die Lage, sich als Individuen zu entfalten, was ihnen notabene in der modernen Gesellschaft als sozialer Zwang begegnet.[53] Die Selbstdarstellung der Menschen in den sozialen Medien wird über die „autorisierte Freigabe von Informationen, die mit der eigenen Person verknüpft sind"[54] verwirklicht. Die sich meist über das Ausfüllen einer Profilseite in sozialen Medien bildende digitale Identität – als bewusste Entscheidung über die Freigabe von Persönlichkeitsmerkmalen – dient dabei dem dynamischen Abgleich von Selbst- und Fremdbild des Nutzers. Hinter ihr verbergen sich einerseits Aspekte anzuzeigender Kommunikationsbereitschaft wie auch die Ungewissheit, inwieweit Online-Repräsentation und „Identität außerhalb des Bildschirms"[55] übereinstimmen. Der soziotechnische Raum der sozialen Netzwerke birgt neben dem Nutzen zudem Risiken für das Identitätsmanagement, die *Maireder* und *Nagl* (2010) als Praktiken struktureller Gewalt im Netz unter dem Begriff „Identitätsraub" bekannt gemacht haben.

Das **Beziehungsmanagement** lässt sich nur schwer vom Identitätsmanagement **45**
trennen, da Identität immer ein Produkt der Schnittmenge des Individuums mit der es umgebenden Gesellschaft ist. Ein Identitätsmanagement ohne Berücksichtigung der Sozialbeziehungen ist schlechthin nicht vorstellbar. Aufbau und Pflege von Kontakten sind in der analogen Welt nie weniger wichtig gewesen, nur sind digitale Medien, die netzwerkartig verbunden sind, eine technische Erleichterung, um Kontakte herzustellen, zu festigen und zu verstetigen. Die Wahl des Kanals für das Beziehungsmanagement präfiguriert dabei die Art der Beziehung. Für die Etablierung und Festigung so genannter *strong ties*[56] gilt der persönliche physische Kontakt auch heute noch immer als funktionaler Modus. *Weak ties* und unverbindlichere Sozialbeziehungen lassen sich einfacher und zielführender über digitale Kanäle bewerkstelligen. Dies schließt jedoch nicht aus, dass feste Sozialbeziehungen (etwa innige Freundschaften unter Jugendlichen) heute häufig selbst unter physischer Anwesenheit auf kleinstem Raum zum mobilen digitalen Modus wechseln und über gruppenorientierte Shortmessage-Dienste wie Whatsapp kommunizieren, also Beziehungen „managen". Es gilt: „Die Zunahme der möglichen Kanäle erhöht einerseits die Optionen für das Beziehungsmanagement, verkompliziert es andererseits aber auch, weil die Kanäle mit jeweils unterschiedlichen Verwendungsregeln verbunden

[52] Maireder und Nagel (2010); vgl. zudem Boyd (2006).
[53] Schmidt 2009; Schroer (2006).
[54] Grieser (2010).
[55] Schmidt (2009).
[56] Granovetter (1983).

sind".[57] So schätzen es Jugendliche in der Regel nicht, wenn Eltern in erzieherischer Absicht in Facebook-Chats und andere digitale soziale Räume eindringen, in denen Jugendliche ihre Sozialbeziehungen pflegen.

46 Der Nutzen sozialer Beziehungen wird in den Sozialwissenschaften unter dem Begriff des **sozialen Kapitals** erfasst.[58] *Bourdieu* (1983) folgend wirkt sich das durch soziale Beziehungen gebildete Sozialkapital auf den Einfluss und die Produktivkraft des Einzelnen aus. Soziale Netzwerke wirken dabei an der Schaffung und Nutzung von Sozialkapital unterstützend mit. Drei Arten von Sozialkapital können in sozialen Netzwerken identifiziert werden: 1) Überbrückendes (bridging) Kapital für schwache Bindungen (*weak ties*) zu räumlich oder sozial entfernten Personen, das vorrangig dem Informationsfluss dient (Information über offene Stellen, Vermittlung von Geschäftskontakten). 2) Bindendes (*bonding*) Kapital, das aus starken, emotionalen Verbindungen zu nahestehenden Personen (Familie, enge Freunde) gewonnen werden kann und das starke immaterielle und materielle Hilfe einschließen kann[59]: Wer seine Sozialbeziehungen pflegt, der kann in schwierigen Zeiten aussichtsreich auf Hilfe hoffen. 3) Bewahrendes (*maintained*) Kapital zur Aufrechterhaltung sozialer Beziehungen über Lebensphasen hinweg. Mit dieser Kapitalart wird dem Umstand Rechnung getragen, dass viele Facebook- und Stayfriends-Nutzer den Wunsch haben, über ihr Netzwerk nach dem Schul- oder Studienabschluss oder nach einem beruflich veranlassten Wechsel des Wohnortes mit ihrem sozialen Umfeld in Verbindung zu bleiben.[60]

47 Als **Einflussgrößen** auf die Bildung von Sozialkapital (als Ertragsform des Beziehungsmanagements) konnten Investitionen in Zeit und das Vorschussvertrauen identifiziert werden.[61] Während eine bloße Vielzahl von Kontakten und Freunden (durch die Dominanz der schwachen Bindungen) nicht automatisch zu einer Erhöhung des Sozialkapitals führt, sind eine aufwändige Pflege der Profile und der einzelnen starken Bindungen, die meist schon aus der Offline-Welt stammen, sowie eine starke Partizipation an Diskussionen in wichtigen Gruppen der Anhäufung sozialen Kapitals zuträglich.

48 Das **Informationsmanagement** betrifft in erster Linie den Umgang mit Informationen in Netzwerkumgebungen. Wenn man mit *Meyer-Lucht* (2008) das Social Web als „multiagorale Gesellschaft" versteht, stellt sich die Frage nach den Praktiken, welche die Nutzer befähigen, Informationen zu bearbeiten. Durch die technischen Möglichkeiten des Auswählens, Filterns, Bearbeitens und Weiterverbreitens hat das Internet einen Wandel von der Suchkultur zur Verweiskultur vollzogen. „Wenn die Nachricht wichtig ist, wird sie mich finden", soll ein amerikanischer College-Student in einer Studie über Onlinenachrichten gesagt haben (Stelter 2008).

49 Was mit RSS-Feeds und Alerts begann, mit denen neue Einträge favorisierter Weblogs und neue Treffer für bestimmte Suchanfragen automatisiert den Empfänger erreichen, hat seit wenigen Jahren mit den Facebook- und Twitter-Schnittstellen,

---

[57] Schmidt (2009).
[58] Leiner und Hohlfeld und Quiring (2010).
[59] Granovetter (1983).
[60] Ellison, Steinfield und Lampe (2007).
[61] Leiner, Hohlfeld und Quiring (2010).

die per Knopfdruck das Gefallen durch „Liken“ (Gefällt mir) oder Favorisieren dokumentieren bzw. das Teilen und gruppenbezogene Weiterleiten ermöglichen, eine komplett **neue Metrik** geschaffen. Im aufmerksamkeitsökonomischen Longtail des Social Web treten an die frühere Stelle harter, nicht revidierbarer Selektionsentscheidungen unidirektionaler Massenmedien nun die „empfehlende Orientierung und revidierbare Auswahl“[62], die durch „Mechanismen des sozialen Filterns“ (Schmidt 2009) erleichtert werden.[63]

An der **Umstellung dieses Modus** haben soziale Medien und die ihnen zugrundeliegenden Techniken einen großen Anteil. Dienste, die das Social Bookmarking und das Social Sharing ermöglichten, haben neben die Pull-Logik (Ziehen von Informationen) eine Push-Logik (Drücken von Informationen) treten lassen, die im Sinne von automatisierten „Das-könnte-Sie-interessieren-Angeboten“ fungieren. Ebenfalls zur informationellen Orientierung genutzt werden können differenziertere Bewertungen, die andere Nutzer vornehmen. Für die Aggregation solcher Bewertungen stehen Social News-Plattformen zur Verfügung. Heute nehmen die vielfach unverlangten Empfehlungen (etwa durch Prinzipien wie das Frictionless Sharing) und die extern generierten Ranking- und Bewertungssysteme Einfluss auf Informationsentscheidungen im Internet und moderieren das Informationsmanagement in sozialen Medien. In welcher Weise und nach welchen Mustern und Regeln das geschieht, die Frage also, ob es ein routinehaftes Informationsverhalten im Social Web gibt, ist noch nicht hinreichend Gegenstand der Rezeptionsforschung.[64] Ebenfalls empirisch ungeklärt sind die Folgen des neuen Informationsmanagements: Erreichen den Nutzer sozialer Medien bessere, weil individualisierte und passgenauere Informationen, die auf die Bedürfnisse und Präferenzen der Kommunikationsteilnehmer abgestimmt sind, oder führt die filterbasierte Verweiskultur in der Kombination mit Algorithmen getriebenen Suchanfragen dazu, dass Nutzer im sozialen Netz immer stärker in einer „Filter Bubble“ leben, wie *Eli Pariser* (2012) glaubt? **50**

2.6 Beitrag sozialer Medien für die Entstehung von Öffentlichkeit

Im kommunikationswissenschaftlichen Sinn wurde **Öffentlichkeit** lange Zeit exklusiv über das Engagement professionell tätiger Kommunikatoren (insb. Journalisten) hergestellt, die für sich einen Sonderstatus bei der Definition relevanter Themen reklamieren konnten. Zusammenfassend lässt sich dieser Prozess aus folgender Definition ableiten: **51**

> Ö. K. ist heute vorwiegend eine durch Massenmedien vermittelte Kommunikation. Die Massenmedien institutionalisieren die Öffentlichkeit, sie erhöhen die Geschwindigkeit der Kommunikationsübermittlung und ermöglichen es, ein allgemeines Publikum zu erreichen

[62] Neuberger (2009).
[63] Vgl. Hohlfeld (2012).
[64] Vgl. Schmidt (2009).

> [. . .] Als Vermittler fungieren in der massenmedialen Öffentlichkeit die professionellen Kommunikatoren. Journalisten wählen Themen aus und beeinflussen durch ihre Berichterstattung, wie diese in der Öffentlichkeit dargestellt und wahrgenommen werden.[65]

52 Die dahinter stehende **Produktionslogik** wird typischerweise mit dem Begriff des Gatekeeping umschrieben. Dieser Ansatz begreift Kommunikatoren mit privilegiertem Medienzugang (etwa Redakteure oder Herausgeber von Publikationen) als Schleusenwärter, die am Tor nur jene Inhalte passieren lassen, die ihren beruflich tradierten Selektionskriterien gerecht werden. Diese Leistung ist aus institutioneller Perspektive unverzichtbar, da vom Publikationsraum über die Rezeptionszeit bis hin zum für die Produktion vorhandenen Budget sämtliche Ressourcen begrenzt sind. Hinzu kommen nicht zwingend im öffentlichen Interesse liegende „Hausregeln“[66], die Ereignisse als hervorhebens- oder ignorierenswert erscheinen lassen, wenn sie nicht mit den Interessen des Medienunternehmens kongruent sind.

53 Diese demokratietheoretisch nicht unbedenkliche Konstruktion war grundsätzlich kennzeichnend für die überwiegende Zeit der Existenz publizistischer Medien, so man deren Beginn in der Zeit der Erfindung des Buchdrucks mit beweglichen Lettern verorten will.[67] Da seitdem stets wenigstens ein technisches Medium auf Seiten des Senders vorhanden sein musste, war der Zugang zu **publizistischer Macht** grundsätzlich mit vergleichsweise hohem Aufwand und allerlei Zugriffsschranken verbunden. Vor dem Aufkommen sozialer Medien ließ sich aktuelle Öffentlichkeit daher als eine starre Dichotomie darstellen, in der das Publikum passiv und dispers (also verstreut) über Gatekeeper Zugang zu von deren Seite monopolisierten Quellen erhielt.

54 Wie *Neuberger* (2009) in Abb. 2.1 zeigt, hat das Internet die Rolle des Journalismus vor diesem Hintergrund nachhaltig verändert. So kommt ihm nur noch außerhalb des Internets seine Rolle als **Gatekeeper** zu. Innerhalb der digitalen Welt können die Nutzer jederzeit in Verbindung zueinander treten und sowohl über den Umweg journalistischer Vermittlung als auch direkt mit Quellen interagieren. Der Journalist wird dabei zu einem Gatewatcher, der Orientierung in der Vielzahl vorhandener Stimmen bietet und Zusammenhänge herstellt. Außerdem moderiert er die in öffentlichen Foren stattfindende Laienkommunikation. Neben den Nutzern sind auch institutionell agierende Kommunikatoren wie die Öffentlichkeitsarbeit nicht mehr darauf angewiesen, dass sie der Journalist die Schleuse zur Öffentlichkeit passieren lässt.

55 Die „entmonopolisierten Herstellung und Bereitstellung von Themen zur öffentlichen Kommunikation“[68] bewirkt durch das Crowdsourcing (kollaborative Zusammenarbeit zur Herstellung und Verbreitung von Medienprodukten) eine Rückkehr der Öffentlichkeit in gesellschaftliche Nischen. Diesem netzwerkbasierten

---

[65] Pfetsch und Bossert (2012).
[66] Bruns (2009).
[67] Wilke (2008).
[68] Hohlfeld und Strobel (2012).

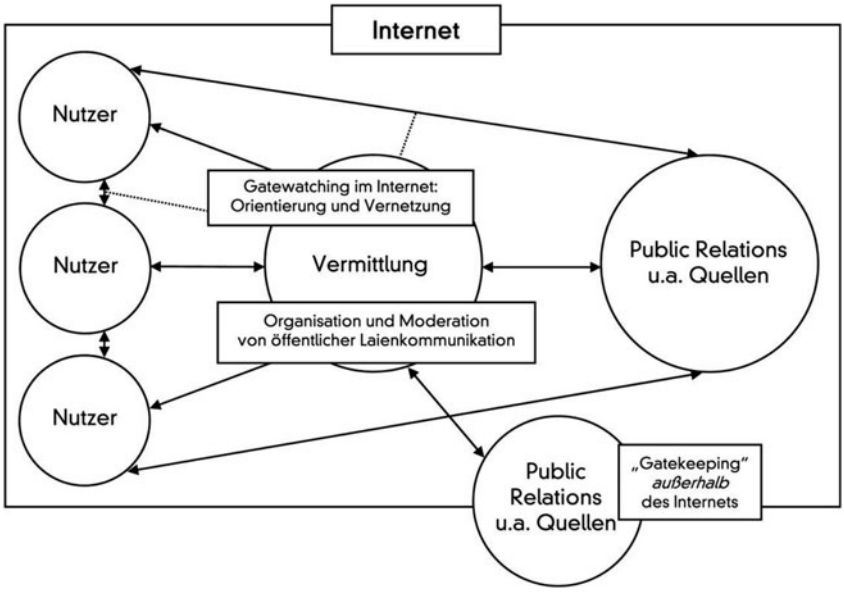

Abb. 2.1 Vermittlungsleistungen in der aktuellen Internetöffentlichkeit (Neuberger). (Quelle: Neuberger 2009, S. 55)

Prinzip wächst nun bei der Vermittlung und Herstellung von Öffentlichkeit eine zunehmend wichtige Rolle zu.[69] Insofern werden in der zeitgemäßen Onlineforschung die Formate der partizipativen Vermittlung als Indikatoren für einen neuerlichen Strukturwandel der Öffentlichkeit gedeutet.[70]

Als Konsequenz der zunehmenden Berücksichtigung von **User Generated Content** (UGC), der vor allem durch soziale Medien produziert wird, verliert das Gatekeeping-Modell zugunsten eines nicht nur von Journalisten verantworteten, sondern auch kollaborativen Gatewatching-Ansatzes an Bedeutung.[71] Dem Gatewatching-Ansatz zufolge weicht die klassische professionelle Nachrichtenselektion allmählich einer kollektiven, netzwerkartigen Nachrichtenbeobachtung. Die Themensetzung (sogenanntes „Agenda-Setting") ist grundsätzlich für alle am Kommunikationsprozess partizipierenden Individuen und Gruppen möglich geworden. **56**

Bei der Betrachtung sozialer Medien muss jedoch auch festgehalten werden, dass die nachweislich vorhandenen **Interaktionspotentiale** nur von einer Minderheit der Anwender genutzt werden. So war 2011 in den Ergebnissen der ARD-ZDF-Onlinestudie zu lesen, dass beispielsweise nur drei von hundert Wikipedia-Nutzern **57**

[69] vgl. Godulla und Hohlfeld (2013).
[70] Engesser und Wimmer (2009).
[71] Bruns (2009); Neuberger (2009).

auch zur Verbesserung der Enzyklopädie beitragen, indem sie dort vorhandene Informationen aktiv verbesserten. In ähnlicher Weise wurden Videoplattformen zwar intensiv rezipiert, jedoch nur von sieben Prozent der Nutzer verwendet, um eigene Inhalte zu präsentierten.[72] Einen nennenswerten Anstieg lässt sich dort auch zwei Jahre später in der Produktionsaktivität nicht verzeichnen.[73]

58 Dennoch wäre es ein Irrtum zu unterstellen, dass soziale Medien langfristig keinen Einfluss auf die öffentliche **Entstehung** und **Priorisierung** von Themen haben. So verfassen beispielsweise im Bereich des Personal Publishings derzeit 1,17 Mio. Deutsche regelmäßig Tweets bei Twitter. Da dabei sogenannte Hashtags Microblogging-Aussagen an bestimmte Themen rückkoppeln, entstand zuletzt rund um Diskussionskomplexe wie #aufschrei oder #neuland ein lebhafter Austausch im Internet.[74] Gleichzeitig stellen soziale Medien ein wirksames Empörungsventil dar, das in Gestalt sogenannter Shitstorms die Aktivitäten von in der Öffentlichkeit stehenden Akteuren kommentiert. Dieses vom Duden als „Sturm der Entrüstung in einem Kommunikationsmedium des Internets" umschriebene Phänomen[75] () löst sich meist von jeder sachlichen Diskussion und nimmt stattdessen einen mehr oder weniger großen Skandal zum Anlass, um ein empfundenes oder tatsächliches Fehlverhalten in der Öffentlichkeit oft unsachlich und schmähend anzuprangern. Die damit verbundene Thematisierungsleistung generiert häufig auch Anschlusskommunikation in klassischen Leitmedien, was die publizistische Macht digitaler Gemeinschaften nachhaltig unterstreicht.

2.7 Fazit

Soziale Medien verursachen einen fundamentalen **Paradigmenwechsel** in der Entwicklung globaler Öffentlichkeit. Spezifische Potentiale wie Partizipation und Interaktion haben die Grenze zwischen Kommunikatoren und Konsumenten auf vielen Kanälen neutralisiert. Gleichzeitig existiert das tradierte Mediensystem jedoch weiter und komplementiert so den für jeden zugänglichen Kommunikationsraum sozialer Medien. Kommunikations- wie Rechtswissenschaftler stellt dies vor die Herausforderung, ihre Begriffs- und Reflexionswerkzeuge zu überdenken und den sich wandelnden Gegebenheiten anzupassen. Die Entwicklung ist damit keinesfalls abgeschlossen: Da sich soziale Medien rasant den an sie gestellten Funktionserwartungen anpassen, ist vielmehr von einer fortschreitenden und an Geschwindigkeit gewinnenden Transformation des Mediensystems durch Social Media auszugehen.

---

[72] Vgl. Busemann und Gscheidle (2011).
[73] Vgl. Busemann (2013).
[74] Vgl. Schmolke (2012).
[75] Vgl. Duden.de (2014).

Literatur

Ahlers, T. (2008). Neue Anwendungen und Geschäftsfelder im Web 2.0. In: M. Meckel, K. Stanoevska-Slabeva (eds), *Web 2.0. Die nächste Generation Internet* (S. 93 ff.). Baden-Baden: Nomos.

Alexa – The Web Information Company (2014). *How popular is wikipedia.org?* Abrufbar unter: http://www.alexa.com/siteinfo/wikipedia.org.

Allfacebook (2014). *Facebook Nutzerzahlen*. Abrufbar unter: http://allfacebook.de/userdata/.

ARD/ZDF-Online-Studie (2013). *Social Media. Nutzung von Web 2.0-Anwendungen 2007 bis 2013*, abrufbar unter: http://www.ard-zdf-onlinestudie.de/index.php?id=397.

BITKOM (2013). *Soziale Netzwerke 2013*. Dritte, erweiterte Studie. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet. http://www.bitkom.org/files/documents/SozialeNetzwerke_2013.pdf.

Bourdieu, P. (1983). Ökonomisches Kapital, kulturelles Kapital, soziales Kapital. In: R. Kreckel (ed), *Soziale Ungleichheiten* (S. 183 ff.). Baden-Baden: Nomos.

Boyd, D. (2006). *Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites*, abrufbar unter: http://firstmonday.org/article/view/1418/1336.

Boyd, D., Ellison N. (2007). Social network sites. Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13(1), 210 ff.

Bruns, A. (2009). Vom Gatekeeping zum Gatewatching. Modelle der journalistischen Vermittlung im Internet. In: C. Neuberger, C. Nuernbergk & M. Rischke (Hrsg.), *Journalismus im Internet. Profession, Partizipation, Technisierung*, S. 107 ff. Wiesbaden: VS Verlag für Sozialwissenschaften.

Bucher, H., Büffel, S. (2005). Vom Gatekeeper-Journalismus zum Netzwerk-Journalismus. Weblogs als Beispiel journalistischen Wandels unter den Bedingungen globaler Medienkommunikation. In: M. Behmer, B. Blöbaum, A. Scholl & R. Stöber (eds), *Journalismus und Wandel. Analysedimensionen, Konzepte, Fallstudien*, S. 85 ff. Wiesbaden: VS Verlag für Sozialwissenschaften.

Busemann, K. (2013). Wer nutzt was im Social Web? Ergebnisse der ARD/ZDF-Onlinestudie 2013. *Media Perspektiven* (7–8), 391 ff.

Busemann, K., Gscheidle, C. (2011). Web 2.0: Aktive Mitwirkung verbleibt auf niedrigem Niveau. Ergebnisse der ARD/ZDF-Onlinestudie 2011. *Media Perspektiven* (7–8), 360 ff.

Busemann, K., Fisch, M., Frees, B. (2012). Dabei sein ist alles – zur Nutzung privater Communitys. Ergebnisse der ZDF-Studie Community 2011. *Media Perspektiven* (5), 258 ff.

van Eimeren, B., Frees, B. (2013). Rasanter Anstieg des Internetkonsums – Onliner fast drei Stunden täglich im Netz. Ergebnisse der ARD/ZDF-Onlinestudie 2013. *Media Perspektiven (7–8)*, 358 ff.

Ellison, N. B., Steinfield, C., Lampe, C. (2007). The Benefits of Facebook „Friends“: Social Capital and College Students' Use of Online Social Networks. *Journal of Computer-Mediated Communication (12/4)*, 1143 ff.

Engesser, S., Wimmer, J. (2009). Gegenöffentlichkeit(en) und partizipativer Journalismus. *Publizistik 54*, 43 ff.

Fleisch, E., Mattern, F. (2005). Das Internet der *Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen*. Berlin: Springer.

Gantt, C. (2014). *WhatsApp sees 50 billion messages per day, more than all SMS combined*, abrufbar unter: http://www.tweaktown.com/news/34968/whatsapp-sees-50-billion-messages-per-day-more-than-all-sms-combined/index.html.

Godulla, A., Hohlfeld, R. (2013). Kommunikationswissenschaft – ein Fach im Umbruch. In: H. Krah, M. Titzmann (eds), *Medien und Kommunikation. Eine interdisziplinäre Einführung* (S. 411–445). Passau: Stutz.

Google (2014). *Account-Anmeldung für Google-Dienste*, abrufbar unter: https://accounts.google.com.

Granovetter, M. (1983). The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory, Vol. 1*, 201 ff.

Grieser, C. (2010). *Selbstdarstellung im Internet: Der unterschätzte* Faktor, abrufbar unter: http://netzwertig.com/2010/09/27/selbstdarstellung-im-internet-der-unterschaetzte-faktor/.

Hamann, G. (2008). Die Medien und das Medium. Web 2.0 verändert die Kommunikation der Gesellschaft. In: M. Meckel, K. Stanoevska-Slabeva (eds), *Web 2.0. Die nächste Generation Internet* (S. 213–228). Baden-Baden: Nomos.

Höflich, J. R., Hartmann, M. (2007). Grenzverschiebungen. Mobile Kommunikation im Spannungsfeld von öffentlichen und privaten Sphären. In: J. Röser (ed), *MedienAlltag. Domestizierungsprozesse alter und neuer Medien* (S. 211 ff.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Hohlfeld, R. (2012). Journalistische Beobachtungen des Publikums. In: K. Meier, C. Neuberger (eds), *Journalismusforschung. Stand und Perspektiven* (S. 135 ff.). Baden-Baden: Nomos.

Hohlfeld, R., Strobel, M. (2012). Öffentlichkeit im Wandel. Neue Herausforderungen für die Kommunikationswissenschaft. In: N. Springer, J. Raabe, H. Haas, W. Eichhorn (eds), *Medien und Journalismus im 21. Jahrhundert* (S. 75 ff.). Konstanz: UVK Verlagsgesellschaft mbH.

Knieper, T., Tonndorf, K. & Wolf, C. (2011). Der Prosument. Öffentlichkeit im Zeitalter Computervermittelter Kommunikation. In: Institut für interdisziplinäre Medienforschung (Hrsg.), *Medien und Wandel. Passauer Schriften zur interdisziplinären Medienforschung* (S. 41 ff.). Berlin: Logos.

Lang, N., Bekavac, B. (2004). World Wide Web. In: W. Faulstich (ed), *Grundwissen Medien* (S. 433 ff.). 5. Aufl. Paderborn, München: Fink.

Leiner, D.J., Hohlfeld, R., Quiring, O. (2010). Sozialkapital in deutschsprachigen Onlinenetzwerken. *Medienjournal (4)*, 48 ff.

Maireder, A., Nagl, M. (2010). Potentiale für Gewalt auf Social Network Sites. Cybermobbing im Kontext der Praktiken des Kommunikationsraumes. *Medienjournal 3*, 36 ff.

Maletzke, G. (1998). *Kommunikationswissenschaft im Überblick: Grundlagen, Probleme, Perspektiven*. Wiesbaden: Westdeutscher Verlag.

Meckel, M., Stanoevska-Slabeva, K. (2008). *Web 2.0. Die nächste Generation Internet*. Baden-Baden: Nomos.

Mende, A., Oehmichen, E., Schröter, C. (2013). Gestaltwandel und Aneignungsdynamik des Internets. Befunde aus den ARD/ZDF-Onlinestudien 1997 bis 2012. *Media Perspektiven* 1, 33 ff.

Meyer-Lucht, R. (2008). *Habermas, die Medien, das Internet*, abrufbar unter: http://www.perlentaucher.de/virtualienmarkt/habermas-die-medien-das-internet.html.

Münker, S. (2010). Die Sozialen Medien des Web 2.0. In: D. Michelis, D. Schildhauer (Hrsg.), *Social Media Handbuch. Theorien, Methoden, Modelle und Praxis* (S. 31 ff.). Baden-Baden: Nomos.

Neuberger, C. (2009). Internet, Journalismus und Öffentlichkeit. Analyse des Medienumbruchs. In: C. Neuberger, C. Nuernbergk & M. Rischke (Hrsg.), *Journalismus im Internet. Profession, Partizipation, Technisierung* (S. 19 ff.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Neuberger, C. (2012). Web 2.0. In: G. Bentele, H. Brosius & O. Jarren (eds), *Lexikon Kommunikations- und Medienwissenschaft* (S. 368). 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

O'Reilly, T. (2006). *Web 2.0 Compact Definition: Trying Again*, abrufbar unter: http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html.

Pariser, E. (2012). *Filter Bubble. Wie wir im Internet entmündigt werden*. Aus dem Amerikanischen von Ursula Held. München: Hanser.

Pfetsch, B., Bossert, R. (2012). Öffentliche Kommunikation. In: G. Bentele, H. Brosius & O. Jarren (Hrsg.), *Lexikon Kommunikations- und Medienwissenschaft* (S. 248 ff.). 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Pingdom (2013). *Internet 2012 in numbers*, abrufbar unter: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/.

Pürer, H. (2003). *Publizistik- und Kommunikationswissenschaft: Ein Handbuch*. Konstanz: UVK Verlagsgesellschaft mbH.

Richter, A., Koch, M. (2008). Funktionen von Social-Networking-Diensten. In: M. Bichler, T. Hess, H. Krcmar, U. Lechner, F. Matthes, A. Picot, B. Speitkamp & P. Wolf (Hrsg.), *Multikonferenz Wirtschaftsinformatik 2008* (S. 1239 ff.). Berlin: Gito.

Rühl, M. (1980). *Journalismus und Gesellschaft. Bestandsaufnahme u. Theorienentwurf*. Mainz: V. Hase und Koehler.

Schmidt, J. (2006). *Weblogs. Eine kommunikationssoziologische Studie*. Konstanz: UVK Verlagsgesellschaft mbH.

Schmidt, J. (2009). *Das neue Netz. Merkmale, Praktiken und Folgen des Web 2.0*. Konstanz: UVK Verlagsgesellschaft mbH.

Schmolke, M. (2012). Theorie der Kommunikationsgeschichte. In: R. Burkart, W. Hömberg (Hrsg.), *Kommunikationstheorien. Ein Textbuch zur Einführung* (S. 234 ff.). 6. Aufl. Wien: nap, New Academic Press.

Schroer, M. (2006). Selbstthematisierung. Von der (Er-)Findung des Selbst und der Suche nach Aufmerksamkeit. In: G. Burkart (ed), *Die Ausweitung der Bekenntniskultur – neue Formen der Selbstthematisierung?* (S. 41 ff.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Schulzki-Haddouti, C., Lorenz-Meyer, L. (2008). *Kooperative Technologien im zivilgesellschaftlichen Einsatz*, abrufbar unter: http://pb21.de/files/2010/02/Schulzki_Zivilgesellschaft.pdf.

Seufert, W., Gundlach, H. (2012). *Medienregulierung in Deutschland. Ziele, Konzepte, Maßnahmen. Lehr- und Handbuch*. Baden-Baden: Nomos.

Stegbauer, C. (2009). *Wikipedia. Das Rätsel der Kooperation*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Stelter, B. (2008). *Finding Political News Online, the Young Pass It On*, abrufbar unter: http://www.nytimes.com/2008/03/27/us/politics/27voters.html?_r=0. [zuletzt abgerufen am 26.02.2014]

Stockmann, R. (2004). Computer. In: W. Faulstich (ed), *Grundwissen Medien* (S. 157 ff.). 5. Aufl. Paderborn, München: Fink.

Tapscott, D., Williams, A. (2009). *Wikinomics. Die Revolution im Netz*. München: Deutscher Taschenbuch Verlag.

Toffler, A. (1980.) *The third wave*. New York: Bantam Books.

Weinberg, T., Pahrmann, C., Ladwig, W. (2012). *Social Media Marketing. Strategien für Twitter, Facebook & Co*. Köln: O'Reilly.

Weiser, M. (1991). *The Computer for the 21st Century*, abrufbar unter: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

Wilke, J. (2008). *Grundzüge der Medien- und Kommunikationsgeschichte*. 2., überarbeitete und ergänzte Auflage. Stuttgart: UTB.

Wolf, C., Hohlfeld, R. (2012). Revolution in Journalism? Mobile Devices as a New Means of Publishing. In: T. von Pape, C. Martin (eds), *Images in Mobile Communication. New Content, New Uses, New Perspectives* (S. 81 ff.). Wiesbaden: VS Verlag für Sozialwissenschaft.

Kapitel 3
Vertragliche Aspekte der Social Media

Peter Bräutigam und Bernhard von Sonnleithner

Inhalt

P. Bräutigam (✉)
Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Honorarprofessor für Medien und Internetrecht an der Universität Passau, Noerr LLP,
Brienner Str. 28, 80333 München, Deutschland
E-Mail: peter.braeutigam@noerr.de

B. von Sonnleithner
Corporate Counsel, EMEA Privacy, salesforce.com Germany GmbH,
Erika-Mann-Str. 63, 80636 München, Deutschland
E-Mail: bvonsonnleithner@salesforce.com

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_3

3.1 Einleitung

1 Social Media (Soziale Medien)[1] sind mittlerweile allgegenwärtig und aus unserem Alltag kaum wegzudenken. Ob Angebote wie Facebook als Archetyp und größtes Soziales Netzwerk[2] mit aktuell über einer Milliarde Nutzern weltweit[3] – davon über 25 Mio. in Deutschland[4] –, der Microbloggingdienst Twitter als schnellstwachsende Online-Community[5] oder die Business-Plattform Linkedln: In der globalen, virtuellen Gemeinschaft des Internets zählen sie mittlerweile vor allem für Jüngere, den *Digital Natives*, zu Konstanten des täglichen Lebens.[6] War noch vor etwa zehn Jahren die Aufnahme und Pflege sozialer Kontakte weitgehend auf die reale Welt beschränkt, sind heute mehr als 74 % der deutschen Internetnutzer und damit mehr als 40 Mio. Menschen in mindestens einem sozialen Netzwerk angemeldet und nutzen dies gemeinhin zumindest einmal wöchentlich – Tendenz steigend.[7] Ständig schießen neue Soziale Medien – teils gestützt auf kreative und innovative Geschäftsmodelle – förmlich aus dem Boden.[8] Vor allem die auf Wiki-Technologie aufgebauten

[1] Umfassend zum Begriff der „Social Media" Hohlfeld/Godulla, Kap. 2. Zur Habhaftwerdung dieses schwer zu umreißenden Begriffs durch Definitionen und Modelle sowie zu synonymen Bezeichnungen (wie Soziales Netzwerk oder Social Web) vgl. exemplarisch etwa auch Michelis, Social Media Modell, in: Michelis/Schildhauer, Social Media Handbuch, S. 19 ff.; Ebersbach et al., Social Web, S. 23 ff., 79 ff.; Boyd/Ellison, Journal of Computer-Mediated Communication 2008, 210 (211 ff.); Pelka/Kalekta, Web 2.0 zwischen technischer und sozialer Innovation, in: Howaldt/Jacobsen, Soziale Innovation, S. 143 ff., jeweils m. w. N.; prägnant auch Lichtnecker, GRUR 2013, 135 m. w. N. Zu den mit sozialen Medien einhergehenden rechtlichen Problemen überblicksartig jüngst Rosenbaum/Tölle, MMR 2013, 209 ff.

[2] Facebook ist zudem auch das in seiner Funktionalität, Ausgestaltung und Nutzung rechtlich wohl komplexeste Soziale Medium; speziell mit Blick auf das Datenschutz- und Arbeitsrecht vgl. Kap. 4 (Hornung) und Kap. 8 (Bayreuther).

[3] Vgl. http://newsroom.fb.com/content/default. aspx?NewsArea Id = 22.

[4] Vgl. http://www.heise.de/newsticker/meldung/Facebook-hat-in-Deutschland-mehr-als-25-Millionen-User-1803867.html.

[5] Vgl. http://blog.wiwo.de/look-at-it/2013/01/30/twitter-schnellstwachsendes-soziales-netzwerk-2012-google-vor-youtube/.

[6] Eingehend Pierce, Membership in the Network, in: Levina/Kien, Post-Global Network and Everyday Life, S. 59 ff.; So ist etwa Facebook die weltweit am meisten aufgerufene Internetseite nach Google (Twitter belegt Rang 10, Linkedln Rang 12), vgl. http://www.alexa.com/topsites.

[7] Vgl. die Studie der BITKOM, Soziale Netzwerke, http://www.bitkom.org/files/documents/SozialeNetzwerke.pdf, S. 3, 10. Vgl. zur globalen Situation auch den sehr differenzierten und umfassenden Nielsen Social Media Report, (http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html).

[8] Siehe zu Entwicklungstendenzen auch Pelka/Kalekta, Web 2.0 zwischen technischer und sozialer Innovation, in: Howaldt/Jacobsen, Soziale Innovation, S. 143 ff.; http://www.spiegel.de/netzwelt/web/soziale-netzwerke-alternativen-zu-facebook-a-868293.html. Zu den vielfältigen Formen vgl. auch Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1, Rn. 1.

Plattformen[9] boomen (immer noch), ebenso die mit Gaming-Elementen angereicherten virtuellen Welten.[10] Das Phänomen der **Hypertrophie** Sozialer Medien, das im Verlauf der letzten Jahre weite Teile der privaten Lebensgestaltung in Beschlag genommen hat, hat mittlerweile auch und gerade staatliche[11] und betriebliche Sphären[12] erfasst und führt dort zu gravierenden **strukturellen und materiellen Veränderungen**, die wiederum Folgen für jeden Einzelnen nach sich ziehen.[13]

Soziale Medien ermöglichen und erleichtern die zwischenmenschliche Kommu- **2**
nikation.[14] Diese erfolgt unabhängig von der jeweils individuellen Ausgestaltung – immer auf Grundlage eines der nachfolgenden **Kommunikationsmodelle** oder einer Kombination aus beidem: Zum einen **asynchron** – also zeitlich versetzt – etwa durch den Versand von elektronischen Nachrichten oder das Einstellen von Informationen jeglicher Art wie etwa Texte, Bilder oder Filme auf eine virtuelle Pinnwand (Wall), zum anderen **synchron** etwa durch Live-Chats.[15] Auch wenn das kommunikative Element von der Selbstdarstellung der eigenen Person verdrängt zu werden droht,[16] so stellt sie dennoch ein prägendes Element aller Sozialen Medien dar.[17]

Nahezu sämtliche Soziale Medien knüpfen den Zugang zu ihren Angeboten an die **3**
Bestätigung von Nutzungs- oder Teilnahmebedingungen durch den jeweiligen Nutzer. Dieser **„Social-Media-Vertrag“** ist im Kern eine vertragliche Abrede über die Nutzung eines Sozialen Mediums, in welchem vornehmlich etwa Art und Umfang der jeweils geschuldeten Leistungen und dabei insbesondere Aspekte wie Entgeltlichkeit, Verfügbarkeit und Ähnliches mehr festgelegt werden.[18] Der Vertragsschluss erfolgt

---

[9] Vgl. hierzu Knauer, NJOZ 2009, 3004 (3007); Sieber, in: Hoeren et al., Multimedia-Recht, 37. EL 2014, Teil 1 Rn. 94; Wimmers/Schulz, Heise Online-Recht, Kap. III., IV.5. Zur „Weisheit der Vielen“ vgl. Surowiecki, in: Michelis/Schildhauer, Social Media Handbuch, S. 104 ff.

[10] Dazu etwa Diegmann/Kuntz, NJW 2010, 561 ff.; Krasemann, MMR 2006, 351 ff.; Rippert/Weimer, ZUM 2007, 272 ff. sowie Backu, ZD 2012, 59 ff.

[11] Eingehend dazu Kap. 10 (Schulz). Vgl. weiterhin Hoffmann et al., ZD 2013, 122 ff. Vgl. ferner auch Ulbricht, KommunalPraxis spezial 2012, 101 ff. sowie grundlegend Frevert/Wagner, NVwZ 2011, 76 ff.

[12] Vgl. grundlegend Back et al., Web 2.0 und Social Media in der Unternehmenspraxis; Hetter, Social Media Marketing. Speziell zur rechtlichen Dimension Braun, NJ 2013, 104 ff. Siehe auch BITKOM, Social Media in Deutschen Unternehmen, http://www.bitkom.org/files/documents/Social_media_in_deutschen_Unternehmen.pdf.

[13] Speziell zu arbeitsrechtlichen Anforderungen Kap. 8 (Bayreuther) sowie Brierley, FA 2012, 103 ff.; Byers/Mößner, BB 2012, 1665 ff.; Melot de Beauregard/Gleich, DB 2011, 2044 ff.; Umfassend auch Thiele, Kommunikationsmanagement im Wandel durch Social Media. Berufsbild, Qualifikation und Tätigkeit 2.0; vgl. außerdem zur Verquickung von Berufs- und Privatleben durch diesen Trend Qualman, Socialnomics.

[14] Vgl. so z. B. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 415 (417); Brinkert et al., ZD 2013, 153; Jandt/Roßnagel, MMR 2011, 637; Lichtnecker, GRUR 2013, 135.

[15] Vgl. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 416; Ebersbach et al., Social Web, S. 23 ff.; 86 ff.

[16] Redeker, IT-Recht, Rn. 1171.

[17] Vgl. auch Münkler, Die sozialen Medien des Web 2.0, in: Michelis/Schildhauer, Social Media Handbuch, S. 45 ff.

[18] Vgl. etwa Redeker, IT-Recht, Rn. 1171 ff. Eingehend zum Social-Media-Vertrag Bräutigam, MMR 2012, 635 ff.

üblicherweise im Rahmen eines zwingend zu durchlaufenden, als „Registrierung“[19] oder „Accounterstellung“ bezeichneten Prozesses.[20]

4 Die **inhaltlichen Anforderungen** an Social-Media-Verträge sowie insbesondere die damit korrelierende rechtliche Ausgestaltung richten sich stets nach den individuellen Regelungsbedürfnissen des betreffenden Sozialen Mediums. Diese wiederum hängen primär von der Zielsetzung und Funktionalität des Sozialen Mediums ab. Hierin divergieren die Sozialen Medien allerdings immens, so dass eine abschließende Klassifikation verbunden mit einer Einteilung in unterschiedliche Fallgruppen in der Praxis nur schwer möglich ist. Folglich lassen sich allgemeinverbindliche Aussagen zu sämtlich denkbaren rechtlichen Problemen pauschal für alle Social-Media-Verträge kaum treffen.

5 In einem gewissen Umfange wird man auf – freilich recht allgemeine – **Differenzierungskriterien** zur Kategorisierung Sozialer Medien zurückgreifen können, denen rechtlich große Bedeutung zukommt. Dies sind vor allem der Sitz des Betreibers, der vom Sozialen Medium territorial angesprochene Nutzerkreis sowie die Frage der Entgeltlichkeit des Angebots. Erstgenannte Aspekte spielen dabei in der Qualifikation des auf die Vertragsbeziehung anwendbaren Rechts eine zentrale Rolle, Letztgenanntem kommt im Rahmen der rechtlichen Einordnung des Social-Media-Vertrags zu einem im BGB kodifizierten Vertragstypus entscheidende Bedeutung zu.

6 Die Unterscheidung zwischen **rein privat** genutzten Plattformen (etwa StayFriends), **beruflich** genutzten Angeboten (z. B. Linkedln, Xing) sowie Mischformen (v. a. Facebook[21] und Twitter) mag soziologisch von Bedeutung sein, spielt aber für die rechtliche Behandlung von Social-Media-Verträgen häufig eine untergeordnete Rolle.

3.2 Social-Media-Vertrag

3.2.1 Begrifflichkeit

7 Der Social-Media-Vertrag bezeichnet das Rechtsgeschäft zwischen einem Social-Media-Anbieter[22] und dessen Nutzern, welches die rechtlichen Rahmenbedingungen

---

[19] So die gängige Terminologie, die etwa Facebook (https://de-de.facebook.com/) und Twitter (https://twitter.com/) verwenden. Youtube spricht etwa von einer Anmeldung (http://www.youtube.com/), LinkedIn von „Jetzt Mitglied werden“ (http://de.linkedin.com/).

[20] Sofern ein solcher Prozess nicht zu durchlaufen ist, kann dennoch im Einzelfall ein konkludenter Vertragsschluss anzunehmen sein. Mit Blick auf die Verkehrssitte dürfte dies aber einen Ausnahmefall darstellen. Insoweit dagegen immer ein Schuldverhältnis annehmend Martini, JZ 2012, 1145 (1147).

[21] Vgl. hierzu etwa Schröder, in: Schröder, Datenschutzrecht, Teil 3.1. a.gg.

[22] Freilich nicht ganz trennscharf und abschließend bestimmen lässt sich indes angesichts der eingangs bereits skizzierten unterschiedlichen Ausgestaltungen von Social Media-Plattformen gepaart mit raschen technischen Weiterentwicklungen, welche Angebote genau als Soziale Medien zu

für die Nutzung eines Sozialen Mediums (beispielsweise eines Sozialen Netzwerks) festschreibt. Die Bezeichnung ist rein beschreibender Natur, da es keine Sondervorschriften für Social-Media-Verträge im eigentlichen Sinne gibt. Insbesondere handelt es sich bei Social-Media-Verträgen nicht um einen im BGB gesetzlich fixierten Vertragstypus. Auf den Social-Media-Vertrag sind vielmehr je nach konkret zu beurteilendem **Einzelfall** die den Leistungspflichten entsprechenden Bestimmungen des besonderen Schuldrechts, hilfsweise die Normen des allgemeinen Schuldrechts, anzuwenden.

Die Bezeichnung Social-Media-Vertrag konnte sich bisher in der rechtlichen Literatur noch nicht durchsetzen.[23] Da der Social-Media-Anbieter letztlich als Betreiber einer Internetplattform fungiert, wird der Social-Media-Vertrag bisweilen auch als Unterfall des Plattformvertrags verstanden.[24] Aufgrund der durchaus vergleichbaren Grundfunktionalitäten bei Web-Portalen lässt sich der von Literatur und Rechtsprechung entwickelte **Rechtsrahmen zu Online-Plattformen** wie Auktionsplattformen[25] oder zum Webhosting auf Social-Media-Verträge übertragen.[26] Denn letztlich besteht die Hauptleistungspflicht des Anbieters in allen Konstellationen zum einen in der Bereitstellung einer Web-Infrastruktur, zum anderen im Regelfall darüber hinaus in der öffentlichen Zugänglichmachung von Inhalten der Nutzer (z. B. Bildern oder Texten). Der Social-Media-Vertrag hat insbesondere mit dem Webhosting-Vertrag[27] gemein, dass der Nutzer durch Einstellung eigener Inhalte auch zum Content-Provider wird, die durch den Anbieter als Host-Provider gespeichert und zugänglich gemacht werden. **8**

qualifizieren sind. Der materielle Gehalt des Begriffs unterliegt den einem steten Wandel unterworfenen tatsächlichen Bedingungen; für die rechtliche Qualifikation soll ausreichen, dass die Kernfunktionalität der Plattform in der Ermöglichung von Kommunikation unter den Nutzern liegt.

[23] Verwendung gefunden hat er – soweit ersichtlich – im Ansatz bei Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1, Rn. 1 ff.; Redeker verwendet hingegen etwa die eingedeutschte Form der Sozialen Netzwerke, vgl. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12, Rn. 415 ff. Weite Teile der Literatur hingegen sehen den Social-Media-Vertrag nicht als eigenen Typus an und verorten ihn in der Gruppe der Plattformverträge.

[24] Hierzu eingehend Nolte/Hecht, ITRB 2006, 188 ff.; Härting, Internetrecht, S. 54 ff. Die Einordnung erweist sich insgesamt als nicht ganz stimmig: Zwar treffen den Anbieter eines Sozialen Mediums Pflichten ähnlich eines Webhosters oder Betreibers einer Auktionsplattform; diese erschöpfen sich aber regelmäßig nicht hierin.

[25] Vgl. hierzu speziell Haase/Hawellek, Heise Online-Recht, Kap. VI.2.3 Rn. 7 ff.; Leupold/Glossner, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 2 Rn. 335 ff.; Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 419; Wiebe/Neubauer, in: Hoeren et al., Multimedia-Recht, Teil 15 Rn. 5 ff.

[26] Vgl. allein Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 5.

[27] Hierzu eingehend Cichon, Internetverträge, Rn. 155 ff.; Schuppert, CR 2000, 227 ff.; vgl. ferner Klett/Pohle, DRiZ 2007, 198 ff.

3.2.2 Überblick über die wesentlichen Leistungen

3.2.2.1 Grundsätzlicher Leistungsumfang

9 Eine der Hauptpflichten des Social-Media-Anbieters ist die **Bereitstellung** der technischen Online-Plattform[28] (insbesondere der Webseite und der dahinterliegenden Datenbanken) sowie des **Zugangs** hierzu. Dies umfasst neben den typischen Hosting-Leistungen[29] zum Teil auch die vertragliche Zusicherung der Verfügbarkeit des jeweiligen Angebots. Bei diesen Leistungen handelt es sich regelmäßig um Elemente ähnlich denen eines klassischen *Software as a Service*-Dienstes (SaaS).[30]

Aufgrund der spezifischen Eigenart von Sozialen Medien wird es sich bei der Bereitstellung der Online-Plattform regelmäßig um den **Schwerpunkt** der Leistung handeln.[31] Denn Soziale Medien sollen dem Nutzer in erster Linie durch die Bereitstellung einer entsprechenden Plattform ermöglichen, mit Dritten zu kommunizieren.

3.2.2.2 Bestimmtheit und Bestimmbarkeit des Leistungsumfangs

10 Der konkrete Leistungsumfang des Anbieters ist zum Zeitpunkt des Vertragsschlusses, insbesondere bei unentgeltlichen Angeboten, oft **nur grob festgelegt**.[32] Im Rahmen des Registrierungsprozesses wird der Leistungsumfang – wenn überhaupt und teils unter Verweis auf die geltenden Nutzungsbedingungen – schlechterdings mit „Ermöglichung der Nutzung des Angebots" oder „Zugang zum Sozialen Medium" umschrieben.[33] Welche konkreten Leistungen der Nutzer erwarten darf, ergibt sich hieraus freilich nicht eindeutig.[34] Insbesondere manifestiert sich meist kein eindeutiger Wille des Anbieters dahingehend, das Soziale Medium dauerhaft (kostenfrei) zur Verfügung zu stellen und/oder eine gewisse Gewähr hinsichtlich des Fortbestands der bei Vertragsschluss vorhandenen Grundfunktionalitäten zu übernehmen. Vielmehr sind Soziale Medien einem steten technischen wie wirtschaftlichen Wandel unterworfen, der zu fortlaufenden Modifikationen des Leistungsumfangs und der

---

[28] Vgl. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 420.

[29] Eingehend hierzu Schuppert, in: Spindler, Vertragsrecht der Internetprovider, Rn. 518 ff.; Cichon, Internetverträge, Rn. 160 ff.

[30] Bräutigam, MMR 2012, 635 (636).; vgl. zum Begriff etwa Busche/Schelinski, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 19 ff.

[31] In diese Richtung auch Paul, in: Hoeren et al., Multimedia-Recht, Teil 7.4 Rn. 142. Insofern besteht eine Parallele zum Webhosting-Vertrag, bei dem das Überlassen des Speicherplatzes als Hauptleistungspflicht anzusehen ist, vgl. Cichon, Internetverträge, Rn. 160.

[32] Vgl. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 416.

[33] Vgl. exemplarisch auch Facebook: „Facebook ermöglicht es Dir, mit den Menschen in Deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen" (http://www.facebook.com/de).

[34] Die Bestimmtheit der Leistung ist allerdings nicht erforderlich, es genügt im Rahmen eines Rechtsgeschäfts die Bestimmbarkeit, vgl. BGH, NJW 1971, 653 ff.; BGH, NJW 2006, 1971 ff.; Schulze, in: Schulze, BGB, § 249 Rn. 2.

bereitgestellten Funktionalitäten führt. Die Gründe hierfür sind die Gewinnmaximierung, die Einstellung unrentabler Funktionalitäten oder die Anpassung derselben an die spezifischen Bedürfnisse der Nutzer.[35]

Hinsichtlich des entwicklungsoffenen Teils bezogen auf die Ausgestaltung des Sozialen Mediums spricht vieles dafür, soweit der Leistungsumfang nicht durch ergänzende Vertragsauslegung bestimmt werden kann,[36] dass der Nutzer dem Anbieter mit Vertragsschluss ein (durch das objektiv erkennbare Nutzerinteresse begrenzte) **Leistungsbestimmungsrecht** im Sinne von § 315 Abs. 1 BGB einräumt.[37] Auch der Nutzer hat gemeinhin ein Interesse daran, von Verbesserungen an den Funktionalitäten der Plattform – und sei es nur am Design –, die er selbst zum Zeitpunkt des Vertrags oft nicht absehen kann, zu profitieren.[38] Ihm ist grundsätzlich ein entsprechender Wille dahin zu attestieren, dass der Anbieter – in den Grenzen des dem Sinn und Zweck des Sozialen Mediums dienlichen – Änderungen und insbesondere Erweiterungen am Angebot des Sozialen Mediums vornimmt. Eine andernfalls für jeden Fall der Modifikation des Angebots gebotene Vertragsänderung dürfte nicht dem Parteiinteresse entsprechen und hätte zudem eine ganze Reihe praktischer Probleme zur Folge. Denn die Beteiligung der Nutzer würde nicht nur zu einem nicht unerheblichen Organisationsaufwand für den Anbieter führen, sondern könnte durchaus von den Nutzern als unnötige Belästigung empfunden werden. Dieses Leistungsbestimmungsrecht kann allein mit Blick auf die Billigkeit nur soweit gehen, wie die Änderungen des Leistungsumfangs im Zeitpunkt des Vertragsschlusses für den Nutzer vorhersehbar waren; für alle anderen Fälle ist eine einvernehmliche Vertragsanpassung erforderlich. **11**

3.2.2.3 Freemium-Modell

Viele Soziale Medien werden als sog. Freemium-Angebote betrieben. Charakteristisches Merkmal eines Freemium-Angebots ist, dass die **Basisdienstleistungen unentgeltlich** angeboten werden, während über das Basisangebot hinausgehende Dienstleistungen **(die Premium-Mitgliedschaft) kostenpflichtig** sind. Die Vorteile dieses Modells liegen auf der Hand: Durch die kostenlose Bereitstellung der Grundfunktionalitäten kann der Plattformbetreiber die für den Betrieb des sozialen Netzwerks erforderliche Nutzeranzahl erreichen, ohne die das Netzwerk nicht sinnvoll betrieben werden kann. Mithilfe attraktiver Zusatzfunktionen können Nutzer in kostenpflichtige Premium-Mitgliedschaften überführt werden und **12**

---

[35] Vgl. Münkler, Die sozialen Medien des Web 2.0, in: Michelis/Schildhauer, Social Media Handbuch, S. 45 ff.; Pelka/Kalekta, Web 2.0 zwischen technischer und sozialer Innovation, in: Howaldt/Jacobsen, Soziale Innovation, 143 ff.

[36] Zum Vorrang der ergänzenden Vertragsauslegung BGH, NJW-RR 2007, 56 f.; BGH, NJW 2006, 2472 ff.

[37] Dies stellt eine Leistungsbestimmungsklausel dar; zu diesen Würdinger, in: MüKo-BGB, § 315 Rn. 16 ff.; Rieble, in: Staudinger, BGB, § 315 Rn. 131 ff.

[38] Insofern entspricht eine Leistungsbestimmung, die ins Ermessen des Anbieters gestellt wird, in diesem Kontext regelmäßig der Billigkeit und ist damit nicht nach § 315 Abs. 3 S. 1 BGB unwirksam.

ein stabiler Umsatz generiert werden. Beispiele für Freemium-Angebote sind die Karriere-Netzwerke Xing und LinkedIn. Beide Netzwerke bieten Grundfunktionalitäten wie die Erstellung eines Profils und die Vernetzung mit anderen Nutzern unentgeltlich an. Gegen ein monatliches Entgelt können Nutzer eine Premium-Mitgliedschaft abschließen, die einen deutlich erweiterten Funktionsumfang bietet. So können Premium-Mitglieder etwa nachvollziehen, wer ihr Profil eingesehen hat sowie Mitglieder außerhalb ihres persönlichen Netzwerkes kontaktieren.

13 Je nach konkreter Ausgestaltung kann hier ein einheitlicher Vertrag oder aber ein unentgeltlicher Rahmenvertrag hinsichtlich der Basisdienstleistungen kombiniert mit einem entgeltlichen Vertrag für die Premium-Mitgliedschaft angenommen werden. Entscheidend für die juristische Einordnung ist, ob nach objektiver Anschauung eine **Teilbarkeit in zwei eigenständige Verträge möglich** ist. Hierfür ist insbesondere die Ausgestaltung des Anmelde- und Kündigungsvorgangs von entscheidender Bedeutung. An einer Teilbarkeit dürfte es etwa dann fehlen, wenn die Beendigung der Premium-Mitgliedschaft zugleich zur Beendigung der Basismitgliedschaft führt. Angesichts der Tatsache, dass der Anbieter ein gewichtiges Interesse an Basismitgliedschaften hat, wird dies in der Praxis allerdings selten anzunehmen sein.

3.2.3 Rechtliche Qualifikation von Social-Media-Verträgen

14 Social-Media-Verträge können – wie bereits dargestellt – wegen ihrer unterschiedlichen Ausformungen nicht pauschal einem im BGB gesetzlich geregelten Vertragstyp zugeordnet werden. Vielmehr muss ausgehend vom **spezifischen Leistungs- und Regelungsumfang** ermittelt werden, ob der Social-Media-Vertrag einem im BGB normierten Vertragstyp entspricht. Hierzu ist der Leistungsumfang durch **Auslegung** des Vertrags zu bestimmen. Besonderes Augenmerk ist dabei auf den Gegenstand des Vertrags – insbesondere der Frage der Entgeltlichkeit – zu richten.[39] Für den Fall, dass kein gesetzlich geregelter Vertragstyp das Pflichtenprogramm des jeweiligen Social-Media-Vertrags abschließend zu erfassen vermag – etwa wenn z. B. die Hauptleistungspflicht des Social-Media-Vertrags gleichermaßen Komponenten eines Miet- und Dienstvertrags aufweist und ein Schwerpunkt nicht zu erkennen ist – so ist eine Klassifikation als Typenkombinationsvertrag denkbar.[40] In der Praxis entfaltet dies lediglich Auswirkungen auf der Ebene der Sekundäransprüche, also im Falle einer Leistungsstörung. Das anwendbare Recht folgt dann der Zuordnung der gestörten Leistungspflicht zu einem gesetzlich geregelten Vertragstypus, soweit dies möglich ist. Subsidiär kommt ferner auch eine Klassifikation des Social-Media-Vertrags als Vertrag *sui generis* in Betracht, § 311 Abs. 1 BGB.

---

[39] Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 30.

[40] So auch Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 31. Vgl. prägnant hierzu Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 15 ff.

3.2.3.1 Vertragsschluss mit dem Nutzer

Auf den Social-Media-Vertrag finden zunächst die Regelungen des allgemeinen Teils des BGB Anwendung. Relevant ist dies insbesondere in Bezug auf den Vertragsschluss: Der Social-Media-Vertrag kommt durch zwei inhaltlich korrelierende, mit Bezug aufeinander abgegebene Willenserklärungen zustande, arg. §§ 145 ff. BGB.[41] In der Regel werden die Willenserklärungen im Rahmen des **Registrierungsprozesses** abgegeben.[42] **15**

Je nach angesprochener Zielgruppe kann es sich bei einem Social-Media-Vertrag sowohl um einen Verbrauchervertrag (vgl. § 310 Abs. 3 BGB) als auch um ein Handelsgeschäft i. S. d. § 343 HGB handeln, was zur Anwendbarkeit der jeweils einschlägigen Normen führt. Die Mehrzahl der Social-Media-Verträge dürften als **Verbraucherverträge** zu qualifizieren sein, da die entsprechenden Plattformen in der Regel für private Zwecke genutzt werden. Dies hat zur Folge, dass die speziellen verbraucherschutzrechtlichen Normen Anwendung finden. Dies betrifft insbesondere die in den §§ 312b ff., 355 ff. BGB geregelten Bestimmungen zu Fernabsatzverträgen, die zumindest bei entgeltlichen Social Media-Angeboten Anwendung finden. **16**

3.2.3.2 Unentgeltliche Social Media-Angebote

In den weit überwiegenden Fällen handelt es sich bei Social-Media-Plattformen um unentgeltliche Angebote, die letztlich über die Einblendung **personalisierter Werbung** finanziert werden.[43] In diesen Fällen entrichtet der Nutzer kein Entgelt im Gegenzug für die Nutzung der Plattform. **17**

Nutzerdaten als Entgelt? Grundsätzlich stieße auch die Klassifikation dieser Angebote als entgeltlich auf keine unüberwindbaren dogmatischen Hindernisse.[44] Obgleich sich bei oberflächlicher Betrachtung die Annahme eines unentgeltlichen, einseitig verpflichtenden Vertrags über die Nutzung der Infrastruktur des Sozialen Netzwerks gepaart mit einer datenschutzrechtlichen Einwilligung in die Nutzung der Daten aufdrängt,[45] so kann es sich doch je nach Einzelfall bei einer lebensnahen, wirtschaftlichen Betrachtungsweise um einen synallagmatischen Austauschvertrag handeln; für das Bereitstellen der Infrastruktur erhält der Plattformbetreiber bisweilen – abhängig von der individuellen Ausgestaltung des Vertrags – im Gegenzug **18**

---

[41] Vgl. grundlegend Säcker, in: MüKo-BGB, Einl., Rn. 205; vgl. auch Hoeren, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, E-Commerce-Verträge, Rn. 43 ff.

[42] Zur Wahl des Accountnamens bei Social-Media-Verträgen vgl. Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 9 ff.

[43] Schwenke, WRP 2013, 37 (38); zur datenschutz- und wettbewerbsrechtlichen Zulässigkeit solcher Werbung vgl. etwa Dietrich/Ziegelmayer, CR 2013, 104 ff.

[44] Eingehend dazu Bräutigam, MMR 2012, 635 ff.

[45] So etwa Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 415 ff.; insb. Schwenke, WRP 2013, 37 ff.; Wintermeier, ZD 2012, 210 ff. In eine ähnliche Richtung LG Berlin, ZUM-RD 2008, 18 f. und LG Berlin, K&R 2012, 300 ff.

umfassende **Nutzungs- und Verwertungsrechte an den Nutzerdaten**. Der Plattformbetreiber gewährt nämlich dann seine Leistung gerade deswegen, um diese Nutzungs- und Verwertungsrechte zu erlangen. Sein gesamtes Geschäftsmodell zielt in derartigen Fällen im Kern auf die **wirtschaftliche Verwertung** dieser Nutzungs- und Verwertungsrechte ab.

19 Das Synallagma besteht damit aus:[46]

> einerseits einer lizenzähnlichen Einräumung der Nutzung personenbezogener Daten für Werbezwecke, die man parallel zur urheberrechtlichen Lizenz je nach Fallgestaltung als **Miete oder Kauf**[47] qualifizieren könnte;
> andererseits der Einräumung der Nutzung von IT-Infrastruktur; die vorliegenden Cloud-Service-Leistungen, die von **miet- und dienstvertraglichen** Elementen geprägt sind, müssen dabei ihrerseits als Kombination von §§ 535 ff. und §§ 611 ff. BGB begriffen werden.

20 Die Nutzungs- und Verwertungsrechte an den Nutzungsdaten können mithin als Leistung des Nutzers angesehen werden; auch rechtsdogmatisch ist schon längst ausgemacht, dass sich aus dem **Persönlichkeitsrecht** kommerzialisierbare Splitter rechtlich herausbrechen lassen, die zum Gegenstand eigenständiger Rechtsgeschäfte gemacht werden können.[48] Entsprechend urheberrechtlichen Wertungen muss eine gebundene/beschränkte Übertragung auch von Teilaspekten des Allgemeinen Persönlichkeitsrechts möglich sein; hier wie dort greifen die verwertungs- und persönlichkeitsrechtliche Dimension ineinander.[49] Diese Betrachtungsweise steht im Übrigen im Einklang mit der ständigen Rechtsprechung des BGH[50] sowie des BVerfG.[51] Der BGH hat etwa in der Marlene-Dietrich-Entscheidung[52] – in konsequenter Fortführung des im Herrenreiter-[53] und im Ginsengwurzelurteil[54] eingeschlagenen Wegs geurteilt, dass das

> allgemeine Persönlichkeitsrecht [...] nicht nur dem Schutz ideeller, sondern auch vermögenswerter Interessen der Persönlichkeit [dient].

21 Auch das geltende Datenschutzrecht gewährt entsprechende Spielräume. Mithin kann rechtlich nachvollzogen werden, was im Rahmen einer Parallelwertung des Vorganges in der Laiensphäre als „deal“,[55] also als Austauschgeschäft „Geld“ gegen

---

[46] Bräutigam, MMR 2012, 635 (640).
[47] Dem Mietvertrag räumt Weichert, NJW 2001, 1463 (1467 f.) den Vorzug ein, da eine lediglich temporär und teleologisch begrenzte Hingabe der Daten vorläge, die nicht zu einem Wegfall der Verfügungsbefugnis führe.
[48] Dazu eingehend Forkel, GRUR 1988, 491 (498 f.); Unseld, GRUR 2011, 982 ff.; Weichert, NJW 2001, 1463 (1469).
[49] Prägnant Bräutigam, MMR 2012, 635 (639).
[50] Anders nur BGH, NJW-RR 1987, 231 ff. [Nena].
[51] BVerfG, NJW 2006, 3409 [Blauer Engel].
[52] BGH, GRUR 1999, 709 (711).
[53] BGH, NJW 1958, 827 ff.
[54] BGH, NJW 1961, 2059 ff.
[55] So der „Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic [CIPPIC] against Facebook Inc. under the Personal Information Protection and Electronic Documents Act by Elisabeth Denham, Assistant Privacy Commissioner of Canada, July 16, 2009“, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

„Daten“ wahrgenommen wird.[56] Es ist kein Grund ersichtlich, einen im konkreten Fall **einheitlichen Lebensvorgang künstlich** in einen (unentgeltlichen) Vertrag über die Nutzung der Infrastruktur im Rahmen eines sozialen Mediums sowie die datenschutzrechtliche Einwilligung in die Nutzung der Daten **aufzuspalten**.

Vertragsrechtliche Einordnung unentgeltlicher Social-Media-Verträge In aller Regel dürften Verträge zur Nutzung **unentgeltlicher** Social-Media-Angebote als Verträge ***sui generis*** i.S.d. § 311 BGB zu qualifizieren sein, sodass allgemeines Schuldrecht Anwendung findet. Eine Qualifizierung als Dienstvertrag oder Werkvertrag scheitert bereits daran, dass in beiden Fällen eine Entgeltlichkeit zwingend vorausgesetzt wird. **22**

Auch die Einordnung als **Auftrag** im Sinne der §§ 662 ff. BGB[57] dürfte im Ergebnis ausscheiden, da sie den tatsächlichen Gegebenheiten regelmäßig nicht gerecht wird.[58] Durch die Annahme eines Auftrags verpflichtet sich der Beauftragte, ein ihm vom Auftraggeber übertragenes Geschäft unentgeltlich zu besorgen. Prägendes Element des Auftrags ist damit das Tätigwerden des Beauftragten in einem fremden Interesse.[59] Angesichts der eindeutig auf die **Gewinnmaximierung** ausgerichteten Tätigkeit von Sozialen Medien wie Facebook, Google+ und Xing ist allerdings nicht ohne Weiteres nachvollziehbar, worin genau ein fremdnütziges Tätigwerden zu sehen sein soll.[60] Insbesondere beauftragt der Nutzer den Anbieter nicht etwa mit der Einblendung personalisierter Werbung. Dies erfolgt vielmehr im wohlverstandenen Interesse des jeweiligen Anbieters, welcher hierdurch Werbeeinnahmen zur Finanzierung des Sozialen Mediums erzeugen kann. **23**

Darüber hinaus wäre der Beauftragte gemäß § 667 BGB verpflichtet, alles, was er zur Ausführung des Auftrags erhält und was er aus der Geschäftsbesorgung erlangt, an den Auftraggeber **herauszugeben**. Der Auftraggeber hingegen wäre verpflichtet, dem Beauftragten die zum Zwecke der Ausführung des Auftrags erforderlichen Aufwendungen zu erstatten (§ 670 BGB). Unabhängig vom Gegenstand der Beauftragung wäre es bereits lebensfremd anzunehmen, der Anbieter beabsichtige, etwaige durch die Verwertung von Nutzerdaten erlangte Werbeeinnahmen an den Nutzer auszukehren. Denn diese dienen ja gerade der Finanzierung der Plattform. Ebenso fernliegend wäre es anzunehmen, die Nutzer wären bereit, im Gegenzug die erforderlichen Aufwendungen des Anbieters nach § 670 BGB zu ersetzen. **24**

---

[56] Vgl. Bräutigam, MMR 2012, 635 (638) m. w. N. in Fn. 47 ff.
[57] So jedenfalls im Ergebnis Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rdnr. 423 f.
[58] Hierzu und zum Folgenden Bräutigam, MMR 2012, 635 (636).
[59] Sprau, in: Palandt, BGB, § 662 Rn. 6.
[60] So auch Brinkert et al., ZD 2013, 153 (154).

Vertragliche Haftung bei unentgeltlichen Social-Media-Angeboten Soweit die
25 Parteien nichts Abweichendes (wirksam) vereinbart haben,[61] finden für die vertragliche Haftung entsprechend obig Gesagtem die Vorschriften des **allgemeinen Schuldrechts**, sprich insbesondere die §§ 280 ff. BGB, Anwendung.[62]

26 Spezifische Besonderheiten dogmatischer Art bestehen hier regelmäßig nicht.[63] Praktische Probleme treten dagegen immer dann auf, wenn **Haupt- und Nebenleistungspflichten** des Social-Media-Vertrags **nicht klar definiert** sind[64] und in der Folge im Haftungsfalle gerade streitig ist, ob die vermeintlich verletzte Pflicht überhaupt als Vertrags- oder Nebenpflicht zu qualifizieren ist.

27 **Kostenpflichtige** Social-Media-Angebote (wie beispielsweise die Premium-Mitgliedschaften bei Karrierenetzwerken wie Xing und LinkedIn) zeichnen sich dadurch aus, dass der Nutzer im Gegenzug für die Gewährung der vertraglichen Leistungen ein Entgelt zu entrichten hat. Die Finanzierung der Plattform erfolgt daher in erster Linie über die Nutzerentgelte und nicht – wie bei unentgeltlichen Angeboten – ausschließlich über die Einblendung von Werbung.

28 Social-Media-Verträge über die Nutzung entgeltlicher Angebote lassen sich regelmäßig als **Werkvertrag mit Dauerschuldcharakter** qualifizieren, da mit der Bereitstellung der Online-Plattform – abhängig von der konkreten Nutzbarkeit – ein tatsächlicher Erfolg geschuldet wird.[65] Dieser Erfolg liegt darin, dem Nutzer Zugang zum Sozialen Medium zu gewähren, also auch die Verfügbarkeit sicherzustellen sowie die Funktionstüchtigkeit sämtlicher das Soziale Medium prägender Funktionen, zu gewährleisten. Eine Qualifizierung als bloßer Dienstvertrag i. S. v. § 611 BGB scheidet daher aus.[66]

---

[61] Zu Haftungsausschlüssen und -begrenzungen siehe unten 3.3.3.7.

[62] Zur Anwendbarkeit der Regeln des TMG vgl. Kap. 5 (Spindler). Viele der im BGB normierten Vertragstypen enthalten Haftungserleichterungen zugunsten desjenigen, der unentgeltlich für einen Anderen tätig wird. So haben etwa der Verleiher und der Schenker gemäß § 599 BGB und § 521 BGB nur Vorsatz und grobe Fahrlässigkeit zu vertreten. Auch bei der unentgeltlichen Verwahrung greifen Haftungserleichterungen zugunsten des Verwahrers. Dieser hat gemäß § 690 BGB nur für diejenige Sorgfalt einzustehen, welche er in eigenen Angelegenheiten anzuwenden pflegt. Eine Ausnahme stellt der unentgeltliche Auftrag (§§ 662 ff. BGB) dar, der trotz Unentgeltlichkeit keine Haftungserleichterung für den Beauftragten vorsieht. Soweit man unentgeltliche Social Media-Angebote als Verträge sui generis i.S.d. § 311 BGB qualifiziert, käme allenfalls eine analoge Anwendung der Haftungserleichterungen in Betracht, die jedoch in aller Regel ausscheiden dürfte (LG Mainz, NJW 1988, 2116 f.; Chiusi, in: Staudinger, BGB, § 521 Rn. 13; Koch, in: MüKo-BGB, § 521 Rn. 8).

[63] Eine rechtliche Analyse von Haftungsfragen im Zusammenhang mit Social Media-Verträgen hat bisher weder in Literatur noch Rechtsprechung Eingang gefunden. Mit Blick auf die Literatur zu strukturell zum Social Media-Vertrag vergleichbaren Plattformverträgen ist allerdings davon auszugehen, dass sich hier keine besonderen Probleme ergeben, vgl. etwa zu Online-Auktionsplattformen Wiebe/Neubauer, in: Hoeren et al., Multimedia-Recht, Teil 15 Rn. 97 ff.

[64] Dies dürfte relativ häufig der Fall sein, vgl. oben 3.2.3.2.

[65] Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 421.

[66] Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 421; für vergleichbare Fälle bei Online-Games Lober/Weber, MMR 2005, 653 (656); a. A. Cichon, Internet-Verträge, Rn. 1094 ff.

In besonderen Einzelfällen könnte auch ein **Mietvertrag** oder mietvertragsähnliches Schuldverhältnis in Betracht kommen. Anknüpfungspunkt könnte hier die virtuelle Gebrauchsüberlassung sein.[67] Dagegen scheint allerdings zu sprechen, dass allein körperliche Gegenstände, nicht aber Rechte, vermietet werden können[68] und es bei Sozialen Medien damit auf den ersten Blick an einer tauglichen Mietsache fehlt.[69] **29**

Eine solche kann aber durchaus auch in der Einräumung von **zeitlich begrenzten Nutzungsrechten** für einen virtuellen Raum zu sehen sein.[70] Als Argument hierfür lässt sich die BGH-Rechtsprechung zur Qualifikation eines ASP/SaaS-Vertrages als Mietvertrag anführen,[71] nach der ein Mietvertrag keine Besitzverschaffung, sondern lediglich eine Gebrauchsverschaffung voraussetze.[72] Die Aussagen des BGH zum ASP/SaaS-Vertrag lassen sich jedoch nicht ohne Weiteres auf Social-Media-Plattformen übertragen.[73] Denn im Gegensatz zu ASP/SaaS-Dienstleistungen kommt der Überlassung einer Software bzw. der Einräumung von Nutzungsrechten bei Social-Media-Plattformen nur eine untergeordnete Rolle zu. **30**

Die vertragliche **Haftung** bestimmt sich bei entgeltlichen Social-Media-Verträgen nach den einschlägigen Bestimmungen des besonderen Schuldrechts, die sich wiederum aus dem im konkreten Einzelfall vorliegenden **Vertragstypus** richten.[74] **31**

3.3 Typische Klauseln in Social-Media-Verträgen

Ob der vielfältigen Spielarten von Social-Media-Verträgen und der daraus resultierenden Bandbreite an unterschiedlichen Allgemeinen Geschäftsbedingungen, lassen sich teilweise doch gewisse **Grundmuster** in der Ausgestaltung einzelner vorformulierter Vertragsbedingungen erkennen, die nahezu allen Social-Media-Verträgen gemein sind. Nach einem knappen Abriss über die Bestimmung des auf Allgemeine Geschäftsbedingungen anwendbaren nationalen Rechts (3.3.1) sowie einem Überblick über allgemeine AGB-rechtliche Probleme im Zusammenhang mit Social-Media-Verträgen (3.3.2), werden die wesentlichen dieser für Social-Media-Verträge typischen Klauseln im Folgenden dargestellt (3.3.3). **32**

---

[67] So etwa Berberich, Virtuelles Eigentum, S. 402 ff.; Schwenke, WRP 2013, 37 (38).
[68] Emmerich, in: Staudinger, BGB, § 535 Rn. 2 ff.; Weidenkaff, in: Palandt, BGB, § 535 Rn. 2.
[69] Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 422.
[70] Vgl. zur insoweit vergleichbaren Situation in Online-Games Krasemann, MMR 2006, 351, (353); Lober/Weber, MMR 2005, 653 (656).
[71] BGH, MMR 2007, 243 ff.; in diese Richtung bereits BGH, NJW 1987, 2004 ff. m. zust. Anm. Köhler, CR 1987, 827 ff. Vgl. auch Bettinger/Scheffelt, in: Spindler, Vertragsrecht der Internet-Provider, Teil XI, Rn. 17 f.
[72] BGH, MMR 2007, 243 ff.; vgl. auch von der Bussche/Schelinski, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 384.
[73] A.A. offensichtlich Berberich, MMR 2010, 736 (739 Fn. 38).
[74] Zu Fragen sinnvoller Haftungsausschlussklauseln bei Mietverträgen vgl. Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 100.

3.3.1 Anwendbares nationales Recht

33 Anbieter von Sozialen Medien haben ihren Sitz oft im außereuropäischen **Ausland**. In dieser Konstellation stellt sich grundsätzlich die Frage des (formell) auf den Vertragsschluss und (materiell) auf die Bestimmungen des Vertrages anwendbaren Rechts.

3.3.1.1 Auf den Vertragsschluss anwendbares Recht

34 Zur Bestimmung des anwendbaren Rechts ist die Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht **–** die sog. **Rom I-VO –** heranzuziehen.[75]

35 Auf das **Zustandekommen**[76] und die Wirksamkeit[77] eines Vertrages ist nach Art. 10 Abs. 1 Rom I-VO das Recht anwendbar, welches auf den wirksam geschlossenen Vertrag anwendbar wäre.[78] Im Falle einer (wirksamen) **Rechtswahl** ist dies gemäß Art. 3 Abs. 1 Rom I-VO das Recht, auf welches sich die Parteien geeinigt haben. Fehlt es an einer wirksamen Rechtswahl, so ist im Falle des Vorliegens eines **Verbrauchervertrages** i. S. v. Art. 6 Abs. 1 Rom I-VO das Recht desjenigen Staates anzuwenden, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat. In der Praxis werden viele Social-Media-Verträge als Verbraucherverträge zu qualifizieren sein, da die Nutzer die Plattformen in aller Regel zu privaten Zwecken nutzen.[79] Liegt im Falle des Fehlens einer wirksamen Rechtswahl kein Verbrauchervertrag vor, so ist auf die Regelanknüpfung des Art. 4 Abs. 2 (Rom I-VO) abzustellen. Anwendbar

---

[75] Vgl. insgesamt hierzu Kitz, in: Hoeren et al., Multimedia-Recht, Teil 13.1 Rn. 251 ff. Zu Art. 29 EGBGB, aber entsprechend auf die Rom I-VO übertragbar Hoeren, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, E-Commerce Verträge, Rn. 84 ff.

[76] Hierunter wird man im Wesentlichen die in §§ 130–161, 305 ff. BGB geregelten Aspekte verstehen müssen; im Einzelnen ist die Abgrenzung der unter „Zustandekommen" und „Wirksamkeit" zu fassenden Normen umstritten, aber praktisch nicht von Bedeutung. Vgl. zum Zustandekommen etwa Staudinger, in: Schulze, BGB, Art. 10 Rom I-VO, Rn. 3; Spickhoff, in: BeckOK-BGB, VO (EG) 593/2008, Art. 10 Rn. 3 ff.; vgl. insb. zu AGB-rechtlichen Bestimmungen Pfeiffer et al., in: Spindler/Schuster, Recht der elektronischen Medien, Art. 10 Rom I-VO, Rn. 3.

[77] Zu den davon umfassten Aspekten, wie insb. die in §§ 119 ff., 134, 138 BGB geregelten Aspekte, vgl. Spickhoff, in: BeckOK-BGB, VO (EG) 593/2008, Art. 10 Rn. 5; Ferrari, in: Ferrari et al., Internationales Vertragsrecht, VO (EG) 593/2008, Art. 10 Rn. 6 ff.

[78] Zur Ermittlung prägnant Staudinger, in: Schulze, BGB, Rom I Art. 10 Rn. 2.

[79] Dies dürfte aus Gründen des Verbraucherschutzes auch bei gemischt genutzten Profilen auf Business-Plattformen wie Xing und LinkedIn gelten, zumindest wenn diese vom Nutzer auch aus privaten Motiven unterhalten und auch für betriebsfremde Zwecke genutzt werden. Etwas anderes kann nur gelten, wenn der Nutzer etwa aufgrund einer arbeitsvertraglichen Verpflichtung einen Account erstellen muss sowie diesen alleine zu betrieblichen Zwecken nutzen darf. Zu den hierfür maßgeblichen Eigentumsverhältnissen an den Accounts vgl. Ernst, CR 2012, 276 ff.; Krüger/Ropel, AuA 2012, 467 ff.

ist dann das Recht des Staates, in dem diejenige Partei ihren Sitz hat, welche die charakteristische Leistung erbringt.[80]

3.3.1.2 Anwendbares materielles Recht

Das anwendbare Recht für **Allgemeine Geschäftsbedingungen** als vertragliches Schuldverhältnis bestimmt sich grundsätzlich nach der privatautonomen Rechtswahl der Parteien, Art. 3 Abs. 1 Satz 1 Rom I-VO. Damit kann prinzipiell ein anderes materielles Recht als das Deutsche gelten.[81] Im Grundsatz kann sowohl für die Allgemeinen Geschäftsbedingungen insgesamt als auch speziell für jede Klausel eine **eigenständige Rechtswahl** vorgenommen werden;[82] in der Folge kann so das auf den Vertrag als solchen sowie das auf die Allgemeinen Geschäftsbedingungen anwendbare Recht divergieren. **36**

3.3.1.3 Einschränkungen

Verbraucherschutz Der Grundsatz der freien Rechtswahl findet seine Grenzen im Verbraucherschutz. Liegt ein Verbrauchervertrag i. S. v. Art. 6 Abs. 1 Rom I-VO vor, so findet der eingangs dargestellte Grundsatz zwar prinzipiell Anwendung, wie Art. 6 Abs. 2 Satz 1 Rom I-VO explizit festschreibt. Allerdings darf diese Rechtswahl nach Art. 6 Abs. 2 Satz 2 Rom I-VO nicht dazu führen, dass der Verbraucher den **zwingenden Schutzvorschriften** des Staates, in dem er seinen gewöhnlichen Aufenthalt[83] hat, entzogen würde. Insoweit muss ein Günstigkeitsvergleich zwischen gewähltem Recht und nach Art. 6 Abs. 1 Rom I-VO anwendbarem Recht vorgenommen werden.[84] **37**

Vorliegen eines Verbrauchervertrages Der Verbrauchervertrag i. S. v. Art. 6 Abs. 1 Rom I-VO ist **autonom definiert**; die Begrifflichkeiten des nationalen Rechts **38**

---

[80] Dies wird beim Social-Media-Vertrag wohl das Bereitstellen der Infrastruktur sein, womit grundsätzlich das Recht des Staates, in dem der Anbieter seinen gewöhnlichen Aufenthalt hat, Anwendung finden wird.

[81] So erklären etwa die Terms of Service von Twitter in Art. 12 B kalifornisches Recht für anwendbar (vgl. http://twitter.com/tos), selbige von Youtube etwa in Art. 16.6 englisches Recht (vgl. http://www.youtube.com/t/terms). Facebook (Art. 17.3. der Terms of Service i.V.m. Nr. 5 der hierauf beruhenden Ergänzungsbestimmungen, vgl. http://www.facebook.com/terms.php) sowie Google (https://accounts.google.com/TOS) erklären dagegen deutsches Recht für anwendbar.

[82] Vgl. zu den Grenzen und Einschränkungen Martiny, in: MüKo-BGB, Art. 3 Rom I-VO, Rn. 70; Spickhoff, in: BeckOK-BGB, VO (EG) 593/2008, Art. 3 Rn. 27.

[83] Zum Begriff des gewöhnlichen Aufenthalts vgl. grundsätzlich Art. 19 Rom I-VO. Bei natürlichen Personen kommt es außerhalb ihrer beruflichen Tätigkeit allein auf die faktische Verortung an, vgl. Spickhoff, in: BeckOK-BGB, VO (EG) 593/2008, Art. 19 Rn. 5; Ferrari, in: Ferrari et al., Internationales Vertragsrecht, VO (EG) 593/2008, Art. 19 Rn. 14 f.; Martiny, in: MüKo-BGB, Art. 19 Rom I-VO, Rn. 11.

[84] Vgl. dazu Remien, in: Prütting et al., BGB, Art. 6 Rom I-VO, Rn. 22 f.; Martiny, in: Reithmann/Martiny, Internationales Vertragsrecht, Rn. 4206.

– insbesondere der §§ 13, 14 Abs. 1, 310 Abs. 3 BGB – sowie deren Auslegung durch die nationalen Gerichte sind für die Beurteilung nicht heranzuziehen.[85] Für die Qualifikation müssen kumulativ folgende Merkmale vorliegen:

39 **Der Unternehmer schließt einen Vertrag mit einem Verbraucher.** Mit Blick auf den **Anbieter** wird sich der Abschluss eines Social-Media-Vertrages nahezu immer als Ausübung der beruflichen oder gewerblichen Tätigkeit darstellen, womit er als **Unternehmer** zu qualifizieren ist. Schwieriger verhält es sich mit den **Nutzern**. Diese sind nur dann Verbraucher, wenn sie **nicht in Ausübung ihrer beruflichen oder gewerblichen Tätigkeit** handeln. Bei der Vielzahl der Nutzer, die Soziale Medien in ihrer Freizeit nutzen, dürfte dies der Fall sein. Bei Geschäften mit sowohl gewerblicher als auch privater Intention liegt ein Verbrauchergeschäft nur dann vor, wenn bei objektivierter Betrachtung die berufliche Nutzung eine gänzlich untergeordnete Rolle spielt.[86]

40 Der Unternehmer übt seine gewerbliche Tätigkeit in dem Staat aus, in dem der **Verbraucher** seinen **gewöhnlichen Aufenthalt** hat oder der Unternehmer richtet seine gewerbliche Tätigkeit auch auf den Staat, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, aus.

41 Bedeutung kommt angesichts der Vielzahl von Anbietern mit Sitz im Ausland vor allem der Alternative des **Ausrichtens** zu. Zum Teil wird vertreten, dass das Internet sich als **weltweit wirkendes Medium** global an jedermann und damit auch an den Aufenthaltsstaat des Verbrauchers richtet.[87] Ein Ausrichten in diesem Sinne soll zumindest dann vorliegen, wenn Unternehmen auf der Webseite zum Abschluss von Verträgen auffordern.[88] Dies sei bei Sozialen Medien bereits aufgrund ihres in die Startseite integrierten Angebots, ein Nutzungsverhältnis durch eine Registrierung einzugehen, der Fall.[89] Diese Einordnung berücksichtigt allerdings nicht ausreichend die spezifischen Gegebenheiten des Einzelfalles. Denn an welche Personen – bzw. welchen territorial determinierten Personenkreis – eine geschäftliche Handlung ausgerichtet ist, bestimmt sich einzelfallbezogen aus der Perspektive eines objektiven Betrachters mit Blick auf die Verkehrssitte. Die **Sprache**, in welcher das Soziale Medium gefasst ist, sowie die **faktisch sinnvolle Nutzbarkeit** allein oder überwiegend

---

[85] Ausdrücklich auf die autonome Interpretation etwa des Verbraucherbegriffs verweist Staudinger, in: Ferrari et al., Internationales Vertragsrecht, VO (EG) 593/2008, Art. 6 Rn. 23; a. A. Pfeiffer et al., in: Spindler/Schuster, Rom I-VO, Art. 6 Rn. 8.

[86] Vgl. zur insoweit vergleichbaren Regelung des Art. 13 Abs. 1 EuGVÜ EuGH, EuZW 2005, 241. Eingehend hierzu Mankowski, IPRax 2005, 505 ff.

[87] Einzelheiten nach dem Urteil des EuGH, NJW 2011, 505 ff. umstritten; grundsätzlich wird man zumindest ein abstraktes Abzielen verlangen müssen, was sich in objektiven Anhaltspunkten (Verfügbarkeit, Sprachwahl u. Ä.) manifestieren muss, vgl. Staudinger, in: Schulze, BGB, Rom I-VO, Art. 6 Rn. 11; vgl. dazu etwa Thorn, in: Palandt, BGB, Rom I-VO, Art. 6 Rn. 6; Staudinger, in: Ferrari et al., Internationales Vertragsrecht, VO (EG) 593/2008, Art. 6 Rn. 51 ff.

[88] Dies wird insofern gestützt durch Erwägungsgrund 24 Satz 3 Rom-I-VO sowie die Gemeinsame Erklärung der Kommission und des Rates zu Artikel 15 der Verordnung (EG) Nr. 44/2001; so im Ergebnis Staudinger, in: Ferrari et al., Internationales Vertragsrecht, VO (EG) 593/2008, Rn. 54.

[89] Vgl. allein Solmecke/Dam, MMR 2012, 71.

für einen territorial eingrenzbaren Raum, sind wichtige Indizien für eine entsprechende Ausrichtung des Anbieters. Bietet dieser etwa das Soziale Medium in einer Sprache an, die nahezu ausschließlich in einem bestimmten Land gesprochen wird, oder handelt es sich um ein Soziales Medium, welches seiner Zweckbestimmung nach auf einen bestimmten Raum beschränkt ist, etwa allein den Austausch zwischen deutschen Schülern über ihre Schularbeiten fördern soll, so kann nicht ohne Weiteres von einer globalen Ausrichtung nur deshalb ausgegangen werden, weil eine Registrierung rein tatsächlich weltweit für jedermann möglich ist.

Zwingendes Verbraucherschutzrecht Bei §§ 305 ff. BGB handelt es sich um zwingende Verbraucherschutzvorschriften i. S. v. Art. 6 Abs. 2 Satz 2 Rom I-VO,[90] da sie ihrem Zweck nach den **schwächeren Vertragsteil schützen** sollen.[91] Eine nationalrechtliche Qualifikation als Verbraucherschutzrecht allein wäre nicht ausreichend.[92] **42**

Eingriffsnormen Art. 9 Abs. 1 Rom I-VO legt fest, dass zwingende Eingriffsnormen des nationalen Rechts unabhängig von der zwischen den Parteien getroffenen Rechtswahl Anwendung finden. Eingriffsnormen sind sämtliche Regelungen, die zumindest auch Gemeinwohlinteressen dienen und dabei für die Wahrung eines **öffentlichen Interesses entscheidend** sind.[93] **43**

Eine in der Praxis bedeutsame Eingriffsnorm stellt § 1 Abs. 5 BDSG dar, der als Kollisionsnorm die **Anwendbarkeit des Bundesdatenschutzgesetzes** bei grenzüberschreitenden Sachverhalten regelt.[94] Art. 9 Abs. 1 Rom-I-VO stellt damit klar, dass durch eine Rechtswahlklausel nicht die Anwendung deutscher Datenschutzgesetze ausgehebelt werden kann. AGB-Klauseln mit datenschutzrechtlichem Bezug sind daher bei Anwendbarkeit deutschen Datenschutzrechts nach § 1 Abs. 5 BDSG immer an diesem zu messen.[95] **44**

---

[90] Spickhoff, in: BeckOK-BGB, VO (EG) 593/2008, Art. 6 Rn. 31; Martiny, in: MüKo-BGB, Art. 6 Rom I-VO, Rn. 44; Thorn, in: Palandt, BGB, Rom I-VO, Art. 6 Rn. 9; Paul, in: Hoeren et al., Multimedia-Recht, Teil 7.4 Rn. 147 f.

[91] So noch zu Art. 29 EGBGB LG Hamburg, K&R 2009, 735 ff.; OLG Düsseldorf, ZEuP 1998, 981 ff.; vgl. Pfeiffer et al., in: Spindler/Schuster, Rom I-VO, Art. 6 Rn. 22.

[92] BGH, NJW-RR 2005, 1071.

[93] Schönbohn, in: BeckOK-BGB, VO (EG) 593/2008, Art. 9 Rn. 4; Pfeiffer et al., in: Spindler/Schuster, Rom I-VO, Art. 9 Rn. 3 f.

[94] Vgl. auch Pfeiffer et al., in: Spindler/Schuster, Rom I-VO, Art. 9 Rn. 17.

[95] Im Ergebnis auch Jotzo, MMR 2009, 232 ff.

3.3.2 Grundsätzliches

3.3.2.1 Nutzungsbedingungen als AGB i. S. d. §§ 305 ff. BGB

45 Die Nutzungsbedingungen Sozialer Medien sind **Allgemeine Geschäftsbedingungen** i. S. v. § 305 Abs. 1 BGB.[96] Bezeichnungen wie „Terms of Service“[97], „Nutzungsbestimmungen“ oder „Erklärung über Rechte und Pflichten“[98] sind im Ergebnis unschädlich, da eine ausdrückliche Bezeichnung der Nutzungsbedingungen als Allgemeine Geschäftsbedingungen nicht erforderlich ist, sofern diese materiell Allgemeinen Geschäftsbedingungen entsprechen.[99]

3.3.2.2 Wirksame Einbeziehung der Nutzungsbedingungen

46 Die Voraussetzungen für die wirksame **Einbeziehung** Allgemeiner Geschäftsbedingungen bestimmen sich nach Maßgabe des § 305 Abs. 2 BGB. Danach muss der Verwender bei Vertragsschluss ausdrücklich auf die Geltung seiner Nutzungsbedingungen hinweisen, der Vertragspartner die Möglichkeit haben, in zumutbarer Weise von den Nutzungsbedingungen Kenntnis zu nehmen und mit ihrer Geltung einverstanden sein.

47 In der Praxis werden die gesetzlichen Anforderungen fast ausnahmslos durch eine **Opt-in-Lösung** umgesetzt. Dies bedeutet, dass der Nutzer den online einsehbaren Nutzungsbedingungen durch das Bestätigen einer Checkbox ausdrücklich zustimmen muss.[100] Ohne diese aktive Bestätigung der Nutzungsbedingungen kann der Registrierungsvorgang nicht vollendet werden. Um die Anforderungen an die Einräumung einer zumutbaren Möglichkeit der Kenntnisnahme zu erfüllen, müssen Nutzer die Möglichkeit haben, die Nutzungsbedingungen dauerhaft elektronisch abzuspeichern und auszudrucken.[101]

48 Problematisch kann eine wirksame Einbeziehung dort sein, wo die Nutzungsbedingungen in **mehreren Einzeldokumenten** enthalten sind, auf die nicht im Einzelnen hingewiesen wird, sondern auf die allein ein pauschaler Hinweis erteilt wird. Als prominentes Beispiel kann Facebook aufgeführt werden. Eine wirksame

---

[96] Vgl. Rippert/Weimer, ZUM 2007, 275; Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 47; Schwenke, WRP 2013, 37 (39). Zum Begriff auch Bussche/Schelinski, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1, Rn. 138 ff.; zu den Problemen von AGB im Internet auch Säcker, in: MüKo-BGB, Einl. Rn. 209 ff.

[97] So etwa die Terminologie bei Twitter, vgl. https://twitter.com/tos/.

[98] So der bei Facebook verwendete Begriff, vgl. http://www.facebook.com/terms.php.

[99] Berberich, MMR 2010, 736; Paul, in: Hoeren et al., Multimedia-Recht, Teil 7.4 Rn. 143.

[100] Vgl. Paul, in: Hoeren et al., Multimedia-Recht, Teil 7.4 Rn. 144.

[101] Vgl. hierzu auch Föhlisch, in: Hoeren et al., Multimedia-Recht, Teil 13.4, Rn. 107. Siehe auch Säcker, in: MüKo-BGB, Einl., Rn. 209 ff.; zu allgemeingültigen Problemen der Dokumentation mit Blick auf Beweisprobleme ferner Mankowski, in: Ferrari et al., Internationales Vertragsrecht, Vorbem. zu Art. 14 ff. CISG, Rn. 33 ff.

Einbeziehung scheint vor dem Hintergrund der strengen Anforderungen der Rechtsprechung zumindest diskutabel, wurde jedoch vom Landgericht Berlin im Ergebnis bejaht.[102]

3.3.2.3 Unvorhersehbare Klauseln

Nach § 305c Abs. 1 BGB werden Klauseln nicht Vertragsbestandteil, mit denen der Nutzer nach konkreter Lage der Umstände vernünftigerweise nicht zu rechnen braucht. Dies sind nach allgemeinem Verständnis solche Klauseln, denen ein erheblicher **Überrumpelungs- und Übertölpelungseffekt** anhaftet.[103] Ob ein solcher vorliegt, ist für jeden Einzelfall gesondert zu beurteilen; dabei kommt dem Aspekt der Branchenüblichkeit und den Geboten von Treu und Glauben erhebliche Bedeutung zu.[104] **49**

Zum Teil wird vor diesem Hintergrund die Unwirksamkeit weitreichender **urheberrechtlicher Nutzungsrechte** in Allgemeinen Geschäftsbedingungen[105] von Anbietern sozialer Netzwerke erwogen,[106] da der Nutzer nicht damit rechnen müsse, dass er den Anbietern Nutzungsrechte einräume, die über das für die Nutzung der Plattform erforderliche Maß hinausgehen.[107] In aller Regel benötigt der Anbieter eines sozialen Netzwerks lediglich Rechte zur Vervielfältigung der Inhalte (§ 16 UrhG), zur öffentlichen Zugänglichmachung (§ 19a UrhG) sowie zur Bearbeitung (§ 23 UrhG).[108] Einer abstraktpauschalierten Lösung ist diese Problematik allerdings nicht zugänglich. Vielmehr bedarf es – entsprechend obiger Ausführungen – einer individuellen Betrachtung jedes konkreten Einzelfalls mit Blick darauf, mit welchen Rechteeinräumungen der Nutzer insbesondere hinsichtlich Natur, Charakteristika und Inhalt des jeweiligen Sozialen Mediums rechnen muss. **50**

Gegen eine Unvorhersehbarkeit umfassender Rechteklauseln könnte generell sprechen, dass Nutzern aufgrund der medialen Beachtung und der mittlerweile weiten Verbreitung bekannt sein dürfte, dass sich soziale Netzwerke derart weitreichende urheberrechtliche Nutzungsrechte einräumen lassen.[109] Diesbezüglich erscheint bereits zweifelhaft, ob von einer Überrumpelung der Nutzer gesprochen werden kann. **51**

---

[102] LG Berlin, K&R 2012, 300 ff.
[103] Vgl. zusammenfassend Basedow, in: MüKo-BGB, § 305c Rn. 10; Grüneberg, in: Palandt, BGB, § 305c Rn. 3 f.
[104] Vgl. BGH, NJW-RR 2003, 1635 ff.; LG Offenburg, BeckRS 2009, 09387; siehe für Internet-Verträge Castendyk, ZUM 2007, 169 (171); Nordemann, NJW 2012, 3121 (3124).
[105] Zur darüber hinaus bestehenden Problematik im Rahmen der Inhaltskontrolle vgl. unten 3.3.3.2.
[106] Überblicksartig hierzu Paul, in: Hoeren et al., Multimedia-Recht, Teil 7.4 Rn. 146.
[107] Berberich, MMR 2010, 736 (737); Nordemann, NJW 2012, 3121; Schwenke, WRP 2013, 37 (39); Solmecke/Dam, MMR 2012, 71 (72).
[108] Solmecke/Dam, MMR 2012, 71 (72).
[109] In diese Richtung schon Berberich, MMR 2010, 736 (737); Solmecke/Dam, MMR 2012, 71 (72).

52 Im Ergebnis jedenfalls sprechen die besseren Gründe dafür, umfangreiche Nutzungsrechtseinräumungen **nicht pauschal** als unvorhersehbare Klauseln i. S. v. § 305c BGB zu qualifizieren, sondern dies von einer **Einzelfallabwägung** abhängig zu machen. Hierbei ist besonderes Augenmerk auf Art und Umfang der Rechteeinräumung zu richten.

3.3.2.4 Drittwirkung

53 Bei der Nutzung sozialer Medien werden vom Plattformbetreiber häufig sogenannte **Verhaltens- oder Communityregeln** verwendet, die den Umgang der Nutzer untereinander regeln. Facebook verbietet seinen Nutzern beispielsweise die Veröffentlichung von Gewalt und Drohungen gegenüber anderen Nutzern in seinen „Standards der Facebook-Gemeinschaft".[110] Verstößt ein Nutzer gegen diese Verhaltensregeln und beleidigt etwa einen anderen Nutzer auf der Plattform des Betreibers, erscheint es daher fragwürdig, ob den Verhaltensregeln des Plattformbetreibers insoweit eine Drittwirkung zukommt. Bei diesen Verhaltensregeln handelt es sich, wie bei den Nutzungsbedingungen,[111] um AGB, welche wirksam einbezogen werden müssen. Zur Begründung einer Pflicht ist ein Vertrag erforderlich, § 311 Abs. 1 BGB (sog. Vertragsprinzip[112]). Die Einbeziehung der Verhaltensregeln erfolgt allerdings nur **vertikal** im Verhältnis zwischen den jeweiligen Nutzern und dem Plattformbetreiber, **nicht hingegen horizontal** zwischen den Nutzern. Eine Drittwirkung kommt den AGB des Plattformbetreibers demnach nicht zu. In seinem „Ebay-Urteil" hatte der BGH eine Drittwirkung zwar ebenfalls abgelehnt. Jedoch wurden hier die AGB **zur Auslegung** des über die Ebay-Plattform abgeschlossenen Kaufvertrags **herangezogen**.[113] Dieser Gedanke kann nicht auf den Fall übertragen werden, dass ein Nutzer gegen den Verhaltenskodex eines sozialen Netzwerkes verstoßen und dadurch einen anderen Nutzer in seinen Rechten verletzt hat. Der entscheidende Unterschied besteht darin, dass über eine Verkaufsplattform der geschäftliche Kontakt hergestellt und damit eine vertragliche Beziehung in Form eines Kaufvertrags begründet wird. Veröffentlicht ein Nutzer eines sozialen Netzwerkes hingegen beleidigende Inhalte über einen anderen Nutzer, **fehlt es an einer solchen vertraglichen Beziehung**. Das Schuldverhältnis, das durch die Veröffentlichung begründet ist und aus dem der Nutzer Schadensersatz geltend machen kann, ist vielmehr gesetzlicher Natur, welches einer Auslegung nicht zugänglich ist, da nach den §§ 133, 157 BGB nur Willenserklärungen und Verträge auslegungsfähig sind.[114] Der verbleibende Regelungsgehalt

---

[110] http://www.facebook.com/communitystandards.
[111] Zur Einbeziehung der Nutzungsbedingungen vgl. oben 3. Rn. 46 ff.
[112] Emmerich, in: MüKo-BGB, § 311 Rn. 1.
[113] BGH, MMR 2002, 95 ff.; BGH, NJW 2011, 2643; Wiebe, in: Spindler/Wiebe, Internetauktionen und elektronische Marktplätze, Kap. 4, Rn. 120 ff.; Wagner/Zenger, MMR 2013, 343 (346 f.); LG Bonn, Urt. v. 05.06.2012–18 O 314/11.
[114] Singer, in: Staudinger, BGB, § 133 Rn. 3.

solcher Verhaltensregeln besteht darin, dass dem Plattformbetreiber durch die Anerkennung dieser Standards die Befugnis eingeräumt wird, Veröffentlichungen, die dagegen verstoßen, zu sperren bzw. zu editieren. Etwas anderes kann nur dann gelten, wenn einer der Nutzer mit der Nutzung des sozialen Netzwerkes kommerzielle Ziele verfolgt und über die Plattform mit dem anderen Nutzer einen Vertrag abschließt. Zu denken wäre hier an Fanpages berühmter Persönlichkeiten oder Unternehmen sowie an Shops oder Apps, die auf dieser Plattform betrieben werden. In diesen Fällen wäre eine Übertragung der o.g. „Ebay-Rechtsprechung" denkbar. Dies gilt jedoch nur dann, wenn die Veröffentlichung auch im Zusammenhang mit dieser kommerziellen Tätigkeit erfolgt ist.

3.3.3 AGB-rechtliche Wirksamkeit typischer Klauseln

Die Wirksamkeit Allgemeiner Geschäftsbedingungen beurteilt sich nach den Vorschriften der **Inhaltskontrolle** (§§ 307 ff. BGB). Auf die §§ 134, 138 BGB ist allenfalls subsidiär zurückzugreifen.[115] Eine allgemeine Billigkeitskontrolle unter Heranziehung des § 242 BGB findet nicht statt.[116] **54**

Die Inhaltskontrolle bezieht sich allein auf solche Klauseln, die von den **gesetzlichen Vorgaben abweichen**, § 307 Abs. 3 BGB. Ihre Kernstücke sind die generalklauselartigen Benachteiligungsverbote des § 307 Abs. 1 Satz 2, Abs. 2 BGB sowie das in § 307 Abs. 1 Satz 2 BGB normierte Transparenzgebot, welches besagt, dass eine Klausel aus sich heraus für den Durchschnittsnutzer ohne Hinzuziehung eines Rechtsrats verständlich sein muss.[117] Die Klauselverbote der §§ 308 f. BGB haben im Bereich der Social-Media-Verträge häufig keine eigenständige Rolle.[118] **55**

Verstöße gegen die Regelungen der Inhaltskontrolle stellen für den Anbieter eines Sozialen Mediums ein erhebliches rechtliches Risiko dar, da er sich nicht nur etwaigen **Ansprüchen der Nutzer**, sondern auch einer möglichen **Verbandsklage** nach §§ 1, 3 UKlaG ausgesetzt sieht. Außerdem besteht die Gefahr, von Mitbewerbern auf Unterlassung nach Maßgabe der §§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 11 UWG in Anspruch genommen zu werden, da die §§ 307 ff. BGB Marktverhaltensregelungen darstellen.[119] **56**

---

[115] Armbrüster, in: MüKo-BGB, § 138 Rn. 5; Ellenberger, in: Palandt, BGB, § 138 Rn. 16.
[116] Roth/Schubert, in: MüKo-BGB, § 242 Rn. 471.
[117] Vgl. Coester, in: Staudinger, BGB, § 307 Rn. 170 ff.
[118] Vgl. Nordemann, NJW 2012, 3121 (3122).
[119] So etwa BGH, MMR 2012, 672; KG, MMR 2005, 466; Köhler, in: Köhler/Bornkamm, UWG, § 4 Rn. 11.153a ff. m. w. N.; a. A. etwa OLG Köln, GRUR-RR 2007, 285; OLG Hamburg, GRUR-RR 2007, 287; Ohly, in: Piper et al., UWG, § 4 Rn. 11.78.

57 Im Folgenden sollen einige der für Social-Media-Verträge **typischen Regelungen** dargestellt werden; eine abschließende Darstellung aller denkbaren Klauseln ist dagegen nicht möglich.[120]

3.3.3.1 Vertragssprache

58 Die Wirksamkeit vieler AGB-Klauseln ist allein deshalb zweifelhaft, weil es sich bei diesen vielfach um schlichte **Übersetzungen aus dem Englischen** (bei weltweit agierenden Social-Media-Angeboten) handelt, ohne eine Anpassung speziell an die Gegebenheiten in Deutschland und das hier geltende Recht vorzunehmen.[121] Allgemeine Geschäftsbedingungen sind insgesamt **intransparent** i. S. v. § 307 Abs. 1 Satz 2 BGB, wenn sie in einer anderen Sprache gehalten sind als der, in der das Soziale Medium angeboten wird; in solchen Fällen muss für die Wirksamkeit der Allgemeinen Geschäftsbedingungen der Nachweis geführt werden, dass der jeweilige Nutzer der Sprache, in welcher die AGB gehalten sind, hinreichend mächtig ist.[122]

3.3.3.2 Einräumung von Nutzungsrechten

59 Anbieter von Sozialen Medien lassen sich in der Praxis häufig umfangreiche Nutzungsrechte an den von ihren Nutzern eingestellten Inhalten einräumen.

60 **Abweichung vom gesetzlichen Leitbild** Zumindest die umfassende Einräumung von Nutzungsrechten an Nutzerinhalten kann im Einzelfall gegen das Verbot der unangemessenen Benachteiligung i. S. v. § 307 Abs. 2 Nr. 1 i.V. m. § 31 Abs. 5 UrhG verstoßen. So hat etwa das Landgericht Berlin eine Klausel der Facebook-AGB[123] für unwirksam erklärt, welche die Einräumung einer nicht exklusiven, übertragbaren, unterlizenzierbaren, unentgeltlichen und weltweiten Lizenz für die Nutzung aller Inhalte des Nutzers (sog. User Generated Content) vorsah.[124] Das Gericht stützte die Unwirksamkeit der Rechteklausel auf eine Unvereinbarkeit mit dem in § 31 Abs. 5 UrhG in Form der **Zweckübertragungslehre** statuiertem gesetzlichen Leitbild. Die Zweckübertragungslehre besagt, dass der Urheber im Zweifel keine weitergehenden Rechte überträgt, als es der Zweck der Verfügung – der zu Grunde liegende Vertrag – erfordert.[125] Damit soll eine möglichst umfassende **Partizipation des Urhebers**

---

[120] Vgl. ergänzend die Ausführungen von Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 zu Webportal-Nutzungsbedingungen, die weitgehend entsprechend auf Social-Media-Nutzungsbedingungen anwendbar sind.

[121] Vgl. Solmecke/Dam, MMR 2012, 71 m. w. N.

[122] Föhlisch, in: Hoeren et al., Multimedia-Recht, Teil 13.4, Rn. 108.

[123] Ziff. 1.1 der damaligen „Erklärung von Rechten und Pflichten".

[124] LG Berlin, ZD 2012, 276 ff. m. Anm. Solmecke. Die Berufung ist derzeit am KG anhängig (Az.: 5 U 42/12). Zur in diesem Kontext auch bedeutsamen Rolle der informationellen Selbstbestimmung in sozialen Netzwerken vgl. Bender, K&R 2013, 218 ff.

[125] St. Rspr., vgl. BGH, GRUR 2003, 234 (236); BGH, GRUR 1996, 121 (122); BGH, GRUR 1984, 119 (121).

an der wirtschaftlichen Verwertung seines Werks bei gleichzeitig verhältnismäßig geringfügiger Einräumung von Ausschließlichkeitsrechten erreicht werden. Übergreifendes Ziel ist demnach der maßvolle Umgang mit Ausschließlichkeitsrechten zur Gewährleistung einer weitreichenden Beteiligung des Urhebers.[126] Aufgrund dieser Funktion der Zweckübertragungslehre geht das Landgericht Berlin – insoweit konform mit der in der Literatur überwiegend vertretenen Meinung[127] – davon aus, dass § 31 Abs. 5 UrhG ein gesetzliches Leitbild darstelle, wodurch jeder Verstoß hiergegen die Unwirksamkeit der Klausel gem. § 307 Abs. 2 Nr. 1 BGB nach sich ziehe. Wie bereits eingangs erläutert, benötigt der Anbieter eines sozialen Netzwerks in aller Regel lediglich Rechte zur Vervielfältigung der Inhalte (§ 16 UrhG), zur öffentlichen Zugänglichmachung (§ 19a UrhG) sowie zur Bearbeitung (§ 23 UrhG). Demgemäß würde jede darüber hinausgehende Rechteeinräumung stets einen Verstoß gegen das Verbot der unangemessenen Benachteiligung darstellen.

61 Bereits im Jahr 1984 hatte der BGH allerdings entschieden, dass es sich bei § 31 Abs. 5 UrhG um eine bloße **Auslegungsregel** handele.[128] In einer jüngeren Entscheidung hat der BGH an dieser Entscheidung festgehalten und erneut bestätigt, dass § 31 Abs. 5 UrhG eine bloße teleologische Auslegungsregel darstelle.[129] Vor dem Hintergrund der Entscheidung des BGH dürfte daher eine Unwirksamkeit unter dem Gesichtspunkt eines Verstoßes gegen ein gesetzliches Leitbild nach § 307 Abs. 2 Nr. 1 BGB i. V. m. § 31 Abs. 5 UrhG ausscheiden.[130]

62 **Weiterübertragung und Unterlizenzierung von Nutzungsrechten** Gleichwohl ist zu beachten, dass § 34 Abs. 1 UrhG, der die Übertragung eines urheberrechtlichen Nutzungsrechts von der **Zustimmung des Urhebers** abhängig macht, gesetzlichen Leitbildcharakter hat.[131] Soweit daher Nutzungsbedingungen eine freie Weiterübertragbarkeit von Nutzungsrechten vorsehen, verstoßen diese Regelungen grundsätzlich gegen § 307 Abs. 2 Nr. 1 BGB. Gleiches gilt im Ergebnis auch für die Unterlizenzierung von Nutzungsrechten. Denn auch dem insoweit maßgeblichen § 35 Abs. 1 UrhG kommt eine gesetzliche Leitbildfunktion zu, sodass die Einräumung eines umfassenden Rechts zur Unterlizenzierung in Allgemeinen Geschäftsbedingungen regelmäßig einen Verstoß gegen § 307 Abs. 2 Nr. 1 BGB darstellen wird.[132]

63 **Transparenzgebot, § 307 Abs. 1 Satz 1 BGB** Unabhängig davon kann sich die Unwirksamkeit umfassender Rechteklauseln häufig ferner aus Verstößen gegen das

---

[126] So Höch/Kadelbach, WRP 2012, 1060 (1061).
[127] Vgl. Schulze, in: Dreier/Schulze, UrhG, § 31 Rn. 110 m. w. N. Ferner Berberich, MMR 2010, 736 (739); ders., ZUM 2006, 205 (207); Nordemann, in: Loewenheim, Handbuch des Urheberrechts, § 60 Rn. 18a; Solmecke/Dam, MMR 2012, 71 (73).
[128] BGH, GRUR 1984, 45 (49).
[129] BGH, K&R 2012, 597 m. w. N. So allerdings auch LG Berlin, ZUM-RD 2008, 18.
[130] Weitergehend zu dieser Problematik Höch/Kadelbach, WRP 2012, 1060 (1061).
[131] BGH, GRUR 1984, 45 (52); Wandtke/Grunert, in: Wandtke/Bullinger, Urheberrecht, § 34 Rn. 40; Schulze, in: Dreier/Schulze, UrhG, § 34 Rn. 51 m. w. N.
[132] Schulze, in: Dreier/Schulze, UrhG, § 35 Rn. 21.

Transparenzgebot des § 307 Abs. 1 Satz 1 BGB ergeben. Aus der Zweckübertragungslehre folgt nämlich auch, dass **bei Vertragsschluss** für den Nutzer **erkennbar** sein muss, welche Nutzungsarten konkret dem Anbieter eingeräumt werden sollen (Spezifizierungslast).[133] Dies wird im Rahmen einer umfassenden Rechteklausel dem Nutzer nicht hinreichend vor Augen geführt.[134] Ihm ist vielmehr im Einzelnen aufzuschlüsseln, welche Nutzungsrechte er dem Anbieter einräumt, damit er die Tragweite der Rechteeinräumung abschätzen kann. Da nach herrschender Ansicht eine geltungserhaltende Reduktion einer – etwa wegen eines Verstoßes gegen das Transparenzgebot – unwirksamen Klausel nicht in Betracht kommt, haben Verstöße gegen das Transparenzgebot die **vollständige Unwirksamkeit** der Klausel, die nicht sinnvoll in zwei eigenständige Bestandteile (eine wirksame und eine unwirksame Komponente) getrennt werden kann, zur Folge.

3.3.3.3 Einwilligungen

64 Gerade bei US-amerikanischen Anbietern von Sozialen Medien sollen Nutzer im Rahmen der **Datenschutzerklärung** (*Privacy Policy*) auch in die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten einwilligen.

65 **Datenschutzrechtliche Dimension** Ein datenschutzrechtliches Erfordernis für die Einholung einer Einwilligung besteht allerdings oftmals nicht oder nur zum Teil. Soweit nämlich die Erhebung und Nutzung personenbezogener Daten des Nutzers von gesetzlichen Erlaubnistatbeständen wie §§ 14 ff. TMG, §§ 28 ff. BDSG gedeckt sind, ist eine Einwilligung des Nutzers entbehrlich.[135] Sitzt der Social-Media-Anbieter im europäischen Ausland, stellt sich jedoch die Frage, ob **deutsches Datenschutzrecht** überhaupt **Anwendung** findet. Das OVG Schleswig verneint diese Frage,[136] wohingegen das Kammergericht von der Anwendbarkeit deutschen Datenschutzrechts ausgeht.[137] Höchstrichterlich wurde diese Frage jedoch bisher nicht geklärt. Im Folgenden soll trotz der bestehenden Unsicherheiten von der Anwendbarkeit deutschen Datenschutzrechts ausgegangen werden.

66 **AGB-rechtliche Dimension** Soweit die Einholung einer Einwilligung datenschutzrechtlich geboten ist (etwa weil die beabsichtigte Verarbeitung nicht auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann), spielt es für die rein AGB-rechtliche Beurteilung letztlich keine Rolle, ob diese in den allgemeinen *Terms of Use* enthalten oder Teil einer separaten Datenschutzerklärung ist.

67 Datenschutzrechtliche Einwilligungen unterliegen grundsätzlich **vollumfänglich der Inhaltskontrolle** nach §§ 307 ff. BGB. Daneben kommt dem **Transparenzgebot** aus § 307 Abs. 1 Satz 2 BGB auch hier eine entscheidende Bedeutung zu: Klauseln,

---

[133] Schwenke, WRP 2013, 37 (39).
[134] So im Ergebnis auch LG Berlin, ZD 2012, 276 ff. m. Anm. Solmecke.
[135] Vgl. dazu eingehend Kap. 4 (Hornung).
[136] OVG Schleswig, ZD 2014, 364 ff.
[137] KG, BeckRS 03648.

die Zweck, Umfang oder Art der Datenverarbeitung nicht eindeutig erkennen lassen, sind intransparent und damit unwirksam.[138]

3.3.3.4 Verwendung personenbezogener Daten für Werbezwecke

Wenngleich die Verwendung von Nutzer-Daten für **Zwecke der personalisierten Werbung** in erster Linie datenschutzrechtliche Fragen berührt,[139] stellen sich auch an dieser Stelle AGB-rechtliche Fragen. **68**

Verwendung von Nutzer-Daten Für die Nutzung personenbezogener Daten der Nutzer zum Zwecke der Einblendung personalisierter Werbung ist häufig die Einholung einer **Einwilligung** erforderlich. Diese muss den formalen Vorgaben der §§ 13 Abs. 2 TMG und 4a BDSG entsprechen. Ohne die Einholung einer ausdrücklichen Einwilligung der Nutzer ist die Nutzung personenbezogener Daten zum Zwecke der Werbung grundsätzlich nur unter den engen Voraussetzungen des § 15 Abs. 3 TMG bei Verwendung eines Pseudonyms zulässig.[140] **69**

Mit Blick auf das AGB-rechtliche Transparenzgebot muss eine Einwilligung dem Nutzer **eindeutig und unmissverständlich** vor Augen führen, welche Rechte und Pflichten sich aus der Klausel im Einzelnen ergeben; soweit eine Verschleierung der Absicht, personalisiert zu werben, in der Einwilligung angelegt ist, ist eine derartige Klausel intransparent und damit unwirksam.[141] **70**

Verwendung fremder Daten Einige Social-Media-Anbieter ermöglichen ihren Nutzern, Freunde und Bekannte über eine plattforminterne Funktion direkt in ihr Netzwerk **einzuladen**. Über den Facebook-Freundefinder beispielsweise können Facebook-Nutzer auf ihr E-Mail-Konto-Adressbuch zugreifen und mit wenigen Klicks Einladungen an ihre dort gespeicherten Kontakte versenden.[142] **71**

Das LG Berlin vertrat die Auffassung, dass der Facebook-Freundefinder nach § 7 Abs. 2 Nr. 3 UWG unlauter sei, was sich insofern mit seiner Rechtsprechung zum sogenannten „Empfehlungsmarketing“ deckt.[143] Diese Form des Anschreibens der Freunde des Nutzers stelle nämlich eine **unzumutbar belästigende Werbung** durch eine geschäftliche Handlung des Anbieters dar, in welche der Betroffene nicht eingewilligt habe. Dies ist durchaus kritisch zu betrachten, weil ein Verstoß gegen § 7 Abs. 2 Nr. 3 UWG zumindest auch einer geschäftlichen Handlung des versendenden Nutzers als Mittäter von Facebook i. S. v. § 830 BGB bedarf; daran wird es allerdings regelmäßig fehlen, da das Versenden der Einladungen allein im rein privaten Bereich anzusiedeln ist.[144] Weiterhin sei die entsprechende Praxis **72**

[138] Schwenke, WRP 2013, 37 (39).
[139] Vgl. dazu eingehend Kap. 4 (Hornung).
[140] Zu den Einzelheiten siehe Bauer, MMR 2008, 435 ff.
[141] LG Berlin, ZD 2012, 276 ff. m. Anm. Solmecke.
[142] Eine exakte Darstellung dieser Funktion beschreibt Wieczorek, WRP 2012, 539 (540).
[143] LG Berlin, K&R 2009, 823.
[144] So auch Piltz, CR 2012, 274.

nach Auffassung des LG Berlin auch unzulässig gemäß §§ 3, 4 Nr. 11 UWG i. V. m. § 4a BDSG, da eine Einwilligung der E-Mail-Empfänger in die Nutzung ihrer personenbezogenen Daten nicht vorliege.[145] Bei § 4a BDSG handelt es sich insofern um eine Marktverhaltensregel i. S. v. § 4 Nr. 11 UWG, als sie den Einzelnen vor der Übermittlung seiner Daten zu kommerziellen Zwecken generell und insbesondere zu Werbezwecken schützt.[146] Trotz der genannten Kritikpunkte wies das Kammergericht die Berufung von Facebook zurück.[147]

3.3.3.5 Kündigung von Social-Media-Verträgen

73 Social-Media-Verträge sind in aller Regel als Dauerschuldverhältnisse ausgestaltet. Als solche sind sie grundsätzlich nur dann kündbar, wenn die Parteien dies ausdrücklich vereinbaren. Daneben tritt von Gesetzes wegen die Möglichkeit der **Kündigung aus wichtigem Grund gem. § 314 BGB**.[148] Hinsichtlich des Umfangs und der Grenzen eines vertraglich vereinbarten Kündigungsrechtes ist zwischen dem Anbieter und den Nutzern zu differenzieren.

74 **Kündigung durch den Anbieter** Insbesondere US-amerikanische Social-Media-Anbieter behalten sich zum Teil weitreichende Kündigungsmöglichkeiten in ihren Nutzungsbedingungen vor. Zum Teil behalten sich die Anbieter auch vor, einzelne Accounts beispielsweise bei gravierendem Fehlverhalten, der Belästigung anderer Nutzer oder wiederholten Gesetzesverstößen zu „sperren", also den Zugang zum Account zeitweilig oder dauerhaft zu verwehren oder den Account vollständig zu löschen.[149] Zwar wird Social-Media-Anbietern in analoger Anwendung der §§ 858, 903, 1004 BGB ein sog. **„virtuelles Hausrecht"** zugestanden, welches bei Störungen zur entsprechenden Handhabe berechtigt.[150] Im Ergebnis kann jedoch eine dauerhafte Sperrung eines Nutzer-Accounts nicht anders behandelt werden als eine Kündigung des Social-Media-Vertrages.

75 So hatte etwa das LG Berlin über die nachfolgende abgedruckte Klausel aus den Facebook-Nutzungsbedingungen zu entscheiden:

---

[145] Vgl. dazu auch Gennen/Kremer, ITRB 2011, 59 ff.

[146] So OLG Karlsruhe, NJW 2012, 3312 ff. m. Anm. Schneider; OLG Köln, GRUR-RR 2010, 34 ff.; OLG Stuttgart, GRUR-RR 007, 330 ff.; im Ergebnis auch Köhler, in: Köhler/Bornkamm, UWG, § 4 Rn. 11.42; Ohly, in: Piper et al., UWG, § 4 Rn. 11.79. A.A. aber KG, NJW-RR 2011, 1264. Krit. Ernst, jurisPK-WettbR 3/2012, Anm. 4.

[147] KG, BeckRS 2014, 03648.

[148] Vgl. Gaier, in: MüKo-BGB, § 314 Rn. 6; Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 11.

[149] Vgl. etwa Art. 5.6 der TOS von Facebook (http://www.facebook.com/terms.php) sowie Art. 10 der TOS von Twitter (https://twitter.com/tos).

[150] So OLG Köln, MMR 2001, 52 f.; LG München I, ZUM-RD 2007, 261 ff.; Maume, MMR 2007, 620 ff.; Leupold/Glossner, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 2, Rn. 335; Spindler/Anton, in: Spindler/Schuster, § 1004 BGB, Rn. 2. Abl. aber OLG Frankfurt a. M., ZUM-RD 2009, 644 ff. Vgl. auch Schwenke, K&R 2012, 305 ff.

„Wenn du gegen den Inhalt oder den Geist dieser Erklärung verstößt oder anderweitig mögliche rechtliche Risiken für uns erzeugst, können wir die Bereitstellung von [. . .] für dich ganz oder teilweise einstellen. Wir werden dich per E-Mail oder wenn du dich das nächste Mal für dein Konto anmeldest darüber informieren."

Das LG Berlin sah diese Regelung insgesamt als intransparent und damit als nach § 307 Abs. 1 Satz 2 BGB unwirksam an. Die Klausel konstituiere ein außerordentliches Kündigungsrecht zugunsten des Anbieters ohne wichtigen Grund oder vorherige Abmahnung, was der gesetzlichen Wertung des § 314 BGB zuwider laufe.[151]

Kündigung durch den Nutzer Bei der Kündigung durch den Nutzer ist hinsichtlich der Wirksamkeit vertraglicher Kündigungsrechte zu unterscheiden, ob es sich um einen entgeltlichen oder unentgeltlichen Vertrag handelt. **76**

Entgeltlicher Vertrag Bei entgeltlichen Verträgen gilt es zu beachten, dass ein grundsätzliches schützenswertes Interesse des Anbieters besteht, den **Nutzer längerfristig an sich zu binden**. Insofern ist der Anbieter grundsätzlich frei, die Kündigungsmodalitäten betreffend die Kündigung des Nutzers in den Grenzen des §§ 307, 309 Nr. 9 BGB zu regeln. **77**

Die AGB-rechtliche Zulässigkeit von Kündigungsregelungen bestimmt sich in erster Linie nach § 309 Nr. 9 BGB, der die rechtlichen Rahmenbedingungen für die Kündigung von Dauerschuldverhältnissen festlegt. Danach gilt, dass Verträge über die regelmäßige Erbringung von Dienst- oder Werkleistungen eine maximale Laufzeit von **zwei Jahren** aufweisen dürfen (§ 309 Nr. 9 lit. a BGB). Ferner ist eine stillschweigende **Verlängerung** allein um jeweils maximal ein Jahr möglich (§ 309 Nr. 9 lit. b BGB). Die Kündigungsfrist darf maximal drei Monate zum Ablauf der Vertragsdauer bzw. des Verlängerungszeitraumes betragen (§ 309 Nr. 9 lit. c BGB). Eine mit diesen Anforderungen im Einklang stehende Kündigungsregelung kann grundsätzlich den Nutzer nicht unangemessen benachteiligen, sodass eine Unwirksamkeit nach dem subsidiär neben § 309 Nr. 9 BGB anwendbaren § 307 Abs. 1 Satz 2 BGB nicht in Betracht kommt. **78**

Unentgeltlicher Vertrag Bei unentgeltlichen Social-Media-Verträgen spielt das Thema Kündigung häufig nur eine **untergeordnete Rolle**, da der Nutzer im Regelfall einfach die Nutzung des Sozialen Mediums einstellen wird.[152] Üblicherweise werden in unentgeltlichen Verträgen auch keine besonderen Regelungen zur Kündigung aufgenommen; allenfalls findet sich bisweilen ein pauschaler Hinweis, dass die Möglichkeit zur Kündigung prinzipiell besteht. **79**

AGB-rechtliche Bedenken bestehen hier nicht. § 309 Nr. 9 BGB ist allein bei Entgeltlichkeit anwendbar und mangels vergleichbarer Interessenslage und Regelungslücke auch nicht analogiefähig. Auch der **faktische Ausschluss** des Kündigungsrechts bei unentgeltlichen Dauerschuldverhältnissen stellt für den Nutzer keine unangemessene Benachteiligung i. S. v. § 307 Abs. 1 Satz 1 BGB dar, sodass sich hieraus auch keine Unwirksamkeit ergeben kann. **80**

---

[151] LG Berlin, ZD 2012, 276 ff., Rn. 55.

[152] So auch Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 128.

3.3.3.6 Änderungsvorbehalte

81 In vielen Social-Media-Verträgen finden sich teils weitreichende Änderungsvorbehalte zu Gunsten des Anbieters. Hintergrund ist, dass deren Angebote oftmals einem **kontinuierlichen und schnelllebigen Wandel** unterworfen sind, sodass das Angebot ständig um neue Funktionalitäten erweitert wird, dessen Nutzung auf eine vertragliche Grundlage gestellt werden muss.

82 Die AGB-rechtliche Zulässigkeit von Änderungsklauseln richtet sich vorrangig nach § 308 Nr. 4 BGB, subsidiär nach § 307 Abs. 1 Satz 2 BGB.

83 Einseitige Änderungsklauseln, auf Basis derer der Anbieter ohne bzw. sogar gegen den Willen des Nutzers die vertragliche Grundlage ändern kann, verstoßen im Regelfall gegen § 307 Abs. 1 Satz 2 BGB aufgrund der darin liegenden einseitigen **Benachteiligung des Nutzers**.[153] Eine Ausnahme besteht nur im Falle eines besonderen und wichtigen Grundes. Das LG Berlin nahm etwa an, dass derartige Klauseln wirksam sein können, wenn sie sich auf die **Beseitigung** nachträglich eingetretener **Äquivalenzstörungen und Regelungslücken** beschränken und insgesamt transparent sind.[154]

84 Änderungsklauseln mit **Zustimmungsvorbehalt** hingegen sind gemeinhin wirksam, da sie letztlich der Natur des Social-Media-Vertrages entsprechen und demgemäß grundsätzlich keine unangemessene Benachteiligung darstellen.[155] Problematisch ist oft allein die Ausgestaltung der Zustimmung des Nutzers. Eine ausdrückliche Zustimmung in Gestalt einer **Einwilligungslösung** erscheint bereits aus Transparenzgründen vorzugswürdig. Innerhalb der Grenzen des § 308 Nr. 5 BGB kann jedoch auch eine Regelung vereinbart werden, nach der Änderungen der Nutzungsbedingungen wirksam werden, wenn der Nutzer nicht innerhalb einer angemessenen Frist widerspricht und die Nutzung des Sozialen Mediums nach Ablauf der Frist fortsetzt.[156]

3.3.3.7 Haftungsausschluss/Haftungsbeschränkungen

85 Kaum ein Social-Media-Vertrag enthält keine Klausel, welche die Haftung des Anbieters weitgehend ausschließt oder zumindest in erheblichem Umfange begrenzt. Solche Regelungen sind oftmals mit Blick auf die Inhaltskontrolle nach §§ 307 Abs. 2 Nr. 2, 309 Nr. 7 und 8 BGB nicht unproblematisch.

86 **Kein Ausschluss der Haftung für Vorsatz und/oder grobe Fahrlässigkeit, § 309 Nr. 7 lit. b BGB** Wie sich aus § 309 Nr. 7 lit. b BGB ergibt, kann der Anbieter des

---

[153] Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 81.
[154] LG Berlin, ZD 2012, 276 ff., Rn. 54.
[155] Vgl. etwa zur strukturell vergleichbaren Situation bei Online-Spielen Lober/Weber, CR 2006, 837 (841); Redeker, IT-Recht, Rn. 1166.
[156] Wurmnest, in: MüKo-BGB, § 308 N. 5 Rn. 3 m. w. N. Siehe auch Schneider, in: Redeker, Handbuch der IT-Verträge, Teil 3.14 Rn. 81.

Sozialen Mediums die Haftung **allein für leichte und mittlere Fahrlässigkeit**,[157] nicht dagegen aber für grobe Fahrlässigkeit oder Vorsatz ausschließen.[158]

Kein Ausschluss der Haftung für Kardinalpflichten, § 307 Abs. 2 Nr. 2 BGB 87
Ferner ist der Ausschluss der Haftung für sogenannte Kardinalpflichtsverletzungen zumindest mit Blick auf § 307 Abs. 2 Nr. 2 BGB bedenklich.[159] Hier kann die Haftung des Social-Media-Anbieters lediglich der Höhe nach auf den **typischerweise vorausSehbaren Schaden** beschränkt werden.[160] Kardinalpflichten sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht, deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Vertragspartner regelmäßig vertraut.[161] Dies sind jedenfalls die im Gegenseitigkeitsverhältnis stehenden Hauptleistungspflichten,[162] wie beispielsweise die Bereitstellung der technischen Online-Plattform sowie die Ermöglichung des Zugangs hierzu. Wenngleich die Sicherung der vom Nutzer überlassenen Informationen (z. B. Informationen über seine Person, Kommunikationsinhalte und Bilder) zwar lediglich eine nicht im Synallagma stehende vertragliche Nebenpflicht darstellt, dürfte sie ebenfalls als Kardinalpflicht zu qualifizieren sein.

Bei der Formulierung von Haftungsbeschränkungen ist zu beachten, dass sowohl 88
die Begriffe „Kardinalpflichten" als auch „wesentliche Vertragspflichten" mit Blick auf § 307 Abs. 1 Satz 1 BGB von der Rechtsprechung als intransparent angesehen werden;[163] daher ist für die Wirksamkeit einer entsprechenden Klausel stets erforderlich, die **Pflichten exakt zu umschreiben** oder zumindest obige Definition der Rechtsprechung zu übernehmen.

Umfang und Ausschluss von Mängelansprüchen, § 309 Nr. 8 lit. b BGB Letzt- 89
lich sind insbesondere die detaillierten Anforderungen des § 309 Nr. 8 lit. b BGB zu beachten, dessen Wertungen auch im geschäftlichen Verkehr Anwendung finden und der eine ganze Reihe von Anforderungen an die Ausgestaltung von **Gewährleistungsansprüchen** enthält.[164]

---

[157] Zu den Fahrlässigkeitskategorien vgl. Grundmann, in: MüKo-BGB, § 276 Rn. 83 ff.
[158] So auch Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 95. Auch für unentgeltliche Social Media-Angebote kann hier nichts anderes gelten. In seinem zweiten Halbsatz enthält § 309 Nr. 7 BGB eine Ausnahmeregelung. Ließe man eine weitergehende Haftungserleichterung zu, würde dies eine analoge Anwendung des zweiten Halbsatzes darstellen. Solche Ausnahmeregelungen sind jedoch stets abschließend und einer Analogie nicht zugänglich (zum ebenfalls unentgeltlichen Open-Source-Vertrag: Bussche/Schelinski, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1, Rn. 234).
[159] So auch Wurmnest, in: MüKo-BGB, § 309 Nr. 7 BGB, Rn. 26.
[160] BGH, NJW 1993, 335 (336).
[161] BGH, NJW 1985, 3016 (3018).
[162] BGH, NJW 2004, 1774 ff.
[163] BGH, NJW 2006, 46; vgl. auch Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 98 m. w. N.
[164] Eingehend dazu Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 82 ff.

3.4 Digitaler Nachlass

90 Unter dem Begriff des digitalen Nachlasses wird in der Praxis diskutiert, inwiefern insbesondere E-Mail-Accounts nach dem Ableben des Inhabers auf den oder die Erben übergehen können.[165] Ähnliche Fragen stellen sich selbstverständlich auch bei Verträgen über die Nutzung Sozialer Medien.

3.4.1 Ausgangslage

91 Auch nach dem Ableben des Inhabers bleibt dessen Social-Media-Account weiter bestehen. Sämtliche Daten und Inhalte verbleiben auf dem Server des Anbieters und können – bei Kenntnis der Zugangsdaten – technisch auch weiterhin abgerufen werden. Nur in den wenigsten Fällen dürfte der Anbieter überhaupt Kenntnis von dem Tode eines seiner Nutzer erhalten.[166] Bei privat genutzten Netzwerken wird der Anbieter häufig durch andere Mitglieder vom Tode eines Nutzers erfahren (z. B. durch entsprechende Kondolenzeinträge im Gästebuch).

92 In privaten E-Mail-Accounts finden sich häufig wichtige Informationen für Hinterbliebene. Versicherungs- und Kreditverträge werden immer häufiger digital hinterlegt.[167] Aber auch Online-Rechnungen der Telekom oder Informationen zu Guthaben bei PayPal finden sich heutzutage fast ausschließlich in E-Mail-Accounts.[168] In der Praxis dürfte eine **Einsichtnahme** in die privaten E-Mail-Accounts des Verstorbenen daher **unabdingbar** sein. Anbieter von E-Mail-Diensten wie GMX und Web.de haben hierauf bereits reagiert und verschaffen Erben gegen **Vorlage des Erbscheins** Zugang zu dem E-Mail-Account des Verstorbenen. Der E-Mail-Anbieter Google bietet sogar eine Art **Testamentsfunktion** im Rahmen seines „Inaktivitätsmanagers" an. Dieser ermöglicht es Nutzern festzulegen, was im Todesfalle mit den in ihrem Google-Account gespeicherten Informationen passieren soll. So kann der Erblasser festlegen, dass die Daten durch Google gelöscht werden oder dass von ihm benannte Personen Zugriff auf den Google-Account erhalten.[169]

93 Im Gegensatz hierzu geht es bei (privaten) Social-Media-Accounts in erster Linie um das Wahren des **Andenkens an den Verstorbenen**. Häufig wünschen sich die Angehörigen, dass das Profil des Verstorbenen für eine gewisse Zeit weiterhin öffentlich zugänglich ist und Freunde und Bekannte Nachrichten im Gästebuch hinterlassen können. Das soziale Netzwerk Facebook bietet mittlerweile sogar die Möglichkeit an, Accounts von Verstorbenen in einen Kondolenz-Modus zu versetzen.

---

[165] Siehe auch die Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht zum Digitalen Nachlass, Nr. 34/2013, Juni 2013.

[166] Marktforscher vermuten sogar, dass bis zu 5 % der Facebook-Accounts verstorbenen Nutzern gehören, Bleich, c't 2013, S. 62.

[167] Vgl. http://www.bitkom.org/de/themen/50792_63078.aspx.

[168] Martini, JZ 2012, 1145 (1146); Deusch, ZEV 2014, 2.

[169] Vgl. http://www.welt.de/wirtschaft/webwelt/article115225643/Google-fuehrt-digitales-Testament-fuer-Userdaten-ein.html.

3.4.2 Vererbbarkeit von Social-Media-Accounts

Nach § 1922 Abs. 1 BGB gehen mit dem Tode einer Person deren **Vermögen** (die Erbschaft) **als Ganzes auf die Erben über**. Dies umfasst sämtliche Rechtspositionen des Erblassers und damit sämtliche vermögenswerte Rechte und Rechtsstellungen.[170] Anders verhält es sich mit **nichtvermögenswerten Rechtsverhältnissen**, die regelmäßig **nicht vererbbar** sind.[171] **94**

Unstreitig ist, dass **Festplatten und sonstige Speichermedien**, die – inklusive der darauf gespeicherten Informationen – ebenfalls Bestandteil des digitalen Nachlasses sind,[172] im Wege der **Gesamtrechtsnachfolge** auf den oder die Erben übergehen.[173] Wie bereits eingangs erläutert, verbleiben jedoch sämtliche auf einer Social-Media-Plattform gespeicherten Daten und Inhalte zunächst auf dem Server des jeweiligen Anbieters. Bis auf wenige Ausnahmefälle – etwa wenn der Nutzer eine Kopie seiner Daten vom Anbieter angefordert hat[174] – liegt **kein nach § 1922 Abs. 1 BGB vererbbares Eigentum** vor. Dennoch kann der Social-Media-Vertrag als Vertragsverhältnis gemäß § 1922 Abs. 1 BGB im Wege der Universalsukzession auf den oder die Erben übergehen.[175] Dies hat zur Folge, dass der Erbe nach § 1922 BGB **in das Vertragsverhältnis** mit dem Social-Media-Anbieter **eintritt**.[176] Mit dem Eintritt in das Vertragsverhältnis gehen auch die Auskunftsansprüche des Erblassers gegen den Anbieter auf Herausgabe der dienstespezifischen Zugangsdaten (d. h. Benutzername und Passwort) auf die Erben über. **95**

3.4.3 Telekommunikations- und Datenschutzrecht

Je nach Ausgestaltung des Sozialen Mediums können sich zusätzlich Fragen nach dem Umgang mit dem **Fernmeldegeheimnis** (§ 88 TKG) stellen. Wenngleich sich Fragen im Zusammenhang mit dem Fernmeldegeheimnis in erster Linie bei E-Mail-Accounts stellen,[177] können auch Social-Media-Anbieter, die ihren Nutzern Nachrichtenfunktionen bereitstellen, als Diensteanbieter im Sinne von § 3 Nr. 6 TKG zu qualifizieren sein. In diesem Falle wären sie ebenfalls verpflichtet, das **96**

[170] Müller-Christmann, in: BeckOK-BGB, § 1922 Rn. 24 ff.
[171] Leipold, in: MüKo-BGB, § 1922 Rn. 19.
[172] Deusch, ZEV 2014, 2.
[173] Einzelheiten zur Gesamtrechtsnachfolge bei lokal gespeicherten E-Mails, vgl. Hoeren, NJW 2005, 2113 (2116).
[174] Facebook bietet seinen Nutzern die Möglichkeit, eine Kopie ihrer Facebook-Daten herunterzuladen und auf einem beliebigen Medium zu speichern bzw. auszudrucken, vgl. https://de-de.facebook.com/help/212802592074644.
[175] Vgl. auch Hoeren, NJW 2005, 2113 (2114); zur Frage des Übergangs von Vertragsverhältnissen im Allgemeinen: Leipold, in: MüKo-BGB, § 1922 Rn. 20.
[176] Martini, JZ 2012, 1145 (1147).
[177] Einen Überblick über den Streitstand liefert Deusch, ZEV 2014, 2 (5 f.).

Fernmeldegeheimnis zu wahren. Zu berücksichtigen ist hierbei, dass das Fernmeldegeheimnis neben dem Erblasser auch den Kommunikationspartner des Erben (z. B. den Absender einer Nachricht) schützt, in dessen Stellung der Erbe gerade nicht eintritt.[178]

97 Dem Zugriff auf Social-Media-Accounts durch den Erben können darüber hinaus auch die einfachgesetzlichen Vorschriften des **Datenschutzrechts** sowie des verfassungsrechtlichen **postmortalen Persönlichkeitsrecht** entgegenstehen.[179] Gerade die privat genutzten sozialen Netzwerke wie etwa Facebook und studiVZ zeichnen sich dadurch aus, dass dort häufig sehr persönliche Inhalte des Erblassers zu finden sein dürften. Hierbei kann es sich entweder um über das interne Nachrichtensystem versandte private Nachrichten handeln, die mit Ausnahme des Kommunikationsteilnehmers nur dem Nutzer (als Account-Inhaber) selbst zugänglich sind oder aber um Bilder aus dem Privatleben des Erblassers, die dieser lediglich einem ausgewählten Kreis von Personen zugänglich gemacht hat.

3.5 Nutzung von Sozialen Medien durch Jugendliche

98 Soziale Medien werden heutzutage in besonderem Maße von Jugendlichen genutzt. Nach einer im Jahr 2010 erstellten Studie sind 50 % aller Kinder und Jugendlichen im Alter von 9 bis 16 mindestens in einem sozialen Netzwerk angemeldet.[180] Inzwischen dürfte die Anzahl sogar noch deutlich höher ausfallen.

3.5.1 Überblick über die gesetzlichen Rahmenbedingungen

99 Die gesetzlichen Rahmenbedingungen für die Beurteilung der **Wirksamkeit** rechtsgeschäftlicher Handlungen[181] Minderjähriger finden sich in den §§ 104 ff. BGB. Hiernach gilt, dass Jugendliche, die das siebente Lebensjahr noch nicht vollendet haben, nicht geschäftsfähig sind und damit keinerlei rechtsgeschäftliche Handlungen vornehmen können.[182] Jugendliche, die zwar das siebente, nicht aber das achtzehnte Lebensjahr vollendet haben, sind nach Maßgabe der §§ 106 ff. BGB in ihrer Geschäftsfähigkeit beschränkt. Im Zuge der **geplanten Novellierung des**

[178] Eingehend zu den damit verbundenen Rechtsfragen und entsprechenden Lösungsvorschlägen: Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht zum Digitalen Nachlass, Nr. 34/2013, Juni 2013.

[179] Hierzu Brinkert et al., ZD 2013, 153 ff.; vgl. insbesondere Martini, JZ 2012, 1145 (1147 ff.), der sich mit diesen Rechtsfragen eingehend auseinandersetzt.

[180] http://de.statista.com/statistik/daten/studie/168409/umfrage/nutzung-von-social-media-durch-kinder-in-europa/.

[181] So nach gängiger Definition der Inhalt der Geschäftsfähigkeit, vgl. etwa Schmitt, in: MüKo-BGB, § 104 Rn. 1; Knothe, in: Staudinger, BGB, Vorbem. zu §§ 104 ff., Rn. 1.

[182] Vgl. etwa Dörner, in: Schulze, BGB, § 104 Rn. 1.

Jugendmedienschutz-Staatsvertrages (JMStV) soll auch der wachsenden Bedeutung sozialer Medien für Jugendliche Rechnung getragen werden. Die in einem Diskussionspapier[183] zusammengefassten Änderungsvorschläge sehen dabei unter anderem vor, auch Beiträge in Sozialen Medien der Alterskennzeichnungspflicht zu unterwerfen. Angesichts des frühen Stadiums, in dem sich das Änderungsverfahren befindet, soll jedoch ein Hinweis an dieser Stelle genügen, ohne dass darauf näher eingegangen wird.

3.5.2 Einwilligung der gesetzlichen Vertreter

Nach § 107 BGB kann ein beschränkt Geschäftsfähiger mit **Einwilligung** seiner gesetzlichen Vertreter – in der Regel seiner Eltern[184] – wirksam Rechtsgeschäfte vornehmen. **100**

Die Einwilligung der gesetzlichen Vertreter kann grundsätzlich auch konkludent erfolgen, etwa auch durch (ausdrückliche) Duldung eines Verhaltens des Minderjährigen.[185] Die Einwilligung muss daher nicht zwingend auf ein konkretes Rechtsgeschäft bezogen sein.[186] Vielmehr ist auch eine **beschränkte Generaleinwilligung** bezogen auf einen durch sachlich abgegrenzte Faktoren bestimmten Bereich von Geschäften denkbar;[187] eine grundsätzliche Generaleinwilligung in sämtliche Geschäfte des Minderjährigen liefe dem Schutzzweck der §§ 106 ff. BGB zuwider.[188] Allerdings wird die Einwilligung zur Nutzung des Internets grundsätzlich nicht auch die Erlaubnis in den Abschluss von Social-Media-Verträgen umfassen.[189] Denn vom natürlichen Einwilligungshorizont und dem daraus gebildeten Willen resultiert nicht, dass die Erlaubnis der generellen Nutzung des Internets als (kostenloses) Medium ohne Weiteres auch die Eingehung rechtlich nachteiliger Social-Media-Verträge einschließt.[190] Zu ähnlichen Ergebnissen wird man in strukturell vergleichbaren Fällen gelangen müssen: So schließt die einem Minderjährigen erteilte Erlaubnis in die Eröffnung eines Kontos nicht auch die Einwilligung in dessen Überziehung ein. Auch die Zustimmung zur Benutzung eines Telefons umfasst nicht die Zustimmung in die Nutzung von kostenpflichtigen 0190-Mehrwertdiensten.[191] Dem folgend kann die Einwilligung in die Nutzung des Internets durch den Minderjährigen **kein belastbares Indiz für eine Einwilligung in den Abschluss von Social-Media-Verträgen** **101**

[183] http://www.jugendmedienschutz.sachsen.de/ecm-politik/sachsen/de/home/file/fileId/952.
[184] Vgl. §§ 1626, 1629 BGB. Bei nicht verheirateten Eltern § 1626a BGB. Beachte ferner §§ 1773 ff., 1909 BGB.
[185] Schmitt, in: MüKo-BGB, § 107 Rn. 12; Knothe, in: Staudinger, BGB, § 107 Rn. 35.
[186] So zumindest die h.M., vgl. Scherner, FamRZ 1976, 673 ff.
[187] Eingehend hierzu Knothe, in: Staudinger, BGB, § 107 Rn. 35; Schmitt, in: MüKo-BGB, § 107 Rn. 14.
[188] Dörner, in: Schulze, BGB, § 107 Rn. 11.
[189] Bräutigam, MMR 2012, 636 (638); Jandt/Roßnagel, MMR 2011, 637 (640).
[190] So auch Jandt/Roßnagel, MMR 2011, 637 (640).
[191] Vgl. dazu insgesamt Ellenberger, in: Palandt, BGB, § 107 BGB Rn. 9 m. w. N.

darstellen. Etwas anderes dürfte allenfalls gelten, wenn der gesetzliche Vertreter durch das Senden einer Einladung in ein soziales Netzwerk an den Minderjährigen gerade seinen Willen zum Ausdruck bringt, dass der Minderjährige dieses Netzwerk nutzen soll.[192]

102 Fehlt es an einer Einwilligung, so ist der Social-Media-Vertrag nach § 108 Abs. 1 BGB zunächst **schwebend unwirksam**. Seine Wirksamkeit hängt – abgesehen von der Sondernorm des § 108 Abs. 3 BGB – von der nachträglichen Genehmigung des gesetzlichen Vertreters ab.

3.5.3 Social-Media-Vertrag als rechtlicher Vorteil im Sinne von § 107 BGB

103 Die Einwilligung des gesetzlichen Vertreters ist jedoch entbehrlich, wenn der Minderjährige durch seine Willenserklärung lediglich einen **rechtlichen Vorteil** erlangt.

3.5.3.1 Beurteilung der rechtlichen Vorteilhaftigkeit

104 Für die Beurteilung der rechtlichen Vorteilhaftigkeit kommt es allein auf die unmittelbaren rechtlichen Folgen eines Rechtgeschäfts an.[193] Da die Norm gerade den Schutz des Minderjährigen vor den schädlichen Folgen seines eigenen rechtsgeschäftlichen Handelns bezweckt,[194] kommt eine rein wirtschaftliche Betrachtungsweise für die Beurteilung nicht in Frage.[195] Demgemäß kann es keine Rolle spielen, ob entgeltliche Social-Media-Angebote für den minderjährigen Nutzer wirtschaftlich vorteilhaft oder ökonomisch sinnvoll sind. Ein rechtlicher Vorteil kann dementsprechend nicht schon dann vorliegen, wenn die Vorteile aus dem Geschäft die Nachteile bei Weitem überwiegen.[196] Ein solcher Vorteil kommt vielmehr allein dann in Betracht, wenn dem Minderjährigen letztlich **keine wie auch immer gearteten nachteiligen Folgen** aus dem Rechtsgeschäft erwachsen.[197]

---

[192] Vgl. Bräutigam, MMR 2012, 636 (638), insb. auch Fn. 39.
[193] Vgl. etwa BGH, NJW 2005, 415 (418); Stürner, AcP 173 (1973), 402 (421 ff.).
[194] Schmitt, in: MüKo-BGB, Vorbem. zu §§ 104 ff., Rn. 2 ff.; Knothe, in: Staudinger, BGB, § 107 Rn. 4.
[195] Ellenberger, in: Palandt, BGB, § 107 Rn. 2; Jauernig, in: Jauernig, BGB, § 107 Rn. 2.
[196] Ellenberger, in: Palandt, BGB, § 107 Rn. 2; Wendtland, in: BeckOK-BGB, § 107 Rn. 8 f.
[197] Eingehend hierzu Schmitt, NJW 2005, 1090; Baldus, in: Heidel et al., BGB, § 107 Rn. 9 ff.

3.5.3.2 Anwendung auf Social-Media-Verträge

Es liegt auf der Hand, dass die Nutzung von **entgeltlichen** Angeboten keinen lediglich rechtlichen Vorteil für den minderjährigen Nutzer darstellt, da hier eine unmittelbare **Zahlungspflicht** gegenüber dem jeweiligen Anbieter begründet wird. **105**

Bei **unentgeltlichen** Verträgen stellt die vertragliche Einbeziehung der Nutzungsbedingungen des Anbieters regelmäßig einen rechtlichen Nachteil für Nutzer dar, da häufig zum Nachteil des Nutzers **von gesetzlichen Vorgaben abgewichen** wird.[198] Gerade die in der Praxis häufig vorkommende Verpflichtung zur umfassenden **Einräumung von Rechten** an Nutzerinhalten stellt eine für den Minderjährigen nachteilige Disposition dar. Darüber hinaus führt bereits die Mitgliedschaft in einem Sozialen Netzwerk dazu, dass der Anbieter unter Berufung auf die §§ 14 und 15 TMG und § 28 BDSG personenbezogene Daten des minderjährigen Nutzers verarbeiten darf. Hierdurch wird das Recht auf informationelle Selbstbestimmung der Kinder und Jugendlichen eingeschränkt.[199] Dies steht im Ergebnis einer Einordnung als lediglich rechtlich vorteilhaftes Geschäft entgegen. **106**

Ein in teleologischer Reduktion des § 107 BGB vom Minderjährigen ohne Einwilligung abschließbares **neutrales Geschäft**[200] scheitert ebenfalls an der Begründung der für ihn nachteiligen Abweichung von gesetzlichen Vorgaben.[201] **107**

3.5.4 Taschengeldparagraph

Nach § 110 BGB kann ein Rechtsgeschäft unabhängig von § 107 BGB[202] von Anfang an wirksam sein, wenn der Minderjährige die vertragsmäßige Leistung mit Mitteln **bewirkt** hat, die ihm von seinem gesetzlichen Vertreter zu diesem Zwecke oder zur freien Verfügung überlassen worden sind. **108**

In aller Regel kommt eine Anwendung des § 110 BGB bei **unentgeltlichen** Verträgen **von vorneherein nicht in Betracht**, da schon keine Leistungspflicht vorliegt, die der Minderjährige bewirken könnte. **109**

Denkbar wäre es allenfalls, die **Offenbarung personenbezogener Daten** durch den minderjährigen Nutzer gegenüber dem Social-Media-Anbieter **als das Bewirken** der vertragsgemäßen Leistung mit Mitteln zu qualifizieren. Als Mittel im Sinne **110**

---

[198] Vgl. Backu, ZD 2012, 59 (63); Jandt/Roßnagel, MMR 2011, 637 (639); Schwenke, WRP 2013, 37 (38); Wintermeier, ZD 2012, 210 (212). Vgl. eingehend hierzu Bräutigam, MMR 2012, 635 (637).

[199] Jandt/Roßnagel, MMR 2011, 637 (640).

[200] H.M., vgl. LG Köln, NJW-RR 1991, 868 ff.; Schmitt, in: MüKo-BGB, § 107 Rn. 34; Jauernig, in: Jauernig, BGB, § 107 Rn. 6; Knothe, in: Staudinger, BGB, § 107 Rn. 20; Flume, Allgemeiner Teil des Bürgerlichen Rechts, Bd. 2, S. 193 f.; a. A. BayObLG, BayObLGZ 1979, 49 ff.; Medicus/Petersen, Bürgerliches Recht, Rn. 542.

[201] Vgl. auch Wintermeier, ZD 2012, 210 (212).

[202] Nach richtiger Ansicht handelt es sich bei § 110 BGB um einen gesetzlich normierten Fall der konkludent erteilten beschränkten Generalvollmacht, vgl. etwa Dörner, in: Schulze, BGB, § 110 Rn. 1.

von § 110 BGB kommt nicht nur das dem Minderjährigen überlassene Taschengeld in Betracht, sondern im Ergebnis jede vermögenswerte Position.[203] Auf die Art und Weise der materiellen Verkörperung kommt es hierbei nicht an.[204] Zu beachten ist allerdings, dass personenbezogene Daten dem Minderjährigen nicht von seinen Eltern „überlassen" werden. Besonders deutlich wird dies bei Nutzungsdaten im Sinne von § 15 TMG; diese werden dem minderjährigen Nutzer nicht überlassen, sondern entstehen durch dessen Nutzung einer Webseite. Folglich scheidet eine direkte Anwendung von § 110 BGB aus. Vereinzelt wird allerdings eine analoge Anwendung mit Blick auf den Erziehungscharakter des § 110 BGB begründet.[205] Dagegen lässt sich jedoch anführen, dass § 110 BGB dem Schutz des Minderjährigen dient und eben dieser Schutzzweck durch eine analoge Anwendung ausgehöhlt würde. Denn § 110 BGB bezweckt in erster Linie den Schutz des Vermögens des Minderjährigen[206] und ermöglicht es dem gesetzlichen Vertreter, dem Minderjährigen im Rahmen von Geschäften ohne weitreichende Folgen einen gewissen Freiraum zur selbstständigen Teilnahme am Rechtsverkehr zu schaffen.[207] Jede Anwendung im Kontext sozialer Netzwerke eröffnet jedoch weitere Risiken, wie insbesondere etwa potentielle Gefahren für das (spätere) berufliche und gesellschaftliche Fortkommen bei unbedachtem Umgang mit der eigenen Privatsphäre. Letztlich verbieten diese kaum überschaubaren Risiken eine analoge Anwendung.

3.6 Ausblick – Durchsetzung von Nutzerinteressen

111 Trotz des konsensualen Charakters von Social-Media-Verträgen und der damit einhergehenden theoretischen Möglichkeit einer gleichberechtigten, privatautonomen Ausgestaltung zwischen Anbieter und Nutzer stellt sich der Social-Media-Vertrag in der Realität zumeist als Oktroy des Anbieters dar. Zwar will speziell das deutsche Recht mit Instrumenten wie der AGB-Inhaltskontrolle sowie den §§ 138, 242 BGB die Interessen der Nutzer von Social-Media-Angeboten schützen und deren effektive Implementierung in Social-Media-Verträge garantieren; jedoch besteht derzeit faktisch keine bzw. kaum eine Möglichkeit für die Nutzer, sich **gegen die Allmacht** der ihnen wirtschaftlich überlegenen Anbieter in der inhaltlichen Ausgestaltung der Verträge **durchzusetzen**.

112 Rechtssoziologisch nämlich handelt es sich beim Recht der Social-Media-Verträge größtenteils um reines **Providerrecht**. Die Anbieter – insbesondere Monopolisten wie Facebook und LinkedIn – haben sowohl aufgrund ihrer Bedeutung

---

[203] Knothe, in: Staudinger, BGB, § 110 Rn. 11 f.; Jauernig, in: Jauernig, BGB, § 110 Rn. 4.
[204] Vgl. eingehend Schmitt, in: MüKo-BGB, § 110, Rn. 18 ff.; A.A. Jandt/Roßnagel, MMR 2011, 637 (640).
[205] So etwa Wintermeier, ZD 2012, 210 (212).
[206] Schmitt, in: MüKo-BGB, § 110 Rn. 1.
[207] Wendtland, in: BeckOK-BGB, § 110 Rn. 1.

als auch ihrer wirtschaftlichen Stellung rein tatsächlich die weitgehende Möglichkeit, den Nutzern Social-Media-Verträge nach ihren Vorstellungen zu diktieren. Den Nutzern bleibt letztlich nur, sich auf die von den Anbietern gestellten Verträge – wenn auch mit Widerwillen – einzulassen oder eben auch nicht.

3.6.1 Take it or leave it

In diesem *Take it or leave it*-Szenario[208] ist der einzelne Nutzer nur ein winzig kleines Rädchen im einzelnen Sozialen Medium, auf dessen individuelle Interessen und Bedürfnisse der Anbieter beim Abschluss des Social-Media-Vertrags nur standardisiert Rücksicht nimmt. Bedenkt man etwa, dass beispielsweise Facebook mehr als eine Milliarde Nutzer weltweit unter seinem Dach vereint, so wird auch klar, dass eine entsprechende **Individualisierung** der Verträge **rein tatsächlich kaum** und nur mit größtem (insbesondere technischem) Aufwand **möglich** wäre.[209] **113**

Umgekehrt ist dagegen auch zu bedenken, dass eine universelle **„one fits all"**-Lösung insbesondere mit Blick auf global agierende Social-Media-Anbieter **kaum möglich** ist; vielmehr haben diese ihre Verträge auf jeweils spezifische Rechtsordnungen aller Länder abzustimmen. Hierin liegt ein grundsätzliches Dilemma, welchem sich weltweit agierende Anbieter ausgesetzt sehen. **114**

Von Zeit zu Zeit regt sich Widerstand gegen derartige Strukturen, der bisher allerdings zu keiner Veränderung am obig dargestellten Befund führen konnte. So kam etwa mit Blick auf die Mitwirkung an Ausgestaltung und Inhalt von Facebook die Idee einer sogenannten **Facebook-Union** auf, die ähnlich einer Gewerkschaft die Interessen der Mitglieder vertreten sollte.[210] Dieser Vorschlag, der bei den Verantwortlichen von Facebook (verständlicherweise) bisher auf wenig Gegenliebe stieß und in ihrer konkreten Umsetzung auch recht konturlos blieb, scheint mittlerweile wieder begraben worden zu sein. Jeder Einzelne kann damit nur entscheiden, „ob" er einen Social-Media-Vertrag abschließt; die Frage nach dem „wie" ist seiner Einflusssphäre dagegen entzogen. **115**

3.6.2 Public/Crowd Pressure

Vor diesem Hintergrund der Ohnmacht jedes einzelnen Users ist letztlich eine Änderung bestehender Strukturen nur durch eine **Abstimmung der Nutzer mit den Füßen** möglich, sprich als homogene Masse zu handeln und allein durch ihre schiere Größe Druck auf die Anbieter auszuüben. **116**

---

[208] Dazu schon Bräutigam, MMR 2012, 635 (640).
[209] Vgl. Bräutigam, MMR 2012, 635 (640); Weichert, NJW 2001, 1463 (1467 f.).
[210] Vgl. http://www.theguardian.com/media/2010/aug/09/facebook-users-union-demands-payment.

117 Wie dies freilich im Einzelnen aussehen könnte und welchen Formen von Crowd Pressure tatsächlich Erfolg beschieden sein könnte, lässt sich schwerlich prognostizieren. Allerdings ist mit Blick auf die in rasanter Geschwindigkeit verlaufenden Nutzermigration durchaus denkbar, dass es sich um ein probates Mittel handelt, Druck auf die Anbieter auszuüben. In der heutigen Zeit, in der Flexibilität und das Streben nach Neuem zum täglichen Leben gehören, ist die noch vor Jahrzehnten vorherrschende Bindung an bestimmte Konstanten weitgehend aufgehoben. Insofern besteht für Anbieter die erhebliche Gefahr, dass **nutzerunfreundliche Angebote** mit dem Überlaufen der Kunden zu anderen Angeboten **abgestraft** werden. Die grundsätzliche Wechselbereitschaft manifestiert sich auch etwa in der enormen Schnelligkeit, in der Angebote immense Nutzerzahlen von etwa 100 Mio. erreichen; dies war bei Facebook nach nur 54 Monaten, bei Google+ gar schon nach nur sieben Monaten der Fall; dies ist beredter Beleg der Schnelllebigkeit und Offenheit der Gesellschaft und der Bereitschaft, sich schnell von Bestehendem zu lösen.

118 Denkbar wäre sicherlich die Implementierung von Abstimmungsmöglichkeiten im Rahmen von Sozialen Medien über deren inhaltliche und damit auch vertragliche Ausgestaltung. Diese sind allerdings gleich mit mehreren Pferdefüßen – einem strukturellen und einem soziologisch-tatsächlichem – behaftet: Zum einen entscheidet nämlich der Social-Media-Anbieter, ob und wie er eine solche Abstimmungsmöglichkeit in seine Plattform implementiert, worüber entschieden werden und ob die Entscheidung bindend sein soll; allein darin manifestiert sich erneut eine **strukturelle Überlegenheit des Anbieters**. Zum anderen wird jeder Anbieter nur dann das Mittel der Abstimmungsmöglichkeit in Erwägung ziehen, wenn der Unmut unter den Nutzern ein solches Maß erreicht hat, dass der Verlust vieler Nutzer droht und Zugeständnisse als letzter Weg erscheinen; selbst dann werden die Anbieter allerdings die Abstimmungen so ausgestalten, dass sie den Nutzern allein den Eindruck geben, sie könnten etwas bewirken. Faktisch bleibt sie aber weitgehend folgenlos. Als Beispiel lässt sich etwa die jüngste Abstimmung über die Facebook-Nutzungsbedingungen anführen.[211] Unter einer (schwer auffindbaren) Unterseite (Facebook Site Governance) wurden die neuen Nutzungsbedingungen zur Disposition gestellt; für die Berücksichtigung der Ergebnisse war ein Quorum von einem Drittel aller global registrierten Facebook-Mitglieder – also über 300 Mio. Nutzern – gefordert, was bei realistischer Betrachtung schlicht nicht zu erreichen war.[212]

119 Möglich wäre aber auch, **politischen Druck** über Verbände, Vereine und andere Interessensgruppen etwa auf den Gesetzgeber auszuüben, allgemeine Leitlinien zu entwickeln oder die Entwicklung zu fördern, um die Interessen von Nutzer und Industrie auszutarieren. Eine bedeutende Möglichkeit bietet hier das ohnehin einem tiefgreifendem Wandel unterliegende Datenschutzrecht, dem zentrale Bedeutung im

---

[211] Hieran wurde zum Teil massive Kritik geübt, vgl. http://www.sueddeutsche.de/digital/abstimmung-ueber-nutzungsbedingungen-facebook-demokratie-eine-frechheit-1.1373411; http://www.zeit.de/digital/internet/2012-06/facebook-abstimmung-nutzungsbedingungen.

[212] Hierzu umfassend Bräutigam, MMR 2012, 635 (640) m. w. N.

Zusammenhang mit Social-Media-Verträgen zukommt. Beachtenswert ist im Speziellen Art. 38 des EU-DS-GVO-E, der die Ausarbeitung von Verhaltungsregeln auf nationaler wie zwischenstaatlicher Ebene fördern will; dabei handelt es sich nicht um eine bloß deklaratorische Postulation: Art. 38 Abs. 4 EU-DS-GVO-E sieht nämlich vor, dass die Kommission die Allgemeingültigkeit entsprechender Verhaltensregeln beschließen kann. Beispielhaft sei im Bereich datenschutzrechtlicher Initiativen auch das in den USA derzeit laufende Projekt „Consumer Data Privacy in a Networked World“[213] erwähnt, das etwa die Einbeziehung relevanter Interessensgruppen vorsieht.[214] In der Tat führten in der Vergangenheit neben der Möglichkeit der Verbandsklage[215] gerade immer wieder datenschutzrechtliche Initiativen zu merklichen Verbesserungen der Nutzungsbedingungen Sozialer Medien. Exemplarisch lassen sich hier die Maßnahmen kanadischer und irischer Datenschutzbehörden in Sachen Facebook[216] ebenso wie das vom schleswig-holsteinischen Landesdatenschutzbeauftragten initiierte Vorgehen in Sachen Facebook-Like-Button[217] aufführen.

Literatur

Acker, L., Thum, K. (2008). Zulässigkeit der Vereinbarung der freien Weiterübertragung von urheberrechtlichen Nutzungsrechten durch AGB. *GRUR*, 671 ff.

Back, A., Gronau, N., Tochtermann, K. (2012). *Web 2.0 und Social Media in der Unternehmenspraxis*. 3. Aufl. München: Oldenbourg.

Backu, F. (2012). Datenschutzrechtliche Relevanz bei Onlinespielen – Überblick über die einzelnen Problemstellungen. *ZD*, 59 ff.

Bauer, S. (2008). Personalisierte Werbung auf Social Community Websites. Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen. *MMR*, 435 ff.

Bender, G. (2013). Informationelle Selbstbestimmung in sozialen Netzwerken. *K&R*, 218 ff.

Berberich, M. (2006). Die Doppelfunktion der Zweckübertragungslehre bei der AGB-Kontrolle. *ZUM*, 205 ff.

Berberich, M. (2010). Der Content „gehört“ nicht Facebook! AGB-Kontrolle der Rechteeinräumung an nutzergenerierten Inhalten. *MMR*, 736 ff.

Berberich, M. (2010). *Virtuelles Eigentum*. Tübingen: Mohr Siebeck.

---

[213] Dazu eingehend http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[214] Dazu Bräutigam, MMR 2012, 635 (640 f.).

[215] Siehe oben Punkt 3.3.

[216] Vgl. etwa Data Protection Commissioner of Ireland, Report of Audit v. 21.2.2011, http://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf; Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic [CIPPIC] against Facebook Inc. under the Personal Information Protection and Electronic Documents Act by Elisabeth Denham, Assistant Privacy Commissioner of Canada, July 16, 2009, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf. Dieses Vorgehen wurde durch die Anzeigen der österreichischen Gruppe „Europe versus Facebook“ um den Wiener Jurastudenten *Max Schrembs* mit angestoßen. Vgl. dazu die Website der Initiative: http://www.europe-v-facebook.org/

[217] Vgl. http://www.stern.de/digital/online/datenschuetzer-thilo-weichert-ein-mann-gegen-facebook-1767485.html.

Bergt, M. (2012). Praktische Probleme bei der Umsetzung neuer gesetzlicher Vorgaben im Webshop. *NJW*, 3541 ff.
BITKOM (2011). *Soziale Netzwerke. Eine repräsentative Studie zur Nutzung sozialer Netzwerke im Internet*. 2. Aufl., abrufbar unter: http://www.bitkom.org/files/documents/SozialeNetzwerke.pdfz.
Boyd, D.-M., Ellison, N.-B. (2008). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, 210 ff.
Braun, S. (2013). Social Media Nutzung – eine Herausforderung (auch) für Unternehmen. *NJ*, 104 ff.
Bräutigam, P. (2012). Das Nutzungsverhältnis bei sozialen Netzwerken. Zivilrechtlicher Austausch von IT-Dienstleistungen gegen personenbezogene Daten. *MMR*, 635 ff.
Brierley, A. (2012). Arbeitnehmer zwischen Arbeitsrecht, Geheimnisschutz und Persönlichkeitsrecht. *FA*, 103 ff.
Brinkert, M., Stolze, M., Heidrich, J. (2013). Der Tod und das soziale Netzwerk. Digitaler Nachlass in Theorie und Praxis. *ZD*, 153 ff.
Brönneke, T. (2012). Verbraucherschutz durch Zivilrecht: Eine Verkürzung? *VuR*, 334 ff.
Byers, P., Mößner, S. (2012). Die Nutzung des Web 2.0 am Arbeitsplatz: Fluch und Segen für den Arbeitgeber. *BB*, 1665 ff.
Castendyk, O. (2007). Lizenzverträge und AGB-Recht. *ZUM*, 169 ff.
Cichon, C. (2005). *Internet-Verträge*. 2. Aufl. Köln: O. Schmidt.
Damm, R., Rehbock, K. (2008). *Widerruf, Unterlassung und Schadenersatz in den Medien*. 3. Aufl. München: C. H. Beck.
Deusch, F. (2014). Digitales Sterben im Web 2.0. *ZEV*, 2 ff.
Diegmann, H., Kuntz, W. (2010). Praxisfragen bei Onlinespielen. *NJW*, 561.
Dietrich, F., Ziegelmayer, D. (2013). Facebook's „Sponsored Stories" – ein personenbezogenes unlauteres Vergnügen. *CR*, 104 ff.
Dopatka, K. (2010). Digitaler Nachlass – Der Umgang mit elektronischen Daten nach dem Tod. *NJW-aktuell*, 14 ff.
Dreier, T., Schulze, G. (2008). *Urheberrechtsgesetz*. 3. Aufl. München: C. H. Beck.
Ebersbach, A., Glaser, M., Heigl, R. (2011). *Social Web*. 2. Aufl. Konstanz: UVK-Verl.-Ges.
Eiermann, H. (2013). Work in Progress – Die Zukunft des technischen Datenschutzes. *DuD*, 92 ff.
Erd, R. (2011). Datenschutzrechtliche Probleme sozialer Netzwerke. *NVwZ*, 19 ff.
Ernst, S. (2010). Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem. *NJOZ*, 1917 ff.
Ernst, S. (2011). Verbraucherschutz und Soziale Netzwerke. *VuR*, 321 f.
Ernst, S. (2012). Verhalten von Facebook im Lichte der Lauterbarkeit. *jurisPR-WettbR*, Anm. 3.
Ferrari, F., Kieninger, E.-M., Mankowski, P., Otte, K., Saenger, I. & Staudinger, A. (2012). *Internationales Vertragsrecht*. 2. Aufl. München: C. H. Beck.
Flume, W. (2013). *Allgemeiner Teil des Bürgerlichen Rechts*. Bd. 2: Das Rechtsgeschäft. Nachdruck der 4. Aufl. 1993. Berlin: Springer.
Forkel, H. (1988). Lizenzen an Persönlichkeitsrechten durch gebundene Rechtsübertragung. *GRUR*, 491 ff.
Frevert, T., Wagner, O. (2011). Rechtliche Rahmenbedingungen behördlicher Internetauftritte. *NVwZ*, 76 ff.
Gennen, K., Kremer, S. (2011). Social Networks und der Datenschutz. *ITRB*, 59 ff.
Gola, P., Schomerus, R. *(2012). Bundesdatenschutzgesetz. Kommentar*. 11. Aufl. München: C. H. Beck.
Graf von Westphalen, F. (Hrsg.). *Vertragsrecht und AGB-Klauselwerke*. Loseblatt (Stand: 34. EL 2014). München: C. H. Beck.
Habel, O. M. (2008). Eine Welt ist nicht genug – Virtuelle Welten im Rechtsleben. *MMR*, 71 ff.
Härting, N. (2010). *Internetrecht*. 4. Aufl. Köln: O. Schmidt.
Haupt, S. (1999). Die Übertragung des Urheberrechts. *ZUM*, 898 ff.
Heckmann, D. (2014). *Juris PraxisKommentar Internetrecht*. 4. Aufl. Saarbrücken: Juris.

Heidrich, J., Forgó, N. & Feldmann, T. (2011). *Heise Online-Recht*. Loseblatt (Stand: 3. EL 2011). Hannover: Heise.
Hetter, U. (2010). *Social Media Marketing*. München: Oldenbourg.
Höch, D., Kadelbach, P. (2012). Hat der Nutzer seine Rechte in sozialen Netzwerken selbst in der Hand? *WRP*, 1060 ff.
Hoeren, T. (2005). Der Tod und das Internet – Rechtliche Fragen zur Verwendung von e-Mail und *http://w-Accounts nach dem Tode des Inhabers. NJW, 2113 ff.*
Hoeren, T. (2008). *Internet- und Kommunikationsrecht*. Köln: O. Schmidt.
Hoeren, T. (2012). *IT-Vertragsrecht*. 2. Aufl. Köln: O. Schmidt.
Hoeren, T., Sieber, U. & Holznagel, B. (2014). *Multimedia Recht*. Loseblatt (Stand: 37. EL 2014). München: C. H. Beck.
Hoffmann, C., Schulz, S.-E. & Brackmann, F. (2013). Die öffentliche Verwaltung in den sozialen Medien? *ZD*, 122 ff.
Howaldt, J., Jacobsen, H. (2010). *Soziale Innovation*. Wiesbaden: VS Verlag.
Jandt, S., Roßnagel, A. (2011). Social Networks für Kinder und Jugendliche. Besteht ein ausreichender Datenschutz? *MMR*, 637 ff.
Jauernig, O. (Hrsg.) (2011). *Bürgerliches Gesetzbuch*. 11. Aufl. München: C.H. Beck.
Jotzo, F. (2009). Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr? *MMR*, 232 ff.
Karg, M., Fahl, C. (2011). Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken. *K&R*, 453 ff.
Klett, D., Pohle, J. (2007). Verträge über Internet-Dienstleistungen. *DRiZ*, 198 ff.
Knauer, F. (2009). Neue juristische Publikationsformate im Internet – Stand, Perspektiven und Auswirkungen von Open Access, Wikis, Blogs, Twittern und Podcasts. *NJOZ*, 3004 ff.
Köhler, H., Bornkamm, J. (Hrsg.) (2013). *Gesetz gegen den unlauteren Wettbewerb*. 31. Aufl. München: C. H. Beck
Krasemann, H. (2006). Onlinespielerecht – Spielwiese für Juristen. *MMR*, 351 ff.
Krüger, A., Ropel, W. (2012). Wem gehören Social Media Accounts? *AuA*, 467 ff.
Lapp, T. (2011). Soziale Medien im Spiegel des Rechts. *ITRB*, 282 ff.
Lerch, H., Krause, B., Hotho, A., Roßnagel, A. & Stumme, G. (2010). Social Bookmarking-Systeme – die unerkannten Datensammler. Ungewollte personenbezogene Datenverarbeitung? *MMR*, 454 ff.
Leupold, A., Glossner, S. (Hrsg.) (2013). *Münchener Anwaltshandbuch IT-Recht*. 3. Aufl. München: C. H. Beck.
Levina, M., Kien, G. (Hrsg.) (2010). *Post-Global Network and Everyday Life*. New York: Peter Lang.
Lichtnecker, F. (2013). Die Werbung in sozialen Netzwerken und mögliche hierbei auftretende Probleme. *GRUR*, 135 ff.
Lober, A., Weber, O. (2005). Money for nothing? Der Handel mit virtuellen Gegenständen und Charakteren. *MMR*, 653 ff.
Loewenheim, U. (Hrsg.) (2010). *Handbuch des Urheberrechts*. 2. Aufl. München: C. H. Beck.
Mankowski, P. (2005). Gemischte Verträge und persönlicher Anwendungsbereich des Internationalen Verbraucherschutzrechts. *IPRax*, 505 ff.
Martinek, M., Semler, J., Habermeier, S. & Flohr, E. (Hrsg.) (2010). *Vertriebsrecht*. 3. Aufl. München: C. H. Beck.
Martini, M. (2012). Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet. *JZ*, 1145 ff.
Maume, P. (2007). Bestehen und Grenzen des virtuellen Hausrechts. *MMR*, 620 ff.
Medicus, D., Petersen, J. (2011). *Bürgerliches Recht*. 23. Aufl. München: C. H. Beck.
Melot de Beauregard, P., Gleich, C. (2012). Social Media am Arbeitsplatz – Chancen und Risiken. *DB*, 2044 ff.
Meyer, S. (2012). Facebook: Freundefinder und AGB rechtswidrig. *K&R*, 309 ff.

Michelis, D., Schildhauer, T. (Hrsg.) (2012). *Social Media Handbuch*. 2. Aufl. Baden-Baden: Nomos.
Moos, F. (2012). Share this – gemeinsame oder geteilte Verantwortung für Datenschutzkonformität in sozialen Netzwerken. *ITRB*, 226 ff.
Moritz, H.-W., Dreier, T. (Hrsg.) (2005). *Rechts-Handbuch zum E-Commerce*. 2. Aufl. Köln: Otto Schmidt.
Müller-Broich, J.-D. (2012). *Telemediengesetz*. 1. Aufl. Baden-Baden: Nomos.
Nolte, N. (2011). Zum Recht auf Vergessen im Internet. *ZRP*, 236 ff.
Nolte, N., Hecht, F. (2006). Plattformverträge. Hinweise zur Vertragsbeziehung zwischen Betreiber und Provider. *ITRB*, 188 ff.
Nord, J., Manzel, M. (2010). „Datenschutzerklärungen" – misslungene Erlaubnisklauseln zur Datennutzung. „Happy-Digits" und die bedenklichen Folgen im E-Commerce. *NJW*, 3756 ff.
Nordemann, J.-B. (2012). AGB-Kontrolle und Nutzungsrechtseinräumung durch den Urheber. *NJW*, 3121 ff.
Palandt, O. (Hrsg.) (2014). *Bürgerliches Gesetzbuch*. 73. Aufl. München: C. H. Beck.
Peifer, K.-N. (2012). Persönlichkeitsschutz und Internet – Anforderungen und Grenzen einer Regulierung. *JZ*, 851 ff.
Piper, H., Ohly, A., & Sosnitza, O. (2010). *Gesetz gegen den unlauteren Wettbewerb*. 5. Aufl. München: C. H. Beck.
Polenz, S. (2012). Die Datenverarbeitung durch und via Facebook auf dem Prüfstand. *VuR*, 207 ff.
Prütting, H., Wegen, G., Weidenreich, G. (Hrsg.) (2011). *BGB. Kommentar*. 2. Aufl. Köln: Luchterhand.
Qualman, E. (2009). *Socialnomics*. Bonn: MITP.
Redeker, H. (Hrsg.) (2011). *Handbuch der IT-Verträge*. Köln: Otto Schmidt.
Redeker, H. (2012). *IT-Recht*. 5. Aufl. München: C. H. Beck.
Reithmann, C., Martiny, D. (2010). *Internationales Vertragsrecht*. 7. Aufl. Köln: Otto Schmidt.
Rippert, S., Weimer, K. (2007). Rechtsbeziehungen in der virtuellen Welt. *ZUM*, 272 ff.
Rosenbaum, B., Tölle, D. (2013). Aktuelle rechtliche Probleme im Bereich Social Media. Überblick über die Entscheidungen der Jahre 2011 und 2012. *MMR*, 209 ff.
Rudkokwski, L., Werner, D. (2012). Neue Pflichten für Anbieter jenseits der „Button-Lösung". Paid Content-Verträge nach der Verbraucherrechte-Richtlinie. *MMR*, 711 ff.
Säcker, F. J., Rixecker, R. (Hrsg) (2012). *Münchener Kommentar zum BGB*. 6. Aufl. München: C. H. Beck.
Salwitzek, A. (2013). Automatische Gesichtserkennung – Verfahren gegen Facebook eingestellt. *MMR-Aktuell*, 342688.
Scherner, K. O. (1976). Generaleinwilligung und Vertretungsnotstand im Minderjährigenrecht. *FamRZ*, 673 ff.
Schmitt, J. (2005). Der Begriff der lediglich vorteilhaften Willenserklärung i. S. v. § 107 BGB. *NJW*, 1090 ff.
Schröder, G. F. (Hrsg.) (2012). *Datenschutzrecht*. München: C. H. Beck.
Schulze, G. (2012). Die Übertragungszwecklehre – Auslegungsregel oder Inhaltsnorm? *GRUR*, 993 ff.
Schulze, R. (Hrsg.) (2012). *Bürgerliches Gesetzbuch*. 7. Aufl. Baden-Baden: Nomos.
Schuppert, S. (2000). Web-Hosting-Verträge. *CR*, 227 ff.
Schwenke, T. (2012). Das virtuelle Hausrecht als Abwehrmaßnahme gegen „Shitstorms" innerhalb von Social Media Plattformen. *K&R*, 305 ff.
Schwenke, T. (2012). Wirksamkeit der Rechteeinräumung an Nutzerinhalten in Nutzungsbedingungen von sozialen Netzwerken und Onlineplattformen. *DSRITB*, 35 ff.
Schwenke, T. (2013). Nutzungsbedingungen sozialer Netzwerke und Onlineplattformen. Wirksamkeit der Rechteeinräumung an Nutzerdaten und nutzergenerierten Inhalten. *WRP*, 37 ff.
Sieling, C., Lachenmann, M. (2012). Wettbewerbsrechtliche Aspekte bei Werbung in Sozialen Netzwerken. *ITRB*, 156 ff.

Sievers, B. (2012). Ist erlaubt, was gefällt? Urheberrechtsverletzung und Verantwortlichkeit beim Social Sharing. *GRURPrax*, 229 ff.
Simitis, S. (Hrsg.) (2011). *Bundesdatenschutzgesetz*. 7. Aufl. Baden-Baden: Nomos.
Solmecke, C. (2012). Wirksamkeit der Nutzungsbedingungen in sozialen Netzwerken. *DSRITB*, 49 ff.
Solmecke, C., Dam, A. (2012). Wirksamkeit der Nutzungsbedingungen sozialer Netzwerke. Rechtskonforme Lösung nach dem AGB- und dem Urheberrecht. *MMR*, 71 ff.
Solmecke, C., Wahlers, J. (2012). Rechtliche Situation von Social Media Monitoring Diensten. *ZD*, 550 ff.
v. Sonnleithner, B. (2011). Datenschutz und Social Media. *ITRB*, 238 f.
Spiecker gen. Döhmann, I. (2012). Die Durchsetzung datenschutzrechtlicher Mindeststandards bei Facebook und anderen Sozialen Netzwerken. *K&R*, 717 ff.
Spindler, G. (Hrsg.) (2004). *Vertragsrecht der Internet-Provider*. 2. Aufl. Köln: Otto Schmidt.
Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien*. 2. Aufl. München: C. H. Beck.
Stadler, T. (2011). Verstoßen Facebook und Google Plus gegen deutsches Recht? Ausschluss von Pseudonymen auf Social Media Plattformen. *ZD*, 57 ff.
v. Staudinger, J. (2013). *BGB – Neubearbeitung*. Berlin: de Gruyter.
Stürner, R. (1973). Der lediglich rechtliche Vorteil. *AcP*, 402 ff.
Taeger, J., Gabel, D. (Hrsg.) (2010). *Kommentar zum BDSG*. Frankfurt a. M.: Verlag Recht und Wirtschaft.
Terhaag, M., Schwarz, C. (2012). Quo vadis, Freundschaftsempfehlung? – Mächtiges PR-Instrument oder wettbewerbswidrige Datenschleuder? *K&R*, 377 ff.
Ulbricht, C. (2012). Social Media & Recht – Praktische Handlungsempfehlungen für Kommunen. *KommunalPraxis spezial*, 101 ff.
Unseld, F. (2011). Die Übertragbarkeit von Persönlichkeitsrechten. *GRUR*, 982 ff.
des Vertragsrechts. *ZD*, 210 ff.
Voigt, P., Alich, S. (2011). Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber. *NJW*, 3541 ff.
Wandtke, A.-A., Bullinger, W. (Hrsg.) (2009). *Urheberrecht*. 3. Aufl. München: C. H. Beck.
Weichert, T. (2001). Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung. *NJW*, 1463 ff.
Weichert, T. (2012). Datenschutzverstoß als Geschäftsmodell – der Fall Facebook. *DuD*, 716 ff.
Wieczorek, M. A. (2012). Facebook: „Freunde-Finder“ und Teile der AGB rechtswidrig. *WRP*, 539 ff.
Wintermeier, M. (2012). Inanspruchnahme sozialer Netzwerke durch Minderjährige. Datenschutz aus dem Blickwinkel des Vertragsrechts. *ZD*, 210 ff.
Wintermeier, M. (2013). Rechtskonforme Erstellung einer Datenschutzerklärung. Anforderungen im Rahmen gewerblicher Werbeangebote. *ZD*, 21 ff.
Wittern, F., Wichmann, M. (2012). Dürfen soziale Netzwerke auf die Adressbücher ihrer Nutzer zugreifen? *ITRB*, 335 ff.
Yazar, C., Ammerich, F. (2012). Facebook, Google & Co. – Chancen und Risiken. *NVwZ*, 1156 fff.
Zscherpe, K. A. (2004). Anforderungen an die datenschutzrechtliche Einwilligung im Internet. *MMR*, 723 ff.

Kapitel 4
Datenschutzrechtliche Aspekte der Social Media

Gerrit Hornung

Inhalt

4.1 Einleitung

Social Media-Anwendungen basieren auf der Verwendung personenbezogener Daten: Namen, Kontaktinformationen, persönliche Vorlieben und Abneigungen, Kommunikationspartner, die soziale Interaktion mit ihnen, jede Form von geteilten **1**

G. Hornung (✉)
Inhaber des Lehrstuhls für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik, Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: gerrit.hornung@uni-passau.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_4

Erlebnissen und Vorkommnissen – all dies sind Daten, die in Social Media jedenfalls typischerweise einer **bestimmten oder bestimmbaren natürlichen Person** zugeordnet sind. Diese Daten sind grundrechtlich durch das Recht auf informationelle Selbstbestimmung und entsprechende internationale Verbürgungen, einfachgesetzlich durch das Datenschutzrecht geschützt.

2 Social Media liegen in einem **Spannungsfeld** zwischen **Ausdruck und Gefährdung informationeller Selbstbestimmung**. Die kommunikativen Chancen sind enorm:[1] Die Teilnahme an sozialen Netzwerken wie Facebook, studiVZ oder XING eröffnet die Gelegenheit, sich selbstbestimmt mit seinen Vorlieben und Handlungen zu präsentieren; Kollektivprojekte wie Wikipedia bündeln vorhandenes und erzeugen neues Wissen über die Nutzer und andere Personen; Bewertungsplattformen sammeln persönliche Erfahrungen der Beteiligten und ermöglichen selbstbestimmte Konsumentenentscheidungen; inhaltsorientierte Anwendungen wie YouTube (Filme), Flickr (Bilder), Delicious (Links) oder Tumblr (multimediale Blogs) zeigen die entsprechenden Vorlieben der Nutzer und eröffnen anderen neue Möglichkeiten.

3 Je mehr diese Chancen allerdings die Erhebung, Verwendung und Nutzung personenbezogener Daten voraussetzen, desto größer werden auch die damit verbundenen Risiken.[2] Die **Geschäftsmodelle** der Betreiber basieren weithin auf der Bildung von **Interessens- und Persönlichkeitsprofilen** ihrer Nutzer, der dadurch ermöglichten individualisierten Werbung und dem Weiterverkauf der entsprechenden Informationen. Nutzer haben keine Möglichkeit der Kontrolle darüber, welche Daten durch Dritte über sie bereitgestellt werden. Einmal verfügbar gemachte Daten können so gut wie nie wieder vollständig aus den entsprechenden Netzwerken oder dem Internet insgesamt entfernt werden. Durch den inhärent grenzüberschreitenden Charakter von Social Media verschärft sich überdies das Problem, dass es keine weltweit anerkannten datenschutzrechtlichen Standards gibt.

4 Jenseits aller wichtigen, mehr kleinteiligen rechtlichen Fragestellungen sind dies die **übergreifenden datenschutzrechtlichen Konfliktlagen** von Social Media: Sind diese Anwendungen ein Ausdruck und Mittel informationeller Selbstbestimmung, oder umgekehrt eine Bedrohung für diese? Wie ist im Dreiecksverhältnis zwischen Anbieter, Nutzer und anderen Nutzern/unbeteiligten Dritten die Verantwortlichkeit näher zu bestimmen? Lassen sich hergebrachte Schutzinstrumente wie Zweckbindung, Erforderlichkeit oder Betroffenenrechte auch im Social Media-Bereich sinnvoll anwenden? Und welche datenschutzrechtlichen Prinzipien sind für weltumspannende Kommunikationsinfrastrukturen sinnvoll, aber auch realistisch durchsetzbar?

---

[1] S. näher Hohlfeld/Godulla, Kap. 2.

[2] S. z. B. Eifert, in: Bieber et al., Soziale Netze in der digitalen Welt, S. 253 ff.; Roßnagel, ebd., S. 269 ff.; Jandt/Roßnagel, MMR 2011, 637 f.; dies., in: Schenk et al., Digitale Privatsphäre, S. 315 ff.; Spiecker gen. Döhmann, K&R 2012, 717 ff.

4.2 Rechtsgrundlagen und Regelungsprinzipien

Personenbezogene Daten sind sowohl durch **grundrechtliche**, als auch durch **einfachgesetzliche Normen** geschützt. **5**

4.2.1 Grundrechtliche Bezüge

Der grundrechtliche Bereich bildet den Hintergrund für die datenschutzrechtlichen Regeln auf der einfachgesetzlichen Ebene. Im deutschen Verfassungssystem bietet das **Recht auf informationelle Selbstbestimmung** eine Art „Grundregulierung" für den Umgang des Staates mit personenbezogenen Daten. Dieses Recht wird in ständiger Rechtsprechung des Bundesverfassungsgerichts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und gewährt dem Einzelnen die Befugnis, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[3] Es schützt damit auch gegen staatliche Zugriffe auf Daten, die in Social Media verwendet werden. Das Bundesverfassungsgericht hat eine **spezifische Schrankendogmatik** für das Recht auf informationelle Selbstbestimmung entwickelt, die sich heute auch in den allgemeinen Regeln des einfachgesetzlichen Datenschutzrechts wiederspiegelt: Zweckbindung und Zweckbegrenzung, Erforderlichkeit der Datenverarbeitung, Transparenzprinzip, Verbot eines allgemeinen Personenkennzeichens und einer Datenspeicherung auf Vorrat zu noch unbestimmten Zwecken, Beschränkung von Profilbildungen, das Prinzip der informationellen Gewaltenteilung sowie organisatorische und verfahrensrechtliche Sicherungsmechanismen.[4] **6**

Je nach Art der Anwendungen und Daten können daneben weitere spezielle Grundrechte eingreifen und dem Recht auf informationelle Selbstbestimmung vorgehen. Soweit Social Media der „unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs"[5] dienen, unterfällt dieser Teil der Kommunikation dem **Fernmeldegeheimnis des Art. 10 GG**. Dies ist beispielsweise bei Nachrichtendiensten, Chat-Funktionen oder integrierten Voice-over-IP Diensten der Fall, die in vielen Plattformen bereitgestellt werden. Übermittlungsart und Ausdrucksform spielen dabei keine Rolle, sodass der Schutz ungeachtet technischer Innovationen auf der Übertragungs- oder Diensteebene besteht. **7**

---

[3] BVerfGE 65, 1 (1. Leitsatz und 43).

[4] S. etwa Roßnagel et al., Modernisierung des Datenschutzrechts, S. 70 ff.; Simitis, in: Simitis, BDSG, Einl. Rn. 33 ff.; Trute, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.5, Rn. 32 ff.; Tinnefeld et al., Einführung in das Datenschutzrecht, S. 237 ff., jeweils m. w. N.; s. a. Albers, Informationelle Selbstbestimmung, S. 164 ff.

[5] So die Formulierung des Bundesverfassungsgerichts, s. z. B. BVerfGE 115, 166 (182); 120, 274 (306 f.); 124, 43 (54).

8 Art. 10 GG schützt sowohl **Inhalte als auch Umstände der Telekommunikation**.[6] Eine technische Besonderheit von Social Media stellt es dar, dass beides teilweise dauerhaft gespeichert und den Nutzern verfügbar gemacht wird. Anders als bei herkömmlicher Telekommunikation gibt es also **kein echtes „Ende" des Kommunikationsvorgangs**, sodass sich die Frage stellt, ob der Schutz von Art. 10 GG dauerhaft eingreift. Genau dies hat das Bundesverfassungsgericht für das vergleichbare Beispiel des IMAP-Verfahrens bejaht: Übermittelte E-Mails sind danach auch dann von Art. 10 GG erfasst, wenn sie nach der Wahrnehmung oder dem Download durch den Nutzer dauerhaft auf dem Mailserver gespeichert werden.[7] Dies ist direkt auf dauerhaft in Social Media gespeicherte Nachrichten übertragbar. Allerdings zeigt sich hier auch die Problematik der Lösung des Bundesverfassungsgerichts: Der Sache nach dürfte es eher um eine Art ausgelagerter Datenspeicherung des Nutzers gehen. Ob die durch das Gericht gewählte Sonderdogmatik (trotz Eröffnung des Schutzbereichs von Art. 10 GG sollen die strafprozessualen Regelungen „der §§ 94 ff. StPO" eine hinreichende Eingriffsgrundlage sein) angemessen ist, lässt sich jedenfalls mit guten Gründen bezweifeln.[8]

9 Das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**[9] ist in den meisten Fällen nicht auf Social Media anwendbar. Zwar stellen die Server der Anbieter, auf denen die entsprechenden Anwendungen laufen, informationstechnische Systeme dar. Eine „grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung" besteht allerdings nur – und der Schutzbereich ist folglich nur dann eröffnet – „soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt."[10] Dies trifft auf die Systeme der Anbieter regelmäßig nicht zu, weil diese die Kontrolle ausüben und den Nutzern zwar einen Teil der Applikation (Profile, Speicherplatz), nicht aber ein System zur selbstbestimmen Nutzung überlassen. Je nach Vertragsmodell und technischer Umsetzung kann sich dies im Einzelfall allerdings anders darstellen. Ein Beispiel hierfür sind **fortgeschrittene Smartphone-Apps**, die Social Media-Daten auf eigenen Endgeräten der Betroffenen speichern und verarbeiten und dabei gegebenenfalls sogar

---

[6] S. BVerfGE 67, 157 (172); 85, 386 (396); 120, 274 (307); 125, 260 (304), st. Rspr.; ebenso für Art. 8 EMRK: EGMR, MMR 2007, 431 (Copland./. Vereinigtes Königreich) m. Anm. Hornung; anders für die USA der US Foreign Intelligence Surveillance Court, s. http://www.heise.de/-1960249.html.

[7] BVerfGE 124, 43 (54 ff.).

[8] Dazu Brunst, CR 2009, 591; s. a. Klein, NJW 2009, 2996.

[9] Entwickelt in BVerfGE 120, 274; s. z. B. Böckenförde, JZ 2008, 925; Heckmann, in: FS für Käfer, S. 129; Hoffmann-Riem, JZ 2008, 1009; Hornung, CR 2008, 299. Dieses Urteil des Bundesverfassungsgerichts zur so genannten Online-Durchsuchung bildet bislang (d. h. nach über sechs Jahren) die einzige Entscheidung des Gerichts, in der das Grundrecht eine Rolle spielt.

[10] BVerfGE 120, 274 (315).

auf andere Anwendungen zugreifen und aus diesen personenbezogene Daten sammeln.[11] Da Smartphones in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fallen,[12] erstreckt sich der Schutz dann auch auf derartige Anwendungen und Daten des Nutzers.

10 Die Europäische Menschenrechtskonvention kennt wie das Grundgesetz kein explizites Recht auf den Schutz personenbezogener Daten. Der Europäische Gerichtshof für Menschenrechte hat diesen aber schon im Jahre 1987 aus dem Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) abgeleitet[13] und in der Folge in vielen Entscheidungen ausgebaut.[14] Der Schutz der „Korrespondenz" in **Art. 8 EMRK** erfasst auch die Nutzung von E-Mail und Internet;[15] dies gilt auch für die Verwendung von Social Media.

11 Demgegenüber enthält die Charta der Grundrechte der Europäischen Union nicht nur mit Art. 7 GRC eine an Art. 8 EMRK angelehnte Vorschrift, sondern in **Art. 8 GRC** ein explizites Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten.[16] Gemäß Art. 8 Abs. 2 GRC dürfen diese nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Art. 8 Abs. 3 GRC schreibt überdies die Kontrolle durch eine unabhängige Stelle vor.

12 Allen deutschen und europäischen Grundrechtsbestimmungen ist gemein, dass sie sich im Ausgangspunkt gegen staatliche Einwirkungen richten. Für Social Media bedeutet dies, dass ein direkter **Schutz gegen staatliche Zugriffe** besteht, die durch Beschlagnahme bei Providern, Kommunikation mittels behördlicher Tarnnamen-Accounts,[17] systematische Erhebung frei verfügbarer Social Media-Daten,[18] Zugriffe auf Endgeräte oder in anderer Art und Weise erfolgen. Allerdings

---

[11] So die Software „Facebook Home", die im April 2013 für das Betriebssystem Android eingeführt wurde.

[12] So explizit das Bundesverfassungsgericht, s. BVerfGE 120, 274 (314): „Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können".

[13] Grundlegend Leander./. Schweden, Urteil v. 26.3.1987, ferner Z./. Finnland, Urteil v. 25.2.1997; Amann./. Schweiz, Urteil v. 16.2.2000, alle abrufbar unter hudoc.echr.coe.int/; s. a. den Bericht der Kommission in Rs. 15220/89 (DR 75, 30) und die Entscheidung in Rs. 25099/94 (DR 81, 136).

[14] Ausf. zur Rechtsprechung des Gerichts und zur Entwicklung Schiedermair, Der Schutz des Privaten als internationales Grundrecht, S. 171 ff.

[15] Erstmals in EGMR, MMR 2007, 431 (Copland vs. Vereinigtes Königreich) m. Anm. Hornung.

[16] S. näher Schiedermair, Der Schutz des Privaten als internationales Grundrecht, S. 333 ff.

[17] Jedenfalls, wenn eine staatliche Stellen dabei „ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde", s. BVerfGE 120, 274 (345).

[18] Die Kenntnisnahme öffentlich zugänglicher Informationen durch staatliche Stellen ist grundsätzlich kein Grundrechtseingriff, s. BVerfGE 120, 274 (344 f.). Dies ändert sich jedoch, wenn es sich um eine gezieltes Zusammentragen, Speichern und Auswerten (ggf. unter Hinzuziehung weiterer Daten) handelt, s. ebd., 345.

kennen sowohl das deutsche als auch das europäische Recht eine **Schutzpflichtendogmatik**.[19] Der Staat hat sich danach „schützend und fördernd“[20] vor die entsprechenden Grundrechte zu stellen. Im Bereich des Datenschutzes bedeutet dies – auch unter Berücksichtigung entsprechender Einschätzungsprärogativen – eine Pflicht, auch gegenüber privaten Datenverarbeitern durch entsprechende gesetzliche Regelungen für einen effektiven Schutz von personenbezogenen Daten[21] und selbstgenutzten IT-Systemen[22] zu sorgen. Wo derartige Regelungen allein nicht ausreichend oder in grenzüberschreitenden Strukturen nur eingeschränkt durchsetzbar sind, muss der Staat überdies dafür sorgen, dass die Grundrechtsträger sich durch den **Einsatz datenschutzfreundlicher Technik** so weit wie möglich selbst schützen können.[23]

4.2.2 Einfachgesetzliche Grundlagen

13 Bei Social Media handelt es sich um **Telemedien i. S. v. § 1 Abs. 1 Satz 1 TMG**. Es werden zwar Signale über Telekommunikationsnetze übertragen, womit ein Merkmal von § 3 Nr. 24 TKG erfüllt ist, Social Media erschöpfen sich aber nicht darin.[24] Ein Dienst nach § 3 Nr. 25 TKG liegt ebenfalls nicht vor. Mangels Linearität, zeitgleichem Empfang und Sendeplan werden Social Media zumindest als solche auch nicht vom Rundfunkbegriff des § 2 Abs. 1 Satz 1 RStV erfasst. Etwas anderes kann sich dann ergeben, wenn Rundfunkangebote in die entsprechenden Anwendungen integriert werden.[25]

14 Für Social Media gelten damit gemäß § 1 Abs. 3 Satz 1 BDSG vorrangig die §§ 11 ff. TMG, „soweit“ sie auf personenbezogene Daten anzuwenden sind. Jenseits dieser speziellen Regelungen bleibt es bei der Anwendung des Bundesdatenschutzgesetzes. Dies wird in § 12 Abs. 3 TMG ausdrücklich klargestellt und

---

[19] S. zur dogmatischen Konstruktion in Deutschland z. B. Herdegen in: Maunz/Dürig, Art. 1 Abs. 3 Rn. 21 f. m. w. N.; Sachs, in: Stern III/1, S. 728 ff.; Stern, DÖV 2010, 241 (243 ff.); Dolderer, Objektive Grundrechtsgehalte, S. 177 ff.; Krings, in: FS für Stern, S. 425 ff.; für die Schutz- und Gewährleistungspflichten nach der EMRK s. Grabenwarter/Pabel, EMRK, § 19.

[20] So die ständige Formulierung des Bundesverfassungsgerichts, s. BVerfGE 35, 79 (113); 39, 1 (1. Leitsatz und 42); 46, 160 (164); 53, 30 (57); 56, 54 (73); 85, 360 (384); 88, 203 (232); 90, 145 (149); 115, 25 (45); 115, 118 (153); 121, 317 (356).

[21] Zur besonderen Situation bei Kindern und Jugendlichen s. Jandt/Roßnagel, MMR 2011, 637 (638).

[22] Zur Drittwirkung des Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme s. Roßnagel/Schnabel, NJW 2008, 3534.

[23] S. zu dieser Überlegung Roßnagel, ZRP 1997, 26 ff.

[24] Differenzierend Karg/Fahl, K&R 2011, 453 (455 ff.) [zusätzliche Anwendung des TKG, wenn bei Teilanwendungen die nichtöffentliche Kommunikation zwischen einzelnen Teilnehmern im Vordergrund steht].

[25] Näher zur einfachrechtlichen Rundfunkeigenschaft von Social Media Beyerbach, Kap. 9 Rn. 13 ff.

ist für viele Bereiche wie die Begriffsbestimmungen (§ 3 BDSG), die Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG), die Anforderungen an eine Einwilligung (§ 4a BDSG) sowie die Aufsichtsregelungen (§ 38 BDSG) unstreitig.[26] Darüber hinaus gilt das **Bundesdatenschutzgesetz** auch für personenbezogene Daten, die den **Inhalt des jeweiligen Social Media-Angebots** bilden. Die Zulässigkeit des Umgangs mit diesen Daten bestimmt sich, da es sich regelmäßig um private Anbieter handelt, folglich nach den §§ 27 ff. BDSG.[27] Die Gegenansicht, die auch Inhaltsdaten dem Telemediengesetz unterstellen will,[28] lässt dessen spezifischen Schutzzweck unberücksichtigt.

15 Aus der weitgehenden Unanwendbarkeit des Telekommunikationsgesetzes folgt insbesondere, dass für individuelle Kommunikation zwischen den Nutzern von Social Media (Nachrichtendienste, Chat, Voice-over-IP) die Anwendbarkeit des einfachgesetzlichen Telekommunikationsgeheimnis (§ 88 TKG) abzulehnen oder zumindest zweifelhaft ist;[29] insoweit kommt es zu einer Inkongruenz zum verfassungsrechtlichen Telekommunikationsgeheimnis nach Art. 10 GG.[30] Das deutsche Recht kennt **kein einfachgesetzliches Telemediengeheimnis**, das gegenüber den Anbietern einen entsprechenden Schutz bieten würde.

16 Die datenschutzrechtlichen Regelungen weisen eine Reihe von **Grundprinzipien** auf, die teilweise Ausfluss der Rechtsprechung des Bundesverfassungsgerichts,[31] inzwischen aber weithin auch europarechtlich[32] vorgegeben sind:

- Nach dem so genannten **Verbotsprinzip** in § 4 Abs. 1 BDSG und § 12 Abs. 1 TMG bedarf jeder Umgang mit personenbezogenen Daten einer Rechtsgrundlage, die entweder in einer Rechtsvorschrift oder einer freiwilligen und informierten Einwilligung (§ 4a BDSG) liegt.

---

[26] S. schon BT-Drs. 14/6098,14; s. auch Roßnagel et al., Datenschutz im Electronic Commerce, 2003, S. 136; Scholz, Datenschutz beim Interneteinkauf, S. 154.

[27] S. für soziale Netzwerke Jandt/Roßnagel, MMR 2011, 637 (639); Karg/Fahl, K&R 2011, 453 (458); Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 94 f.; allgemein Scholz, Datenschutz beim Internet-Einkauf, S. 258 f.; Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG, Rn. 3; Bizer/Hornung, in: Roßnagel, Recht der Telemediendienste, § 12 TMG, Rn. 101 m. w. N.

[28] Schmitz, in: Spindler et al., TDG, § 6 TDDSG Rn. 16 ff.; Imhof, CR 2000, 110 ff.; Buchner, in: BeckOK BDSG, § 29 Rn. 35 ff.; Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, S. 396 f.; tendenziell auch Schüßler, in: Taeger, Digitale Evolution, S. 242.

[29] S. näher am Beispiel von Smartphone-Messengern wie WhatsApp Schneider, in: Taeger, Law as a Service (LaaS), S. 89 ff.

[30] S. z. B. Bizer/Hornung, in: Roßnagel, Recht der Telemediendienste, 2013, § 12 TMG, Rn. 18 f.

[31] S. o. 4.2.1.

[32] Europäische Vorgaben finden sich in der Richtlinie 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 v. 23.11.1995, 31 sowie in der Richtlinie 2002/58/EG vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L. 201 vom 31.7.2001, 37 (zuletzt geändert durch die Richtlinie 2009/136/EG vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG, ABl. EU Nr. L337, 11); zum Ineinandergreifen s. Bizer/Hornung, in: Roßnagel, Recht der Telemediendienste, § 12 TMG, Rn. 20 ff.

- Daten dürfen nur für spezifische Zwecke erhoben und verwendet werden (**Zweckbindung**). Zweckänderungen bedürfen dementsprechend – wie sich beispielhaft aus § 12 Abs. 2 TMG ergibt – einer selbstständigen Grundlage und sind andernfalls rechtswidrig.
- Der konkrete Umgang mit den Daten muss in Bezug auf den Zweck erforderlich sein; dies ist beispielsweise in § 14 Abs. 1 und § 15 Abs. 1 TMG niedergelegt. Das **Erforderlichkeitsprinzip** umfasst auch die Pflicht zur Löschung oder Anonymisierung, sobald die Daten entweder überhaupt nicht mehr oder jedenfalls nicht mehr in personenbezogener Form vorliegen müssen.
- Der Grundsatz der **Datenvermeidung und Datensparsamkeit** (§ 3a BDSG) enthält weitergehende Anforderungen auch an die Auswahl und Gestaltung von Datenverarbeitungssystemen. Soweit möglich und zumutbar, sind Verfahren der Anonymisierung und Pseudonymisierung einzusetzen; dies wird für Telemedien nochmals in § 13 Abs. 6 TMG geregelt.
- Nach dem **Transparenzprinzip** müssen die Betroffenen über Art und Umfang der Datenverarbeitung informiert werden. Personenbezogene Daten sind folglich nach Möglichkeit direkt bei ihnen zu erheben (§ 4 Abs. 2 BDSG); daneben bestehen spezifische Informationspflichten wie in § 13 Abs. 1 TMG und korrespondierende Auskunftsansprüche.
- Das Datenschutzrecht enthält umfassenden **Rechte der Betroffenen**, insbesondere auf Auskunft (§§ 19, 34 BDSG) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35 BDSG). Diese Rechte können nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
- Der Umgang mit so genannten **besonderen Arten personenbezogener Daten** (§ 3 Abs. 9 BDSG) unterliegt besonderen Restriktionen.
- Jede verantwortliche Stelle hat nach § 9 BDSG i. V. m. der zugehörigen Anlage **technische und organisatorische Maßnahmen** zu treffen, um die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten. Hinzu kommen spezielle Anforderungen wie in § 13 Abs. 4 TMG. Die entsprechenden Maßnahmen müssen verhältnismäßig sein und richten sich dementsprechend einerseits nach der Sensibilität der betroffenen Daten, andererseits nach dem Aufwand für die Umsetzung.
- Die Datenverarbeitung sowohl im öffentlichen als auch im nicht-öffentlichen Bereich unterliegt der **Kontrolle durch spezifische Behörden**, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen.

17 Sofern es sich nicht ausschließlich um persönliche oder familiäre Zwecke handelt (§ 1 Abs. 2 Nr. 3 BDSG), unterliegt praktisch jeder Umgang mit personenbezogenen Daten datenschutzrechtlichen Regelungen. Dies kommt in sehr vielen Wirtschafts- und Verwaltungsbereichen sehr häufig vor und führt dazu, dass es sich beim Datenschutzrecht um eine – vielleicht um die – **rechtliche Querschnittsmaterie** handelt. Als solche weist sie Bezüge zu praktisch allen anderen Kapiteln dieses Buches auf: Verträge (Kap. 3) können die Grundlage für eine Datenverarbeitung bilden. Haftungs- (Kap. 5) und persönlichkeitsrechtliche Aspekte (Kap. 6) werden häufig durch die

missbräuchliche oder verfälschende Verwendung personenbezogener Daten ausgelöst. Diese kann auch strafrechtlichen Charakter annehmen; davon abgesehen besteht praktisch der gesamte Strafprozess aus der Verarbeitung personenbezogener Daten (Kap. 7). Der Datenschutz von Beschäftigten ist eines der umstrittensten Themen der arbeitsrechtlichen Aspekte von Social Media (Kap. 8). Auch medien- und internetrechtliche Anforderungen (Kap. 9) werden teilweise durch Datenschutzfragen ausgelöst. Schließlich bilden die datenschutzrechtlichen Probleme einen wesentlichen Faktor bei der Frage, ob öffentliche Stellen sich an Social Media beteiligen oder diese sogar selbst anbieten dürfen (Kap. 10).

4.3 Grundsätzliche datenschutzrechtliche Einordnung

Social Media werfen eine Fülle **datenschutzrechtlicher Einzelfragen** auf, die im Folgenden erörtert werden. Soweit sich durch den aktuellen Reformvorschlag der Europäischen Kommission vom 25. Januar 2012 für eine Datenschutz-Grundverordnung (DS-GVO-E)[33] wesentliche Änderungen ergeben würden, werden diese jeweils berücksichtigt. **18**

4.3.1 Anwendbares Recht und Zuständigkeitsfragen

Zunächst stellt sich die grundsätzliche Problematik, **welches Datenschutzrecht** auf die entsprechenden Verarbeitungsvorgänge anwendbar ist. Die Zuständigkeitsfrage für die Aufsicht ist davon losgelöst zu beurteilen, weil die deutschen Behörden in bestimmten Fällen auch das Datenschutzrecht anderer EU-Mitgliedstaaten anwenden (§ 38 Abs. 1 Satz 1 BDSG). **19**

Social Media sind praktisch stets für Nutzer aus verschiedenen Ländern verwendbar und werden auch entsprechend eingesetzt. Nationale Lösungen haben sich zumindest in Ländern wie Deutschland nicht durchgesetzt. Selbst Anbieter in Staaten, die wie China über einen hinreichend großen eigenen Markt verfügen, um sich dauerhaft als nationales Angebot zu behaupten, stellen ihre Angebote technisch meist auch Nutzern aus anderen Staaten zur Verfügung.[34] Dies führt unmittelbar zu dem Problem, welche datenschutzrechtlichen Regelungen auf **grenzüberschreitende Konstellationen** im Internet anwendbar sind. **20**

---

[33] Vorschlag für eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)", KOM(2012) 11 endg; zur Diskussion statt vieler Hornung, in: Funk/Scholz, DGRI-Jahrbuch 2012, S. 1 ff.; zu den Auswirkungen auf Social Media s. Kipker/Voskamp, DuD 2012, 737; Hornung, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 123 ff.

[34] Das gilt beispielsweise für den Mikroblogging-Dienst Weibo, der sich (u. a. aufgrund von Restriktionen gegenüber der Nutzung von Facebook und Twitter) in China etabliert hat.

4.3.1.1 Grundsätze

21 Dabei stellt sich vorrangig die Frage, ob der Konflikt durch eine **Rechtswahlklausel** gelöst werden kann. Dies hat das LG Berlin in Anwendung von Art. 3 Abs. 1 Rom I-VO bejaht, da es sich um einen Vertrag zwischen Anbieter und Nutzer von Social Media (konkret: Facebook) handele und die anwendbaren Normen des Datenschutzrechts zivilrechtlicher Natur seien.[35] Dagegen nimmt das VG Schleswig-Holstein umgekehrt einen öffentlich-rechtlichen Charakter der Vorschriften an, sieht in ihnen **Eingriffsnormen i. S. v. Art. 9 Rom I-VO** und lehnt eine Rechtswahl folglich ab.[36] Der Sache nach spricht mehr für die zweite Lösung, weil sich die Parteien sonst der Anwendung des deutschen oder eines anderen nationalen Datenschutzrechts entziehen könnten.[37] Verträge können zwar im Rahmen von § 28 Abs. 1 Satz 1 Nr. 1 BDSG den Datenumgang legitimieren, auch wenn sie ausländischem Recht unterliegen. Welche datenschutzrechtlichen Vorgaben aus dieser Anknüpfung resultieren, richtet sich dann aber nach dem Bundesdatenschutzgesetz.

22 Die Frage des anwendbaren Rechts ist damit auf der **Basis des Bundesdatenschutzgesetzes** zu entscheiden. Das gilt auch, wenn es um die Regelungen der §§ 11 ff. TMG geht. Zwar greift für Telemedien gemäß § 3 TMG im Grundsatz das auch europarechtlich vorgegebene Herkunftslandsprinzip, dies gilt jedoch gemäß § 3 Abs. 3 Nr. 4 TMG ausdrücklich nicht für das Datenschutzrecht.[38] Diese Ausnahme ist europarechtlich auch zwingend, da sich der deutsche Gesetzgeber sonst in Widerspruch zu den Vorgaben aus Art. 4 DSRL setzen würde, die auch den Datenschutz bei Telemedien umfasst.

23 De lege lata sind folgende **Fallgruppen** zu unterscheiden:[39]

1. Bundesdatenschutzgesetz und Telemediendatenschutz gelten gemäß § 1 Abs. 2 Nr. 3 BDSG im Grundsatz für jede Datenverarbeitung durch nicht-öffentliche Stellen. Hiervon gibt es für **inländische Stellen** keine Ausnahme. In Deutschland ansässige Anbieter von Social Media werden also unabhängig davon erfasst, ob sie auch (oder sogar ausschließlich) personenbezogene Daten von Ausländern verarbeiten.

---

[35] LG Berlin, ZD 2012, 276 (278); das KG Berlin, DuD 2014, 417 (421) unterscheidet zwischen zivilrechtlichen und öffentlich-rechtlichen Regelungen des Bundesdatenschutzgesetzes und bestätigt mit diesem Argument die Entscheidung.

[36] VG Schleswig-Holstein, ZD 2013, 245 (246); der anschließende Beschl. des OVG Schleswig-Holstein, NJW 2013, 1977, äußert sich nicht zu dieser Frage.

[37] Ebenso Piltz, CR 2012, 274; ausf. ders., K&R 2012, 640 ff.; Kremer/Buchalik, CR 2013, 789 (791 ff.); s. a. Karg, ZD 2013, 247 (248); zum anwendbaren AGB-Recht s. Solmecke/Dam, MMR 2012, 71.

[38] Jotzo, MMR 2009, 232 (234); Schüßler, in: Taeger, Digitale Evolution, S. 234; Karg, ZD 2013, 247 (248); Dietrich/Ziegelmayer, CR 2013, 104 (105); Moos, in: Taeger/Gabel, BDSG, Einf. TMG, Rn. 11 f.

[39] S. in Bezug auf Social Media z. B. Schüßler, in: Taeger, Digitale Evolution, S. 235 ff.; Piltz, K&R 2013, 292.; Anwendungsbeispiele bei Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 98 ff.

2. Handelt es sich um einen Anbieter mit Sitz in der Europäischen Union oder im Europäischen Wirtschaftsraum, so findet deutsches Recht nach § 1 Abs. 5 Satz 1 BDSG Anwendung, soweit das Unternehmen eine **Niederlassung im Inland** hat und **durch diese** Niederlassung **in Deutschland** personenbezogene Daten erhebt, verarbeitet oder nutzt.
3. Verfügt ein solcher Anbieter **nicht über eine Niederlassung in Deutschland**, gilt dagegen – ebenfalls nach § 1 Abs. 5 Satz 1 BDSG – nicht das deutsche Datenschutzrecht, sondern das Recht des jeweiligen Sitzlandes. Dieselbe Rechtsfolge ergibt sich, wenn zwar eine Niederlassung im Inland besteht, der Umgang mit den Daten aber **nicht „durch" diese** erfolgt.
4. Anbieter aus so genannten **Drittstaaten** (also außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums) unterfallen gemäß § 1 Abs. 5 Satz 2 BDSG dem Bundesdatenschutzgesetz und dem Telemediendatenschutz, wenn sie „im Inland" personenbezogene Daten erheben, verarbeiten oder nutzen.

Die Anwendung dieses ohnehin komplexen Systems wird zusätzlich dadurch erschwert, dass der deutsche Gesetzgeber ein **von den europäischen Vorgaben** mehrfach **abweichendes System** geschaffen hat, dessen Richtlinienkonformität zweifelhaft ist. Die deutschen Gerichte haben darauf verzichtet, die entsprechenden Fragen dem **Europäischen Gerichtshof** zur Vorabentscheidung vorzulegen und sind jetzt damit konfrontiert, dass dieser in der jüngsten Entscheidung zur Löschungspflicht von Suchmaschinen eine deutlich **abweichende Auslegung** von Art. 4 Abs. 1 lit. a DSRL vertritt.[40] **24**

4.3.1.2 Folgen für Social Media

Sowohl die erste als auch die dritte Variante setzen eine Datenverarbeitung „durch" die inländische verantwortliche Stelle oder die inländische Niederlassung voraus. Gemeinsam setzen diese Alternativen Art. 4 Abs. 1 lit. a DSRL um, wonach das nationale Recht auf Datenverarbeitungen anzuwenden ist, „die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt". Die Richtlinie kennt also hinsichtlich des Anwendungsbereichs **keine Unterscheidung zwischen verantwortlicher Stelle und Niederlassung**. Vor allem hat aber der Europäische Gerichtshof in seiner jüngsten Entscheidung darauf abgestellt, dass **„im Rahmen" der Tätigkeit** einer Niederlassung gerade nicht dasselbe sei wie „von" der betreffenden Niederlassung.[41] Mit diesem Argument lässt das Gericht es ausreichen, dass eine Tochtergesellschaft in einem Mitgliedstaat (konkret: Google Spain), die mit der eigentlichen Datenverarbeitung (hier: dem Betrieb der Suchmaschine durch Google Inc. in den USA) **25**

[40] EuGH, Rs. C-131/12 (Google/AEPD), Urteil v. 13.5.2014, Rn. 42 ff.
[41] EuGH, Rs. C-131/12 (Google/AEPD), Urteil v. 13.5.2014, NJW 2014, 2257, Rn. 52.

in keiner Weise befasst ist, in diesem Mitgliedstaat Werbeflächen verkauft und als Anlaufstelle für Beschwerden fungiert.[42]

26 Diese Auslegung führt **de lege lata zu praktisch unlösbaren Problemen**, die der Europäische Gerichtshof offenbar nicht bedacht, mindestens aber nicht thematisiert hat.[43] Bislang waren jedenfalls praktisch alle Beteiligen – einschließlich der deutschen Aufsichtsbehörden – davon ausgegangen, dass in derartigen Fällen das deutsche Recht nicht anzuwenden ist. Nicht zuletzt im Wissen um die Rechtsfolge von § 1 Abs. 5 Satz 1 BDSG wurde nicht selten versucht, die Tätigkeit der deutschen Niederlassung eines globalen Konzerns auf **Marketing-, Rechts- und Lobbytätigkeiten zu beschränken** und den Umgang mit personenbezogenen Daten auszuklammern.[44] Nach dem Urteil des Europäischen Gerichtshofs muss man wohl davon ausgehen, dass dieser Weg **künftig versperrt** sein wird. Dem ist durch eine europarechtskonforme, weite Auslegung des Begriffs „durch" in § 1 Abs. 2 und Abs. 5 Satz 1 BDSG Rechnung zu tragen.

27 **Unklar** ist allerdings, ob das Gericht die weite Auslegung von Art. 4 Abs. 1 lit. a DSRL auch für den Fall vertreten wird, dass eine mit der Datenverarbeitung tatsächlich direkt befasste **Niederlassung in einem anderen Mitgliedstaat** existiert, auf die das dortige Umsetzungsgesetz anzuwenden ist. Für eine entsprechende Differenzierung könnte sprechen, dass das Urteil unter anderem darauf abstellt, bei einer engen Auslegung würde die Richtlinie überhaupt keine Anwendung finden.[45] Nur unter der Voraussetzung einer solchen Unterscheidung kann die deutsche Rechtsprechung zum Anwendungsbereich des Bundesdatenschutzgesetzes noch Relevanz entfalten.

28 Da die Auswirkungen der jüngsten Entscheidung auf die Auslegung von § 1 BDSG durch die deutschen Gerichte bislang nur andiskutiert ist und letztere eine andere datenschutzrechtliche Risikolage betraf (nämlich im konkreten Fall von Facebook das Dreiecksverhältnis zwischen der US-amerikanischen Muttergesellschaft, der nach der internen Aufgabenverteilung für die Datenverarbeitung zuständigen irischen Tochtergesellschaft und der deutschen Tochtergesellschaft, die ausschließlich mit Marketing-, Rechts- und Lobbytätigkeiten befasst ist), sollen die **in den letzten Jahren ergangenen deutschen Urteile** hier erläutert werden. Diese thematisieren ebenfalls die Frage der Verarbeitung „im Rahmen der Tätigkeit einer Niederlassung" nach Art. 4 Abs. 1 lit. a DSRL. Der Begriff der Niederlassung wird im Bundesdatenschutzgesetz nicht legaldefiniert und überhaupt nur in § 1 Abs. 5 Satz 1 BDSG als

---

[42] EuGH, Rs. C-131/12 (Google/AEPD), Urteil v. 13.5.2014, NJW 2014, 2257, Rn. 42 ff.

[43] Nach der Konzeption des Gerichts finden im konkreten Fall alle Umsetzungsgesetze aller Mitgliedstaaten Anwendung, in denen Google Inc. vergleichbare Tochtergesellschaften hat. Da letztere aber mit der Datenverarbeitung nicht befasst sind, betrifft die Anwendung der nationalen Gesetze die Muttergesellschaft. Diese unterliegt also allen nationalen Regelungen und der Kontrolle aller Aufsichtsbehörden zugleich. Da die Datenschutzrichtlinie keinen Abstimmungsmechanismus kennt, ist dies evident nicht in ihrem Sinne.

[44] So ausweislich des Handelsregistereintrags im Fall der Facebook Germany GmbH, s. Schüßler, in: Taeger, Digitale Evolution, S. 239; s. a. VG Schleswig-Holstein, ZD 2013, 245 (246); OVG Schleswig-Holstein, NJW 2013, 1977 (1978).

[45] EuGH, Rs. C-131/12 (Google/AEPD), Urteil v. 13.5.2014, NJW 2014, 2257, Rn. 53 ff.

negative Abgrenzung verwendet, während ansonsten an die verantwortliche Stelle (§ 3 Abs. 7 BDSG) angeknüpft wird. Art. 4 Abs. 1 lit. a DSRL ordnet dagegen positiv die Anwendung des jeweiligen nationalen Datenschutzrechts auf alle Niederlassungen im Hoheitsgebiet des jeweiligen Mitgliedsstaats an. Daraus schließen das VG Schleswig-Holstein und das OVG Schleswig-Holstein, in richtlinienkonformer Auslegung der deutschen Vorschriften komme es nicht auf die Belegenheit der verantwortlichen Stelle in einem Drittstaat, sondern **ausschließlich auf die der Niederlassung** an.[46] An das Vorliegen einer Niederlassung seien überdies **keine hohen Anforderungen** zu stellen, es reiche – ungeachtet der Rechtsform – aus, dass eine ortsfeste Zweigstelle mit Personal in den tatsächlichen Datenumgang einbezogen sei.[47]

29 Akzeptiert man dieses Kriterium, so gilt beispielsweise für **Facebook irisches Datenschutzrecht**, obwohl die Strukturen der Datenverarbeitung weltweit durch die US-Muttergesellschaft vorgegeben werden und sich nach gerichtlicher Feststellung[48] sämtliche Server in den USA befinden. Ob dies unter Schutzzweckgesichtspunkten wirklich von der Datenschutzrichtlinie gewollt ist, lässt sich allerdings mit guten Gründen **bezweifeln**.[49] Kritisieren lässt sich überdies, dass die Gerichte maßgeblich auf das „Data Transfer and Processing Agreement" zwischen der amerikanischen Muttergesellschaft und der irischen Tochter abgestellt haben; wenn derartige konzerninterne Vereinbarungen ohne Prüfung der tatsächlichen Implementierung über das anwendbare Recht entscheiden, wird den betroffenen Konzernen ein sehr weites Gestaltungsinstrument eröffnet. Dementsprechend ist dem KG Berlin beizupflichten, das einen **hinreichenden Vortrag zur eigenen effektiven und tatsächlichen Erhebung und Verarbeitung der Daten** verlangt; hieran fehlte es nach Ansicht des Gerichts im Fall von Facebook.[50] Zutreffend sind überdies die Überlegungen des KG Berlin, dass die Rechtsbeziehungen zwischen der amerikanischen Mutter- und der irischen Tochtergesellschaft nicht allein auf Basis des genannten Agreements beurteilt werden können, sondern maßgeblich zu berücksichtigen ist, dass die

[46] VG Schleswig-Holstein, ZD 2013, 245 (246 f.); OVG Schleswig-Holstein, NJW 2013, 1977 f. und Beschl. v. 22.4.2013, 4 MB 10/13 (nicht veröffentlicht); zustimmend Piltz, K&R 2013, 292 (295 f.); übervereinfachend Kremer/Buchalik, CR 2013, 789 (790), wonach das Ergebnis „dem Wortlaut von § 1 Abs. 5 BDSG" entsprechen soll (s. aber ebd., 792 f.).

[47] Noch weiter die erwähnte Auslegung des EuGH, die einen wirtschaftlichen Zusammenhang ausreichen lässt: EuGH, Rs. C-131/12 (Google/AEPD), Urteil v. 13.5.2014, NJW 2014, 2257, Rn. 42 ff.; enger z. B. Dammann, in: Simitis, BDSG, § 1 Rn. 201 ff.; Karg, ZD 2013, 371 (373 ff.) [dort auch zu den Problemen der Intransparenz der Konzernstrukturen]; nach Ansicht der Art. 29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht v. 16.12.2010, S. 16, kommt es darauf an, „in welchem Maß die Niederlassung(en) an den Tätigkeiten, in deren Rahmen personenbezogene Daten verarbeitet werden, beteiligt ist bzw. sind" und „welche Tätigkeiten von welcher Niederlassung ausgeführt werden".

[48] VG Schleswig-Holstein, ZD 2013, 245 (247); zu den Zweifeln am tatsächlichen Einfluss der irischen Tochter s. Piltz, K&R 2013, 283 (284).

[49] Krit. z. B. Karg, ZD 2013, 247 (248); zum Problem auch Polenz, VuR 2012, 207 ff.; Dietrich/Ziegelmayer, CR 2013, 104 (105 ff.).

[50] KG Berlin, DuD 2014, 417 (420).

Muttergesellschaft gesellschaftsrechtlich die Entscheidungsprozesse jederzeit (durch Anweisungen an die Organe oder deren Austausch) an sich ziehen kann.[51] Freilich stehen wie erwähnt alle diese Überlegungen unter dem **Vorbehalt** des Einflusses der jüngsten Entscheidung des **Europäischen Gerichtshofs** auch auf den Fall einer Datenverarbeitung durch eine Tochtergesellschaft in einem anderen Mitgliedstaat.

30 Existiert demgegenüber **gar keine Niederlassung** in der Union oder dem EWR oder erfolgt der Datenumgang – auch unter Berücksichtigung der weiten Auslegung von Art. 4 Abs. 1 lit. a DSRL durch den Europäischen Gerichtshof[52] – nicht „im Rahmen der Tätigkeit" der Niederlassung, so ist die alles entscheidende Frage die der Erhebung, Verarbeitung oder Nutzung „**im Inland**". Ist dies zu bejahen, so kommt nach § 1 Abs. 5 Satz 2 BDSG deutsches Recht zur Anwendung. Andernfalls gilt das Recht des Drittstaates, das regelmäßig nicht denselben oder sogar gar keinen Schutz gewährt.

31 Eine Meinung stellt insoweit auf den **Standort der datenverarbeitenden Systeme** ab.[53] Dies lässt sich mit einer richtlinienkonformen Auslegung begründen, da nach Art. 4 Abs. 1 lit. c DSRL entscheidend ist, ob die verantwortliche Stelle „auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden". Als solche „Mittel" kann man insbesondere Server auffassen, über die Datenverarbeitungsprozesse abgewickelt werden. **Zu weit** geht es hingegen, den **Computer des Nutzers** von Social Media ausreichen zu lassen. Zwar befindet sich dieser im Inland, wird für die Dateneingabe verwendet und ist insoweit unverzichtbar für das Angebot des Diensts. Eine solche Auslegung der Vorschrift würde aber dazu führen, dass auch reine Online-Angebote stets vom deutschen Datenschutzrecht erfasst würden und dieses dementsprechend weltweit für alle Internetdienste gelten würde, soweit nicht § 1 Abs. 5 Satz 1 BDSG greift. Das wäre erkennbar nicht angemessen.[54]

32 Nach **anderer Ansicht** soll nicht die technische Infrastruktur entscheidend sein, sondern ob sich ein Online-Dienst **erkennbar an deutsche Nutzer** richtet.[55] Dieses Kriterium erscheint in vielen Fällen sachgerecht, lässt sich aber de lege lata

---

[51] KG Berlin, DuD 2014, 417 (420).

[52] S. o. Rn. 25 f.

[53] S. Dammann, in: Simitis, BDSG, § 1 Rn. 220; Gusy, in: BeckOK BDSG, § 1 Rn. 112 ff.; Gabel, in: Taeger/Gabel, BDSG, § 1 Rn. 58 f.

[54] S. Schüßler, in: Taeger, Digitale Evolution, S. 236; diskutabel ist die Anwendung der Norm bei der Verwendung von Cookies, dafür z. B. KG Berlin, DuD 2014, 417 (420); Dammann, in: Simitis, BDSG, § 1 Rn. 227; Gusy, in: BeckOK BDSG, § 1 Rn. 113; Gabel, in: Taeger/Gabel, BDSG, § 1 Rn. 59; Weichert, in: Däubler et al., BDSG, § 1 Rn. 17a; Polenz, VuR 2012, 207 f.; ebenso, aber noch weitergehend auch für Javascript und Bannerwerbung Art. 29-Datenschutzgruppe, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU, WP 56, S. 12 f.

[55] Z. B. Spindler, Gutachten F zum 69. DJT, S. 89 f. m. w. N.; Weichert, in: Däubler et al., BDSG, § 1 Rn. 17a (alternatives Kriterium zur Verwendung von Cookies); in Verbindung mit einer Ausrichtung auf den deutschen Markt auch Ott, MMR 2009, 158 (160); Jotzo, MMR 2009, 232 (236 f.).

nur schwer begründen.[56] Der Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung geht hingegen in diese Richtung. Nach **Art. 3 DS-GVO-E** soll die Verordnung auf Niederlassungen in der Union sowie auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen gelten, wenn die Datenverarbeitung entweder „dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten", oder „der Beobachtung ihres Verhaltens dient". Die zweite Alternative wird in EG 21 damit beschrieben, dass Internetaktivitäten mithilfe von Datenverarbeitungstechniken nachvollzogen würden, durch die einer Person ein Profil zugeordnet werde, das die Grundlage für sie betreffende Entscheidungen bilde oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollten. Das dürfte zumindest auf diejenigen sozialen Netzwerke zutreffen, die wie Facebook über in andere Webseiten eingebettete Elemente („Like-Button" und andere) Daten über ihre Kunden sammeln.[57] Die erste Alternative wird demgegenüber nicht näher erläutert, sodass nicht deutlich wird, wann Online-Dienstleistungen wie Social Media „in" der Union angeboten werden. Sinnvoll wäre jedenfalls eine Anknüpfung an die sprachliche und sonstige **Webseitengestaltung**.

Eine weitere wesentliche Änderung würde sich nach dem Entwurf der Kommission hinsichtlich der **Zuständigkeit der Aufsichtsbehörden** ergeben: Gemäß Art. 51 Abs. 2 DS-GVO-E soll bei Unternehmen mit Niederlassungen in verschiedenen Staaten der Union nur noch die Behörde am Sitz der Hauptniederlassung zuständig sein. Diese Änderung gegenüber § 1 Abs. 5 Satz 1 BDSG könnte zu einem erheblichen Kompetenzverlust der deutschen Behörden führen, der durch die vorgeschlagenen Kooperationsvorschriften („**Kohärenzverfahren**", Art. 57 ff. DS-GVO-E) nur unvollkommen kompensiert würde und jedenfalls nur dann zu rechtfertigen ist, wenn die jeweiligen Behörden hinreichende Ressourcen erhalten und die künftigen europäischen Standards einheitlich durchsetzen. Grundsätzlich abzulehnen ist überdies die geplante Letztentscheidungsbefugnis der Kommission.[58] **33**

4.3.2 Personenbezogene Daten und Betroffene

Datenschutzrechtliche Normen sind nur anwendbar, soweit es sich um personenbezogene Daten handelt (s. z. B. § 1 Abs. 2 BDSG). § 3 Abs. 1 BDSG definiert dies als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder **34**

---

[56] Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Orientierungshilfe „Soziale Netzwerke", S. 13 f.) soll primär auf die technische Perspektive abgestellt, die Ausrichtung des Dienstes aber im Rahmen einer normativen Perspektive ergänzend herangezogen werden.

[57] S. schon Hornung, ZD 2012, 99 (102).

[58] S. näher zu diesem Punkt Hornung, ZD 2012, 99 (104 ff.); ferner Dix, DuD 2012, 318 ff.; Caspar, ZD 2012, 555 ff.; Kahler, RDV 2013, 69 ff.; Ziebarth, CR 2013, 60 (67 f.).

bestimmbaren natürlichen Person". Wichtiger als die **Unterscheidung** zwischen „bestimmt" und „bestimmbar" ist die **zwischen „bestimmbar" und „anonym"**, denn anonyme Daten sind nicht personenbezogen. Daten sind gemäß § 3 Abs. 7 BDSG anonym, wenn sie nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Daraus folgt, dass Anonymität und Bestimmbarkeit keine absoluten, sondern **relative Begriffe** sind. Es kommt jeweils auf die verantwortliche Stelle, das bei ihr verfügbare Zusatzwissen sowie ihr Interesse an der Herstellung des Personenbezugs an, weil dieses Interesse Einfluss auf die Frage der Verhältnismäßigkeit des Aufwands hat.[59] Was für den einen Diensteanbieter ein anonymes Datum ist, kann für den anderen bereits ein personenbeziehbares oder sogar bestimmtes Datum sein.[60]

4.3.2.1 Daten in Nutzerprofilen

35 **Für die Anbieter** von Social Media, die eine Anmeldung erfordern, sind die in Nutzerprofilen gespeicherten Daten danach in den allermeisten Fällen **personenbezogene Daten**. Einschränkungen können sich ergeben, wenn Betroffene sich nicht mit ihrem echten Namen anmelden und dieser auch nicht aus weiteren verfügbaren Informationen ableitbar ist.[61] Insbesondere bei sozialen Netzwerken wie Facebook wird es bei entsprechendem, oft jahrelangem Nutzungsverhalten regelmäßig möglich sein, aus Bildern, Nachrichten, Vorlieben und Kontakten auch dann auf die konkrete Person zu schließen, wenn diese ihren Namen nicht angegeben hat.

36 Wenn Nutzer **Daten Dritter** in ihren Profilen bereitstellen, so handelt es sich zumindest um personenbezogene Daten der Nutzer, etwa die Information über eine persönliche Beziehung zu dem Dritten. Sind Letztere ebenfalls Nutzer, so handelt es sich um Daten mit „Doppelbezug". Im Übrigen kann die Frage des Personenbezugs nicht pauschal beantwortet werden.

37 Sowohl für die Daten der Nutzer als auch für die Dritter kann sich die Frage des Personenbezugs auch ergeben, wenn **externe Stellen** auf die Daten aus Blogs, Wikis oder sozialen Netzwerken zugreifen. Hier kommt es darauf an, ob aus den jeweils verfügbaren Informationen (gegebenenfalls mit Zusatzwissen) auf den Betroffenen geschlossen werden kann.

4.3.2.2 Daten außerhalb von Nutzerprofilen

38 **Problematisch** und umstritten ist die Frage des Personenbezugs bei Daten, die außerhalb von Social Media im Internet erhoben werden. Dies lässt sich exemplarisch

---

[59] Dammann, in: Simitis, BDSG, § 3 Rn. 33; Roßnagel, in: Roßnagel, Kap. 7.9 Rn. 111; Spindler/Nink, in: Spindler/Schuster, § 11 TMG, Rn. 5b.

[60] Näher zu Konzepten von Anonymität und Pseudonymität Roßnagel/Scholz, MMR 2001, 721 ff.

[61] Das Sonderproblem, wann bei vielfach gebrauchten Namen ein Personenbezug vorliegt, wird hier vernachlässigt.

an **Social Plug-Ins** darstellen, die nicht nur von Facebook („Like-Button"), sondern auch von anderen Anbietern verwendet werden. Diese Plug-Ins werden durch beliebige Dritte in ihre Webseiten eingebunden.[62] Wird die Seite aufgerufen, so wird ein Programmcode vom Server des Social Media-Anbieters nachgeladen. Dabei erfährt der Anbieter die IP-Adresse des Nutzers und hat die Möglichkeit, auf dessen Computer einen Cookie abzulegen.[63] Dieser Cookie wiederum erlaubt die Wiedererkennung des Nutzers (wenn auch als solcher nur in pseudonymer Form) sowie die Erhebung der Ablaufumgebung des Browsers (Bildschirmauflösung, Browser Plug-Ins etc.).[64] Die mit dem Nutzungsverhalten verbundenen Statistiken (Reichweitenanalyse) stellt Facebook den einbindenden Webseitenbetreibern zur Verfügung.

39 Für die rechtliche Bewertung ist bedeutsam, dass der gesamte Prozess nicht erst dann abläuft, wenn der Besucher der Webseite auf den entsprechenden Button klickt, sondern je nach Webseitengestaltung **bereits beim Aufrufen der Webseite**. Der Social Media-Anbieter erhält also von jedermann, der die Seite besucht, die IP-Adresse; er kann überdies Cookies anlegen. Beim **Klick auf den Button** erfolgt eine weitere Datenübermittlung, die dann – im Fall von Facebook – dazu führt, dass die entsprechende Information (dem Nutzer „gefällt" eine Webseite) in dessen Profil angezeigt wird.

40 Ob und inwieweit auf diesen Vorgang Datenschutzrecht anzuwenden ist, hängt im Wesentlichen von dem **Personenbezug** der IP-Adresse und des Cookies ab.[65] Insoweit ist zu **differenzieren**: Ist der Nutzer während des Webseitenbesuchs beim Social Media-Dienst angemeldet, so kann dessen Anbieter IP-Adresse und Cookie ohne weiteres zuordnen. Für ausgeloggte Nutzer besteht in zwei Fällen Personenbezug: Erstens, wenn diese innerhalb derselben Internet-Session (das heißt mit derselben dynamischen IP-Adresse) den Social Media-Dienst nutzen, unabhängig davon, ob dies vor oder nach dem Besuch der anderen Webseite erfolgt; zweitens, wenn ihr Browser – wie regelmäßig – den durch Facebook gesetzten Cookie dauerhaft speichert, weil dieser auch sessionübergreifend eine Zuordnung ermöglicht.

---

[62] S. zu den technischen Aspekten und der aufsichtsbehördlichen Sicht ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf; zu den Hintergründen auch Piltz, CR 2011, 657 ff.; speziell zur Funktionsweise und rechtlichen Bewertung der Cookie-Verwendung durch Facebook s. den Prüfbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 2.11.2011, http://www.datenschutz-hamburg.de/uploads/media/Pruefbericht_Facebook-Cookies.pdf.

[63] Im Fall von Facebook erfolgt dies nur, wenn die Plug-Ins aktiv angeklickt werden, s. ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, 7 f.

[64] Die Ablaufumgebung kann ein datenschutzrechtliches Problem darstellen, weil sie meist hochgradig individuell ist und deshalb schon als solche die Zuordnung einer eindeutigen Identität ermöglicht. In einem Test der Electronic Frontier Foundation (EFF) mit 47.000 Computern gelang dies in 83,6 % aller Browserkonfigurationen, s. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,782939,00.html; dazu Voigt, in: Taeger, Law as a Service (LaaS), S. 157 ff.

[65] Zu den weiteren Anforderungen an den Einsatz von Cookies s. Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 137 ff.

41 Problematisch sind damit nur die **Fallgruppe der Nicht-Nutzer** des Social Media-Dienstes sowie die **derjenigen Nutzer**, die sich innerhalb derselben Internet-Session **nicht beim Social Media-Dienst einloggen** und zusätzlich über ihre Browser-Konfiguration regelmäßig **Cookies löschen**. In diesem Fall ist eine Session-übergreifende Identifizierung mangels Cookie nicht möglich, und der Anbieter hat zur Verknüpfung nur die Information der IP-Adresse. (Nur) in diesen beiden Fallgruppen kommt es folglich auf die Frage an, ob IP-Adressen „an sich" personenbezogene Daten sind. Da die Anbieter von Social Media regelmäßig keine Möglichkeit haben, rechtmäßig an die durch den Access-Provider des Nutzers vorgenommene Zuordnung der IP-Adresse zu gelangen, kann man einen Personenbezug nicht pauschal bejahen.[66] Es ist aber jeweils im Einzelfall sorgfältig zu analysieren, ob aufgrund des Vorliegens von statischen IP-Adressen oder verfügbaren **Webtracking-Werkzeugen** nicht doch so viel Zusatzwissen des Anbieters verfügbar ist, dass man die Personenbeziehbarkeit annehmen muss. Ob daneben für den Betreiber der einbindenden Webseiten Personenbezug besteht, ist separat zu beurteilen und hängt maßgeblich davon ab, ob sie ihre Kunden registrieren.

4.3.3 Verantwortliche Stellen

42 Verantwortliche Stelle ist nach § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten **für sich selbst erhebt, verarbeitet oder nutzt** oder dies durch andere im Auftrag vornehmen lässt. Im Rahmen einer solchen Auftragsdatenverarbeitung wird der Auftragnehmer dem Auftraggeber „zugerechnet", sodass eine Datenweitergabe, wenn die Anforderungen von § 11 BDSG eingehalten werden, keiner besonderen Legitimation bedarf. Bei diesen datenschutzrechtlichen Bestimmungen handelt es sich um eine selbstständige Regelung zur Verantwortlichkeit, sodass die Haftungsprivilegierungen der **§§ 7 ff. TMG nicht anwendbar** sind. Ein Widerspruch zu Art. 14 der E-Commerce Richtlinie besteht nicht, weil diese in Art. 1 Abs. 5 lit. b die Datenschutzrichtlinie ausdrücklich unberührt lässt.[67]

4.3.3.1 Anbieter von Social Media

43 **Anbieter** von Social Media verarbeiten in aller Regel die Daten der Nutzer und Dritter **„für sich selbst" i. S. v. § 3 Abs. 7 BDSG**. Nur dann, wenn ein Anbieter sich tatsächlich auf eine völlig neutrale Rolle beschränkt und die Daten auch

[66] Spindler/Nink, in: Spindler/Schuster, § 11 TMG, Rn. 5b; näher Dammann, in: Simitis, BDSG, § 3 Rn. 29 ff.; Martini/Fritzsche, VerwArch 2013, 449 (455 ff.); a. A. AG Berlin-Mitte, DuD 2007, 856; LG Frankenthal, MMR 2008, 687; Pahlen-Brandt, DuD 2008, 34 ff.; tendenziell auch Weichert, in: Däubler et al., BDSG, § 3 Rn. 13 f.; s. a. die Zusammenfassung der Diskussion bei Bizer/Hornung, in: Roßnagel, Recht der Telemediendienste, § 12 TMG, Rn. 42 ff. und Spindler, Gutachten F zum 69. DJT, S. 70 ff.

[67] S. Spindler, Gutachten F zum 69. DJT, S. 82 ff.

nicht anderweitig nutzt, käme eine Auftragsdatenverarbeitung für die Nutzer überhaupt in Betracht. Dies ist aber bei allen gängigen Anbietern nicht der Fall, weil diese erhebliche **eigene wirtschaftliche Interessen** verfolgen, im Bereich personalisierter Werbung die Verarbeitungsprozesse vollkommen selbstständig steuern und regelmäßig auch Daten an Kooperationspartner weitergeben.[68]

Aufgrund dieser Eigeninteressen ist eine datenschutzrechtliche (ebenso wie eine wettbewerbsrechtliche)[69] Verantwortlichkeit **auch dort** zu bejahen, wo ein konkreter Verarbeitungsvorgang **durch den Nutzer angestoßen** wird. Ob dieser selbst unter das Datenschutzrecht fällt, ist belanglos.[70] Eine Auftragsdatenverarbeitung scheitert in der Praxis überdies regelmäßig zusätzlich daran, dass der Auftragsdatenverarbeiter nach geltendem Recht seinen Sitz nicht in Drittstaaten haben darf. In diesem Fall ist der Auftragnehmer vielmehr nach der Definition des § 3 Abs. 8 Satz 2 und 3 BDSG „Dritter" und eine Weitergabe der Daten an ihn gemäß § 3 Abs. 4 Nr. 1 BDSG eine Übermittlung, die einer entsprechenden Verarbeitungsgrundlage bedarf. **44**

4.3.3.2 Nutzer als verantwortliche Stellen?

Social Media sind auf die Mitwirkung der Nutzer und darauf angelegt, dass diese unterschiedlichste Informationen bereitstellen, abrufen und untereinander austauschen. Auch die verfügbaren personenbezogenen Daten sind ganz überwiegend nicht durch die Anbieter, sondern **durch die Nutzer bereitgestellt** worden. Damit stellt sich die Frage, inwieweit letztere neben den Anbietern datenschutzrechtlich verantwortlich sind. **45**

Das geltende Datenschutzrecht nimmt Datenverarbeitungen durch nichtöffentliche Stellen gemäß § 1 Abs. 2 Nr. 3 BDSG vom Anwendungsbereich aus, wenn die Erhebung, Verarbeitung oder Nutzung der Daten **„ausschließlich für persönliche oder familiäre Tätigkeiten"** erfolgt. Aufgrund der persönlichkeitsrechtlichen Gefährdungen durch private Datenverarbeiter und in völkerrechtsfreundlicher Auslegung[71] ist dies **eng zu verstehen**.[72] Sofern es sich also um ausschließlich geschäftlich **46**

---

[68] Das wird grundsätzlich übersehen von Moser, in: Taeger, Die Welt im Netz, S. 595 ff., die explizit – und unzutreffend – davon ausgeht, dass die Anbieter die Daten „nicht für eigene Zwecke verarbeiten" (ebd., 596). Zutreffend Spindler, Gutachten F zum 69. DJT, S. 81 m. w. N.; s. a. OLG Hamburg, NJW-RR 2011, 1611 (1612) für den vergleichbaren Fall eines Forenbetreibers; gegen eine Auftragsdatenverarbeitung auch Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 351.

[69] Für den Fall von Facebooks „Friend Finder" (dazu z. B. Meyer, in: Taeger, Die Welt im Netz, S. 536 f.; ders., K&R 2012, 309 ff.) haben das LG Berlin (ZD 2012, 276, 277) und das KG Berlin (DuD 2014, 417, 418 f.) insoweit zu Recht eine gemeinsame Verantwortlichkeit bejaht und in dem Versenden von Einladungen deshalb eine Werbung durch Facebook i. S. v.§ 7 Abs. 2 Nr. 3 UWG gesehen; ebenso allgemein für Empfehlungs-E-Mails BGH, GRUR 2013, 1259.

[70] S. Schneider, in: BeckOK-BDSG, Syst. B Rn. 57; zur Verantwortlichkeit der Nutzer unten 4.3.3.2.

[71] Die durch die Bundesrepublik ratifizierte Datenschutzkonvention des Europarats (BGBl. II 1985, 538) enthält keine entsprechende Ausnahme, s. Dammann, in: Simitis, BDSG, § 1 Rn. 148.

[72] S. Simitis, in: Simitis, BDSG, § 1 Rn. 147 ff. Art. 2 II d) DS-GVO-E behält die Ausnahme weitgehend wortgleich bei.

orientierte Social Media handelt (beispielsweise Portale wie XING oder LinkedIn) oder im Einzelfall eine solche Orientierung des Nutzers besteht, ist dieser vom Datenschutzrecht erfasst. Dasselbe gilt für institutionelle Nutzer wie Unternehmen oder Behörden, die Social Media im Rahmen ihrer Geschäftsstrategie einsetzen. Ein Beispiel sind die „Fanseiten" von Facebook. Für die eigene Datenverarbeitung besteht hier zweifellos eine Verantwortlichkeit, während umstritten ist, ob die institutionellen Nutzer auch für die begleitenden Datenverarbeitungsprozesse der Anbieter verantwortlich sind.[73]

47 Der Europäische Gerichtshof hat Art. 3 Abs. 2 DSRL (der durch § 1 Abs. 2 Nr. 3 BDSG umgesetzt wird) überdies für **„offensichtlich" unanwendbar** erklärt, wenn die Verarbeitung personenbezogener Daten „in deren **Veröffentlichung im Internet** besteht, sodass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden".[74] Wendet man dieses Kriterium auf Social Media an, so greift die Ausnahme der ausschließlich persönlichen oder familiären Zwecke nicht ein, wenn die bereitgestellten Informationen nicht durch Zugriffsmechanismen geschützt sind. Dies ist bei Bewertungsportalen oder Plattformen zur Verbreitung von Videos und Bildern vielfach der Fall. Für die praktisch bedeutsame Gruppe der sozialen Netzwerke muss man maßgeblich danach differenzieren, welche **Privatsphäreneinstellungen** der Nutzer vorgenommen hat. Sind die verwendeten personenbezogenen Daten für jeden Internetnutzer auch ohne Anmeldung bei dem jeweiligen Anbieter abrufbar, so kann sich der Nutzer auf die Ausnahme nicht berufen. Dasselbe muss zumindest bei weltweiten, jedermann offenstehenden Plattformen (und schon weit unterhalb von Nutzerzahlen wie bei Facebook) gelten, wenn die Daten allen anderen Nutzern verfügbar gemacht werden. Hier greift eine gemeinschaftliche Verantwortlichkeit mit dem Anbieter.

48 Sofern die Daten **nur für einen begrenzten Kreis** von „Freunden" im hergebrachten Sinn des Wortes verfügbar sind, ist dagegen eine ausschließlich persönliche Zwecksetzung zu bejahen,[75] und der Anbieter ist allein verantwortlich. Teilweise wird vertreten, eine Verantwortlichkeit der Nutzer bestehe auch in dieser Situation, wenn die Daten (wie meist) durch den Plattformbetreiber zu Analyse- und Werbezwecken verwendet werden und der Nutzer dies wissentlich in Kauf nehme.[76] § 1

---

[73] Dafür v. a. das ULD, s. https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf; a. A. (Vorschlag eines abgestuften Verantwortungssystems) Hoffmann et al., ZD 2013, 122.

[74] EuGH, MMR 2004, 95 (96, Rn. 46 f.) – Lindqvist/Schweden; EuZW 2009, 108 (109 f., Rn. 43 f.) – Satakunnan und Satamedia.

[75] Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163, S. 6 f.; Helberger/van Hoboken, CRi 2010, 101 (103) [mit Fokus auf die Fälle, in denen soviele Kontakte bestehen, dass die Ausnahme nicht greift]; Dix, in: Simitis, BDSG, § 35 Rn. 8; Hornung/Hofmann, JZ 2013, 163 (167 f.).

[76] Jandt/Roßnagel, ZD 2011, 160 (161 f.); dies., in: Schenk et al., Digitale Privatsphäre, S. 349; ebenso Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Soziale Netzwerke", S. 12.

Abs. 2 Nr. 3 BDSG stellt aber nicht auf die weitere Zwecksetzung durch andere, sondern auf den Zweck ab, den der Nutzer verfolgt. Ob die weitere Datenverwendung durch den Anbieter zulässig ist, ist davon losgelöst zu beurteilen.

Das **Hauptproblem** ist nach geltendem Recht, dass es **keine abgestuften Pflichten** des Verantwortlichen gibt: Bejaht man die Anwendung auf die Nutzer, so greifen sämtliche Pflichten des Datenschutzrechts. Für diese fundamentale Frage erscheint das reine Zählen von Kontakten grundsätzlich wenig geeignet. Allerdings bieten andere Kriterien wie die Qualität der bereitgestellten Daten ebenfalls keine Rechtssicherheit für den Nutzer. Die Verantwortlichkeit Privater sollte deshalb differenziert gesetzlich geregelt werden.[77] **49**

4.3.3.3 Dritte

Im Fall von **Social Plug-Ins**[78] stellt sich die Frage, ob der Social Media-Anbieter, der einbindende Webseiten-Betreiber oder beide gemeinsam verantwortliche Stellen sind. Aufgrund des Interesses des Webseiten-Betreibers an der Reichweitenanalyse und dessen Entscheidungsgewalt über die Einbindung in die Webseite ließe sich vertreten, dass er allein verantwortlich und der Social Media-Anbieter nur als Auftragsdatenverarbeiter tätig wird. Dies scheitert aber regelmäßig (und ganz sicher im Fall von Facebook) daran, dass der Anbieter die Daten zumindest auch „für sich selbst" verwendet[79] und überdies die Anforderungen an das Vorliegen einer Auftragsdatenverarbeitung („Datenherrschaft") nicht vorliegen. Mit der Annahme eines Auftragsverhältnisses wäre letztlich auch nichts gewonnen, weil die Anforderungen von **§ 11 BDSG** im Verhältnis zu weltweit operierenden Social Media-Anbietern **kaum umsetzbar** sind. Soweit teilweise umgekehrt angenommen wird, allein diese Anbieter seien verantwortliche Stellen, da der Webseiten-Betreiber die Daten gar nicht erhebe,[80] so vernachlässigt dies, dass erst die Einbindung des Plug-Ins den gesamten Vorgang ermöglicht und der Webseiten-Betreiber ein eigenes wirtschaftliches Interesse verfolgt.[81] **50**

Soweit für beide Seiten ein Personenbezug besteht, sind folglich **beide** auch **verantwortliche Stellen** i. S. v. § 3 Abs. 7 BDSG.[82] Der Webseitenbetreiber hat allerdings die Möglichkeit, durch eine entsprechende Gestaltung des Social Plug-Ins **51**

---

[77] Zu Überlegungen de lege ferenda und in der DS-GVO-E s. Hornung, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 133 ff.

[78] S. zum technischen Ablauf oben, Rn. 38 ff.

[79] Dies ist ein wesentlicher Unterschied gegenüber der sonstigen Einbindung von Inhalten Dritter in Webseiten.

[80] So Piltz, CR 2011, 657 (662) [der allerdings eine zivilrechtliche Störerhaftung für möglich hält]; Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, S. 128 f.; tendenziell auch Voigt/Alich, NJW 2011, 3541 (3543 f.).

[81] Ernst, NJOZ 2010, 1917 (1918); Maisch, AnwZert ITR 19/2010, Anm. 2; Höppner, in: Taeger, Die Welt im Netz, S. 478; zum Problem auch Meyer, ebd., S. 537 ff.

[82] In diese Richtung auch Polenz, VuR 2012, 207 (210 ff.).

(„**Zwei-Klick-Lösung**“) diesen rechtskonform einzusetzen. Dabei werden die IP-Adresse und die Nummer eines etwaigen Cookies nicht schon beim bloßen Besuch der Webseite an den Social Media-Anbieter übermittelt, sondern erst nach einer Freischaltung durch den Besucher (erster Klick), bevor mit einem weiteren Klick gegebenenfalls eine inhaltliche Aussage wie „gefällt mir“ verbunden wird.[83] In diesem Fall wird der Übermittlungsvorgang letztlich durch den Nutzer, nicht durch den einbindenden Webseitenbetreiber initiiert.

52 Ein weiterer Zweifelsfall der Verantwortlichkeit Dritter ist der Betrieb so genannter **Fanpages** in sozialen Netzwerken wie Facebook. Die Betreiber sind hier natürlich für ihre eigenen Datenverarbeitungsprozesse verantwortlich. Nach Ansicht des VG Schleswig-Holstein besteht jedoch keine Verantwortlichkeit hinsichtlich der Datenverwendung durch Facebook, da kein Einfluss auf das Angebot genommen werden könne und auch kein Zugriff auf die personenbezogenen Daten bestehe.[84] Die Argumentation ist zumindest angreifbar: Es ist zwar richtig, wie das Gericht feststellt, dass sich die Entscheidung der Fanpage-Betreiber „auf die Annahme eines für sie unabänderlichen Angebots [beschränkt], die Fanpage einzurichten und mit Inhalten zu füllen oder nicht“.[85] Genau in dieser Entscheidung kann man aber eben mit guten Gründen eine **Entscheidung über Zwecke und Mittel der Datenverarbeitung** sehen, die durch den Anbieter vorgenommen wird.[86]

4.3.4 Grundlage und Zulässigkeit der Verarbeitung

53 Sowohl nach § 4 Abs. 1 BDSG als auch nach § 12 Abs. 1 TMG bedarf es für jeden Umgang mit personenbezogenen Daten einer entsprechenden Grundlage (Verbotsprinzip), nämlich einer **Rechtsnorm oder einer Einwilligung**. Entsprechend der abgestuften datenschutzrechtlichen Regelungssystematik ist insoweit zu unterscheiden. Soweit es um die Bestands- und Nutzungsdaten des Social Media-Angebots selbst geht, verlangt § 12 Abs. 1 TMG eine Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht. Dies wird durch § 14 und § 15 TMG,[87] nicht aber durch Befugnisnormen des Bundesdatenschutzgesetzes erfüllt. **§ 12 Abs. 1 TMG versperrt** also insbesondere den Rückgriff auf die **§§ 28 ff. BDSG**.

---

[83] S. http://www.heise.de/-1333879.html; s. a. Piltz, CR 2011, 657 (663). Weitere Rechtsfragen des Like-Buttons werden hier ausgeklammert; s. z. B. zum Wettbewerbsrecht LG Hamburg, MMR 2013, 250.

[84] VG Schleswig-Holstein, ZD 2014, 51 mit abl. Anm. Karg; zustimmend Härting, K&R 2013, 828 ff.

[85] VG Schleswig-Holstein, ZD 2014, 51, 54.

[86] In diese Richtung Polenz, VuR 2012, 207 (211); für eine zumindest partielle gemeinsame Verantwortlichkeit auch Martini/Fritzsche, VerwArch 2013, 449 (462 ff.); s. a. Karg, ZD 2014, 51 ff.; Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 109 ff.

[87] S. zur Anwendung auf Social Media Karg/Fahl, K&R 2011, 453 (457 f.); Martini/Fritzsche, VerwArch 2013, 449 (455 ff.).

4.3.4.1 Bestands- und Nutzungsdaten

Gemäß **§ 14 Abs. 1 TMG** darf der Social Media-Anbieter personenbezogene Daten eines Nutzers erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung des Nutzungsvertrags erforderlich sind (**Bestandsdaten**). Hierzu zählen je nach Angebot der bei der Anmeldung erhobene Name, E-Mail Adresse, Passwort, Geburtsdatum oder Zahlungsinformationen. Ob der Datenumgang zulässig ist, bestimmt sich nach dem **Erforderlichkeitsprinzip**; bei kostenlosen Angeboten dürfen beispielsweise keine Bankkontodaten erhoben werden. **54**

§ 15 Abs. 1 Satz 1 TMG gestattet dem Anbieter, personenbezogene Daten eines Nutzers zu erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Social Media zu ermöglichen und abzurechnen (**Nutzungsdaten**).[88] Nach § 15 Abs. 1 Satz 2 TMG können dies insbesondere Identifikationsmerkmale (also etwa PIN und TAN oder die IP-Adresse), Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und über die in Anspruch genommenen Dienste sein. Auch hier gilt das Erforderlichkeitsprinzip,[89] das beispielsweise die Verwendung von Abrechnungsdaten über den konkreten Nutzungsvorgang hinaus gestattet (§ 15 Abs. 4 Satz 1 TMG). Bedeutsam ist daneben die Regelung zur Datenverarbeitung für Zwecke der **Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung** der Telemedien. Gemäß § 15 Abs. 3 TMG dürfen insoweit Nutzungsprofile erstellt werden, aber nur unter zwei Voraussetzungen: Erstens sind Pseudonyme zu verwenden, die nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen, zweitens darf der Nutzer nicht widersprochen haben, und er ist auf dieses Recht hinzuweisen.[90] **55**

Im Übrigen enthält das Telemediengesetz keine Grundlage für die Datenverarbeitung zu Werbezwecken; insbesondere ist diese bei kostenfreien Angeboten zwar gegebenenfalls ökonomisch, nicht aber rechtlich „erforderlich“ i. S. v. § 15 Abs. 1 Satz 1 TMG zur Inanspruchnahme von Social Media.[91] Etwaige gesetzliche Grundlagen außerhalb des Telemediengesetzes beziehen sich jedenfalls nicht ausdrücklich auf Telemedien und werden deshalb durch § 12 Abs. 1 TMG gesperrt. Für die Verwendung von Bestands- und Nutzungsdaten **zu Werbezwecken** ist damit regelmäßig eine **Einwilligung** erforderlich.[92] **56**

---

[88] Die Abgrenzung zwischen Bestands- und Nutzungsdaten ist nicht immer eindeutig; s. am Beispiel von Social Media Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 356 ff.

[89] S. z. B. Lerch et al., MMR 2010, 454 (456).

[90] Zur Anwendung von § 15 Abs. 3 TMG auf Social Media s. Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, 2012, S. 119 ff.; Polenz, VuR 2012, 207 (212).

[91] Martini/Fritzsche, VerwArch 2013, 449, 457 f.

[92] S. a. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Orientierungshilfe „Soziale Netzwerke“, S. 32); zur Einwilligung s. u. 4.3.4.4.

4.3.4.2 Inhaltsdaten der Nutzer

57 Stellt ein Nutzer von Social Media innerhalb der Anwendung Informationen über sich bereit, handelt es sich um Inhaltsdaten, die nach zutreffender Ansicht **nicht** durch den **Telemediendatenschutz** erfasst werden.[93] Die Zulässigkeit der Erhebung und Verwendung der Daten bestimmt sich damit nach § 28 und § 29 BDSG.

58 In der Literatur wird oftmals pauschal vertreten, Social Media fielen unter **§ 29 BDSG**,[94] auf den der Bundesgerichtshof die Datenverwendung in der Spickmich-Entscheidung gestützt hat.[95] Bei derartigen Bewertungsplattformen stellen die – oftmals anonymen – Nutzer allerdings hauptsächlich Daten über Dritte bereit, und der Zweck der Anwendung besteht (und erschöpft sich) in der Übermittlung an andere Nutzer. Geben Nutzer hingegen auf der Basis eines Nutzungsvertrags[96] Daten über sich selbst preis, so spricht zunächst einiges dafür, **§ 28 Abs. 1 Satz 1 Nr. 1 BDSG** anzuwenden, wonach der Umgang mit den Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Die **Abgrenzung** zwischen den beiden Normen erfolgt danach, ob der Verantwortliche mit der Übermittlung einen eigenen Geschäftszweck verfolgt und diese damit Mittel zur Erreichung eines von der Übermittlung zu trennenden Zwecks ist (dann § 28 BDSG) oder die Übermittlung selbst der angestrebte Zweck ist (dann § 29 BDSG).[97]

59 Werden Daten durch den Anbieter nur selbst verarbeitet und nicht an Dritte übermittelt (beispielsweise die heftig umstrittenen biometrischen Gesichtsdaten in manchen sozialen Netzwerken),[98] so muss sich dies folglich an § 28 BDSG messen lassen. Dasselbe gilt, wenn der Anbieter weitere Zwecke verfolgt. Dies kann man bei systematischen Übermittlungen mit dem Ziel der Datenverknüpfung, um personalisierte Werbung zu ermöglichen, durchaus bejahen.[99] Ist § 28 Abs. 1 Satz 1 Nr. 1 BDSG einschlägig, so sind im Zuge der Vertragsanbahnung, Durchführung und Beendigung alle Verarbeitungsschritte zulässig, die jeweils tatsächlich erforderlich sind. Insbesondere bei Social Media mit **weiten und volatilen Verwendungszwecken**

---

[93] Zur Regelungssystematik s. oben 4.2.2.
[94] Schüßler, in: Taeger, Digitale Evolution, S. 242 ff.; Ehmann, in: Simitis, BDSG, § 29 Rn. 96; Taeger, in: Gabel-Taeger, BDSG, § 28 Rn. 37.
[95] BGHZ 181, 328 (335 ff.).
[96] S. Kap. 3; zum Problem des Vertragsschlusses bei Minderjährigen s. u. Rn. 78 ff.
[97] S. Ehmann, in: Simitis, BDSG, § 29 Rn. 20 ff.; BGHZ 181, 328 (336); ähnlich Gola/Schomerus, BDSG, § 28 Rn. 4, wo maßgeblich auf das Interesse der verantwortlichen Stelle rekurriert wird.
[98] Dazu Karg, HFR 2012, 120 (127 ff.); Caspar, DuD 2013, 767 (769 f.); zur Verarbeitung von Bildern auch Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 365 ff.
[99] S. Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 358 f.; anders für den Fall nichtpersonalisierter Werbeanzeigen BGHZ 181, 328 (336).

wird der Datenumgang dabei **regelmäßig zulässig** sein.[100] De lege lata gibt es praktisch keine Grenzen für derart weite Zweckbestimmungen, auch wenn diese drohen, das Erforderlichkeitsprinzip ad absurdum zu führen.

60 Erschöpft sich der Zweck des Datenumgangs in der **Übermittlung an Dritte**, so ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG zulässig, wenn kein Grund zu der Annahme besteht, dass der Nutzer ein **schutzwürdiges Interesse an dem Ausschluss** dieser Vorgänge hat.[101] Die Übermittlung der Daten ist nach § 29 Abs. 2 Satz 1 BDSG zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Grundproblem von § 29 BDSG ist, dass er nach herkömmlichem Verständnis eine **Einzelfallprüfung** durch die verantwortliche Stelle voraussetzt,[102] die im Massengeschäft von Social Media **nicht zu leisten** ist. Allerdings kann für die Inhaltsdaten des Nutzers mittelbar auf den Nutzungsvertrag abgestellt werden, der ja die Rechtsbeziehungen der Parteien regeln soll. Stellt der Nutzer die Daten selbst bereit (und kontrolliert er gegebenenfalls über Privatsphäreneinstellungen ihre Weitergabe), so wird überdies kein Grund zu der Annahme bestehen, dass er ein entgegenstehendes Interesse hat. Dieses ist allerdings sorgfältig zu prüfen, wenn die Daten aus anderen Quellen stammen oder aus den bereitgestellten Daten im Wege weitergehender Analysen zusätzliche Informationen gewonnen werden. Insbesondere bei sensiblen Daten oder Daten Minderjähriger kann die Abwägung nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG auch zugunsten des Nutzers ausfallen.

61 **Einschränkungen** bestehen schließlich nach § 28 Abs. 3 bis Abs. 3b BDSG (der gemäß § 29 Abs. 1 Satz 2 BDSG auch in dessen Anwendungsbereich gilt) für die Verarbeitung und Nutzung **zu Werbezwecken**. Soweit nicht das so genannte Listenprivileg nach § 28 Abs. 3 Satz 2 BDSG greift, ist gemäß § 28 Abs. 3 Satz 1 BDSG stets eine Einwilligung erforderlich, die nach § 28 Abs. 3a BDSG auch elektronisch erteilt werden kann.[103]

4.3.4.3 Inhaltsdaten Dritter

62 Lässt sich die Zulässigkeit im Verhältnis zwischen Anbieter und Nutzer von Social Media mit dem geltenden Recht noch relativ gut in den Griff kriegen, so führt die **Verarbeitung von Daten Dritter** zu **erheblichen Friktionen**, weil weder

---

[100] Das gilt beispielsweise für soziale Netzwerke, deren Zweck man kaum enger als „Kommunikation mit anderen über das Internet“ umschreiben kann; für die Anwendung auf Social Bookmarking-Systeme s. Lerch et al., MMR 2010, 454 (455 ff.).

[101] S. zur Anwendung auf den Like-Button von Facebook Piltz, CR 2011, 657 (661 f.).

[102] Das gilt insbesondere für die glaubhafte Darlegung des berechtigten Interesses nach § 29 Abs. 2 Satz 1 BDSG, s. Ehmann, in: Simitis, BDSG, § 29 Rn. 224 ff. m. w. N.; Weichert, in: Däubler et al., BDSG, § 29 Rn. 49b ff.; verlangt wird üblicherweise z. B. die Identitätsfeststellung der anfragenden Stelle, s. ebd., Rn. 49c.

[103] S. noch unten 4.3.4.4.

das Bundesdatenschutzgesetz[104] noch der Telemediendatenschutz[105] auf derartige Dreiecksverhältnisse eingestellt sind.

63 **Erhebung und Verwendung durch Anbieter** Wenn Nutzer Daten über Dritte bereitstellen (beispielsweise als personenbezogene Bewertungen auf entsprechenden Plattformen, aber auch in beliebiger Form in sozialen Netzwerken), so kann der Datenumgang durch den Anbieter nur dann über § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt werden, wenn diese **Dritten ebenfalls einen Nutzungsvertrag** mit demselben Anbieter haben. Dies ist beispielsweise in sozialen Netzwerken häufig, allerdings nicht immer der Fall.

64 **Im Übrigen** bleibt hier – jenseits der Verwendung allgemein zugänglicher Daten (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG) – nur der Weg über § 28 Abs. 1 Satz 1 Nr. 2 BDSG[106] oder über § 29 BDSG. In der nach beiden Varianten erforderlichen **Abwägung** kann aber, anders als bei den Inhaltsdaten der Nutzer,[107] hinsichtlich der unbeteiligten Dritten weder mit dem Abschluss eines Nutzungsvertrags, noch mit der Einflussmöglichkeit durch Privatsphäreneinstellungen argumentiert werden.

65 Die Anwendung des regelmäßig **einschlägigen § 29 BDSG**[108] führt für die Anbieter zu zwei Problemen. Zum einen müssten sie bei der Abwägung im Rahmen der Erhebung, Speicherung, Veränderung oder Nutzung (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG) und der Übermittlung (§ 29 Abs. 2 Satz 1 Nr. 2 BDSG) **Einzelfallprüfungen** vornehmen – wenn Nutzer beispielsweise sensible Daten, ehrabschneidende Tatsachen oder Unwahrheiten über Dritte verbreiten, wird es nahe liegen, dass deren Interessen überwiegen. Zum anderen müsste im Rahmen der Übermittlung gemäß § 29 Abs. 2 Satz 1 Nr. 1 BDSG **jeder (!) Dritte**, an den die Daten übermittelt werden (also jeder weitere Nutzer, der diese wahrnimmt), gegenüber dem Anbieter ein **berechtigtes Interesse an der Kenntnis glaubhaft darlegen**; der Anbieter müsste die Darlegung nach § 29 Abs. 2 Satz 3 BDSG aufzeichnen. Da beides in der Praxis nicht erfolgt (und auch nicht durchführbar ist), wäre die praktisch allgemein übliche Speicherung und Übermittlung personenbezogenen Daten Dritter in Social Media damit rechtswidrig.[109]

66 Der Bundesgerichtshof hat diese Rechtsfolge in der **Spickmich-Entscheidung** durch eine **verfassungskonforme Auslegung** vermieden, die die datenschutzrechtliche Bewertung im Ergebnis stark an hergebrachte äußerungsrechtliche Kriterien bindet.[110] Im Rahmen von § 29 Abs. 1 Satz 1 Nr. 1 BDSG sind danach das Recht

---

[104] Ehmann, in: Simitis, BDSG, § 29 Rn. 96.
[105] Dazu schon Jandt, MMR 2006, 652.
[106] Dafür Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 117 f.
[107] S. o. 4.3.4.2.
[108] S. zur Abgrenzung oben 4.3.4.2; a. A. offenbar Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 117, wonach „ein großer Teil" der Datenverarbeitungen bei Social Media über § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt werden können soll; § 29 BDSG wird freilich mit keinem Wort erwähnt.
[109] Dies wird vom BGH durchaus gesehen, s. BGHZ 181, 328 (343); für Bewertungsportale Weigl, Meinungsfreiheit contra Persönlichkeitsschutz am Beispiel von Web 2.0-Applikationen, S. 223.
[110] BGHZ 181, 328 (336 ff.); s. näher zu diesem Urteil Müller-Terpitz, Kap. 6 Rn. 41 f.

auf informationelle Selbstbestimmung und die Kommunikationsfreiheiten nach Art. 5 Abs. 1 GG gegeneinander abzuwägen; hierbei komme es auf die Sensibilität der Daten, ihre Zuordnung zu verschiedenen Persönlichkeitssphären sowie die Unterscheidung zwischen Meinungsäußerungen und Tatsachengehalten an. Unsachliche Schmähkritik und Formalbeleidigungen seien unzulässig. Die Verbreitung über das Internet sei zu berücksichtigen, führe aber ebensowenig per se zum Überwiegen der Betroffeneninteressen wie eine etwaige Anonymität des Äußernden. Die Darlegung und Aufzeichnung eines Interesses durch Empfänger seien entgegen § 29 Abs. 2 Satz 1 Nr. 1 und Satz 3 BDSG nicht erforderlich, weil ansonsten die Meinungsäußerung der Bewertenden unzulässig eingeschränkt würde.

Die Lösung des Bundesgerichtshofs eröffnet – jenseits der Frage, ob die gefundene Abwägungsentscheidung in allen Einzelheiten überzeugt[111] – im Ergebnis einen Abwägungsmechanismus, mit dem die Konflikte der Verarbeitung von Daten Dritter bearbeitet werden können. **Methodisch** ist die verfassungskonforme Auslegung für § 29 Abs. 2 Satz 1 Nr. 1 und Satz 3 BDSG allerdings angesichts des klaren Wortlauts **nicht haltbar**.[112] Datenschutz- und Äußerungsrecht sind an dieser Stelle nicht hinreichend aufeinander abgestimmt.[113] Das Medienprivileg des § 41 BDSG ist nur teilweise zur Konfliktvermeidung geeignet.[114] An dieser Stelle wird besonders deutlich, dass das geltende **Datenschutzrecht** dringend an die Besonderheiten des Internets und von Social Media **angepasst werden muss**. **67**

Erhebung und Verwendung durch die Nutzer Soweit die Nutzer von Social Media selbst unter das Datenschutzrecht fallen,[115] benötigen sie gemäß § 4 Abs. 1 BDSG **68**

[111] Neben einer stärkeren Gewichtung der Verschiebung von der Schulhof- zur Internetöffentlichkeit lässt sich insbesondere kritisieren, dass das konkrete Angebot keinerlei Identifizierung der Bewertenden bereithielt. Dabei ist weniger die Anonymität nach außen das Problem, sondern die Tatsache, dass nicht nur Schüler eines konkreten Lehrers, sondern auch beliebige Dritte unkontrolliert Bewertungen abgeben können. S. zur Kritik an der Entscheidung und zur weiteren Diskussion Kaiser, NVwZ 2009, 1474; Gounalakis/Klein, NJW 2010, 566; Köhler, Persönlichkeitsrechte im Social Web – verlorene Grundrechte?; Weigl, Meinungsfreiheit contra Persönlichkeitsschutz am Beispiel von Web 2.0-Applikationen, v. a. S. 221 ff., 227 ff.; Kamp, Bewertungsportale (danach soll das BDSG Bewertungsportale überhaupt nicht erfassen, s. S. 97 ff.; ebenso Wilkat, Bewertungsportale im Internet, S. 171 ff.); Lauber-Rönsberg, in: Taeger, Law as a Service (LaaS), S. 181 ff.; zur Übertragung auf Arztbewertungsportale s. Lacher, Rechtliche Grenzen der Kommunikation über ärztliche Leistungen, S. 117 ff. (auch zu Gestaltungsanforderungen); zu den konfligierenden Interessen und der Abwägung auch v. Coelln, in: Detterbeck et al., FS Bethge, S. 274 ff.

[112] Krit. z. B. Taeger, in: Taeger/Gabel, BDSG, § 28 Rn. 37; v. Coelln, in: Detterbeck et al., FS Bethge, S. 287 ff. erwägt eine verfassungskonforme Auslegung unter Verweis auf andere Fälle, in denen eine Einzelfallprüfung ebenfalls nicht erfolge (v. a. Kreditauskunfteien); im Ergebnis spreche aber viel dafür, dass ein Verstoß gegen §§ 4 Abs. 1, 29 Abs. 2 BDSG vorliege.

[113] Die Instanzgerichte hatten in Sachen Spickmich das Datenschutzrecht nur am Rande behandelt, s. dazu Peifer/Kamp, ZUM 2009, 185 ff.; völlig ignoriert wird diese Materie auch von Köhler, Persönlichkeitsrechte im Social Web – verlorene Grundrechte?.

[114] Der BGH hat die Anwendung von § 41 BDSG auf die reine Sammlung und Weitergabe personenbezogener Bewertungen zu Recht abgelehnt, s. BGHZ 181, 328 (334 f.); näher Lacher, Rechtliche Grenzen der Kommunikation über ärztliche Leistungen, S. 138 ff.

[115] S. o. Rn. 45 ff.

ebenfalls eine Grundlage für den Datenumgang. Diese kann sich beispielsweise aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG ergeben, wenn der Nutzer mit dem Dritten außerhalb des Dienstes in einer Vertragsbeziehung steht. Im Rahmen von § 29 BDSG stellen sich **dieselben Probleme** wie bei der Erhebung und Verwendung durch die Anbieter;[116] diese sind analog zu behandeln.

69 Bejaht man **entgegen der hier vertretenen Auffassung** eine datenschutzrechtliche Verantwortlichkeit der Nutzer auch bei der Bereitstellung für einen kleinen Kreis von Kontakten, wenn der Social Media-Anbieter die Daten zu Analyse- und Werbezwecken verwendet,[117] so benötigt der Nutzer eine rechtliche Verarbeitungsgrundlage. Daraus ergeben sich **praktisch unlösbare Schwierigkeiten**, weil mangels eigener Geschäftstätigkeit weder § 28 noch § 29 BDSG einschlägig und sonst keine Rechtsgrundlage ersichtlich ist. Private Nutzer müssten für jedes hochgeladene personenbezogene Datum eine Einwilligung einholen; andernfalls wäre der Vorgang rechtswidrig.[118] Die als Lösung vorgeschlagene Analogie zu §§ 28 ff. BDSG[119] ist schon aus prinzipiellen Gründen abzulehnen, weil die datenschutzrechtlichen Erlaubnistatbestände unter Schutzzweckgesichtspunkten nicht analogiefähig sind. Der Sache nach spricht das Fehlen jeglicher derartiger Tatbestände vielmehr zusätzlich dafür, dass diese Form des Datenumgangs nicht vom geltenden Datenschutzrecht erfasst ist.

4.3.4.4 Datenschutzrechtliche Einwilligung

70 Wenn kein gesetzlicher Erlaubnistatbestand für den Datenumgang eingreift, so verbleibt stets die Möglichkeit einer Einwilligung des Betroffenen (§ 4 Abs. 1 BDSG, § 12 Abs. 1 TMG).[120] Sie muss nach § 4a Abs. 1 BDSG **informiert und freiwillig** erfolgen und **zeitlich vor** der Erhebung oder Verwendung der Daten eingeholt werden.[121] Der Betroffene muss zwar nicht geschäftsfähig sein, wohl aber die für den konkreten Datenumgang erforderliche **Einsichtsfähigkeit** aufweisen.[122]

71 Nicht ausreichend für eine informierte Einwilligung ist es beispielsweise, im Rahmen des Anmeldeprozesses weitreichende Datenerhebungen (konkret: Zugriff auf

---

[116] S. o. Rn. 63 ff.
[117] S. o. Rn. 48.
[118] Dies gilt im Übrigen auch für andere Datenverwendungen im privaten Bereich: Da beispielsweise auch viele ausländische E-Mail-Provider die Daten zu Analyse- und Werbezwecke verwenden, dürften Privatpersonen beispielsweise ohne ausdrückliche Einwilligung keine Adressbücher mit Daten Dritter anlegen (oder diesen sogar noch nicht einmal E-Mails senden).
[119] Jandt/Roßnagel, ZD 2011, 160 (162 ff.); dies., in: Schenk et al., Digitale Privatsphäre, S. 353 ff.
[120] Zu den Strukturen der durch die Anbieter verwendeten Einwilligungserklärungen s. aus empirischer Sicht im europäischen Vergleich Rogosch/Hohl, Data Protection and Facebook; zu den Erwartungen der Nutzer an eine informierte Einwilligung s. auf der Basis einer Online-Umfrage Custers et al., SCRIPTed 2013, 435 ff.
[121] Zur Problematik des vielfach von den Anbietern verwendeten Opt-Out Prinzips s. Caspar, DuD 2013, 767 ff.
[122] Dazu näher unten Rn. 78 ff.

Webmail-Adressbücher einschließlich der Adressen von Personen, die nicht Nutzer des Social Media-Angebots sind) vorzunehmen, ohne darauf explizit hinzuweisen.[123] Dasselbe gilt für **undeutliche Formulierungen** über die Datenverwendung für geplante individuelle Werbeanzeigen.[124] Insgesamt ist gerade bei komplexen Social Media-Anwendungen ein hinreichendes Maß an Transparenz zu verlangen, damit den Nutzern die Verwendungszwecke und etwaige Datenübermittlungen an Dritte erkennbar werden.[125] Dies kann im Einzelfall durchaus kompliziert sein, weil zu umfangreiche und komplizierte Datenschutzerklärungen abschreckend wirken und deshalb **kontraproduktiv** sein können. Im Verhältnis zu diesen Formulierungsproblemen dürfte es eher nebensächlich sein, einem erkennbar auf umfassende Datenerhebung angelegten sozialen Netzwerk vorzuhalten, bei der Anmeldung werde nicht hinreichend deutlich gemacht, dass überhaupt personenbezogene Daten verwendet würden.[126]

Die Einwilligung bedarf gemäß § 4a Abs. 1 Satz 2 BDSG der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie nach § 4a Abs. 1 Satz 3 BDSG besonders hervorzuheben. Wie allgemein im Rechtsverkehr ersetzt die qualifizierte elektronische Signatur die Schriftform. **72**

Im Geltungsbereich des Telemediengesetzes kann die Einwilligung überdies **elektronisch erklärt werden**, wenn der Diensteanbieter sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen und diese jederzeit mit Wirkung für die Zukunft widerrufen kann (§ 13 Abs. 2 TMG). Entsprechend der Regelungssystematik gilt dies an sich nur für Bestands- und Nutzungsdaten von Social Media, während für Inhaltsdaten § 4a Abs. 1 Satz 2 BDSG gilt. Im Bundesdatenschutzgesetz enthält allerdings § 28 Abs. 3 Satz 1, Abs. 3a Satz 1 BDSG für den Bereich von Adresshandel und Werbung eine Regelung, die § 13 Abs. 2 TMG entspricht. Greift diese nicht, so sollte zumindest für **nicht risikobehaftete Social Media** ebenso verfahren werden, weil die Schriftform insoweit nicht praktikabel ist. **73**

---

[123] S. LG Berlin, ZD 2012, 276 (278); KG Berlin, DuD 2014, 417 (421 f.). Der angegriffene Dienst (Facebooks „Friend Finder“) wurde inzwischen so verändert, dass erheblich mehr Transparenz über die Abläufe hergestellt wird. Zum konkreten Problem des Friend Finder s. z. B. Meyer, in: Taeger, Die Welt im Netz, S. 536 f.; ders., K&R 2012, 309 ff.; Wittern/Wichmann, ITRB 2012, 133.

[124] S. LG Berlin, ZD 2012, 276 (278 f.); KG Berlin, DuD 2014, 417 (422); zur Klausel für Facebooks „Sponsored Stories“ s. Dietrich/Ziegelmayer, CR 2013, 104 (108 f.); zu Transparenzproblemen auch Erd, NVwZ 2011, 19 (20 ff.); Spiecker gen. Döhmann, K&R 2012, 717 (719 f.); Martini/Fritzsche, VerwArch 2013, 449 (458 f.).

[125] Zu den Problemen am Beispiel Facebook s. z. B. Erd, in: Taeger, Digitale Evolution, S. 259 ff.

[126] So aber LG Berlin, ZD 2012, 276 (279).

Dies lässt sich über „besondere Umstände“ nach § 4a Abs. 1 Satz 2 BDSG[127] oder über eine Analogie zu § 13 Abs. 2 TMG[128] begründen.

74 In jedem Fall kann ein Nutzer von Social Media **nur** in die Erhebung und Verwendung **seiner eigenen personenbezogenen Daten** einwilligen. Soweit Anbieter versuchen, sich in ihren AGB dahin abzusichern, dass Nutzer nur Daten Dritter bereitstellen, wenn diese zugestimmt haben, stellt dies keinen selbstständigen Erlaubnistatbestand dar und schützt die Anbieter nicht vor einer etwaigen Rechtswidrigkeit des Datenumgangs.[129]

4.3.4.5 Insbesondere: Datenerhebung außerhalb von Social Media

75 Im Fall der Datenerhebung außerhalb von Social Media – insbesondere durch Social Plug-Ins[130] – ist wiederum nach Personengruppen zu unterscheiden. Soweit es um die **Nutzer von Social Media** geht, lässt sich die Datenerhebung auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG stützen, wenn man einen entsprechend weiten Geschäftszweck annimmt und in den erhobenen Daten (zum Beispiel der Information, dass auf einen Like-Button geklickt wurde) ein Inhaltsdatum sieht.[131]

76 Fehlt es hieran, handelt es sich um einen Nicht-Nutzer oder lehnt man den Charakter als Inhaltsdatum grundsätzlich ab,[132] so besteht nach geltendem Recht **regelmäßig keine Grundlage** für die Verarbeitung. Die Datenerhebung ist nicht zur Ermöglichung oder Abrechnung des Angebots erforderlich (§ 15 Abs. 1 TMG).[133] § 15 Abs. 3 TMG bildet nur eine Grundlage, soweit Pseudonyme verwendet und diese nicht mit den Namen zusammengeführt werden, dem Nutzer ein Widerspruchsrecht eingeräumt und er auf dieses hingewiesen wird. Dies wird von den Anbietern regelmäßig, jedenfalls aber im Verhältnis zu Nicht-Nutzern nicht erfüllt. Eine nachträgliche Anonymisierung durch den Anbieter (beispielsweise durch das Löschen eines Teils der IP-Adresse) stellt eine erhebliche Verbesserung dar und ist deshalb nachdrücklich zu fordern, ändert aber nichts daran, dass zunächst ein Personenbezug vorliegt. Auch die Ergänzung durch technische Schutzinstrumente des Nutzers[134]

---

[127] Dafür Taeger, in: Taeger/Gabel, BDSG, § 4a Rn. 37; Raabe/Lorenz, DuD 2011, 279 ff. m. w. N.; Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 121; a. A. Schaar, MMR 2001, 644 (647).

[128] Helfrich, in: Hoeren/Sieber, Teil 16.1 Rn. 67 ff.; wohl auch Redeker, IT-Recht, Rn. 943; wegen der oben Rn. 69 angesprochenen Probleme der Analogie im Datenschutzrecht spricht mehr für die erste Lösung.

[129] S. dazu Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 124 f.

[130] S. zum technischen Ablauf oben Rn. 38 ff.

[131] Dafür z. B. Ernst, NJOZ 2010, 1917 (1918).

[132] Zur Regelungssystematik oben 4.2.2

[133] A.A. mit Blick auf die Erforderlichkeit hinsichtlich der einbindenden Webseite Voigt/Alich, NJW 2011, 3541 (3544); wie hier Ernst, NJOZ 2010, 1917 (1919); Solmecke, in: Hoeren/Sieber, Teil 21.1 Rn. 29.

[134] Im Fall von Social Plug-Ins (und anderer Skripte, die Webseiten nachladen) betrifft dies z. B. Angebote wie Ghostery, die das Nachladen transparent machen und ein individuelles Blockieren ermöglichen.

sollte gefördert werden; ihre Nichtnutzung legitimiert aber nicht die Datenerhebung durch die Anbieter.

Damit verbleibt jenseits der eingangs genannten Fälle der Erhebung bei Nutzern nur die **Lösung über eine Einwilligung** auf der Webseite desjenigen, der den Plug-In einbindet. Da eine vorgeschaltete Webseite abschreckend wirken würde und deshalb unrealistisch ist, bietet sich auch hier die so genannte „Zwei-Klick-Lösung" an.[135] Sofern auch die weiteren Anforderungen an die wirksame Einwilligung – insbesondere die Informiertheit nach § 4a Abs. 1 Satz 2 BDSG – gegeben sind, ist der Gesamtvorgang dann zulässig.[136] **77**

4.4 Spezifische Einzelfragen

4.4.1 Datenschutz bei Minderjährigen

Das eingangs beschriebene **Spannungsfeld** zwischen kommunikativen Chancen und Risiken von Social Media wird **nirgends deutlicher** als bei der Verwendung durch Kinder und Jugendliche.[137] Diese nutzen vor allem soziale Netzwerke als Orte der Selbstdarstellung und Selbsterfahrung und durchleben in ihnen verschiedene Phasen der Persönlichkeitsentwicklung. Sie ernten dabei Anerkennung, Bestätigung und Respekt für bestimmte Verhaltensweisen und Eigenschaften, während andere auf Ablehnung, Spott und massiven Widerstand stoßen. **78**

All dies **teilen soziale Netzwerke** mit **anderen Orten der Adoleszenz**. Insofern ist kein Anlass für Panik, wohl aber für eine genaue Analyse der datenschutzrechtlichen Risiken, die sich durch die weltweite Vernetzung und die Perpetuierung der Informationen anders darstellen können als in der herkömmlichen Offline-Welt, in der Äußerungen und Handlungen schneller vergessen, jedenfalls aber nicht entsprechend dokumentiert werden. Wie groß die Probleme wirklich sind, ist zwar immer noch Gegenstand von Forschung. Insbesondere lässt sich kaum empirisch belegen, wie relevant das oft bemühte Beispiel kompromittierender Party-Bilder ist, die später zu Vorhaltungen im Bewerbungsgespräch (oder – noch schwieriger zu belegen – zur Nichteinladung) führen. Immerhin gibt es aus den USA Berichte, dass Arbeitgeber sogar die Freischaltung von Facebook-Accounts in der Bewerbungssituation **79**

---

[135] S. o. Rn. 51.

[136] Nach KG, NJW-RR 2011, 1264, spricht im Fall von Facebook einiges für eine Verletzung von § 13 Abs. 1 TMG; dies wurde letztlich wegen des angenommenen fehlenden Charakters als Marktverhaltensregel offengelassen; s. zur Einwilligungsfrage auch Piltz, CR 2011, 657 (659 f.); zum ähnlich gelagerten Problem der Datenübermittlung bei der Nutzung des „Facebook-Login" durch Drittanbieter Moser-Knierim, ZD 2013, 263.

[137] S. o. 4.1 sowie näher Niemann/Schenk, in: Schenk/Niemann/Reinmann/Roßnagel, Digitale Privatsphäre, S. 15 ff.; zu den Rechtsfragen im schulischen Umfeld Steenhoff, NVwZ 2013, 1190 ff.

verlangen, um die dort gespeicherten Daten einzusehen.[138] Die einzelnen Ausprägungen des so genannten Cybermobbings (verletzende Bilder und Kommentare, „Hassgruppen" gegen einzelne Personen, Profile unter falscher Identität zur Verbreitung ehrverletzender Informationen etc.) sind jedenfalls ebenso Realität wie die Konfrontation mit jugendgefährdenden Inhalten, die Verleitung zu kostenpflichtigen Diensten und die Probleme der Online-Sucht und anderer psychologischer Folgen. Da die Profile in sozialen Netzwerken zumindest bislang nicht portierbar sind, besteht überdies ein **natürliches Interesse** der Anbieter, **immer jüngere Kunden** für sich zu gewinnen.[139]

80 Datenschutzrechtlich können sich Erhebungs- und Verwendungsbefugnisse der Anbieter aus denselben Rechtsgründen ergeben wie bei Erwachsenen: Rechtsnormen und Einwilligungen. Von den einschlägigen Rechtsnormen erfordert nur **§ 29 BDSG kein Vertragsverhältnis**. Im Rahmen der erforderlichen Abwägung nach dieser Norm ist das geringe Alter der Nutzer zu berücksichtigen und wird häufig, insbesondere aber bei fehlender Einsichtsfähigkeit zum **Vorliegen überwiegender Interessen** führen, die den Datenumgang ausschließen.[140]

81 Im Übrigen setzen § 28 BDSG (für Inhaltsdaten) sowie § 14 Abs. 1 und § 15 Abs. 1 TMG (für Bestands- und Nutzungsdaten) ein **wirksames Vertragsverhältnis** voraus. Unabhängig von der vertragstypologischen Einordnung[141] richtet sich die Wirksamkeit jedenfalls nach den §§ 104 ff. BGB. Da die vertragliche Leistung des Minderjährigen (die Bereitstellung seiner Daten) nicht i. S. v. § 110 BGB mit Mitteln bewirkt wird, die der Vertreter ihm zu diesem Zweck zur Verfügung gestellt hat, und die Teilnahme an Social Media nur selten zu wirtschaftlichen Tätigkeiten nach § 112 und § 113 BGB gehören wird, bedarf die Willenserklärung nach § 107 BGB einer **Einwilligung des gesetzlichen Vertreters**, sofern der Minderjährige nicht lediglich einen rechtlichen Vorteil erlangt. Bei kostenpflichtigen Social Media ist der rechtliche Nachteil unmittelbar erkennbar. Dasselbe gilt, wenn im Rahmen von Allgemeinen Geschäftsbedingungen Nutzungsrechte übertragen werden.[142] Da für § 107 BGB jedoch auch nicht-wirtschaftliche Nachteile relevant sind,[143] ist im Ergebnis auch die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung als nachteilhaft anzusehen,[144] sodass eine Einwilligung des Vertreters erforderlich und der Vertrag

[138] Dies führte 2012 sogar zu einer Gesetzesinitiative (Password Protection Act), s. http://www.heise.de/-1573684.html.

[139] Nach Medienberichten testet Facebook z. B. eine Zugangslösung für Kinder unter 13 Jahren, deren Account an den der Eltern gekoppelt sein soll, s. www.heise.de/-1590289.html.

[140] S. Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 339.

[141] S. dazu Bräutigam/v. Sonnleithner, Kap. 3.

[142] Zu den Grenzen der Übertragung durch AGB s. Berberich, MMR 2010, 736; Solmecke/Dam, MMR 2012, 71.

[143] Wirtschaftliche oder sonstige tatsächliche Auswirkungen des Geschäfts sind unerheblich, s. Staudinger-Knothe, § 107 BGB Rn. 2 m. w. N.

[144] S. ausf. Jandt/Roßnagel, MMR 2011, 637 (639 ff.); dies., in: Schenk et al., Digitale Privatsphäre, S. 336 ff.; ebenso Bräutigam, MMR 2012, 635 (637); Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 144 f.; ähnlich Wintermeier, ZD 2012, 210 (213 f.) [in etwas künstlicher Differenzierung zwischen wirksamer Anmeldung und unwirksamer Nutzung].

ohne eine solche gemäß § 108 Abs. 1 BGB schwebend unwirksam ist. Die **Zustimmung** kann vorher oder nachträglich, ausdrücklich oder konkludent, gegenüber dem Minderjährigen oder gegenüber dem Diensteanbieter erklärt werden – unabhängig von diesen Modalitäten stellt sie jedoch eine erhebliche Herausforderung für die Anbieter von Social Media dar, weil ihr Vorliegen im Massengeschäft **kaum geprüft werden** kann.[145]

82 Die Alternative zum Weg über § 28 BDSG, § 14 Abs. 1 und § 15 Abs. 1 TMG besteht in der datenschutzrechtlichen **Einwilligung**. Eine solche ist auch im Rahmen von § 29 BDSG erforderlich, soweit es um Adresshandel oder Werbung geht (§ 29 Abs. 1 Satz 2 i. V. m. § 28 Abs. 3 bis Abs. 3b BDSG).

83 Derzeit existiert keine Regelung, ab welchem Alter Minderjährige eine solche wirksam vornehmen können.[146] Im **Entwurf der Kommission** ist eine entsprechende Festsetzung dagegen enthalten. In bekannt gewordenen Entwürfen war zunächst eine – als Pauschallösung sicher zu hohe – Grenze von 18 Jahren vorgesehen.[147] In einer bemerkenswerten Parallele zur US-amerikanischen Rechtslage[148] setzt Art. 8 Abs. 1 DS-GVO-E dagegen die Einwilligungsfähigkeit nunmehr für Dienste der Informationsgesellschaft auf die **Vollendung des 13. Lebensjahres** fest.

84 **De lege lata** wird überwiegend davon ausgegangen, dass nach der Wertung des § 104 Nr. 1 BGB jedenfalls bis zur Vollendung des siebten Lebensjahres eine eigene Einwilligung des Minderjährigen nicht möglich ist und im Anschluss seine Einsichtsfähigkeit entscheidet.[149] Diese steigt mit zunehmendem Alter und abnehmender Komplexität der konkreten Datenerhebung und -verwendung. Die **Einsichtsfähigkeit** ist mit Blick auf den **Schutzzweck** zu bestimmen und hängt folglich von der Art der Social Media-Anwendung, der Menge und Sensibilität der erhobenen Daten, den weiteren Datenflüssen (vor allem in Drittstaaten) und den Einflussnahmemöglichkeiten der Betroffenen ab. Das OLG Hamm hat unlängst entschieden, es könne nicht davon ausgegangen werden, dass Minderjährige ab dem 15. Lebensjahr grundsätzlich die nötige Reife hätten, um die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen.[150] Da die Entscheidung den Fall einer lediglich singulären Werbemaßnahme betraf, wäre es

---

[145] An dieser Situation wird auch der Entwurf der Kommission nichts ändern, weil nach Art. 8 Abs. 2 DS-GVO-E das allgemeine Vertragsrecht der Mitgliedstaaten, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Minderjährigen, unberührt bleiben.

[146] Zur Verbindung mit der grundrechtlichen Bewertung (Grundrechtsfähigkeit und Grundrechtsmündigkeit) s. Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 334 ff.

[147] Diese Fassung vom November 2011 ist abrufbar unter http://www.statewatch.org/eu-dp.htm.

[148] Der Children's Online Privacy Protection Act of 1998 enthält eine entsprechende Altersgrenze, s. Schüßler, in: Taeger, Digitale Evolution, S. 247.

[149] S. in Bezug auf soziale Netzwerke Jandt/Roßnagel, MMR 2011, 637 (640); dies., in: Schenk et al., Digitale Privatsphäre, S. 334 ff.; Wintermeier, ZD 2012 (210, 212); anders Tinnefeld et al., Einführung in das Datenschutzrecht, S. 401 f. und Kipker/Voskamp, DuD 2012, 737 (739): Vermutung des Fehlens der Einsichtsfähigkeit bis zum vollendeten 13. Lebensjahr.

[150] OLG Hamm, ZD 2013, 29.

konsequent, für weitreichende Profile und nutzerspezifische Werbung höhere Altersgrenzen anzunehmen.[151] All dies führt dazu, dass auch die Einwilligung **kaum als generelles Instrument** der Anbieter geeignet ist.

85 Rechtspraktisch stellt sich daneben vor allem die Frage, wie die Einsichtsfähigkeit und das Alter des Nutzers überhaupt feststellbar sind.[152] Eine nicht-typisierende (also vom Alter losgelöste) **individuelle Prüfung der Einsichtsfähigkeit** ist in Massenanwendungen des Online-Bereichs de facto **nicht möglich**. Insofern ist die Bestimmung handhabbarer Altersgrenzen (ob durch den Gesetzgeber oder durch die Rechtsprechung) der richtige Weg.[153] Sichere **Altersverifikationsverfahren** wie das PostIdent-Verfahren,[154] der elektronische Identitätsnachweis des neuen Personalausweises[155] oder das DE-Mail Konto sind verfügbar, aus der Perspektive weltweiter Anbieter (nicht nur von Social Media) bislang aber nationale, aufwändige und teure **Insellösungen**. Dementsprechend vertrauen die Anbieter weithin auf die Selbstauskunft der Nutzer und gehen damit die beschriebenen Risiken unwirksamer Verträge und Einwilligungen ein.

86 Insgesamt ist die Nutzung von Social Media durch Minderjährige ein prototypisches Beispiel dafür, dass man datenschutzrechtlichen Risiken nicht allein mit dem Datenschutzrecht beikommen kann. Insofern ist **Datenschutz Bildungsaufgabe**[156] und bedarf als solcher einer stärkeren Berücksichtigung in Schule und Erziehung. Durch entsprechende Förderungsmaßnahmen kommt der Staat auch seinem grundrechtlichen Auftrag nach, sich „schützend und fördernd" vor das Recht auf informationelle Selbstbestimmung zu stellen.[157]

4.4.2 Datenschutz durch technische Gestaltung

87 Ihre Grundfunktionen können Social Media oftmals erfüllen, ohne weitreichende datenschutzrechtliche Probleme aufzuwerfen. Wenn diese auftreten, dann meist wegen der unzureichenden Transparenz des Datenumgangs, der umfassenden – über den Basiszweck hinausgehenden – Datenverwendung, der weitreichenden Datenübermittlungen an Dritte oder der unzulänglichen Möglichkeiten der Nutzer, auf die weitere Datenverwendung Einfluss zu nehmen. Viele dieser Punkte

---

[151] De lege ferenda für eine Grenze von 13 Jahren: Härting, BB 2012, 459 (464); für 18 Jahre: Spindler, Gutachten F zum 69. DJT, S. 107 f., wo allerdings zusätzlich zur Einwilligung der Erziehungsberechtigten ab einem bestimmten Altern die des Minderjährigen verlangt wird, um ihn gegen Datenveröffentlichungen durch die Erziehungsberechtigten zu schützen.

[152] Schüßler, in: Taeger, Digitale Evolution, S. 250.

[153] S. Schüßler, in: Taeger, Digitale Evolution, S. 249 f.

[154] Dazu aus rechtlicher Sicht Möller, NJW 2005, 1605.

[155] Zum Einsatz als Altersverifikationsmittel Altenhain/Heitkamp, K&R 2009, 619; zur Konzeption Roßnagel/Hornung, DÖV 2009, 301; Schulz, CR 2009, 267; Borges, NJW 2010, 3334; Möller, in: Hornung/Möller, PassG/PAuswG, 2011, § 18 PAuswG Rn. 3 ff.

[156] S. v. a. Wagner, DuD 2010, 557; ders., DuD 2012, 83.

[157] S. o. Rn. 12.

können durch eine datenschutzfreundliche Gestaltung und den Einsatz datenschutzfreundlicher Technik (**Privacy Enhancing Technologies**) verbessert werden.[158] Dies setzt allerdings eine entsprechende Verpflichtung der Anbieter oder deren eigenes ökonomisches Interesse voraus.

Für ein derartiges Interesse bedarf es einer **entsprechenden Nachfrage**. Das Bewusstsein für die datenschutzrechtlichen Fragen von Social Media ist nach Umfragen durchaus vorhanden: Im Jahre 2011 gaben 77 % der Befragten in Deutschland an, sich nicht nur mit den Privatsphäreneinstellungen des von ihnen genutzten sozialen Netzwerks auseinandergesetzt, sondern diese auch verändert zu haben.[159] Datensicherheit und Privatsphäreneinstellungen sind danach auch die wichtigsten Auswahlkriterien für soziale Netzwerke.[160] Allerdings steht die Bewertung der Datenschutzfreundlichkeit der Anbieter in **deutlicher Diskrepanz zur tatsächlichen Nutzung**.[161] Offenbar ist den Nutzern die Transparenz über den Datenumgang wichtig, im Ergebnis überwiegen aber doch die Nutzungsvorteile durch große Verbreitung und besondere Funktionen. **Datenschutzaudits und Gütesiegel** für datenschutzfreundliche Produkte sind sinnvolle Ansätze, dem entgegenzuwirken.[162] Nach den genannten Erfahrungen steht aber zu erwarten, dass sie (von der Gruppe derjenigen abgesehen, die auf Datenschutz besonderen Wert legt) Nutzungsentscheidungen nur zwischen funktional im Wesentlichen gleichwertigen Angeboten beeinflussen werden. **88**

Die Alternative der **verbindlichen Vorgaben** für die Technikentwicklung und -gestaltung ist im geltenden Recht nur rudimentär entwickelt. § 3a BDSG enthält einen Ansatz in diese Richtung: Danach sind Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Diese Formulierung ist so offen („auszurichten"), dass sie praktisch nicht konkret gegenüber verantwortlichen Stellen durchzusetzen ist.[163] Die aktuelle **europäische Reform** bietet hier die Möglichkeit, zumindest in bestimmten Bereichen zu verbindlichen Regeln überzugehen, die dann auch für die Anbieter von Social Media gelten würden. Die Regelungen **89**

---

[158] S. dazu allgemein Borking, DuD 1998, 636; ders., DuD 2001, 607, Rost/Pfitzmann, DuD 2009, 353, sowie die Beiträge in Roßnagel, Allianz von Medienrecht und Informationstechnik, 2001; für soziale Netzwerke Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, S. 109; Spiecker gen. Döhmann, K&R 2012, 717 (721 f.); mit Blick auf die europäische Reform Hornung, ZD 2011, 51.

[159] BITKOM, Soziale Netzwerke, S. 24.

[160] BITKOM, Soziale Netzwerke, S. 22 f.

[161] Für das Jahr 2011 ergab die Studie des BITKOM (Soziale Netzwerke, 2011, S. 28) deutliche Vorteile für die Anbieter StayFriends, wer-kennt-wen und die VZ-Gruppe. Genutzt wurde aber mit großem Abstand (51 % der Befragten) das in puncto Datenschutz schlechter bewertete Angebot von Facebook.

[162] S. dazu allgemein Roßnagel, DuD 1997, 505; ders., Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, 2000; ders., in: Hempel et al., Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, S. 263; Bäumler, CR 2001, 795; ders., DuD 2002, 325; ders., DuD 2004, 80; mit Blick auf die europäische Datenschutzreform Hornung/Hartl, ZD 2014, 291 ff.

[163] Zur umstrittenen Rechtsnatur s. Scholz, in: Simitis, BDSG, § 3a Rn. 27 f. m. w. N.; für eine nähere Analyse Roßnagel, in: Eifert/Hoffmann-Riem, Innovation, Recht und öffentliche Kommunikation, S. 41ˆff.; in Bezug auf die europäische Reform Hornung, ZD 2011, 51 (53 f.).

im Entwurf der EU-Kommission bleiben aber auf dem Stadium von Ankündigungen stehen und sind zu diesem Punkt insgesamt eine völlige Enttäuschung.[164]

90 Eine **datenschutzfreundliche Gestaltung** von Social Media kann auf **mehreren Grundsätzen** aufbauen.[165] Auf die Verarbeitung bestimmter sensibler Daten kann ganz verzichtet oder vor ihrer Verarbeitung zumindest gewarnt werden. Automatische Löschungsfristen, gegebenenfalls in Verbindung mit erneuten Einwilligungen, können einer ungewollten dauerhaften Speicherung entgegenwirken. Die Transparenz kann durch automatisierte Benachrichtigungen der Nutzer verbessert werden, sobald ihre Daten von anderen Nutzern verarbeitet werden (etwa bei dem Markieren auf Bildern in sozialen Netzwerken).[166] Für Social Plug-Ins wie Facebooks Like-Button kann mittels der so genannten Zwei-Klick-Lösung verhindert werden, dass Daten schon mit dem Aufruf der Webseiten von Drittanbietern übertragen werden.[167]

91 **Datenschutzfreundliche Voreinstellungen (Privacy by Default)** können dafür sorgen, dass der Nutzer sich über die konkrete Datenverwendung bewusst wird und weitreichende Datenverarbeitungen (insbesondere Übermittlungen an Dritte und die Bereitstellung von Profildaten über den Freundeskreis hinaus) nur nach einer expliziten Änderung der Privatsphäreneinstellungen erfolgen.[168] Sofern Daten allen Nutzern oder sogar allgemein im Internet verfügbar sind, kann der Zugriff durch automatisierte Verfahren (Crawler) verhindert und so das massenhafte Speichern von Daten aus Social Media begrenzt werden. Eine effektive Umsetzung der nach § 9 BDSG erforderlichen Maßnahmen zur **Datensicherheit** vermindert das Risiko von Datenmissbrauch; dies ist nicht zuletzt seit der Einführung von Meldepflichten bei „Datenpannen" (**data breach notification**) auch im Eigeninteresse der Anbieter.[169] Auch einige **Betroffenenrechte** (vor allem der Auskunftsanspruch) können technisch unterstützt oder sogar automatisiert werden.

92 Die **Anonymisierung und Pseudonymisierung** von Nutzerdaten kann ihre Persönlichkeitsrechte gegenüber anderen Nutzern wahren, aber auch beim Anbieter

---

[164] S. näher Hornung, ZD 2012, 99 (103 f.); ders., INNOVATION 2013, S. 181 ff.

[165] S. zum Folgenden schon Hornung, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 143 ff.; Einzelheiten z. B.: Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Ein modernes Datenschutzrecht für das 21. Jahrhundert, S. 24 ff.; Helberger/van Hoboken, CRi 2010, 101 (106 ff.); Spindler, Gutachten F zum 69. DJT, S. 124 f.; Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 436 ff.; Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, S. 116 ff.

[166] Zu den rechtlichen Transparenzanforderungen und Beispielen für die Umsetzung bei Social Media s. Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 125 ff.

[167] S. o. Rn. 51.

[168] Dies ist z. B. in § 13a Abs. 1 Satz 1 und Satz 3 TMG-E des Entwurfs des Bundesrats aus dem Jahre 2011 vorgesehen (BT-Drs. 17/6765), dazu Jandt/Roßnagel, MMR 2011, 637 (641); dies., in: Schenk et al., Digitale Privatsphäre, S. 381 ff.; s. ferner Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163, S. 8; Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, S. 135 ff.

[169] Derartige Pflichten sind inzwischen in § 42a BDSG, § 15a TMG, § 93 Abs. 3 und § 109a TKG, § 83a SGB X sowie einigen Landesdatenschutzgesetzen enthalten; s. zur Entwicklung und den Hintergründen näher Hornung, NJW 2010, 1841 ff.

sinnvoll sein, sofern Daten nur für Zwecke der Produktverbesserung verwendet werden. Soweit es nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, verlangt § 3a Satz 2 BDSG ein entsprechendes Vorgehen. Für Social Media greift – soweit deutsches Recht anwendbar ist[170] – überdies der spezielle § 13 Abs. 6 TMG,[171] der eine Rechtspflicht der Diensteanbieter enthält, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

93 Technisch möglich ist die anonyme oder pseudonyme Nutzung von Social Media praktisch immer. Ob sie auch zumutbar ist, wird anhand der bei manchen Anbietern üblichen „**Klarnamenpflicht**" diskutiert, die Nutzer zur allgemeinen Offenlegung ihres echten Namens innerhalb von Social Media zwingen soll.[172]

94 Die Zumutbarkeit ist aus der Sicht der Anbieter zu beurteilen,[173] sodass die Interessen Dritter (beispielsweise an einer Verfolgung von Rechtsverletzungen) nur insoweit mittelbar eine Rolle spielen, als der Anbieter gegebenenfalls einem eigenen Haftungsrisiko unterliegt. Bei nahezu allen Social Media (jedenfalls aber bei Blogs und Foren) ist damit **zumindest eine pseudonyme Nutzung** gegenüber anderen Nutzern **zumutbar**, weil hier der Anbieter die wahre Identität kennt und im Streitfall gegen den Nutzer vorgehen kann. Soweit berufliche soziale Netzwerke auf die Reputation der Nutzer setzen, kann im Einzelfall eine Klarnamenpflicht gerechtfertigt werden. Für allgemeine soziale Netzwerke wie Facebook oder Google Plus gilt dies nicht.[174]

95 Schließlich verdrängt § 13 Abs. 6 TMG nicht andere Regelungen, die zu einer Aufhebung der Anonymität oder Pseudonymität führen. Soweit beispielsweise Nutzerprofile in sozialen Netzwerken einer **Impressumspflicht** nach § 5 TMG oder § 55 RStV unterliegen, ist diese vorrangig.[175]

---

[170] § 13 Abs. 6 TMG war ein Gegenstand der Verfahren im Zusammenhang mit Facebook, in denen die schleswig-holsteinischen Gerichte die Anwendbarkeit verneinten, s. OVG Schleswig-Holstein, NJW 2013, 1977 sowie Beschl. v. 22.4.2013, 4 MB 10/13 (unveröffentlicht) und oben 4.3.1.2. Eine Pflicht zur Anonymisierung und Pseudonymisierung ist nicht explizit in der Datenschutzrichtlinie enthalten, kann aber auf Art. 6 Abs. 1 lit. c DSRL zurückgeführt werden, s. Scholz, in: Simitis, BDSG, § 3a Rn. 17.

[171] S. für Blogs z. B. LG Kassel, Urteil v. 12.7.2010, 8 O 644/10 – juris; s. a. Roßnagel, in: ders., Handbuch Datenschutzrecht, Kap. 7.9 Rn. 113 ff.

[172] Näher Schnabel/Freund, CR 2010, 718 ff.; Stadler, ZD 2011, 57 ff.; s. a. Splittgerber, in: ders., Praxishandbuch Rechtsfragen Social Media, S. 104.

[173] Moos, in: Taeger/Gabel, BDSG, § 13 TMG, Rn. 55; Breyer, MMR 2009, 14 (16); a. A. Gabriel/Albrecht, ZUM 2010, 392 (394).

[174] Ebenso Stadler, ZD 2011, 57 (59); Niemann/Scholz, in: Peters et al., Innovativer Datenschutz, S. 116 ff.; weitergehend unter verbrauchervertragsrechtlichen Gesichtspunkten Ziebarth, ZD 2013, 375 ff.; zu den AGB-rechtlichen Folgen einer rechtswidrigen Klarnamenpflicht Schnabel/Freund, CR 2010, 718 (720 f.).

[175] S. OLG Düsseldorf, K&R 2013, 594; LG Regensburg, MMR 2013, 246; näher Stadler, ZD 2011, 57 (59 f.); Lange, ZJS 2013, 141; Solmecke, in: Hoeren/Sieber, Teil 21.1 Rn. 2 ff.

4.4.3 Betroffenenrechte und prozessuale Fragen

96 Soweit das Recht eines Staates im Geltungsbereich der europäischen Datenschutzrichtlinie anwendbar ist, bestehen bestimmte, **durch Art. 12 DSRL vorgegebene Rechte der Betroffenen**. Im deutschen Recht sind dies die Rechte auf Auskunft (§§ 19, 34 BDSG) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35 BDSG); in bestimmten Fällen (§ 20 Abs. 5, § 28 Abs. 4 und § 35 Abs. 5 BDSG) besteht auch ein Widerspruchsrecht.

97 Im Bereich von Social Media[176] ist **insbesondere das Auskunftsrecht** praktisch relevant geworden. Hier zeigen sich exemplarisch die praktischen Probleme eines Datenschutzrechts, das in der Europäischen Union zwar normativ harmonisiert ist, aber unterschiedlich vollzogen wird. Der inzwischen bekannte Fall des Österreichers Max Schrems, der in längeren Auseinandersetzungen mit Facebook insgesamt 1.222 PDF-Seiten mit über ihn gespeicherten personenbezogenen Daten erhielt,[177] zeigt überdies ein **grundsätzliches Transparenzproblem** auf. Zumindest dieser Anbieter speichert nämlich nicht nur erheblich mehr Daten über die Nutzer, als diesen in ihren Profilen angezeigt werden. Überdies werden die Daten auch dann – und offenbar dauerhaft – gespeichert, wenn die Nutzer einzelne Informationen, Nachrichten, Chats oder ähnliche Daten „löschen". Im Zuge der öffentlichen Diskussion hat Facebook inzwischen die Erfüllung des Auskunftsanspruchs automatisiert. Dies ist eine effektive Möglichkeit zur Umsetzung dieses wichtigen Betroffenenrechts. Es verbleibt aber das Problem, ob wirklich über alle, auch im Hintergrund erfassten Daten (insbesondere im Zusammenhang mit Social Plug-ins) Auskunft erteilt wird.

98 Im Reformvorschlag der EU-Kommission sind zwei neue Betroffenenrechte enthalten, die relativ deutlich durch das Internet und die Erfahrungen mit Social Media beeinflusst worden sind: das **Recht auf Vergessenwerden** und das **Recht auf Datenübertragbarkeit**.[178] Bei beiden ist aufgrund konzeptioneller Probleme[179] derzeit noch nicht abzusehen, ob und in welcher Form sie tatsächlich verabschiedet werden.

---

[176] S. zu den Nutzerrechten z. B. Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163, S. 13.

[177] Die Auseinandersetzungen gehen inzwischen weit über das Auskunftsrecht hinaus und betreffen neben der Zulässigkeit vieler einzelner Verarbeitungsschritte insbesondere das Handeln der irischen Aufsichtsbehörde. Einzelheiten sind unter http://europe-v-facebook.org dokumentiert.

[178] S. für das Recht auf Vergessenwerden die Aussage der zuständigen Kommisarin Reding: „I want to introduce the ‚right to be forgotten'. Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles", http://europa.eu/rapid/press-release_SPEECH-10–700_en.htm.

[179] Das Recht auf Vergessenwerden (Art. 17 DS-GVO-E) weist insbesondere eine extreme Diskrepanz zwischen dem kraftvollen Titel und dem praktisch völlig fehlenden normativen Innovationsgehalt auf, s. schon Hornung, ZD 2012, 99 (103) sowie ausf. Hornung/Hofmann, JZ 2013, 163 ff.; mit unterschiedlich starker Kritik: Costa/Poullet, CLSR 2012, 254 (256 f.); Jaspers, DuD 2012, 571 (572 f.); Koreng/Feldmann, ZD 2012, 311; Kort, DB 2012, 1020 (1022 f.); Lang, K&R 2012, 145 (149); Wybitul/Fladung, BB 2012, 509 (510 f.); Kodde, ZD 2013, 115; zu mehr konzeptionellen Grundüberlegung s. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age; Ausloos, CLSR 2012, 143. Das Recht auf Datenübertragbarkeit (Art. 18 DS-GVO-E) wird kaum genutzt werden, solange die alten Kontakte eines wechselwilligen Nutzers beim neuen Anbieter nicht verfügbar sind, was nur durch Interoperabilitätsvorgaben gelöst werden könnte, die weit in das Vertrags- und Wettbewerbsrecht hineinreichen würden, s. De Hert/Papakonstantinou,

4.4.4 Zugriff durch Dritte

Die in Social Media gesammelten personenbezogenen Daten sind vielfach nicht nur für die Anbieter, sondern auch für Dritte von großem Interesse. Im staatlichen Bereich kann dies Datenerhebungen und -verwendungen **durch Behörden** im Electronic Government oder zu Zwecken der Gefahrenabwehr und Strafverfolgung betreffen. Technisch kann die Datenerhebung durch eigene Accounts (gegebenenfalls im Rahmen von verdeckten Ermittlungen), die Ermittlung und Nutzung von Passwörtern der Betroffenen oder – wie das Beispiel PRISM eindrücklich gezeigt hat – durch **Zugriffe bei den Anbietern** von Social Media erfolgen; dies wirft jeweils spezifische Probleme insbesondere bei grenzüberschreitenden Sachverhalten auf.[180] **99**

Eine letzte Möglichkeit besteht in der **Erhebung frei zugänglicher Informationen**, die in vielen Angeboten verfügbar sind. Dies ist auch die gängigste Methode der Datenerhebungen durch Private. Diese können unterschiedlichste Zwecke verfolgen, beispielsweise die Markt- und Meinungsforschung, die Beurteilung der Kreditwürdigkeit der Nutzer[181] oder das so genannte „**Social Media Monitoring**“, bei dem Unternehmen Social Media beobachten, um Entwicklungen und Trends zu erfahren, die für ihre Unternehmensstrategie relevant sein können.[182] Dabei sollen insbesondere Gefahren erkannt werden, die sich aus der Kommunikation über das Unternehmen, seine Geschäftspolitik, Produkte und Dienstleistungen ergeben.[183] **100**

Während die weitere Verwendung der Daten je spezifische Probleme (beispielsweise im Rahmen des Kreditscorings) aufwirft und deshalb hier außer Betracht bleibt, müssen für alle genannten Vorgehensweisen spezifische **Befugnisse für die Erhebung** von Daten aus Social Media vorliegen. Dabei kommen vor allem zwei allgemeine Normen in Betracht, nämlich § 28 Abs. 1 Satz 1 Nr. 3 BDSG (bei der Erhebung für eigene Geschäftszwecke) und § 29 Abs. 1 Satz 1 Nr. 2 BDSG (bei der Erhebung zum Zweck der Übermittlung);[184] im speziellen Fall der Markt- und Meinungsforschung greift der für die Erhebung inhaltsgleiche § 30a Abs. 1 Satz 1 **101**

CLSR 2012, 130 (137 f.); s. ferner Kipker/Voskamp, DuD 2012, 737 (740 f.); zu weitgehend die Kritik von Härting, BB 2012, 459 (465); Dehmel/Hullen, ZD 2013, 147 (153).

[180] S. zur Anwendbarkeit des deutschen Strafrechts näher Esser, Kap. 7 Rn. 6 ff.

[181] Ein Forschungsprojekt zur Ermittlung von Zusammenhängen zwischen Social Media Daten und Kreditwürdigkeit wurde nach öffentlicher Kritik im Sommer 2012 nicht durchgeführt, s. www.heise.de/-1614109.html.

[182] S. aus rechtlicher Sicht z. B. Hoormann, in: Taeger, Die Welt im Netz, S. 587 ff.; Solmecke/Wahlers, ZD 2012, 550; Venzke-Caprarese, DuD 2013, 775. Solmecke/Wahlers stützen sich maßgeblich auf § 30a BDSG, legen aber den Begriff der „Markt- und Meinungsforschung“ dort viel zu weit aus. Dieser umfasst keineswegs jede Form des „Social Media Monitoring“, sondern setzt die Einhaltung bestimmter Standards (v. a. das Anonymisierungsgebot gegenüber Auftraggebern entsprechender Umfragen) voraus, s. Ehmann, in: Simitis, BDSG, § 30a Rn. 67 ff., 107 ff. m. w. N.; ausf. Hornung/Hofmann, WRP 2014, 776 ff.

[183] Der umgekehrte Fall, nämlich die Beeinflussung der Meinungsbildung durch Unternehmen und beauftragte Dienstleister, stellt regelmäßig kein datenschutzrechtliches Problem dar. Dass derartige Aktivitäten erfolgen, ist offensichtlich, Art und Umfang sind aber regelmäßig nicht (genau) bekannt.

[184] Zur Abgrenzung s. o. Rn. 63 ff.

Nr. 2 BDSG.[185] Die drei Vorschriften können Datenerhebungen jedenfalls dann legitimieren, wenn es sich nicht um besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG handelt.[186] Im Übrigen setzen sie alle voraus, dass die **Daten allgemein zugänglich** sind. Dieses Tatbestandsmerkmal lässt sich in Anlehnung an § 10 Abs. 5 Satz 2 BDSG auslegen. Es ist bei der Abrufbarkeit für jedermann im Internet (zum Beispiel bei Blogs und Foren), aber auch bei solchen Informationen zu bejahen, die in Social Media für alle Nutzer einsehbar sind, soweit die Anmeldung unproblematisch für jedermann möglich ist.[187] Bei geschlossenen Nutzergruppen fehlt es an der Allgemeinzugänglichkeit.

102 Auf **§ 29 Abs. 1 Satz 1 Nr. 2 BDSG** können sich beispielsweise Auskunfteien stützen. Sofern man in der Norm eine Rechtsvorschrift i. S. v.§ 4 Abs. 2 Nr. 1 BDSG sieht,[188] wird auch der Konflikt mit dem Grundsatz der Direkterhebung vermieden. Die allgemein zugänglichen Daten dürfen dann erhoben und verwendet werden, sofern das **schutzwürdige Interesse des Betroffenen** an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle nicht „offensichtlich überwiegt". Hierzu ist eine Einzelfallbetrachtung vorzunehmen, bei der aber Typisierungen zulässig sind.[189] Ein wesentlicher Faktor wird dabei sein, inwieweit die Betroffenen durch eine entsprechende **Einstellung der Zugangsmöglichkeiten** Einfluss schon auf die Allgemeinzugänglichkeit nehmen können. Dies ist etwa bei sozialen Netzwerken weithin der Fall und führt in Verbindung mit dem Erfordernis der Offensichtlichkeit dazu, dass eine Vermutung für die Zulässigkeit der Erhebung und Nutzung besteht, soweit es um die Daten der Nutzer geht.

103 Haben **hingegen Dritte die Daten bereitgestellt**, fällt das Argument der Einflussmöglichkeit des Bewerbers weg, sodass die Abwägung anders ausfallen kann. Dies gilt ebenso bei einer besonderen Sensibilität der erhobenen Daten oder der geplanten Verwendungszwecke. Insbesondere eine Kombination dieser Faktoren (also etwa die Erhebung intimer, durch Dritte bereitgestellter Daten für die Anlegung von Profilen mit dem Ziel weitreichender Entscheidungen wie Kreditvergaben) kann dann zu einer Unzulässigkeit führen.[190] Überwiegende Interessen können sich auch

---

[185] Zu dieser Norm s. in Bezug auf Social Media Solmecke/Wahlers, ZD 2012, 550 (553 f.); s. aber Fn. 182.

[186] In diesem Fall gelten die restriktiveren Vorgaben nach § 28 Abs. 6 bis Abs. 9 BDSG, die auch über die Verweisungsnormen in § 29 Abs. 5, § 30 Abs. 5 und § 30a Abs. 5 BDSG gelten.

[187] Ebenso Oberwetter, BB 2008, 1562 (1564); Ernst, NJOZ 2011, 953 (955 f.); Solmecke/Wahlers, ZD 2012, 550 (552); Venzke-Caprarese, DuD 2013, 775 (776); abl. Forst, NZA 2010, 427 (431), soweit die AGB des Anbieters eine Datenerhebung durch Arbeitgeber ausschließen; grds. einschränkend gegenüber der Verarbeitung allgemein zugänglicher Daten Simitis, in: Simitis, BDSG, § 28 Rn. 145 ff.

[188] S. Oberwetter, BB 2008, 1562 (1564); Gola/Schomerus, BDSG, § 4 Rn. 24; Venzke-Caprarese, DuD 2013, 775 (für den parallelen Fall des § 28 Abs. 1 Satz 1 Nr. 3 BDSG); a. A. Däubler, in: Däubler et al., BDSG, § 32 Rn. 56 ff.

[189] S. in Bezug auf Social Media Venzke-Caprarese, DuD 2013, 775 (777).

[190] Weitere Problemfälle bei Venzke-Caprarese, DuD 2013, 775 (778 f.) [z. B. das Anlegen von Profilen über „Meinungsführer"].

ergeben, wenn die **Daten nicht valide** sind, also beispielsweise unklar ist, ob ein Account überhaupt dem Betroffenen zugeordnet werden kann oder es um Angaben Dritter geht, die nicht verifiziert werden können. In jedem Fall sind die Verwendungszwecke nach § 29 Abs. 1 Satz 2 i. V. m. § 28 Abs. 1 Satz 2 BDSG konkret festzulegen; überdies ist regelmäßig eine Benachrichtigung des Betroffenen erforderlich (§ 33 Abs. 1 BDSG).

104 Ein weiteres Beispiel der Datenerhebung durch Dritte ist die **Einsicht durch potentielle Arbeitgeber** in der Bewerbungssituation. Hier kommt hinzu, dass mit § 32 BDSG eine Spezialregelung für den Bereich der Beschäftigungsverhältnisse besteht. Diese verdrängt jedenfalls § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Dies hat allerdings wenig Bedeutung, weil der Norminhalt faktisch identisch, im konkreten Fall aber nicht einschlägig ist: Eine Datenerhebung aus Social Media ist nicht für die Vertragsbegründung erforderlich. Entscheidend ist deshalb, ob auch § 28 Abs. 1 Satz 1 Nr. 3 BDSG verdrängt wird. Die wohl überwiegende Auffassung verneint das unter Berufung auf die Gesetzesbegründung (die Nr. 3 nicht nennt).[191] Die Erhebung und Verwendung ist dann nach dem **Maßstab von § 28 Abs. 1 Satz 1 Nr. 3 BDSG** zulässig, wenn man die Vorschrift ebenfalls als Ausnahme von § 4 Abs. 2 Nr. 1 BDSG versteht und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Wie bei § 29 Abs. 1 Satz 1 Nr. 2 BDSG kommt es folglich zu einer **Interessenabwägung**, bei der etwaige Einflussmöglichkeiten der Betroffenen wie Privatsphäreneinstellungen maßgeblich zu berücksichtigen sind.[192] Wie schon erläutert, gilt dies nicht für durch Dritte bereitgestellte Daten;[193] im Übrigen können auch Besonderheiten der Bewerbungssituation einfließen.

105 Während die Regelungsbedürftigkeit des Beschäftigtendatenschutzes im Allgemeinen praktisch einhellige Meinung ist, ist durchaus fraglich, ob die **Datenerhebung** über Bewerber aus dem Internet und **aus sozialen Netzwerken** speziell normiert werden sollte. Der **Entwurf der Bundesregierung** aus dem Jahre 2010[194] sah in § 32 Abs. 6 eine Abwägungsklausel entsprechend § 28 Abs. 1 Satz 1 Nr. 3 BDSG und zusätzlich eine Pflicht des Arbeitgebers vor, auf die Erhebung aus öffentlichen Quellen hinzuweisen.[195] Für soziale Netzwerke sollte hingegen das schutzwürdige Interesse per se überwiegen. Eine Datenerhebung wäre damit vollständig unzulässig gewesen, sofern nicht (so die Rückausnahme) ein Netzwerk

---

[191] Rolf/Rötting, RDV 2009, 263 (264 f.); Forst, NZA 2010, 427 (429 ff.); Gola/Schomerus, BDSG, § 32 Rn. 35 f.; Hoormann, in: Taeger, Die Welt im Netz, S. 581; Solmecke, in: Hoeren/Sieber, Teil 21.1 Rn. 44; a. A. Däubler, in: Däubler et al., BDSG, § 32 Rn. 8 ff.; differenzierend Hilbrans, in: Däubler et al., Arbeitsrecht, § 28 BDSG Rn. 3.

[192] Hoormann, in: Taeger, Die Welt im Netz, S. 582 f. m. w. N.; ähnlich Forst, NZA 2010, 427 (431).

[193] Dazu Rolf/Rötting, RDV 2009, 263 (265 f.).

[194] BT-Drs. 17/4230.

[195] S. z. B. Ernst, NJOZ 2011, 953 (954 f., 956); Oberwetter, NJW 2012, 417 (418).

vorliegt, das zur Darstellung der beruflichen Qualifikation bestimmt ist.[196] Diese Unterscheidung ist in Zeiten der Mischnutzung großer Angebote wie Facebook allerdings kaum durchzuhalten. Ohnehin ergibt sich das Problem, wie etwaige Einschränkungen effektiv durchgesetzt werden könnten. Ein Verbot mag denjenigen den Rücken stärken, die sich in größeren Personalabteilungen entsprechenden Ansinnen verweigern. Im Übrigen sind Datenerhebungen aus dem Internet aber faktisch nicht zu kontrollieren, zumal in Zeiten allgegenwärtiger Smartphone-Nutzung noch nicht einmal die Protokollierung der Internetzugriffe von Recruiting-Abteilungen (die ihrerseits datenschutzrechtlich problematisch wäre) einen Effekt hätte.

4.4.5 Beendigung des Nutzungsverhältnisses: Kündigung und Tod

106 Je nach Art der Social Media-Angebote werden diese in der Praxis unterschiedlich lange genutzt. Endet ein solches Nutzungsverhältnis, so stellt sich die Frage, was mit den beim Anbieter gespeicherten Daten zu geschehen hat. Bei befristeten Verträgen oder Kündigungen handelt es sich dabei um ein allgemeines datenschutzrechtliches Problem: Unter welchen Voraussetzungen, in **welchem Umfang und wie lange** darf ein Vertragspartner die im Rahmen des Vertragsverhältnisses rechtmäßig erhobenen Daten weiterhin speichern?

107 Daten sind **insbesondere dann zu löschen**, wenn ihre Speicherung (nunmehr) unzulässig ist (§ 35 Abs. 1 Satz 1 Nr. 1 BDSG), wenn sie für eigene Zwecke verarbeitet werden (§ 28 BDSG) und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 1 Satz 1 Nr. 3) oder eine Verarbeitung zum Zweck der Übermittlung erfolgt (§ 29 BDSG) und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist (§ 35 Abs. 1 Satz 1 Nr. 4). Die Erforderlichkeit ist im Einzelfall zu bestimmen und besteht bei Austauschverträgen regelmäßig über das eigentliche Vertragsende hinaus. Eine noch laufende zivilrechtliche Verjährung reicht als solche für die weitere Speicherung nicht aus, wohl aber die **Wahrscheinlichkeit von Rechtsstreitigkeiten**.[197] Ergibt sich eine andere Berechtigung für die weitere Datenspeicherung (beispielsweise im Marketingbereich), so muss keine Löschung erfolgen.

108 Im Fall von Social Media ergibt sich das Sonderproblem, dass sich viele der **Daten zugleich auch auf andere Nutzer beziehen** und deshalb deren Interessen zu berücksichtigen sind. Würden Chatprotokolle, gemeinsame Aktivitäten oder Bilder

[196] Für eine vergleichbare Unterscheidung im Rahmen der Interessenabwägung de lege lata Hoormann, in: Taeger, Die Welt im Netz, S. 583; Taeger/Gabel-Zöll, BDSG, § 32 Rn. 22.
[197] Dix, in: Simitis, BDSG, § 35 Rn. 38; Gola/Schomerus, BDSG, § 35 Rn. 13 f.

im Fall der Kündigung eines Kommunikationspartners ohne weiteres entfernt, so würde das Profil des jeweils anderen Partners unvollständig. Dies ist zumindest dann nicht angemessen, wenn insoweit eine eigene Verwendungsbefugnis fortbesteht.[198]

109 Insbesondere bei sozialen Netzwerken stellt sich zusätzlich die Frage, was mit den teilweise sehr umfassenden Datensammlungen **nach dem Tod des Nutzers** zu geschehen hat.[199] Dies ist teilweise einer **vertraglichen Gestaltung** zugänglich.[200] Fehlt es an dieser, so greift mangels einer datenschutzrechtlichen Regelung (das Datenschutzrecht schützt nicht die personenbezogenen Daten Verstorbener,[201] auch wenn ein verfassungsrechtlicher postmortaler Schutz der Persönlichkeit in Deutschland weitgehend anerkannt ist[202]) die **Universalsukzession** des § 1922 Abs. 1 BGB. Das Erbrecht unterscheidet zwischen übertragbaren Vermögenswerten und höchstpersönlichen Positionen, die unabhängig von der Erbfolge durch den nächsten Angehörigen oder einen vom Erblasser ausgewählten anderen Treuhänder wahrgenommen werden.[203]

110 Personenbezogene Daten sind als solche kein Vermögenswert. Sofern man den Account eines sozialen Netzwerks nicht für insgesamt unübertragbar hält,[204] tritt der **Erbe** aber bei Fehlen einer speziellen Klausel **in den Nutzungsvertrag** ein. Gegen einen Zugriff auf vermögenswerte Positionen wie urheberrechtlich geschützte Werke spricht dabei nichts, wohl aber gegen den Zugriff auf höchstpersönliche Daten und

---

[198] Dies erkennt im Grundsatz auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an, s. Orientierungshilfe „Soziale Netzwerke", 2013, S. 27 f. Den Versuch einer Regelung unternimmt der Entwurf des Bundesrats von 2011, BT-Drs. 17/6765. Zu pauschal Jandt/Roßnagel, in: Schenk et al., Digitale Privatsphäre, S. 373, wonach ein Löschungsanspruch „eindeutig immer dann" gegeben sein soll, wenn sich eine Person bei einem sozialen Netzwerk abmeldet.

[199] S. zum Phänomen aus empirisch-psychologischer Sicht Kasket, SCRIPTed 2013, 7 ff.

[200] S. zum „digitalen Nachlass" näher Bräutigam/v. Sonnleithner, Kap. 3 Rn. 90 ff.

[201] Gola/Schomerus, BDSG, § 3 Rn. 12; Weichert, in: Däubler et al., BDSG, § 3 Rn. 4. Eine Ausnahme bildet § 4 Abs. 1 Satz 2 BlnDSG, wonach auch Daten über Verstorbene geschützt sind, „es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können". Für eine grundsätzliche Anwendung auf die zu Lebzeiten entstandenen Daten auch nach dem Tod: Martini, JZ 2012, 1145 (1149 ff.); Heinemann/Heinemann, DuD 2013, 242; Haase, in: Taeger, Law as a Service (LaaS), S. 385 ff.; Culmsee, ebd., 413 (416 f.); s. a. Deusch, ebd., S. 429 ff.; zur Auswirkung der europäischen Reform Harbinja, SCRIPTed 2013, 19 ff.

[202] S. BVerfGE 30, 173; BVerfG, NJW 2006, 3409; s. allgemein Herdegen, in: Maunz/Dürig, Art. 1 Abs. 1 Rn. 56 ff. m. w. N.; in Bezug auf Internetdienste Martini, JZ 2012, 1145 (1150 ff.); ein wesentlicher Grund ist die Gefahr einer Selbstbeschränkung in rechtlich geschützten Kommunikationsbeziehungen, wenn nach dem eigenen Tod eine Offenbarung drohen würde.

[203] S. z. B. Leipold, in: MüKo-BGB, § 1922 Rn. 19, 98; ausf. Schwab, in: Damrau/Muscheler, FS Bengel/Reimann, S. 345 ff.; für E-Mail Accounts Hoeren, NJW 2005, 2113 (2114); im hier diskutierten Bereich Martini, JZ 2012, 1145 (1147 ff.); für eine weitgehend erbrechtliche Lösung Herzog, NJW 2013, 3745 ff.

[204] Dagegen zu Recht Martini, JZ 2012, 1145 (1147); Brinkert/Stolze/Heidrich, ZD 2013, 152 (154 f.); Haase, in: Taeger, Law as a Service (LaaS), S. 383 ff.

insbesondere vertrauliche Kommunikation.[205] Aus erbrechtlicher Sicht steht die Entscheidung über den weiteren Umgang mit diesen Daten **den nächsten Angehörigen** oder dem gewählten Treuhänder zu. In der Praxis dürfte die Unterscheidung der beiden Bereiche allerdings eine kaum durchführbare manuelle Kontrolle erfordern;[206] viele Anbieter verweigern deshalb Erben und Angehörigen jeden Zugriff.

111 Die prinzipielle Vererblichkeit des Accounts bedeutet nicht, dass dieser nunmehr durch die Erben oder nächsten Angehörigen unter dem Namen des Erblassers weiterbetrieben werden dürfte. Vielmehr besteht ein legitimes Interesse der Anbieter von Social Media und der anderen Nutzer daran, einer Identitätsverwirrung vorzubeugen. Dementsprechend bieten einige Anbieter inzwischen die Umstellung der Seiten auf einen „**Gedenkstatus**" an. Insgesamt sollte der Bereich des postmortalen Datenschutzes bei Social Media durch Vertragsgestaltungen und entsprechende Optionen für die Nutzer gelöst werden,[207] die die Möglichkeit beinhalten, niemandem den Zugang zu eröffnen. Wie bei der Kündigung zu Lebzeiten sind überdies auch die Interessen von Kommunikationspartnern berücksichtigen, bestimmte Daten trotz der Kündigung aufzubewahren.

4.5 Fazit und Ausblick

112 Social Media zeigen **paradigmatisch die heutigen Herausforderungen** des Datenschutzes im Internet: extreme Zunahme der Datenflüsse, fehlende weltweite Standards, hohe Attraktivität datenintensiver Anwendungen für die Nutzer, mangelndes Eigeninteresse vieler Anbieter am Datenschutz (weil Geschäftsmodelle auf Datennutzung und -weitergabe basieren), hohes Vollzugsdefizit und Auseinanderfallen zwischen rechtlichen Anforderungen und Rechtspraxis. Die mutmaßlich **wichtigste Frage** ist dabei derzeit die des **anwendbaren Rechts** und der daraus resultierenden aufsichtsbehördlichen Zuständigkeit. Die konkreten Folgen des jüngsten Urteils des Europäischen Gerichtshofs sind derzeit noch unklar, weil im Fall von Googles Suchmaschine – anders als bei vielen Social Media-Anbietern – keine Niederlassung in der Europäischen Union mit der tatsächlichen Datenverwendung befasst war.[208] Sollte sich für diesen Fall doch die Auffassung der deutschen Verwaltungsgerichte durchsetzen,[209] so würde sich für die Anbieter von Social Media

[205] S. Brinkert et al., ZD 2013, 152 (156); zum Zugriff auf E-Mails s. Hoeren, NJW 2005, 2113 ff.; Brisch/Müller-ter Jung, CR 2013, 446 (448 ff.); überwiegend a. A. Herzog, NJW 2013, 3745 (3749 ff.).

[206] Brinkert et al., ZD 2013, 152 (157); für eine Pflicht zur Selektion durch die Diensteanbieter Martini, JZ 2012, 1145 (1152).

[207] Zur Umsetzung in der Praxis z. B. Martini, JZ 2012, 1145 (1146 f.) [s. a. ebd., 1154 f. zu weiteren rechtlichen und tatsächlichen Gestaltungsüberlegungen]; Brinkert et al., ZD 2013, 152 (156 f.); Brisch/Müller-ter Jung, CR 2013, 446 (447 f.); die Problematik der Vermögensrechte bleibt hier außer Betracht.

[208] S. o. Rn. 24 ff.

[209] S. o. Rn. 28 ff.

ein erheblicher Gestaltungsspielraum hinsichtlich des anwendbaren Rechts eröffnen. Im Rahmen eines solchen „Forum Shoppings" spricht nichts dafür, dass sich die Anbieter ausgerechnet für das vergleichsweise strenge deutsche Datenschutzrecht entscheiden. Die in diesem Kapitel erläuterten Anforderungen wären damit weithin **ohne praktische Relevanz** gerade bei den beliebtesten Social Media.

Dieses und weitere der aufgezeigten Probleme könnten im Rahmen der aktuellen **113**
europäischen Reform angegangen werden. Bislang sind die Vorschläge vor allem der Europäischen Kommission allerdings noch von einem Abstraktionsgrad, der in Verbindung mit den ausufernden Befugnisnormen zur Verabschiedung von delegierten Rechtsakten und Durchführungsakten nicht nur primärrechtlich problematisch ist,[210] sondern auch Aussagen über die konkreten Folgen der Reform für Social Media erschwert.

Wie auch immer die künftige datenschutzrechtliche Regulierung von Social Me- **114**
dia strukturiert sein wird – es spricht alles dafür, dass die mit ihnen verbundene Verarbeitung personenbezogener Daten sogar noch zunehmen wird. Den damit verbundenen Risiken für die Persönlichkeit der Nutzer kann mit rechtlichen Vorgaben nur begrenzt begegnet werden. Neben der erforderlichen Förderung von Medienkompetenz (Datenschutz als Bildungsaufgabe[211]) führt dies letztlich im Kern zur **Notwendigkeit neuer sozialer Regeln für den Umgang mit dem perpetuierten Wissen über andere**. Hierfür sind freilich bislang höchstens Ansätze erkennbar.

Literatur

Albers, M. (2005). *Informationelle Selbstbestimmung*. Baden-Baden: Nomos.
Altenhain, K., Heitkamp, A. (2009). Altersverifikation mittels des elektronischen Personalausweises. *K & R*, 619 ff.
Art. 29-Datenschutzgruppe. *Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU*. Brüssel 2002.
Art. 29-Datenschutzgruppe. *Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke*. Brüssel 2009.
Art. 29-Datenschutzgruppe. *Stellungnahme 8/2010 zum anwendbaren Recht*. Brüssel 2010.
Ausloos, J. (2012). The ‚Right to be Forgotten' – Worth remembering? *CLSR*, 143 ff.
Bäumler, H. (2001). Audits und Gütesiegel im Datenschutz. *CR*, 795 ff.
Bäumler, H. (2002). Marktwirtschaftlicher Datenschutz. Audit und Gütesiegel à la Schleswig-Holstein. *DuD*, 325 ff.
Bäumler, H. (2004). Ein Gütesiegel für den Datenschutz. Made in Schleswig-Holstein. *DuD*, 80 ff.
Berberich, M. (2010). Der Content „gehört" nicht Facebook! AGB-Kontrolle der Rechteeinräumung an nutzergenerierten Inhalten. *MMR*, 736 ff.
Böckenförde, T. (2008). Auf dem Weg zur elektronischen Privatsphäre. *JZ*, 925 ff.

[210] S. schon Hornung, ZD 2012, 99 (104 ff.); ebenfalls krit. zur Rolle der Kommission im Entwurf Costa/Poullet, CLSR 2012, 254 (560 f.); Roßnagel, DuD 2012, 553; Schild/Tinnefeld, DuD 2012, 312 (316 f.); Traung, Cri 2012, 33 (34 f.); Roßnagel et al., ZD 2013, 103 (104).
[211] S. v. a. Wagner, DuD 2010, 557; ders., DuD 2012, 83.

Borges, G. (2010). Der neue Personalausweis und der elektronische Identitätsnachweis. *NJW*, 3334 ff.
Borking, J. J. (1998). Einsatz datenschutzfreundlicher Technologien in der Praxis. *DuD*, 636 ff.
Borking, J. J. (2001). Privacy-Enhancing Technologies (PET). Darf es ein bisschen weniger sein? *DuD*, 607 ff.
Bräutigam, P. (2012). Das Nutzungsverhältnis bei sozialen Netzwerken. Zivilrechtlicher Austausch von IT-Leistungen gegen personenbezogene Daten. *MMR*, 635 ff.
Breyer, P. (2009). Verkehrssicherungspflichten von Internetdiensten im Lichte der Grundrechte. *MMR*, 14 ff.
Brinkert, M., Stolze, M. & Heidrich, J. (2013). Der Tod und das soziale Netzwerk. Digitaler Nachlass in Theorie und Praxis. *ZD*, 152 ff.
Brisch, K., Müller-ter Jung, M. (2013). Digitaler Nachlass – Das Schicksal von E-Mail- und De-Mail-Accounts sowie Mediencenter-Inhalten. Anforderungen an Internet-Provider nach dem Tode des Account-Inhabers. *CR*, 446 ff.
Brunst, P. W. (2009).Zur Frage des Eingriffs in das Fernmeldegeheimnis durch die Beschlagnahme von E-Mails. *CR*, 591 ff.
Bundesverband Informationswirtschaft, Telekomminikation und neue Medien e. V. (BITKOM). (2011). *Soziale Netzwerke*.
Caspar, J. (2012). Das aufsichtsbehördliche Verfahren nach der EU-Datenschutz-Grundverordnung, Defizite und Alternativregelungen. *ZD*, 555 ff.
Caspar, J. (2013). Soziale Netzwerke – Endstation informationelle Selbstbestimmung? Ein Bericht aus der Behördenpraxis. *DuD*, 767 ff.
Costa, L., Poullet, Y. (2012). Privacy and the regulation of 2012. *CLSR*, 254 ff.
Custers, B., Hof, S. van der Schermer, B., Appleby-Arnold, S. & Brockdorff, N. (2013). Informed Consent in Social Media Use. The Gap between User Exspectations and EU Personal Data Protection Law. *SCRIPTed*, 435 ff.
Däubler, W., Hjort, J. P., Schubert, M., Wolmerath, M., Ahrendt, M. & Mayer, U. R. (Hrsg.) (2010). *Arbeitsrecht. Handkommentar*. 2. Aufl. Baden-Baden: Nomos.
Däubler, W., Klebe, T., Wedde, P. & Weichert, T. (Hrsg.) (2013). *Bundesdatenschutzgesetz. Kompaktkommentar*. 4. Aufl. Frankfurt am Main: Bund Verlag.
Dehmel, S., Hullen, N. (2013). Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher. *ZD*, 147 ff.
Dietrich, F., Ziegelmayer, D. (2013). Facebook's „Sponsored Stories" – ein personenbezogenes unlauteres Vergnügen. Anwendbares Recht und AGB-rechtliche Beurteilung der Werbeform „Sponsored Stories" (Gesponserte Meldungen). *CR*, 104 ff.
Dix, A. (2012). Datenschutzaufsicht im Bundesstaat – ein Vorbild für Europa. *DuD*, 318 ff.
Dolderer, M. (2000). *Objektive Grundrechtsgehalte*. Berlin: Duncker & Humblot.
Eifert, M. (2009). Freie Persönlichkeitsentfaltung in sozialen Netzen: rechtlicher Schutz von Voraussetzungen und gegen Gefährdungen der Persönlichkeitsentfaltung im Web 2.0, in: Christoph Bieber, Martin Eifert Thomas Groß & Jörn Lamla, *Soziale Netze in der digitalen Welt. Das Internet zwischen egalitärer Teilhabe und ökonomischer Macht*, 253 ff. Frankfurt: Campus.
Eifert, M., Hoffmann-Riem, W. (2011). *Innovation, Recht und öffentliche Kommunikation*. Berlin: Duncker & Humblot.
Erd, R. (2010). Soziale Netzwerke und Datenschutz – am Beispiel Facebook, in: Jürgen Taeger (Hrsg.), *Digitale Evolution. Herausforderungen für das Informations- und Medienrecht, Tagungsband Herbstakademie 2010*, 253 ff. Edewecht: OlWIR.
Erd, R. (2011). Datenschutzrechtliche Probleme sozialer Netzwerke. *NVwZ*, 19 ff.
Ernst, S. (2010). Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem. *NJOZ*, 1917 ff.
Ernst, S. (2011). Social Networks und Arbeitnehmer-Datenschutz. *NJOZ*, 953 ff.
europe-v-facebook.org – Verein zur Durchsetzung des Grundrechts auf Datenschutz (2012). Wien. Abrufbar unter: http://europe-v-facebook.org/.
Forst, G. (2010). Bewerberauswahl über soziale Netzwerke im Internet? *NZA*, 427 ff.

Gabriel, U., Albrecht, S. (2010). Filesharing-Dienste. Grundrechte und (k)eine Lösung? *ZUM*, 392 ff.

Gola, P., Schomerus, R. (2012). *Bundesdatenschutzgesetz, Kommentar*. 11. Aufl. München: C. H. Beck.

Gounalakis, G., Klein, C. (2010). Zulässigkeit von personenbezogenen Bewertungsplattformen. Die „Spickmich"-Entscheidung des BGH vom 23.6.2009. *NJW*, 566 ff.

Grabenwarter, C., Pabel, K. (2012). Europäische Menschenrechtskonvention. Ein Studienbuch. 5. Aufl. München: C. H. Beck.

Haase, M. S. (2013), Rechtsfragen des digitalen Nachlasses, in: Jürgen Taeger (Hrsg.), *Law as a Service (LaaS). Recht im Internet- und Cloud-Zeitalter, Tagungsband Herbstakademie 2013*, 379 ff. Edewecht: OlWIR.

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI). (2011). *Prüfung der nach Abmeldung eines Facebook-Nutzers verbleibenden Cookies*.

Harbinja, E. (2013). Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives? *SCRIPTed*, 19 ff.

Härting, N. (2012). Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf. *BB*, 459 ff.

Härting, N. (2013). Anmerkung zum Urteil des Schleswig-Holsteinischen Verwaltungsgerichts vom 9.10.2013 (8 A 14/12; K & R 2013, 824), Zur rechtswidrigen datenschutzrechtlichen Untersagung von Facebook-Fanpages. *K & R*, 828.

Heinemann, M. J., Heinemann, D. (2013). Postmortaler Datenschutz. *DuD*, 242 ff.

Helberger, N., van Hoboken, J. (2010). Little Brother Is Tagging You. Legal and Policy Instruments of Amateur Data Controllers. *CRi*, 101 ff.

Hert, P., Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *CLSR*, 130 ff.

Herzog, S. (2013). Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, *NJW*, 3745 ff.

Hoeren, T. (2005). Der Tod und das Internet. Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers. *NJW*, 2113 ff.

Hoeren, T., Sieber, U. (2013). *Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs*. München: C. H. Beck (Stand: 36. Ergänzungslieferung 2013).

Hoffmann, C., Schulz, S. E. & Brackmann, F. (2013). Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten. *ZD*, 122 ff.

Hoffmann-Riem, W. (2008). Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. *JZ*, 1009 ff.

Hoormann, M. O. (2011). Beschäftigtendatenschutz und Social Media, in: Jürgen Taeger (Hrsg.), *Die Welt im Netz. Folgen für Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2011*, 577 ff. Edewecht: OlWIR.

Höppner, J. (2011). Web Analytics und Datenschutz, in: Jürgen Taeger (Hrsg.), *Die Welt im Netz. Folgen für Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2011*, 477 ff., Edewecht: OlWIR.

Hornung, G. (2007). Anmerkung zum Urteil des EGMR vom 03.04.2007 (Application no. 62617/00). *MMR*, 431 ff.

Hornung, G. (2008). Ein neues Grundrecht. Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme. *CR*, 299 ff.

Hornung, G. (2010). Informationen über „Datenpannen". Neue Pflichten für datenverarbeitende Unternehmen. *NJW*, 1841 ff.

Hornung, G. (2011). Datenschutz durch Technik in Europa. Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht. *ZD*, 51 ff.

Hornung, G. (2012). Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012. *ZD*, 99 ff.

Hornung, G. (2013a). Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework, Innovation. *The European Journal of Social Science Research*, 181 ff.

Hornung, G. (2013b). Die europäische Datenschutzreform – Stand, Kontroversen und weitere Entwicklung, in: Matthias Scholz & Axel Funk (Hrsg.), *DGRI-Jahrbuch 2012*, 1 ff., Köln: Otto Schmidt.

Hornung, G. (2014). Europa und darüber hinaus. Konzepte für eine Neuregelung des Datenschutzes im Internet und in sozialen Netzwerken, in: Hermann Hill & Utz Schliesky (Hrsg.), *Die Neubestimmung der Privatheit. E-Volution des Rechts- und Verwaltungssystems IV*, 123 ff. Baden-Baden: Nomos,

Hornung, G., Hartl, K. (2014). Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und -audit. *ZD*, 219 ff.

Hornung, G., Hofmann, K. (2013). Ein „Recht auf Vergessenwerden"? Anspruch und Wirklichkeit eines neuen Datenschutzrechts. *JZ*, 163 ff.

Hornung, G., Hofmann, K. (2014). Die Zulässigkeit der Markt- und Meinungsforschung nach Datenschutz- und Wettbewerbsrecht (Teil 1), *WRP*, 776 ff.

Hornung, G., Möller, J. (2011). *Passgesetz, Personalausweisgesetz. Kommentar*. München: C. H. Beck.

Imhof, R. (2000). One-to-One-Marketing im Internet. Das TDDSG als Marketinghindernis. *CR*, 110 ff.

Jandt, S. (2006). Das neue TMG. Nachbesserungsbedarf für den Datenschutz im Mehrpersonenverhältnis. *MMR*, 652 ff.

Jandt, S., Roßnagel, A. (2011). Datenschutz in Social Networks. Kollektive Verantwortlichkeit für die Datenverarbeitung. *ZD*, 160 ff.

Jandt, S., Roßnagel, A. (2011). Social Networks für Kinder und Jugendliche. Besteht ein ausreichender Datenschutz? *MMR*, 637 ff.

Jaspers, A. (2012). Die EU-Datenschutz-Grundverordnung. Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens. *DuD*, 571 ff.

Jickeli, J., Knothe, H.-G., Singer, R., Stieper, M., Habermann, N., Staudinger, J. von & Albrecht, K.-D. (Begr.) (2012). *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch. Mit Einführungsgesetz und Nebengesetzen*. Neubearb. 2012. Berlin: Sellier – de Gruyter.

Jotzo, F. (2009). Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr? *MMR*, 232 ff.

Kahler, T. (2013). Die Europarechtswidrigkeit der Kommissionsbefugnisse in der Grundverordnung. Oder: Die überfällige Reform der deutschen und europäischen Datenschutzaufsicht. *RDV*, 69 ff.

Kaiser, A.-B. (2009). Bewertungsportale im Internet. Die spickmich-Entscheidung des BGH. *NVwZ*, 1474 ff.

Kamp, J. (2011). *Personenbewertungsportale. Eine datenschutzrechtliche und äußerungsrechtliche Untersuchung unter besonderer Berücksichtigung des Lehrerbewertungsportals spickmich.de*. München: C. H. Beck.

Karg, M. (2012). Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken. *HFR*, 120 ff.

Karg, M. (2013). Anmerkung: VG Schleswig: Keine Anwendbarkeit deutschen Datenschutzrechts auf Facebook. *ZD*, 245 ff.

Karg, M. (2013). Anwendbares Datenschutzrecht bei Internet-Diensteanbietern TMG und BDSG vs. Konzernstrukturen? *ZD*, 371 ff.

Karg, M. (2014). Anmerkung: VG Schleswig: Verbot von Facebook-Fanseiten, Urteil vom 9.10.2013 – 8 A 14/12. *ZD*, 51 ff.

Karg, M., Fahl, C. (2011). Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken. *K & R*, 453 ff.

Kasket, E. (2013). Access to the Digital Self in Life and Death: Privacy in the Context of Posthumously Persistent Facebook Profiles. *SCRIPTed*, 7 ff.

Kipker, D.-K., Voskamp, F. (2012). Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung. *DuD*, 737 ff.

Klein, O. (2009). Offen und (deshalb) einfach. Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider. *NJW*, 2996 ff.

Kodde, C. (2013). Die „Pflicht zu Vergessen". „Recht auf Vergessenwerden" und Löschung in BDSG und DS-GVO. *ZD*, 115 ff.

Köhler, C. M. (2011). *Persönlichkeitsrechte im Social Web – verlorene Grundrechte? Der Lehrer am Pranger in der virtuellen Welt*. Hamburg: Verlag Dr. Kovac.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder. (2010). *Ein modernes Datenschutzrecht für das 21. Jahrhundert*.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2013). *Orientierungshilfe „Soziale Netzwerke"*.

Koreng, A., Feldmann, T. (2012). Das „Recht auf Vergessen". Überlegungen zum Konflikt zwischen Datenschutz und Meinungsfreiheit. *ZD*, 311 ff.

Kort, M. (2012). Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda. *DB*, 1020 ff.

Kremer, S., Buchalik, B. (2013). Zum anwendbaren Datenschutzrecht im internationalen Geschäftsverkehr. Internationales Privatrecht und rechtliche Vorgaben in Deutschland in der Korrektur von LG Berlin, Urt. v. 30.4.2013–15 O 92/12. CR 2013, 402 ff. *CR*, 789 ff.

Lacher, J. (2012). *Rechtliche Grenzen der Kommunikation über ärztliche Leistungen. Arztwerberecht Ärzte-Rankings Arztbewertungsportale*. Hamburg: Verlag Dr. Kovac.

Lang, M. (2012). Reform des EU-Datenschutzrechts. Einheitliche Regelungen mit hohem Datenschutzniveau geplant. *K & R*, 145 ff.

Lange, C. (2013). Impressumspflichten in sozialen Netzwerken. *ZJS*, 141 ff.

Lauber-Rönsberg, A. (2013). Rechtliche Rahmenbedingungen für Personenbewertungsportale, in: Jürgen Taeger (Hrsg.), *Law as a Service (LaaS). Recht im Internet- und Cloud-Zeitalter, Tagungsband Herbstakademie 2013*, 181 ff., Edewecht: OlWIR.

Lerch, H., Krause, B., Hotho, A., Roßnagel, A. & Stumme, G. (2010). Social Bookmarking-Systeme – die unerkannten Datensammler. Ungewollte personenbezogene Datenverarbeitung? *MMR*, 454 ff.

Maisch, M. M. (2010). Facebooks Social Plugins als Herausforderung im Datenschutz- und Telemedienrecht. *AnwZert ITR*.

Martini, M. (2012). Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet. *JZ*, 1145 ff.

Martini, M., Fritzsche, S. (2013). Zwischen Öffentlichkeitsauftrag und Gesetzesbindung: zum Dilemma deutscher Behörden bei der Einbindung privater Social-Media-Werkzeuge und Geodatendienste in ihre Internetangebote. *VerwArch*, 449 ff.

Maunz, T., Dürig, G. (Begr.) (2013). *Grundgesetz, Kommentar*. München: C. H. Beck (Stand: 69. Ergänzungslieferung 2013).

Mayer-Schönberger, V. (2011). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press.

Meyer, S. (2011). Datenschutz – Gefällt mir!, in: Jürgen Taeger (Hrsg.), *Die Welt im Netz. Folgen für Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2011*, 545 ff., Edewecht: OlWIR.

Meyer, S. (2012). Facebook: Freundefinder und AGB rechtswidrig. Zugleich Kommentar zu LG Berlin, Urt. v. 8.3.2012–16 O 551/10, K & R 2012, 300 ff. *K & R*, 309 ff.

Möller, M. (2005). Rechtsfragen im Zusammenhang mit dem Postident-Verfahren. *NJW*, 1605 ff.

Moser, J. (2011). Datenverarbeitung im Auftrag des Nutzers, in: Jürgen Taeger (Hrsg.), *Die Welt im Netz. Folgen für Wirtschaft und Gesellschaft, Tagungsband Herbstakademie 2011*, 595 ff., Edewecht: OlWIR.

Moser-Knierim, A. (2013). „Facebook-Login" – datenschutzkonformer Einsatz möglich? Einsatz von Social Plug-ins bei Authentifizierungsdiensten. *ZD*, 263 ff.

Niemann, F., Scholz, P. (2012). Privacy by Design und Privacy by Default. Wege zu einem funktionierenden Datenschutz in Sozialen Netzwerken, in: Falk Peters, Heinrich Kersten

& Klaus-Dieter Wolfenstetter (Hrsg.), *Innovativer Datenschutz*, 109 ff., Berlin: Duncker & Humblot.
Oberwetter, C. (2008). Bewerberprofilerstellung durch das Internet – Verstoß gegen das Datenschutzrecht? *BB*, 1562 ff.
Oberwetter, C. (2011). Soziale Netzwerke im Fadenkreuz des Arbeitsrechts. *NJW*, 417 ff.
Ott, S. (2009). Das Internet vergisst nicht – Rechtsschutz für Suchobjekte? *MMR*, 158 ff.
Pahlen-Brandt, I. (2008). Datenschutz braucht scharfe Instrumente. *DuD*, 34 ff.
Peifer, K.-N., Kamp, J. (2009). Datenschutz und Persönlichkeitsrecht. Anwendung der Grundsätze über Produktkritik auf das Bewertungsportal spickmich.de? *ZUM*, 185 ff.
Piltz, C. (2011). Der Like-Button von Facebook. Aus datenschutzrechtlicher Sicht: "gefällt mir nicht". *CR*, 657 ff.
Piltz, C. (2012). Anmerkung zu einer Entscheidung des LG Berlin, Urteil vom 06.03.2012 (16 O 551/10; CR 2012, 270) – Zur Zulässigkeit einer Erteilung von so genannten IP-Lizenzen in den Allgemeinen Geschäftsbedingungen von Facebook und zur Geltung deutschen Datenschutzrechts für diese Plattform sowie zur Mittäterschaft bei der Versendung von Einladungen zum Eintritt in das soziale Netzwerk. *CR*, 274 f.
Piltz, C. (2012). Rechtswahlfreiheit im Datenschutzrecht? „Diese Erklärung unterliegt deutschem Recht". *K & R*, 640 ff.
Piltz, C. (2013). Anmerkung zur Entscheidung des Schleswig-Holsteinischen VG vom 14.02.2013 (8 B 60/12) – Zur Rechtmäßigkeit der Sperrung von Nutzerkonten ohne Klarnamen in sozialen Netzwerken. *K & R*, 283 f.
Piltz, C. (2013). Der räumliche Anwendungsbereich europäischen Datenschutzrechts. Nach geltendem und zukünftigem Recht. *K & R*, 292 ff.
Polenz, S. (2012). Die Datenverarbeitung durch und via Facebook auf dem Prüfstand. *VuR*, 207 ff.
Raabe, O., Lorenz, M. (2011). Die datenschutzrechtliche Einwilligung im Internet der Dienste. Zur Notwendigkeit qualifizierter elektronischer Signaturen. *DuD*, 279 ff.
Redeker, H. (2012). *IT-Recht*. 5. Aufl. München: C. H. Beck.
Reding, V. (2010). *Privacy matters – Why the EU needs new personal data protection rules. The European Data Protection and Privacy Conference*. Brüssel.
Rogosch, P., Hohl, E. (2012). *Data protection and Facebook. An empirical analysis of the role of consent in social networks*. Münster: Lit Verlag.
Rolf, C., Rötting, M. (2009). Google, Facebook & Co als Bewerberdatenbank für Arbeitgeber? *RDV*, 263 ff.
Roßnagel, A. (1997). Datenschutz-Audit. *DuD*, 505 ff.
Roßnagel, A. (1997). Globale Datennetze – Ohnmacht des Staates – Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society". *ZRP* 1997, 26 ff.
Roßnagel, A. (2000). Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung. Wiesbaden: Vieweg.
Roßnagel, A. (Hrsg.) (2001). *Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz Datenschutz Jugendschutz und Vielfaltschutz, Tagungsband Stiftungstagung (zugleich EMR-Workshop)*. Baden-Baden: Nomos.
Roßnagel, A. (Hrsg.) (2003). *Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung*. München: C. H. Beck.
Roßnagel, A. (2011). Datenschutzaudit – ein modernes Steuerungsinstrument, in: Leon Hempel, Susanne Krasmann & Ulrich Bröckling (Hrsg.), *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010, 263 ff.*, Wiesbaden: VS Verlag.
Roßnagel, A. (2012). Datenschutzgesetzgebung. Monopol oder Vielfalt? *DuD*, 553 ff.
Roßnagel, A. (Hrsg.) (2013). *Beck'scher Kommentar zum Recht der Telemediendienste*, München: C. H. Beck.
Roßnagel, A., Hornung, G. (2009). Ein Ausweis für das Internet. Der neue Personalausweis erhält einen „elektronischen Identitätsnachweis". *DÖV*, 301 ff.

Roßnagel, A., Schnabel, C. (2008). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht. *NJW*, 3534 ff.
Roßnagel, A., Scholz, P. (2000). Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. *MMR*, 721 ff.
Roßnagel, A., Pfitzmann, A. & Garstka, H. (2001). *Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern*. Berlin.
Roßnagel, A., Banzhaf, J. & Grimm, R. (2003). *Datenschutz im electronic commerce*. Heidelberg: Fachmedien Recht und Wirtschaft.
Roßnagel, A., Richter, P. & Nebel, M. (2013). Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DS-GVO, *ZD*, 103 ff.
Rost, M., Pfitzmann, A. (2009). Datenschutz-Schutzziele – revisited. *DuD*, 353 ff.
Schaar, P. (2001). Datenschutzrechtliche Einwilligung im Internet. *MMR*, 644 ff.
Schenk, M., Niemann, J., Reinmann, G., Roßnagel, A. (Hrsg.) (2012), *Digitale Privatsphäre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen*, Berlin: Vistas.
Schiedermair, S. (2012). *Der Schutz des Privaten als internationales Grundrecht*. Tübingen: Mohr Siebeck.
Schild, H.-H., Tinnefeld, M.-T. (2012). Datenschutz in der Union. Gelungene oder missglückte Gesetzentwürfe? *DuD*, 312 ff.
Schlichting, G. (Begr.) (2010). *Münchner Kommentar zum Bürgerlichen Gesetzbuch (BGB)*. Bd. 9 Erbrecht §§ 1922–2385, §§ 27–35 BeurkG. 5. Aufl. München: C. H. Beck.
Schnabel, C., Freund, B. (2010). „Ach wie gut, dass niemand weiß. . .“ – Selbstdatenschutz bei der Nutzung von Telemedienangeboten. *CR*, 718 ff.
Schneider, M. (2013). Die datenschutzrechtliche Dimension von Smartphone-Messengern wie WhatsApp, in: Jürgen Taeger (Hrsg.), *Law as a Service (LaaS). Recht im Internet- und Cloud-Zeitalter, Tagungsband Herbstakademie 2013*, 89 ff., Edewecht: OlWIR.
Scholz, P. (2003). *Datenschutz beim Internet-Einkauf*. Baden-Baden: Nomos.
Schulz, S. E. (2009). Der neue „E-Personalausweis“ – elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement? *CR*, 267 ff.
Schüßler, L. (2010). Facebook und der Wilde Westen – Soziale Netzwerke und Datenschutz, in: Jürgen Taeger (Hrsg.), *Digitale Evolution. Herausforderungen für das Informations- und Medienrecht, Tagungsband Herbstakademie 2010*, 233 ff., Edewecht: OlWIR.
Schwab, D. (2012). Persönlichkeitsrecht und Erbe, in: Jürgen Damrau & Karlheinz Muscheler (Hrsg.), *Erbrecht und Vermögensnachfolge, Festschrift für Manfred Bengel und Wolfgang Reimann zum 70. Geburtstag*, 345 ff. München: C. H. Beck,
Simitis, S. (Hrsg.) (2011). *Bundesdatenschutzgesetz*. 7. Aufl. Baden-Baden: Nomos.
Solmecke, C., Dam, A. (2012). Wirksamkeit der Nutzungsbedingungen sozialer Netzwerke. *MMR*, 71 ff.
Solmecke, C., Wahlers, J. (2012). Rechtliche Situation von Social Media Monitoring-Diensten. Rechtskonforme Lösungen nach dem Datenschutz- und dem Urheberrecht. *ZD*, 550 ff.
Spiecker gen. Döhmann, I. (2012). Die Durchsetzung datenschutzrechtlicher Mindestanforderungen bei Facebook und anderen sozialen Netzwerken. *K & R*, 717 ff.
Spindler, G. (2012). *Persönlichkeitsschutz im Internet. Anforderungen und Grenzen einer Regulierung, in: Deutscher Juristentag (Hrsg.), Verhandlungen des 69. Deutschen Juristentages*. Teil F. München: C. H. Beck.
Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien. Kommentar*. 2. Aufl. München: C. H. Beck.
Spindler, G., Schmitz, P. & Geis, I. (2004). *Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz. Kommentar*. München: C. H. Beck.
Splittgerber, A. (Hrsg.) (2014). *Praxishandbuch Rechtsfragen Social Media*. Berlin: De Gruyter.
Stadler, T. (2011). Verstoßen Facebook und Google Plus gegen deutsches Recht? Ausschluss von Pseudonymen auf Social-Media-Plattformen. *ZD*, 57 ff.
Steenhoff, H. (2013). Das Internet und die Schulordnung. *NVwZ*, 1190 ff.

Stern, K. (1988). *Das Staatsrecht der Bundesrepublik Deutschland. Band III/1: Allgemeine Lehren der Grundrechte*. München: C. H. Beck.

Stern, K. (2010). Die Schutzpflichtenfunktion der Grundrechte: Eine juristische Entdeckung. *DÖV*, 241 ff.

Taeger, J., Gabel, D. (Hrsg.) (2013). *Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG*. 2. Aufl. Frankfurt am Main: Verlag Recht und Wirtschaft.

Tinnefeld, M.-T., Buchner, B. & Petri, T. (2012). *Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht*. 5. Aufl. München: Oldenbourg.

Traung, P. (2012). The Proposed New EU General Data Protection Regulation. *CRi*, 33 ff.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). *Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook*, abrufbar unter: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf, 2011.

Venzke-Caprarese, S. (2013). Social Media Monitoring. Analyse und Profiling ohne klare Grenzen? *DuD*, 775.

Voigt, P. (2013). Webbrowser Fingerprints – Tracking ohne IP-Adressen und Cookies?, in: Jürgen Taeger (Hrsg.), *Law as a Service (LaaS). Recht im Internet- und Cloud-Zeitalter, Tagungsband Herbstakademie 2013*, 157 ff., Edewecht: OlWIR.

Voigt, P., Alich, S. (2011). Facebook-Like-Button und Co. Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber. *NJW*, 3541 ff.

von Coelln, C. (2009). Zwischen Gütegarantie und Professorenpranger: Die Evaluation der Hochschullehre, in: Steffen Detterbeck, Jochen Rozek & Christian v. Coelln (Hrsg.), *Recht als Medium der Staatlichkeit. Festschrift für Herbert Bethge zum 70. Geburtstag*, 271 ff. Berlin: Duncker & Humblot.

Wagner, E. (2010). Datenschutz als Bildungsaufgabe. *DuD*, 557 ff.

Wagner, E. (2012).Datenschutz als Bildungsauftrag. *DuD*, 83 ff.

Weigl, M. (2011). *Meinungsfreiheit contra Persönlichkeitsschutz am Beispiel von Web-2.0-Applikationen*. Hamburg: Verlag Dr. Kovac.

Wilkat, A. (2013). *Bewertungsportale im Internet*. Baden-Baden: Nomos.

Wintermeier, M. (2012). Inanspruchnahme sozialer Netzwerke durch Minderjährige. *ZD*, 210 ff.

Wittern, F., Wichmann, M. (2012). Dürfen soziale Netzwerke auf die Adressbücher ihrer Nutzer zugreifen? *ITRB*, 133 ff.

Wolff, H.-A., Brink, S. (Hrsg.) (2013). *Beck'scher Online-Kommenar zum Datenschutzrecht*. 6. Aufl. München: C. H. Beck.

Wybitul, T., Fladung, A. (2012). EU-Datenschutz-Grundordnung. Überblick und arbeitsrechtliche Betrachtung des Entwurfs. *BB*, 509 ff.

Ziebarth, W. (2013). Das Datum als Geisel. Klarnamenspflicht und Nutzeraussperrung bei Facebook. *ZD*, 375 ff.

Ziebarth, W. (2013). Demokratische Legitimation und Unabhängigkeit der deutschen Datenschutzbehörden. Warum das durch die Rechtsprechung des EuGH (Rs. C-518/07, CR 2010, 339 und Rs. C-614/10) Erreichte durch den Entwurf für eine Datenschutz-Grundverordnung gefährdet wird. *CR*, 60 ff.

Kapitel 5
Haftungsrechtliche Probleme der Social Media

Gerald Spindler

Inhalt

5.1 Phänomene und relevante Sachverhalte

Soziale Netzwerke haben sich zu einem der wichtigsten Kommunikationsmittel der letzten fünf Jahre entwickelt und beginnen selbst traditionelle Dienste wie E-Mail, Suchmaschinen und eigene Webseiten zu verdrängen, indem diese Dienste in das **1**

G. Spindler (✉)
Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen, Deutschland
E-Mail: lehrstuhl.spindler@jura.uni-goettingen.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_5

soziale Netzwerk aufgenommen werden. Neben dem bekannten Netzwerk Facebook existieren zahlreiche spezialisierte, teilweise auch für bestimmte Sprachen oder Regionen entwickelte soziale Netzwerke, sei es für Berufstätige wie XING im deutschen Sprachraum oder LinkedIn für den angelsächsischen bzw. internationalen Raum, seien es etwa chinesische soziale Netzwerke wie Sina Weibo oder Qzone.[1] Charakteristisch für soziale Netzwerke ist neben dem Betreiben des Online-Portals die Dreiecksbeziehung zwischen dem Betreiber des Netzwerks und den jeweiligen Nutzern untereinander; dabei kann die Kommunikation von einer bilateralen Struktur bis hin zu massenmedienähnlichen Verbreitungen reichen.[2]

2 Aus haftungsrechtlicher Sicht kommen entlang dieser Beziehungen mehrere Problemfelder in Betracht: Zum einen Haftungen der Nutzer für deliktische Handlungen, etwa im Bereich der Kommunikationsdelikte (Beleidigung, unwahre Tatsachen etc.) oder von Urheberrechtsverletzungen, zum anderen eine Verantwortlichkeit der Netzwerkbetreiber für die Sicherheit der Plattformen, aber auch ihre Haftung als Teilnehmer (im weitesten Sinne) der Delikte der Nutzer selbst, hier insbesondere im Rahmen der Störerhaftung. Schließlich ist auch danach zu differenzieren, ob deliktische Handlungen Teilnehmer auf der Plattform selbst treffen oder außenstehende Dritte.

3 Auf Fragen der datenschutzrechtlichen Verantwortlichkeit sowie der zivilrechtlichen Haftung wegen Verletzung von Strafgesetzen als Schutzgesetze gem. § 823 Abs. 2 BGB wird im Folgenden nicht näher eingegangen, da sie Gegenstand anderer Kapitel sind.[3]

5.2 Delikte

5.2.1 Deliktische Handlungen der Nutzer

4 Entsprechend der Vielfalt der Nutzungshandlungen über soziale Netzwerke, die letztlich die gleichen Möglichkeiten wie das Internet als Kommunikationsplattform selbst bieten, ergeben sich zahlreiche in Betracht kommende Delikte:

5.2.1.1 Kommunikationsdelikte

5 In Betracht kommen zunächst Kommunikationsdelikte der Nutzer untereinander. Bekannt ist das sog. **Cyberbullying**, indem andere Nutzer angeprangert werden. Die

---

[1] Näher dazu Hohlfeld, Kap. 2 Rn. 32 ff.

[2] S. dazu Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen des 69. Deutschen Juristentages, Band I, 2012, F 11.

[3] Zu in Betracht kommenden Strafnormen s. Esser, Kap. 7, zu datenschutzrechtlichen Fragen und der entsprechenden Haftung Hornung, Kap. 4.

aus dem klassischen Medienrecht bzw. Kommunikationsrecht bekannten Tatbestände sind auch hier einschlägig, allen voran die Verletzung des allgemeinen Persönlichkeitsrechts[4] nach § 823 Abs. 1 BGB (bzw. Art. 2 Abs. 1 GG)[5] sowie die Haftung für unwahre Tatsachenbehauptungen bzw. Kreditschädigung nach § 824 BGB, abgesehen von der Verletzung strafrechtlicher Schutzgesetze wie §§ 185 ff. StGB. Dabei kommt es nicht darauf an, ob ein Nutzer eine Vielzahl von Empfängern mit seiner ehrverletzenden Nachricht erreicht hat, was allerdings für die Schadensberechnung relevant sein kann; vielmehr genügt auch die rein bilaterale Ehrverletzung.[6] Entsprechend der von der Rechtsprechung herangezogenen Sphärentheorie hängt die Abwägung davon ab, ob die jeweilige Äußerung in der Privat- oder Sozialsphäre vorgenommen wurde, zudem welches Vorverhalten die Kommunikationsstrukturen geprägt hat. Auch die Verletzung des Rechts am eigenen Bild, §§ 22, 23, KunstUrhG gehört zu den Kommunikationsdelikten im Rahmen des Persönlichkeitsrechts. Einzelheiten hierzu bei *Müller-Terpitz* (Kap. 6).[7]

5.2.1.2 Urheberrechtsverletzungen und andere Immaterialgüterrechte

Urheberrecht Neben den eigentlichen Kommunikationsdelikten nehmen offenbar in der letzten Zeit Urheberrechtsverletzungen durch Nutzer zu. Festzuhalten ist hier zunächst, dass jedes Hochladen auf ein soziales Netzwerk zum Tausch eines urheberrechtlich geschützten Werkes (Musik, Bild, Film, Texte, Software, Datenbanken etc.)[8] bereits bedingt, dass der Nutzer das Werk vervielfältigen darf, da eine neue Kopie des Werkes auf dem Server des sozialen Netzwerkes angefertigt wird, § 16 UrhG – auch wenn es sich nur um ein sog. Miniatur- bzw. Vorschaubild handelt.[9] **6**

Stellt der Nutzer diese Kopie nur einem eng begrenzten „Freundes"-Kreis zur Verfügung, kommt der Nutzer in den Genuss der Schranke der **Privatkopie**, § 53 Abs. 1 UrhG. Entscheidend ist allerdings, dass es sich noch um einen privaten Kreis handelt, im Gegensatz zur Öffentlichkeit gem. § 15 Abs. 3 UrhG. Andernfalls liegt ein öffentliches Zugänglichmachen nach § 19a UrhG vor,[10] für das keinerlei Schranke **7**

---

[4] Dazu jüngst OLG Frankfurt, GRURPrax 2013, 342, im Volltext: JurPC Web-Dok. 149/2013, abrufbar unter: http://www.jurpc.de/jurpc/show?id=20130149.

[5] Zum – allerdings eher akademischen – Streit um die anwendbare Anspruchsgrundlage s. Müller, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 51 Rn. 321 ff.

[6] Rixecker, in: MüKo-BGB, Anhang zu § 12 Rn. 3278 f.; zur Beleidigung nach § 185 StGB: Kühl, in: Lackner/Kühl, StGB, § 185 Rn. 322; Lenckner/Eisele, in: Schönke/Schröder, StGB, § 185 Rn. 321.

[7] Eingehend auch Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen des 69. Deutschen Juristentages, Band I, 2012, F 41 zu sozialen Netzwerken und Sphärentheorie sowie F 53 zum Recht am eigenen Bild; ferner Peifer, JZ 2013, 853 ff.

[8] Auf die Voraussetzungen des Urheberrechtsschutzes kann hier nicht näher eingegangen werden, s. dazu Loewenheim, in: Schricker/Loewenheim, UrhR, § 2 UrhG Rn. 328 ff.; Schack, Urheber- und Urhebervertragsrecht, S. 98 ff.

[9] Rosenbaum/Tölle, MMR 2013, 209 (212).

[10] S. nur LG Halle, BeckRS 2012, 13612.

zugunsten des Nutzers eingreift. Der Begriff der „**Öffentlichkeit**“ wurde in diesem Zusammenhang als ein überschaubarer Kreis persönlich bekannter Personen von max. 15–20 Teilnehmern angesehen; allerdings stammen diese Kriterien aus einer Zeit, die keine virtuelle Kommunikation kannte, so dass es fraglich erscheint, ob zum einen tatsächlich ein real-physischer Kontakt zwischen den „Freunden“ erforderlich ist, zum anderen ob die Zahl der persönlich Bekannten noch auf eine Zahl von bis zu 20 Personen eingeschränkt werden kann. Eine moderate Modifizierung des Öffentlichkeitsbegriffs scheint hier angebracht; andererseits kann kaum noch von privat bekannten Freunden gesprochen werden, wenn deren Zahl mehr als 50 beträgt, erst recht nicht bei „Freunden von Freunden“, die zum Teilen von Werken zugelassen werden.

8 Unter dem Begriff der „Öffentlichkeit“ wird in diesem Zusammenhang überwiegend ein Kreis persönlich bekannter Personen verstanden, wobei keine absolute Grenze an Teilnehmern besteht.[11] Je größer aber deren Kreis ist, desto eher wird eine Öffentlichkeit zu bejahen sein.[12] Allerdings kommt es nicht darauf an, ob ein real-physischer Kontakt besteht.[13] Zwar wird in der „analogen Welt“ teilweise auch dann nicht der persönliche Bezug ausgeschlossen, wenn zu einer Veranstaltung vereinzelt Freunde oder Bekannte der Gäste zugelassen werden.[14] Diese Grenze wird im sozialen Netzwerk aber jedenfalls dann überschritten, wenn generell auch Freunde von Freunden einbezogen werden.[15] Andererseits spricht der „Freunde-Status“ alleine nicht für eine persönliche Beziehung.[16] Denn es muss ein Bewusstsein einer persönlichen Verbindung bestehen, das über die bloße Bekanntschaft hinausgeht,[17] was aber nicht bedeutet, dass die Verbindung freundschaftlicher oder familiärer Natur

[11] Schulze, in: Dreier/Schulze, UrhG, § 15 Rn. 3243; Heerma, in: Wandtke/Bullinger, UrhR, § 15 Rn. 3220; v. Ungern-Sternberg, in: Schricker/Loewenheim, UrhR, § 15 Rn. 3275; Dustmann, in: Fromm/Nordemann, UrhR, § 15 Rn. 3231; Hoeren, in: Loewenheim, Handbuch Urheberrecht, § 21 Rn. 3224.

[12] Hoeren, in: Loewenheim, Handbuch des Urheberrecht, § 21 Rn. 24; Schulze, in: Dreier/Schulze, UrhG, § 15 Rn. 43; Heerma, in Wandtke/Bullinger, UrhR, § 15 Rn. 20; als extremes Beispiel: AG Bochum GRUR-RR 2009, 166 (167), das 600 Teilnehmer einer Hochzeit noch als persönlich verbunden anerkannte; a. A. v. Ungern-Sternberg, in: Schricker/Loewenheim, UrhR, § 15 Rn. 75, der bei „Hunderten von Beteiligten“ den persönlichen Charakter verneint.

[13] v. Ungern-Sternberg, in: Schricker/Loewenheim, UrhR, § 15 Rn. 75.

[14] Heerma, in Wandtke/Bullinger, UrhR, § 15 Rn. 19; v. Ungern-Sternberg, in: Schricker/Loewenheim, UrhR, § 15 Rn. 76; a. A. Schulze, in: Dreier/Schulze, UrhG, § 15 Rn. 43; BGH, GRUR 1955, 549 (551); GRUR 1960, 338 (339).

[15] Entsprechend will Heerma, in: Wandtke/Bullinger, UrhR, § 15 Rn. 19 dann den persönlichen Charakter entfallen lassen, „wenn gezielt auch dieser Personenkreis angesprochen wird.“

[16] Ebenso Schapiro, ZUM 2008, 273 (276) für eine Musiktauschbörse, auf der nur mit Freunden getauscht werden kann.

[17] Heerma, in Wandtke/Bullinger, UrhR, § 15 Rn. 18; Schulze, in: Dreier/Schulze, UrhG, § 15 Rn. 43; BGH, GRUR 1984, 734 (735) – Vollzugsanstalten; GRUR 1996, 875 (876) – Zweibettzimmer im Krankenhaus.

sein muss.[18] Die bloße Mitgliedschaft in einer gemeinsamen Gruppe alleine genügt nicht, da ein bloßes sachbezogenes, gemeinsames Interesse nicht für eine persönliche Verbundenheit ausreicht.[19]

9 Nach bislang gefestigter Rechtsprechung stellt dagegen das Anbieten eines Links, der zu einem Werk führt, noch keinen urheberrechtlich relevanten Verwertungsvorgang dar, da es sich um sozialadäquate Nutzungshandlungen im Internet handelt.[20] Allerdings kann dies zweifelhaft werden, wenn der Link derart in einem Angebot eingebettet wird, dass er die unmittelbare Wiedergabe ersetzt (inline-linking, **Framing**). Nach Ansicht des BGH liegt zwar keine öffentliche Zugänglichmachung nach § 19a UrhG vor[21], da hier entsprechend der Beurteilung in der *Paperboy*-Entscheidung weiterhin derjenige über die Verfügbarkeit des Inhalts entscheide, der es ursprünglich ins Netz gestellt hat.[22] Allerdings erspare sich hier der Nutzer das eigene (zustimmungsbedürftige) Vorhalten des (verlinkten) Inhalts und nehme so eine zentrale Rolle bei der Werkvermittlung ein, ähnlich einem Deep Link, der eine Schutzmaßnahme umgeht[23], so dass bei wertender Betrachtung eine öffentliche Wiedergabe i. S. d. Art. 3 Abs. 1 der Richtlinie 2001/29/EG[24] vorläge,[25] womit in richtlinienkonformer Auslegung eine dem deutschen Recht bislang unbekannte Nutzungsart gem. § 15 Abs. 2 UrhG anzunehmen sei.[26] Der Unterschied zu einem gewöhnlichen Link[27] sei, dass der Nutzer hier nicht nur den Zugang zum Werk erleichtere, sondern es sich zu eigen mache.[28]

10 Diese Wertung ist in dieser generellen Form nicht zwingend, denn man kann genauso gut einwenden, dass die Position des Einbettenden gerade nicht wie bei einem

---

[18] BGH, GRUR 1996, 875 (876) – Zweibettzimmer im Krankenhaus; GRUR 1984, 734 (735) – Vollzugsanstalten; OLG München, ZUM 1986, 482 (483); Hoeren, in: Loewenheim, Handbuch Urheberrecht, § 21 Rn. 25; Heerma, in: Wandtke/Bullinger, UrhR, § 15 Rn. 18; Dreier, in: Dreier/Schulze, § 15 Rn. 43; Schapiro, ZUM 2008, 273 (275 f.).

[19] So im Ergebnis auch für ein Online-Seminar auf einer E-Learning Plattform: Schöwerling, E-Learning und Urheberrecht an Universitäten, S. 136 ff.; Dustmann, in: Fromm/Nordemann, UrhR, § 15 UrhG Rn. 34; v. Ungern-Sternberg, in: Schricker/Loewenheim, UrhR, § 15 Rn. 76; Schulze, in: Dreier/Schulze, UrhG, § 15 Rn. 43; Hoeren, in: Loewenheim, Handbuch Urheberrecht, § 21 Rn. 24.

[20] BGHZ 156, 1 (18 f.) – Paperboy.

[21] Ebenso OLG München, ZUM-RD 2013, 398 (401); a. A. aber das OLG Düsseldorf, ZUM 2012, 327 (328).

[22] BGH, GRUR 2013, 818 (819) Rn. 9 – Die Realität.

[23] BGH, GRUR 2011, 56 Rn. 25 ff. – Session-ID.

[24] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. L 167 v. 22.6.2001, S. 10.

[25] Zur Öffentlichen Wiedergabe in der Rechtsprechung des EuGH ausführlich von Ungern-Sternberg, GRUR 2012, 1198; kritisch zur Erstreckung von Art. 3 Abs. 1 der Richtlinie 2001/29/EG auf Hyperlinks: Bentley/Derclaye et al., University of Cambridge Faculty of Law Research Paper No. 6/2013, abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220326.

[26] EuGH-Vorlage des BGH, GRUR 2013, 818 (820 f.) Rn. 26; siehe ferner das ähnliche Vorabentscheidungsersuchen des Svea hovrätt (Schweden), BeckEuRS 2012, 692873.

[27] BGHZ 156, 1 – Paperboy.

[28] BGH, GRUR 2013, 818 (820) Rn. 26 – Die Realität.

die Schutzvoraussetzungen umgehenden **Deep Link**[29] hervorgehoben ist, sondern vielmehr der Einbindung eines einfachen Links entspricht.[30] Das Argument, es dürfe nicht darauf ankommen, wie die technische Verwirklichung *in concreto* aussieht – also Speicherung auf der eigenen Web-Präsenz oder direkte Einbindung des Elements von einer fremden – lässt sich genauso gut dahingehend umkehren, dass es für eine anerkannt zulässige Verlinkung nicht darauf ankommen kann, in welcher optischen Form sie sich präsentiert, sondern nur, dass er weiterhin eine Verweisung darstellt. Letztlich sollte daher jedenfalls von einer generellen Erlaubnispflicht des Framings Abstand genommen und die konkrete Einbindung in die Seite betrachtet werden.[31] Entspricht der eingebundene Inhalt funktional einem gewöhnlichen Hyperlink, so sollte eine Einbindung auch in Form des Framing zulassungsfrei sein. Wird dagegen der Inhalt so in die Webpräsenz eingebunden, dass er ein integraler Bestandteil der Seite ist,[32] spricht mehr für eine Erlaubnispflicht – wobei dies im Interesse der Kommunikationsfreiheiten möglichst eng ausgelegt werden sollte. In sozialen Netzwerken ist das Framing weit verbreitet und wird v. a. als Mechanismus zum Teilen, auf der Pinnwand, Timeline, o. ä. oder in privaten Nachrichten relevant. Während die privaten Nachrichten in der Regel schon mangels Öffentlichkeit herausfallen werden, soll mit dem Teilen auf der Pinnwand hauptsächlich auf fremden Content hingewiesen werden, die Inhalte werden so aber nicht zu einem integralen Bestandteil der Präsenz. Damit stehen sie funktional lediglich einem einfachen Hyperlink gleich. Sollte der EuGH entscheiden, dass das Framing generell eine öffentliche Wiedergabe i. S. d. Richtlinie ist – was angesichts der bisherigen Rechtsprechung zumindest nicht ausgeschlossen werden kann[33] –, so wären soziale Netzwerke jedoch in erheblichem Maße davon betroffen. Das Teilen über Inline-Linking oder Framing wäre dann nur zulässig, sofern der Urheber zugestimmt hat.

11 Verletzt ein Nutzer fremde Urheberrechte, hat er nach § 97 UrhG den entsprechenden Schaden zu ersetzen, der nach der sog. dreifachen **Schadensberechnung** ermittelt werden kann:[34] entweder den tatsächlich konkret eingetretenen Schaden für den Rechteinhaber, oder den Schaden auf der Grundlage einer Lizenzanalogie, schließlich die Abschöpfung des Gewinns beim Verletzer, was indes bei den meisten Nutzern (sofern sie nicht gewerblich tätig sind) kaum in Betracht kommen dürfte.

12 Im Vorfeld sieht sich der Nutzer häufig **Abmahnungen** ausgesetzt, die gem. § 97a Abs. 2 UrhG für einfache Fälle nicht über 100 € hinausgehen dürfen, solange sie

---

[29] BGH, GRUR 2011, 56 Rn. 25–27 – Session-ID.

[30] So auch Rauer/Ettig, K&R 2013, 429 (431).

[31] Ähnlich, aber enger schon Ott, ZUM 2004, 357 (364), der dies nur annimmt, wenn der Nutzer im „Mittelpunkt der Handlung steht", das Framing also von den Eingaben des Benutzers abhängt, was aber wohl hauptsächlich nur bei Suchmaschinen der Fall wäre.

[32] Worauf der BGH, GRUR 2013, 818 – Die Realität in Rn. 26 abstellt.

[33] S. dazu die Prüfung des BGH, GRUR 2013, 818 (819 f.) Rn. 14 ff.; sowie Dreier/Leistner, GRUR 2013, 881 (887); ferner Bentley/Derclaye et al., University of Cambridge Faculty of Law Research Paper No. 6/2013, abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220326.

[34] Grundlegend zur dreifachen Schadensberechnung BGHZ 20, 345 (353) – Paul Dahlke; BGH, GRUR 1962, 509 (511 f.) m. Anm. Moser v. Filseck – Dia Rähmchen II; Wild, in: Schricker/Loewenheim, UrhR, § 97 Rn. 145 ff.

nicht im geschäftlichen Verkehr erfolgen.[35] Hier bereiten allerdings die Tatbestandsmerkmale des einfachen Falles und des geschäftlichen Verkehrs Probleme bzw. die Regelung erfasste nicht den großen Anteil der Abmahnung wegen Filesharings, da dies vielfach nicht als einfacher Fall bzw. als Handlung des geschäftlichen Verkehrs angesehen wurde.[36] Dementsprechend soll nach der jüngst beschlossenen Änderung durch das Gesetz gegen unseriöse Geschäftspraktiken[37] Abs. 2 durch eine neue Regelung ersetzt werden. Im neuen § 97a Abs. 2 UrhG muss einerseits die Abmahnung zukünftig speziellen Formerfordernissen genügen, deren Nichteinhaltung Unwirksamkeit zur Folge hat. Zweites Element ist ein neuer § 97a Abs. 3 UrhG, nach dessen erstem Satz die anwaltlichen Gebühren für die Abmahnung nach einem festen Gegenstandswert des Unterlassungs- und Beseitigungsanspruches i. H. v 1000 € berechnet werden sollen. Allerdings nur, sofern der Abgemahnte eine natürliche Person ist, welche die urheberrechtlich geschützten Werke nicht für ihre gewerbliche oder selbstständige berufliche Tätigkeit verwendet und nicht bereits wegen eines anderen Anspruches aufgrund eines Vertrages, eines rechtskräftigen Urteils oder einer einstweiligen Verfügung zur Unterlassung verpflichtet ist (§ 97a Abs. 3 S. 2 UrhG). Allerdings bleibt es auch hier möglich, von dem fixen Gegenstandswert abzuweichen, wenn die 1000 € „den besonderen Umständen nach" als unbillig anzusehen sind.[38] Schließlich soll auch der sog. fliegende Gerichtsstand bekämpft werden, der vor allem bei über das Internet begangenen Delikten dazu führte, dass konzentriert an dem Ort geklagt wurde, an dem die Gerichte die für den Urheber günstigsten Urteile fällten. Nach § 104a Abs. 1 UrhG ist bei Klagen gegen natürliche Personen, die nicht für ihre gewerbliche oder selbständige berufliche Tätigkeit urheberrechtlich geschützte Gegenstände verwendet, ausschließlich das Gericht am Wohnort des Abgemahnten zuständig sein.

Andere Immaterialgüterrechte Keine Besonderheiten stellt die Verletzung fremder Markenrechte auf sozialen Netzwerken dar: Wie auch bei Auktionsplattformen etc. kann die unbefugte Benutzung einer fremden Marke das Markenrecht verletzen, allerdings gem. §§ 14 Abs. 2, 4; 15 Abs. 2, 3 MarkenG nur, wenn der Nutzer im geschäftlichen Verkehr handelt. Für private Nutzer, die nicht als Unternehmer i. S. **13**

[35] Näher zur urheberrechtlichen Abmahnung: Wild, in: Schricker/Loewenheim, UrhR, § 97a Rn. 1; Dreier, in: Dreier/Schulze, UrhG, § 97a Rn. 1; Spindler, in: Spindler/Schuster, § 97a UrhG, Rn. 1 ff.; insbesondere gegenüber Privaten: Malkus, MMR 2010, 382; Hoeren, CR 2009, 378.

[36] Wild, in: Schricker/Loewenheim, UrhR, § 97a Rn. 34; LG Köln, ZUM 2012, 350 (352); LG Berlin, MMR 2011, 401; Ewert/von Hartz, MMR 2009, 84 (86 f.); offen gelassen von: LG Hamburg, ZUM 2010, 611 (612); a. A. Hoeren, CR 2009, 378 (380), der allerdings für möglich hält, dass dann keine unerhebliche Rechtsverletzung mehr vorläge; Malkus, MMR 2010, 382 (385); AG Hamburg, GRUR-RR 2010, 311 (311 f.).

[37] vom 8.10.2013 BGBl. 2013, Teil I Nr. 59, S. 3714.

[38] Krit. zum vorangegangenen Entwurf mit teils abweichenden, aber größtenteils gleich gebliebenen Regelungen Maaßen, GRUR-Prax 2013, 153.

v. § 13 BGB zu qualifizieren sind, [39] wird daher in aller Regel keine Markenverletzung in Betracht kommen. Handeln sie demgegenüber als Unternehmer, erst recht wenn es sich um gewerbliche Nutzer handelt (fanpages etc.), kommen sämtliche Markenrechte und –Verletzungshandlungen zur Anwendung.

14 Gleiches gilt für andere Immaterialgüterrechte, etwa dem Geschmacksmusterrecht; auch hier ergeben sich keine Besonderheiten gegenüber Rechtsverletzungen auf sonstigen Plattformen.[40]

5.2.1.3 Andere Delikte

15 Zwar nicht unmittelbar mit den sozialen Netzwerken verknüpft, aber doch durch diese wesentlich erleichtert sind alle Formen der Teilnahme, Anstiftung oder Verleitung zu Delikten. Bekannt geworden sind etwa die Fälle von „**Facebook-Parties**“, zu denen aufgrund einer versehentlich unterlassenen Einschränkung von Einladungen praktisch die Öffentlichkeit auf eine (Geburtstags -) Feier aufmerksam gemacht wurde, zu der dann auch mehrere Hundert Personen erschienen, mit entsprechende Schäden und Begleiterscheinungen bei Nachbarn.[41] Fraglich sind hier weniger die eingetretenen Rechtsgutsverletzungen im Sinne von § 823 Abs. 1 BGB am Eigentum (Grundstücke) der Nachbarn, sondern die Vorhersehbarkeit für den Nutzer der sozialen Netzwerke. Zwar scheitert die Haftung des Nutzers hier nicht an der Kausalität, da es im Sinne der Adäquanz-Formel[42] nicht völlig außerhalb jeder Wahrscheinlichkeit liegt, dass eine ungehindert verbreitete Einladung entsprechend zahlreiche Menschen anzieht. Indes ist zweifelhaft, ob den Nutzer eines sozialen Netzwerks eine Verkehrspflicht im Interesse Dritter trifft, sorgsam Voreinstellungen bei der Erstellung und Verbreitung von Nachrichten vorzunehmen, wenn es sich um seltene und unwahrscheinliche Ereignisse handelt. Erst bei einer bestimmten Typizität, etwa zahlreich auftretenden Facebook-Parties, kann man hier dem Nutzer entsprechende Pflichten auch im Interesse von potentiell geschädigten Dritten auferlegen.

16 Selbstverständlich ist demgegenüber bei (bedingt) vorsätzlichem Handeln eine Haftung gegeben, unter Umständen bereits aus § 830 Abs. 1 BGB. Wird etwa über

---

[39] S. aus der umfangreichen Rspr. zur Unternehmereigenschaft bei Internet-Auktionen: OLG Hamm, MMR 2010, 608; OLGR Hamburg 2008, 374; OLG Frankfurt, NJOZ 2008, 836; NJW 2005, 1438; OLG Koblenz, MMR 2006, 236 m. Anm. Mankowski; LG Hof, CR 2003, 854 = VuR 2004, 109 m. Anm. Mankowski; LG München, MMR 2009, 504 = BeckRS 2009, 11967; LG Mainz, NJW 2006, 783; AG Bad Kissingen, NJW 2005, 2463; AG Radolfzell, NJW 2004, 3342.

[40] Zur Verletzung von Geschmacksmusterrechten bei Internetauktionen: LG Düsseldorf, Urteil v. 28.11.2011 Az: 34 O 130/08, bei Vertrieb über Internetseiten: OLG Hamburg, GRUR-RR 2013, 138.

[41] Zand-Vakili, Anzeigen nach ungewollter Facebook-Party, welt.de vom 6.6.2011, abrufbar unter: http://www.welt.de/print/die_welt/hamburg/article13414319/Anzeigen-nach-ungewollter-Facebook-Party.html; s. auch die Übersicht der sog. „Facebook-Partys“ auf Zeit Online, abrufbar unter: http://www.zeit.de/2011/27/Deutschlandkarte-Facebook-Party.

[42] Zur Adäquanztheorie: Schiemann, in: Staudinger, BGB, § 249 Rn. 12 ff.; Schubert, in: BeckOK-BGB, § 249 Rn. 51 f.; Oetker, in: MüKo-BGB, § 249 Rn. 109 ff.

soziale Netzwerke gezielt zu einer Demonstration oder einer Art Streik aufgerufen („flash-mob“[43]), so ist die Verantwortlichkeit des Aufrufenden nicht anders als über andere Medien zu beurteilen.[44]

5.2.2 Deliktische Handlungen der Netzwerkbetreiber

5.2.2.1 Haftung für Sicherheit der Netzwerke

Aus Sicht der Nutzer ist die Sicherung der sozialen Netzwerke und der Daten, die sie auf ihren Account geladen haben, sowie der Kommunikation mit anderen Nutzern essentiell. Zwar handelt es sich nicht um Hauptleistungspflichten im Synallagma,[45] doch können die Sicherungspflichten als wichtige Nebenleistungspflichten der Netzwerkbetreiber, mithin als **Kardinalpflichten** qualifiziert werden, ähnlich auch anderen Internetvertragstypen.[46] Demgemäß kann die Verletzung dieser Sicherungspflichten nicht in Allgemeinen Geschäftsbedingungen abbedungen werden, auch nicht für leichte Fahrlässigkeit.[47] Begreift man zudem auch auf den ersten Blick kostenlose soziale Netzwerke als entgeltliche Verträge, da mit ihnen die Einwilligung in die Weiterverarbeitung von personenbezogenen Daten sowie **17**

[43] Zur arbeitsrechtlichen Zulässigkeit des Flashmobs als Mittel des Arbeitskampfes: BAGE 132, 140 Rn. 32 ff. = NJW 2010, 631 m. Anm. Brötzmann, derzeitig anhängig beim BVerfG (Az.: 1 BvR 3185/09); Rehder et al., ArbuR 2012, 103; Krieger/Günther, NZA 2010, 20; Fuhlrott/Fabritius, EWiR 2010, 51 (51 f.); Richardi/Fischinger, in: Staudinger, BGB, Vorb. §§ 611 ff., Rn. 950.

[44] Zu Aufrufen zur Demonstration: BGHZ 89, 383 (393 ff.); LG Hamburg, NJW 1998, 1411 f. – Rave; Spindler, in: BeckOK-BGB, § 823 Rn. 359 f.; Hager, in: Staudinger, BGB, § 823 E, Rn. 15; Aufrufe zum Boykott bzw. rechtswidrigem Streik: BVerfGE 25, 256 (263 ff.) = NJW 1969, 1161 – Blinkfüer; BGH, NJW 1964, 29 (30 ff.) – Blinkfüer; OLG Frankfurt, NJW 1969, 2095 (2096) – Robbenjagd; NJW-RR 1988, 52 (52 f.) – Pelzmäntel; LG München I, NJW-RR 1988, 54– Pelzmäntel; BAGE 2, 75 (77) = NJW 1955, 1373; BAGE 15, 174 (195) = NJW 1964, 883 (884); BAGE 15, 211 (215 f.) = NJW 1964, 1291 (1292); BAGE 41, 209 (222); 46, 322 (345) = NJW 1985, 85; BAGE 48, 160 (165 f.) = NJW 1985, 2545; BAGE 58, 364 (389) = BAG NJW 1989, 57 (60 f.); 1989, 63; Wagner, in: MüKo-BGB, § 823 Rn. 278 ff., 284 ff je m. w. N.

[45] S. zum Vertragsrecht und den Hauptleistungspflichten Bräutigam/v. Sonnleitner, Kap. 3 Rn. 9 ff.

[46] S. bspw. für Internet-Intermediäre allgemein Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, 2007, S. 273 Rn. 663, bzw. S. 281, Rn. 684 abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile; ders., Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2011a, S. 48; für E-Mail-Provider: ders., in Spindler, Vertragsrecht der Internet-Provider, Teil IV Rn. 147; zu Access-Providern: ders., in: Spindler, Vertragsrecht der Internet-Provider, Teil IV Rn. 81.

[47] Zu entsprechenden Konsequenzen für die AGB-Kontrolle sowie Haftungsausschlussklauseln s. Bräutigam/v. Sonnleitner, Kap. 3 Rn. 85 ff.

entsprechende Werbung einher geht,[48] so können die bei unentgeltlichen Verträgen üblichen Haftungsbeschränkungen etwa auf grobe Fahrlässigkeit nicht eingreifen.

18 Aber auch jenseits des Vertragsrechts spielen die Sicherungspflichten eine bedeutsame Rolle: Können Dritte sich etwa Zugang zu Daten der Nutzer verschaffen und diese ausspähen, können Rechtsgüter der Nutzer verletzt sein. Bei urheberrechtlich geschützten Rechten liegt dies auf Hand, auch hinsichtlich des Rechts am eigenen Bild, das von einem Dritten durch unbefugten Zugriff verwandt wird. Da für diese Rechtsgüter auch Fahrlässigkeit genügt, kommen hier Haftungsrisiken für die Netzwerkbetreiber in Betracht, wenn sie ihre Sicherungspflichten verletzt haben (fahrlässige Nebentäterschaft) und damit Dritten den Zugang ermöglicht haben.[49]

19 Ob dies allerdings für sämtliche Daten von Nutzern gilt, ist derzeit noch offen. Da das Deliktsrecht keine Vermögensschäden erfasst, kommt der Frage, ob **Daten als sonstige Rechte** nach § 823 Abs. 1 BGB begriffen werden kann, eminente Bedeutung zu. Allerdings kommt gerade für private Nutzer bei personenbezogenen Daten häufig das BDSG als Schutzgesetz in Betracht, zumal § 9 BDSG technisch-organisatorische Pflichten für den Datenverarbeiter enthält,[50] zu deren Einhaltung auch der soziale Netzwerkbetreiber verpflichtet ist.[51] Handelt es sich nicht um personenbezogene Daten, kann nur die Qualifikation der Daten als sonstiges Recht[52] einen Schadensersatzanspruch gegen den Netzwerkbetreiber begründen, ggf. auch des Besitzes an (den stets irgendwo verkörperten) Daten, da der Nutzer einen (Mit −) Besitz an den Daten als Accountinhaber hat;[53] allerdings bestehen hier nach wie vor

---

[48] Bräutigam, MMR 2012, 635 (638 ff.); Bräutigam/v. Sonnleitner, Kap. 3 Rn. 18 ff.; zur Kommerzialisierung von Daten s. Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen des 69. Deutschen Juristentages, Band I, F 100 je m. w. N.

[49] Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, 2007, S. 281 ff., Rn. 684 ff. abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile.

[50] Etwa §§ 4, 4a, 5, 6a, 9, 10, 11 BDSG, Gola/Schomerus, BDSG, § 1 Rn. 3, zusätzlich für §§ 19 ff., 33 ff. BDSG etwa Simitis, in: Simitis, BDSG, § 4 Rn. 68; s. auch OLG Hamm, ZIP 1983, 552 (554); NJW 1996, 131; Wagner, in: MüKo-BGB, § 823 Rn. 424.

[51] Allerdings stellt sich hier häufig die Frage der internationalen Anwendbarkeit: So hat das OVG Schleswig, NJW 2013, 1977 (1978 f.) für Facebook die Anwendbarkeit des deutschen BDSG zugunsten des irischen Datenschutzrechts verneint. Da die technisch-organisatorischen Pflichten aber Teil der EU-Datenschutz-Richtlinie sind (Art. 17 DSRL), kommt dann das irische Pendant als Schutzgesetz in Betracht.

[52] So bspw. Meier/Wehlau, NJW 1998, 1585 (1588).

[53] Spindler, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2011a, S. 48 f.; entsprechend zu „virtuellen Gegenständen“: ders., ZGE 2011, 129 (147); so wohl auch Spickhoff, Der Schutz von Daten durch das Deliktsrecht, in: Leible et al., Unkörperliche Güter im Zivilrecht, S. 233 (237), der als Beispiel allerdings einen Fall wählt, bei welchem physischer Zugang zu dem speichernden PC gegeben ist; Joost, in: MüKo-BGB, § 854 Rn. 5 verlangt zwar ein räumliches Verhältnis für den Besitz, allerdings nur um den Gebrauch der Sache zu gewährleisten: Dieser ist aber beim Zugriff auf den Rechner gewährleistet; s. aber auch BGH, NJW 2007, 2394 (2395) Rn. 18: kein Besitz an den verkörperten Computerprogrammen, sondern nur Zugang; Besitz abl. Berberich, Virtuelles Eigentum, S. 164 f.; s. auch Hoeren, MMR 2013, 486, der eine Möglichkeit diskutiert, aus § 303a StGB analog § 903 BGB ein Dateneigentum zu konstruieren.

grundlegende Probleme der Reichweite des Schadensersatzes. So wird bei einem Ausspähen von Daten nicht das eigentliche Datum verletzt oder der Besitz gestört, sondern nur Informationen abgezogen; anders formuliert: die Exklusivität der Information, also der Zuweisungsgehalt des Datums, wird gestört, nicht aber der Inhalt verändert, erst recht nicht die Existenz des Datums bzw. der Information. Das reine **Ausspähen von Daten** kann daher nur dann haftungsrelevant sein, wenn rechtlich geschützte Geheimnisse betroffen sind, wozu auch personenbezogene Daten zählen, nicht aber Daten generell. Zwar enthält das Strafrecht entsprechende Tatbestände gegen das Ausspähen von Daten ebenso wie Datenveränderung und Computersabotage, §§ 202a, 303a, 303b StGB;[54] doch betreffen diese Normen nur vorsätzliches Handeln eines Dritten, nicht aber das fahrlässige Ermöglichen solcher Handlungen.[55] Für nicht-personenbezogene Daten kommen daher Haftungsrisiken aufgrund des Eindringens Dritter in der Regel nur bei Veränderungen und Zerstörungen der Daten in Betracht – hier gilt es dann aber, das rechtliche nicht geschützte Affektionsinteresse von eigentlichen Schäden abzugrenzen,[56] so dass gerade bei privaten Nutzern häufig keine Ansprüche bestehen werden.

Das konkrete Ausmaß der Sicherungspflichten der Netzwerkbetreiber (im Sinne von Verkehrssicherungspflichten) hängt von den berechtigten Sicherheitserwartungen des Verkehrs ab[57], die wiederum durch vertragliche Leistungsbeschreibungen überlagert werden können. Ob z. B. derzeit eine ständige verschlüsselte Verbindung (https) zwischen Nutzer und Netzwerkbetreiber erforderlich ist, lässt sich nicht sicher beantworten: Während bislang der Verkehr weitgehend unverschlüsselte Verbindungen akzeptiert hat, beginnt seit den Enthüllungen durch *Snowden* ein Umdenken. Die von großen deutschen Providern angekündigte Umstellung auf verschlüsselte Zugänge[58] dürfte nicht ohne Auswirkung auf die allgemein berechtigten Sicherheitserwartungen des Verkehrs sein, so dass in absehbarer Zeit schon aus deliktsrechtlicher Sicht es zu den Verkehrssicherungspflichten gehören kann, verschlüsselte (und damit etwas sicherere) Verbindungen anzubieten. **20**

Schließlich gehört zu den – allerdings vertraglich überlagerten – Sicherungspflichten des Netzwerkbetreibers der Schutz der Daten des Nutzers vor Zerstörung bzw. **21**

---

[54] Schutzgesetzeigenschaft angenommen von OLG Dresden, NJW-RR 2013, 27, AG Brandenburg, BeckRS 2002, 11438, für § 202a StGB: OLG Celle, NJW-RR 2011, 1047; Harte-Bavendamm, in: Kilian/Heussen, Computerrechts-Handbuch, Teil V (Wettbewerbsrecht), Rn. 54.

[55] Zur vorsätzlichen Schädigung durch Nutzer: Spindler, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2011a, S. 57; ders., Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, 2007, S. 118, Rn. 276 ff. abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile.

[56] Sie stellen allenfalls einen immateriellen Schaden dar, dazu: Schiemann, in: Staudinger, BGB, § 253 Rn. 14; Oetker, in: MüKo-BGB, § 249 Rn. 25; Schubert, in: BeckOK-BGB, § 249 Rn. 20.

[57] BGH, NJW 1985 (1076); NJW 1994, 3348 (3349); ferner Spindler, in: BeckOK-BGB, § 823 Rn. 234; Hager, in: Staudinger, BGB, § 823 E, Rn. 27; je m. w. N.

[58] Initiative „E-Mail Made in Germany“, dazu https://www.e-mail-made-in-germany.de/; s. aber auch die Kritik daran: Chaos Computer Club, Das Sommermärchen von der sicheren E-Mail v. 9.8.2013, abrufbar unter: http://ccc.de/de/updates/2013/sommermaerchen.

Verlust aufgrund anderer Ursachen, z. B. Zerstörung von Servern etc. Allerdings treffen den Nutzer hier eigenständige Pflichten zu einem **Backup** im Rahmen von § 254 BGB, sofern dies technisch möglich, zumutbar und vom Netzwerkbetreiber auch nahegelegt wird, was bis heute – soweit ersichtlich – allerdings nicht der Fall ist.

5.2.2.2 Haftung für bereit gestellte Tools, Apps, Suchfunktionen

22 Den Sicherungspflichten nahe stehend ist die Verantwortlichkeit für bereitgestellte bzw. bereitgehaltene Tools und Apps, einschließlich von (beliebten) Spielen.

23 **Haftung für eigene Dienste** Sofern der soziale Netzwerkbetreiber selbst diese Software bereitstellt, kann er nicht anders behandelt werden als andere Softwarehersteller, die für Schäden an Rechnern und Daten ihrer Kunden im Rahmen der deliktischen Produkthaftung einzustehen haben, insbesondere für Virenfreiheit etc., nicht aber für deren Funktionalität, die allein vom vertraglichen Äquivalenzinteresse erfasst wird.[59]

24 **Haftung für fremde Software** Hat der Netzwerkbetreiber dagegen nur fremde Software (Spiele etc.) bereitgehalten und deutlich darauf hingewiesen, dass es sich um fremde Inhalte handelt,[60] kommen nur wesentlich verringerte Pflichten in Betracht. Allerdings greifen auch hier Kontroll- und Sicherungspflichten hinsichtlich der **Freiheit von Schadsoftware, Viren** in Betracht – was aber auch von den Sicherheitserwartungen der Nutzer abhängt. Bei einer völlig offenen Plattform etwa werden wesentlich reduzierte, ggf. gar keine Sicherheitserwartungen bestehen, während von Plattformen, die den Zugang und das Angebot beschränken, gar Entgelt von den Softwareherstellern fordern, höhere Sicherungs- und Kontrollpflichten verlangt werden können.[61]

25 **Verantwortlichkeit für datenschutzgerechte Gestaltung** Wenig geklärt ist bislang schließlich die Frage, inwiefern Netzwerkbetreiber auch für die datenschutzgerechte Ausgestaltung und Einhaltung der datenschutzrechtlichen Pflichten von Apps, Tools etc. auf ihren Plattformen einzustehen haben, wenn die Netzwerkbetreiber selbst nicht Hersteller (und auch nicht Vertriebspartner) dieser Software sind. Fraglich ist insbesondere, ob die von der höchstrichterlichen Rechtsprechung

---

[59] Allerdings sind hier zahlreiche Probleme nach wie vor umstritten, s. dazu Spindler, in: Bamberger/Roth, BGB, § 823 Rn. 564; Graf von Westphalen, in: Foerste/Graf von Westphalen, Produkthaftungshandbuch, § 47 Rn. 40 ff.; Littbarski, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 18 Rn. 42.

[60] Zur Frage, ob in diesem Fall Haftungsprivilegierungen nach §§ 7 ff. TMG eingreifen, s. unten Rn. 30 ff.

[61] Zu einer ähnlichen Abstufung bei klassischen App-Stores gelangen: Baumgartner/Ewald, Apps und Recht, Rn. 519.

angenommene Pflicht zur Kontrolle auf die Einhaltung von jugendmedienschützenden Inhalten bei Auktionsplattformen[62] auf soziale Netzwerke übertragen werden kann. Hiergegen spricht, dass im Falle des Jugendmedienschutzes entsprechende Indexlisten vorliegen, anhand derer der Provider die Inhalte prüfen kann – was im Datenschutz nicht der Fall ist. Zudem würde eine solche Pflicht erst im Rahmen der Störerhaftung eingreifen, wofür in der Regel die Kenntnis des Plattformbetreibers über entsprechende Verstöße erforderlich ist.[63] Sie ist zudem durch wirtschaftliche und technische Zumutbarkeit für den Netzwerkbetreiber begrenzt; so können etwa datenschutzrechtliche Zertifizierungen bzw. Audits den Netzwerkbetreiber entsprechend entlasten.

Haftung für Suchfunktionen Schließlich zählt zu den Haftungsbereichen auch die inzwischen von einigen Netzwerkbetreibern zur Verfügung gestellten Suchfunktionen: Auch hier wird die Haftung des Netzwerkbetreibers nicht anders behandelt als die eines „klassischen" Suchmaschinenbetreibers,[64] so dass häufig die Sozialadäquanz der Suchfunktionen etwaige Rechtsverletzungen überwiegen wird. Ebenso ist hier die Rechtsprechung zur konkludenten Einwilligung, etwa bei Urheberrechten, einschlägig, zumal häufig explizit sogar die entsprechenden Rechte eingeräumt sein dürften in den einschlägigen AGB.[65] Die Integration der Suchmaschinenfunktion in das soziale Netzwerk ändert hier nichts an den allgemeinen Haftungsmaßstäben, die an Suchmaschinen angelegt werden – allerdings auch mit der Folge einer Störerhaftung nach Kenntnisnahme im Rahmen der jüngsten Rechtsprechung im Bereich des Persönlichkeitsrechts.[66] **26**

5.2.2.3 Verletzungen der Urheber- und Persönlichkeitsrechte der Nutzer

Greift der Betreiber des sozialen Netzwerke selbst in Urheber- oder Persönlichkeitsrechte der Nutzer ein, insbesondere beim Recht am eigenen Bild, etwa bei fehlender Einwilligung bzw. fehlenden Rechteeinräumungen, haftet er selbstverständlich nach **27**

---

[62] BGHZ 173, 188 – Jugendgefährdende Medien bei eBay.

[63] BGH NJW 2013, 2348 (2350) Rn. 30 – Autocomplete-Funktion; NJW 2012, 2345 Rn. 19–RSS-Feeds; NJW 2012, 148 Rn. 24 – Blog-Eintrag; Spindler/Anton, in: Spindler/Schuster, § 1004 BGB, Rn. 9; Jandt, in: Roßnagel, Recht der Telemediendienste, § 10 TMG Rn. 62.

[64] Haftung für Snippets: KG, MMR 2006, 817, MMR 2010, 495; OLG Hamburg, MMR 2010, 490, m. Anm. Kazemi; OLG Stuttgart, CR 2009, 187; zu Autocomplete: BGH, NJW 2013, 2348 – Autocomplete-Funktion; OLG München, MMR 2012, 108; zu Adwords: BGH, GRUR 2013, 290 – MOST-Pralinen; GRUR 2011, 828 – Bananabay II; MMR 2011, 608 – Impuls II; Bilder- und Personensuche: BGHZ 185, 291 – Vorschaubilder I; BGH, NJW 2012, 1886 – Vorschaubilder II; zur Übersicht zur Haftung von Suchmaschinen s. ferner Meyer, K&R 2013, 221; Härting, K&R 2012, 633; Ott, WRP 2011,655; grundlegend: Sieber/Liesching, MMR-Beil. 8/2007, 1.

[65] So z. B. bei Facebook, abrufbar unter: https://www.facebook.com/legal/terms; twitter: https://twitter.com/tos; LinkedIn, abrufbar unter: http://www.linkedin.com/legal/user-agreement; Pinterest, abrufbar unter: http://de.about.pinterest.com/terms/; nicht aber bei Xing, abrufbar unter: http://www.xing.com/terms.

[66] BGH, NJW 2013, 2348 Rn. 23 ff. – Autocomplete-Funktion.

den jeweils einschlägigen Regeln (§§ 97 UrhG, 823 Abs. 1 BGB etc.). Dies gilt erst recht gegenüber ausgeschiedenen Nutzern, deren Inhalte oder Bilder nach wie vor verwandt werden, wenn nicht über die Beendigung der Mitgliedschaft hinaus die Rechte daran wirksam eingeräumt wurden.[67]

5.2.2.4 Haftung gegenüber Dritten

28 Eine Haftung für Schadensersatz gegenüber Dritten für die Handlungen der Nutzer bzw. deren Inhalte auf sozialen Netzwerken wird in der Regel an den Haftungsprivilegierungen des sozialen Netzwerkbetreibers gem. §§ 7 ff. TMG scheitern[68] – was indes nicht für die Störerhaftung gilt. So kann ein Netzwerkbetreiber nicht für fehlerhafte Facebook-Parties und die dabei entstehenden Schäden haftbar gemacht werden, zumal er auch kaum Möglichkeiten hat, die Inhalte auf deren potenzielle Gefährlichkeit hin zu kontrollieren.[69]

29 Handelt es sich dagegen um eigene Inhalte, haftet der Netzwerkbetreiber selbstverständlich nach den allgemeinen Regeln.

5.3 Haftungsprivilegierungen

30 Wie bereits angedeutet, hängt die Haftung der Betreiber von sozialen Netzwerken, aber auch von anderen Inhalteanbietern im Internet davon ab, ob die Haftungsprivilegierungen der §§ 7 ff. TMG bzw. Art. 12 ff. E-Commerce-RL für sie eingreifen. Die Haftungsprivilegierung erfasst zivilrechtlich aber nur Schadensersatzansprüche (und privilegiert auch gegenüber der strafrechtlichen Verantwortlichkeit); die in die Zukunft gerichtete Störerhaftung ist demgegenüber nach § 7 Abs. 2 TMG und inzwischen gefestigter europäischer[70] sowie deutscher Rechtsprechung[71] davon unberührt.[72] Nach § 10 TMG (bzw. Art. 14 E-Commerce-RL) sind Diensteanbieter für fremde Inhalte nicht verantwortlich, wenn

„*1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder*

---

[67] Zu den vertragsrechtlichen Fragen s. Bräutigam/v. Sonnleitner, Kap. 3 Rn. 59 ff.
[68] Dazu sogleich Rn. 30 ff.
[69] Zu den zumutbaren Prüfungspflichten im Rahmen der Störerhaftung s. unten Rn. 46 ff.
[70] EuGH, Slg. 2011, I – 6011 = K&R 2011, 567 = MMR 2011, 596– L'Oréal./. eBay.
[71] Grundlegend BGHZ 158, 236 (246 ff.). – Internetauktionen I; dem folgend aus der Rspr. des I. Zivilsenats BGHZ 172, 119 – Internet-Versteigerung II; GRUR 2008, 702 – Internet-Versteigerung III; BGHZ 191, 19 – Stiftparfüm des VI. Zivilsenats BGHZ 191, 219 Rn. 19 – Blog-Eintrag; 181, 328 Rn. 14 – spickmich.de; BGH, MMR 2009, 752 Rn. 17; NJW 2007, 2558 – Meinungsforum.
[72] Ausführlich dazu aus jüngster Zeit zusammenfassend Leistner, ZUM 2012, 722; ders., GRUR-Beil. 2010, 1 (zur urheberrechtlichen Haftung); s. bereits Spindler/Volkmann, WRP 2003, 1; Volkmann, Der Störer im Internet, S. 100 f.

Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder

2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben"

5.3.1 Diensteanbieter

Zunächst muss es sich um Anbieter von elektronischen Informations- und Kommunikationsdiensten handeln (§ 1 Abs. 1 TMG). Dabei kann gem. § 2 Nr. 1 TMG als Diensteanbieter jede natürliche oder juristische Person in Betracht kommen, „die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert". Dabei kommt es gem. § 1 Abs. 1 S. 2 TMG nicht darauf an, ob für den Dienst ein Entgelt verlangt wird. **31**

Während die Betreiber der sozialen Netzwerke daher ohne Zweifel als Anbieter von elektronischen Informations- und Kommunikationsdiensten angesehen werden können, da sie sowohl das klassische Hosting von Inhalten für andere betreiben als auch Informationen zum Abruf bereithalten sowie weitere Dienste bereitstellen, stellt sich die Frage, ob auch die **Nutzer dieser Netzwerke selbst als Diensteanbieter** begriffen werden können. Denkbar ist dies etwa im Hinblick auf Inhalte (Postings, Bilder etc.) von Dritten („Freunden" etc.), die in das Profil des Nutzers eingestellt werden, z. B. auch Kommentierungen zu Nachrichten des Nutzers selbst. Allerdings bedient sich der Nutzer nicht eigener Tools oder Webseiten, sondern bekommt den entsprechenden Rahmen vom sozialen Netzwerkbetreiber zur Verfügung gestellt; indes kommt es nicht darauf an, ob der Anbieter eines Informationsdienstes nur eigene Software, Webseiten etc. verwendet, die Nutzung vorgegebener Strukturen genügt. So ist im Prinzip jede Homepage, jedes Profil das Angebot elektronischer Inhalte und Informationen, somit ein elektronischer Kommunikationsdienst, so dass auch der Nutzer eines sozialen Netzwerks selbst zum „Content"-Provider, aber auch zum „Hostprovider" werden kann, mit der Folge, dass die Haftungsprivilegierungen für ihn eingreifen. Allerdings kann die Frage, ob der Nutzer selbst die Kontrolle über fremde Inhalte ausüben kann, etwa fremde Postings oder Kommentare entfernen kann, bei der Störerhaftung relevant werden.[73] **32**

[73] Insoweit zutr. Stadler, Haftungsrisiko Facebook?, v. 10.4.2012, abrufbar unter: http://www.internet-law.de/2012/04/haftungsrisiko-facebook.html.

5.3.2 Netzwerk-Betreiber

5.3.2.1 Fremde Inhalte und Hosting (§ 10 TMG)

33 Entscheidend für die Haftungsprivilegierung der sozialen Netzwerkbetreiber (aber auch der Nutzer) ist demnach die Frage, ob es sich aus Sicht des Betreibers um fremde Inhalte handelt; denn nur dann gelangen die Haftungsprivilegierungen des § 10 TMG bzw. Art. 14 ECRL zur Anwendung. Die deutsche Rechtsprechung ordnet aber auch – wie schon zum alten TDG – die sog. sich-zu-eigen-gemachten Inhalte den eigenen Inhalten zu, wofür ein Bündel an Kriterien zur Anwendung gelangt. So sollen etwa die Einholung der Rechte von Dritten, die Einbettung in (sonstige) eigene Inhalte – wie bspw. das Gestalten oder Umrahmen mit eigenen Logos oder Markenzeichen – und die redaktionelle Kontrolle im Rahmen einer Gesamtabwägung dazu führen, dass auch diese Inhalte Dritter dann als eigene Inhalte des Webseitenbetreibers gelten.[74] Daher kann es unter Umständen nicht genügen, dass erkenntlich ist, dass es sich um vom Nutzer erstelltem Inhalt handelt, um sich ernsthaft und genügend davon zu distanzieren, wenn die sonstige Gestaltung für ein Zu-eigen-Machen spricht.[75]

34 Allerdings beruhen die europäischen Haftungsprivilegierungen eher auf einem technischem Verständnis, insbesondere der mangelnden Kontrolle und Aufsicht durch den Betreiber hinsichtlich der Inhalte des Nutzers.[76] Dies hat auch der EuGH jüngst in seiner Entscheidung *L'Oréal* v. *eBay* betont, indem er die neutrale Rolle der Hostprovider hervorhob.

35 Entscheidend ist daher, ob der Betreiber aktiv die Nutzer bei der Optimierung oder Bewerbung von ihren Inhalten und den Angeboten unterstützt, dadurch die Möglichkeit hat Kenntnis oder Kontrolle über die Daten zu erlangen und damit seine neutrale Rolle verlässt.[77] Allerdings sind die im Einzelfall eingreifenden Kriterien noch höchst unklar, ob etwa schon eine Design-Hilfe oder die Bildung von Kategorien genügt, um eine aktive Rolle anzunehmen.[78] Allein die Bildung von Kategorien oder die Zurverfügungstellung von bestimmten Diensten wie Nachrichten, Fotos teilen etc. wird nicht ausreichen, um eine aktive Rolle des Netzwerkbetreibers anzunehmen. Entsprechend der Entscheidung des EuGH[79] wird eine solche nicht mehr neutrale Rolle anzunehmen sein, wenn der Betreiber sich etwa aktiv in die Werbung für einen

---

[74] S. dazu BGH, MMR 2010, 556 Rn. 24 ff. – marions-kochbuch.de; nicht damit zu verwechseln ist die urheberrechtliche Frage, ob eine eigenständige Veröffentlichung nach § 15 Abs. 2 UrhG bzw. § 19a UrhG durch Einbettung vorliegt, s. dazu oben Rn. 6 ff.

[75] So wie im Fall BGH, MMR 2010, 556 Rn. 27 – marions-kochbuch.de.

[76] Spindler, MMR 2004, 440 (441); zust. Hoffmann, in: Spindler/Schuster, § 7 TMG, Rn. 20; Jandt, in: Roßnagel, Recht der Telemediendienste, § 7 TMG, Rn. 35 f.; Berger/Janal, CR 2004, 917 (918 f.); wohl auch Sobola/Kohl, CR 2005, 443 (445); a. A. Roggenkamp, K&R 2010, 499; Leible/Sosnitza, WRP 2004, 592 (595); Matthies, Providerhaftung für Online-Inhalte, S. 143.

[77] EuGH Slg. 2011, I – 6011 Rn. 123 = K&R 2011, 567 = MMR 2011, 596– L'Oréal./. eBay.

[78] Dagegen Spindler, MMR 2011, 703 (704 f.); ähnlich H.-P. Roth, WRP 2011, 1258 (1264); Wiebe, WRP 2012, 1182 (1186).

[79] EuGH Slg. 2011, I –6011 Rn. 123 = K&R 2011, 567 = MMR 2011, 596– L'Oréal./. eBay.

Nutzer einschaltet[80] oder auf die Inhalte Einfluss nimmt und diese außerhalb von gesetzlichen Pflichten kontrolliert, was insoweit auch den Kriterien der *Marions-Kochbuch*-Entscheidung des BGH entspricht.[81]

In der Regel sind daher die Betreiber von sozialen Netzwerken als Hostprovider im Sinne von § 10 TMG bzw. Art. 14 ECRL zu qualifizieren, selbst wenn sie bestimmte Kategorien oder Einordnungen bzw. Dienste vorgeben, wie etwa Chroniken, Fotos etc. **36**

Anders kann dies für bereitgehaltene Software zu beurteilen sein, wenn hier von vornherein nur nach entsprechender Prüfung die fremde Software auf der Plattform angeboten wird. Erst recht gerät der Provider in die Nähe einer aktiven Rolle, die für die Haftungsprivilegierungen schädlich ist, wenn er die Software auch noch bewirbt und sich nach eigenen Kriterien vorbehält, die Software auch wieder zu entfernen bzw. Bedingungen an ihre Funktionalitäten zu stellen.[82] **37**

5.3.2.2 Suchfunktionen, Hyperlinks und private Nachrichten

Die von den Netzwerkbetreibern angebotenen Dienste unterfallen indes nicht immer den Haftungsprivilegierungen: So hat der Gesetzgeber des TMG ebenso wie der ECRL davon abgesehen, die Suchmaschinen einer Haftungsprivilegierung zuzuordnen, so dass entgegen einer mitunter geäußerten Auffassung diese nicht in den Genuss der Haftungsprivilegierung kommen können, auch nicht in Analogie.[83] Dennoch ist auch nach allgemeinen haftungsrechtlichen Regeln eine Verantwortlichkeit für das Betreiben der Suchmaschinendienste im Wesentlichen ausgeschlossen, da den Betreiber kaum Garanten- oder Sicherungspflichten treffen. Die weitgehende Automatisierung schließt eine Vorabkontrolle der Suchergebnisse weitgehend aus; hinzu kommt die Sozialadäquanz der Informationsvermittlungen.[84] Selbst bei sozialen Netzwerken ist aufgrund ihrer Zahl an Teilnehmern und Inhalten die Informationsvermittlung und –suche unabdingbar, um entsprechende Inhalte aufzufinden. **38**

Gleiches gilt für **Hyperlinks**, die der Betreiber von sozialen Netzwerken setzt: auch diese dienen nach gefestigter Rechtsprechung der sozialadäquaten Informationsvermittlung und stellen ein unerlässliches Hilfsmittel der Navigation im Internet, **39**

---

[80] Nicht aber, wenn der Betreiber bloß Adwords für sich selbst schaltet, s. dazu Wiebe, WRP 2012, 1182 (1188); ebenso Rössel, CR 2011, 589 (591).

[81] Spindler, JZ 2012, 311 (312); Volkmann, CR 2011, 607.

[82] Anders Baumgartner/Ewald, Apps und Recht, 2013 Rn. 477 ff., insbesondere Rn. 505 ff., die hier immer noch von einem fremden Inhalt ausgehen, aber reduzierte Anforderungen an die Kenntnis annehmen.

[83] So vor allem Sieber/Höfinger, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 18.1 Rn. 107 ff; s. auch Sieber/Liesching, MMR-Beil. 8/2007, 1 (11 ff.) in diese Richtung auch Wimmers/Schulz, in: Heidrich et al., Heise Online-Recht, B.III.87; dagegen: Spindler, CR 2007, 239 (245); Altenhain, in: MüKo-BGB, Vorb. §§ 7 ff. Rn. 51 m. w. N.

[84] BGHZ 185, 291 Rn. 399; BGH, NJW 2003, 3406 (3410); Sieber/Liesching, MMR-Beil. 8/2007, 1 (3); Spieker, MMR 2005, 727; Spindler, in: Spindler et al., TDG, vor § 8 TDG, Rn. 61.

aber auch in sozialen Netzwerken dar, ohne dass der Linksetzer unmittelbar für die verlinkten Inhalte verantwortlich wäre. Allerdings ist auch hier zwischen der Linksetzung selbst und dem Zeitraum danach zu unterscheiden, da bei Linksetzung der Linksetzende Kenntnis von den Inhalten hat, insoweit also haftungsrechtlich verantwortlich sein kann.[85]

40 Die Funktion zur Übermittlung privater Nachrichten an einen oder einzelne Nutzer in sozialen Netzwerken stellen häufig einen Hybrid aus E-Mail und Chatroom dar. Die in den Nachrichten übertragenen Inhalte unterfallen dabei dem TMG. Die eigentliche Übermittlungsleistung wird über § 8 TMG privilegiert,[86] nicht aber die nicht nur automatische, kurzzeitige Speicherung durch den Betreiber – sie unterfällt § 10 TMG.[87]

5.3.3 Nutzer

41 Auch für den Nutzer greifen die gleichen Kriterien ein – allerdings aufgrund der wesentlich geringeren Möglichkeiten, fremde Inhalte bereitzuhalten, in entsprechend abgeschwächten Umfang. So ist etwa ein Nutzer nicht für die Kommentare anderer „Freunde" verantwortlich, die zu seinen Äußerungen oder Nachrichten, Fotos etc. angebracht werden. Allerdings nimmt der Nutzer in der Regel spätestens dann Kenntnis von diesen Äußerungen etc., wenn er sein Profil besucht, so dass dann § 10 TMG nicht mehr zu seinen Gunsten eingreifen kann.

42 Hat der Nutzer dagegen andere Inhalte übernommen und verändert oder andere Inhalte hinzugefügt, z. B. Musik oder Videos (**Mash-Ups**), liegt ohne jeden Zweifel ein neuer eigener Inhalt vor, der sich auch auf den übernommenen Inhalt erstreckt, so dass Haftungsprivilegierungen nicht greifen können.

43 Auch wenn der Nutzer nur **Inhalte teilt** oder weiter empfiehlt, kann er sich nicht auf die Haftungsprivilegierungen berufen: Abgesehen davon, dass bei einer Teilung von Inhalten unter Umständen bereits ein Sich-zu-eigen-Machen vorliegt, wird der Nutzer zumindest Kenntnis von diesen Inhalten erhalten haben, so dass § 10 TMG von vornherein nicht eingreifen kann.

---

[85] Gabel, WRP 2005, 1102 (1117); Spindler, GRUR 2004, 724 (728); ders., MMR 2002, 495 (499 f., 502); Stadler, Haftung für Informationen im Internet, Rn. 188a; Mann/Smid, in: Spindler/Schuster, Presserecht im Internet und „elektronische Presse", Rn. 59 ff.; aus der Rechtsprechung: BGHZ 187, 240 – AnyDVD = NJW 2011, 2436 m. Anm. Bölke; BGHZ 158, 343 – Schöner Wetten; 156, 1 – Paperboy; LG Frankfurt a. M., MMR-Aktuell 2010, 302790; LG München I, K&R 2005, 184.

[86] Spindler, in: Spindler/Schmitz, TMG, § 8 TMG, erscheint demnächst; Sieber/Höfinger, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 18.1 Rn. 62; OLG Brandenburg, ZUM 2012, 691 (692).

[87] Altenhain, in: MüKo-BGB, § 8 TMG, Rn. 13; Sieber/Höfinger, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 18.1 Rn. 66.

5.4 Störerhaftung

Wie dargelegt, bleibt die Störerhaftung im Grundsatz von den Haftungsprivilegierungen unberührt, auch wenn *en détail* noch zahlreiche Fragen ungeklärt sind, etwa das genaue Verhältnis der durch die Störerhaftung spezifischen Überwachungspflichten der Provider zu dem Verbot der allgemeinen Überwachungspflichten in Art. 15 ECRL.[88] **44**

Die Störerhaftung ist akzessorisch zu den oben dargelegten möglichen deliktischen Handlungen der Nutzer, geht aber wesentlich weiter als die reine Teilnahme nach § 830 BGB, da nach der Rechtsprechung jeder als Störer qualifiziert werden kann, wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung des geschützten Rechtsguts beiträgt.[89] Da dieser Störerbegriff zu einer grenzenlosen Haftung auszuufern droht, hat die Rechtsprechung gerade für internetgestützte Handlungen und für die Störerhaftung von Internetintermediären das Konzept der „zumutbaren Prüfungspflichten" eingeführt,[90] das den Besonderheiten der automatisierten Tätigkeiten der Provider Rechnung tragen soll.[91] **45**

5.4.1 Netzwerkbetreiber

Diese Grundsätze greifen auch für Betreiber sozialer Netzwerke ein: Zunächst kann in der Regel davon ausgegangen werden, dass es sich in der Regel um von der Rechtsordnung gebilligte Geschäftsmodelle handelt, außer wenn sie überwiegend der Kontaktaufnahme und Austausch von Informationen zu Zwecken rechtswidriger Aktivitäten dienen – was nicht ausgeschlossen ist, etwa in den Grenzbereichen von Netzwerken, die rein oder ganz überwiegend der Anbahnung strafbarer sexueller Aktivitäten dienen. Gleiches gilt für Hacker-Communities oder vergleichbare Netzwerke. **46**

Die Störerhaftung der Netzwerkbetreiber hängt von mehreren Bedingungen ab: **47**

---

[88] Obergfell, NJW 2013, 1995; Spindler, JZ 2005, 37 (39); ders., NJW 2002, 921 (925); Sieber/Höfinger, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 18.1 Rn. 56 ff.; BGH, Urt. vom 15. August 2013, I ZR 80/12 Rn. 30 – File-Hosting-Dienst; BGHZ 194, 339 Rn. 19 – Alone in the Dark; BGH, GRUR 2007, 890 Rn. 39 ff. – Jugendgefährdende Medien bei eBay; BGHZ 158, 236 = MMR 2004, 668 m. Anm. Hoeren – Internetversteigerung I.

[89] S. nur BGH, Urt. vom 15.08.2013, I ZR 80/12 Rn. 30 – File-Hosting-Dienst; GRUR 2008, 702 Rn. 50 – Internet-Versteigerung III; BGHZ 194, 339 Rn. 19– Alone in the Dark; BGHZ 185, 330 Rn. 19 – Sommer unseres Lebens je m. w. N.; s. aber auch die Abweichung des VI. Senats im Autocomplete-Urteil: BGH, NJW 2013, 2348 Rn. 24; dazu Härting, CR 2013, 443 (444).

[90] Grundlegend BGHZ 158, 236 – Internet-Versteigerung I, fortgeführt in BGHZ 172, 119 – Internet-Versteigerung II; BGH, GRUR 2008, 702 – Internet-Versteigerung III; BGHZ 185, 330 Rn. 19– Sommer unseres Lebens; BGH, GRUR 2011, 617 Rn. 37 – Sedo; BGHZ 191, 19 – Stiftparfüm; BGHZ 194, 339 Rn. 19 – Alone in the Dark.

[91] Deutlich etwa BGH, GRUR 2011, 152 Rn. 38 ff. – Kinderhochstühle im Internet; dazu Spindler, GRUR 2011, 101 (104 f.).

Zunächst entsteht die Haftung auf Unterlassung erst, wenn der Betreiber überhaupt in **Kenntnis** von der rechtswidrigen Handlung bzw. Aktivität gesetzt worden ist; eine vorbeugende Unterlassungshaftung wäre mit § 10 TMG schwer vereinbar.[92] Die Rechtsprechung folgt dem jetzt, wenngleich auch mit anderer Begründung, indem erst bei Kenntnisnahme der konkreten Verletzung eine Störerhaftung eines Plattformbetreibers entstehen kann.[93] Demgemäß muss der Betreiber konkret über die Verletzungshandlung informiert werden, eine allgemein gehaltene Nachricht genügt nicht, um den Betreiber in die Lage zu versetzen, den Verstoß beurteilen zu können. Andererseits ist der Beleg der im Hinweis enthaltenen Tatsachen nur dann nötig, wenn schutzwürdige Interessen des Betroffenen dies rechtfertigen – namentlich wenn Zweifel am Bestand oder der Befugnis zur Geltendmachung des betroffenen Rechts oder am Wahrheitsgehalt insgesamt bestehen.[94] Doch selbst wenn diese Zweifel bestehen, darf der auf den Verstoß Hingewiesene nicht untätig bleiben, sondern muss den Hinweisgeber darüber informieren.[95] Die Offenkundigkeit der Rechtsverletzung kann sich aus allen dem Hinweisempfänger bekannten Umständen ergeben. Unerheblich ist dabei, ob die Information vom Betroffenen, vom Verletzer oder aus einer dritten Quelle stammen.[96] Einzelheiten der „notice" sind allerdings immer noch ungeklärt und harren der europäischen Harmonisierung.

48 Selbst wenn aber die entsprechende Nachricht klar genug ist, bedeutet dies noch nicht, dass der Provider bzw. Betreiber sozialer Netzwerke zu jeder Unterlassung und Unterbindung von rechtswidrigen Inhalten in Zukunft verpflichtet wäre. Vielmehr setzt dies zumutbare Prüfungspflichten voraus, die wiederum ins Verhältnis zu den gebilligten, auf Automatisierung beruhenden Geschäftsmodellen in Bezug gesetzt werden müssen. Wie der BGH in dem *Kinderhochstühle*-Fall entschieden hat, kann dabei zu berücksichtigen sein, ob der Netzwerkbetreiber eine Art Beschwerdemanagement eingerichtet hat, an das sich Betroffene zunächst zu wenden haben.[97] Eine händische Kontrolle ist jedenfalls weitgehend ausgeschlossen, auch wenn sich in jüngster Zeit hier Aufweichungstendenzen in der Rechtsprechung gezeigt haben, die allerdings besonders gelagerte Fälle betrafen. So sollte es dem Filehoster Rapidshare zuzumuten sein, nicht nur automatisierte Suchvorgänge auf seinen Servern, sondern auch manuelle Suchvorgänge über sog. Linklisten durchzuführen. Die Besonderheit bestand hier darin, dass die automatisierte Suche auf den eigenen Servern nur nach Dateinamen erfolgen konnte und damit nur solche Dateien erfassen kann, die korrekt

---

[92] Spindler, CR 2012, 176 (178); ders./Volkmann, WRP 2003, 1 (3 f.); Jandt, in: Roßnagel, Recht der Telemediendienste, § 10 Rn. 71; OLG Zweibrücken, MMR 2009, 541 (542); s. aber auch: BGHZ 172, 119 Rn. 41 = MMR 2007, 507 m. abl. Anm. Spindler – Internet-Versteigerung II; OLG Hamburg ZUM-RD 2009, 317 (324); ZUM 2006, 414 (419).

[93] BGHZ 194, 339 Rn. 22 – Alone in the Dark.

[94] BGHZ 191, 19 Rn. 31 – Stiftparfüm.

[95] BGHZ 191, 19 Rn. 32 – Stiftparfüm.

[96] BGHZ 191, 19 Rn. 36 – Stiftparfüm.

[97] BGH, GRUR 2011, 152 = MMR 2011, 172 m. Anm. Engels = K&R 2011, 117 m. Anm. Nelles – Kinderhochstühle im Internet.

nach ihrem Inhalt benannt sind. Allerdings werden gerade bei Urheberrechtsverletzungen die Dateien absichtlich – um diesem Suchmechanismus zu entgehen – anders benannt. Der Uploader trägt sie dann aber in eine der sog. Linklisten ein, damit sie für Interessierte auffindbar bleiben. Diese Linklisten werden nicht vom Filehoster selbst betrieben. Er hat somit nur Zugriff auf das Suchinterface des Linklistenbetreibers, das auch dem normalen Internetnutzer zur Verfügung steht. Da diese Methode dennoch durch die Suchfunktion der jeweiligen Linkliste, die ja gerade dazu gedacht ist entsprechende Ergebnisse zu finden, effektiv ist, sei die Überprüfung einer einstelligen Anzahl von Seiten zumutbar.[98] Diese Prüfungspflichten hat der BGH jüngst erneut erweitert: Auch eine Suche über allgemeine andere Suchmaschinen und Social Networks wie Facebook oder Twitter kann demnach zumutbar sein, unter der Prämisse, dass der Anbieter durch sein Geschäftsmodell Urheberrechtsverletzungen in erheblichem Umfang Vorschub leiste. Die widersprüchlichen Feststellungen, dass derselbe (!) File-Hoster einmal Urheberrechtsverletzungen fördert (File-Hosting-Dienst) und einmal nicht (Alone in the Dark), sind dem BGH zufolge auf die jeweiligen zugrunde liegenden tatrichterlichen Beurteilungen zurückzuführen.[99]

49 Welche **Prüfungspflichten** den sozialen Netzwerkbetreibern zumutbar sind, lässt sich *ex ante* und abstrakt kaum bestimmen: Bei leicht zu überprüfenden Rechtsverstößen können dem Netzwerkbetreiber höhere Prüfungspflichten zugemutet werden als bei komplexen Rechtsverletzungen. Insbesondere bei Persönlichkeitsrechtsverletzungen kann der Netzwerkbetreiber eine entsprechende Nachricht zunächst an den vermeintlichen Verletzer weiterleiten mit der Aufforderung zur Stellungnahme; reagiert dieser nicht, kann der Betreiber ohne Weiteres die entsprechende Äußerung sperren bzw. löschen; meldet sich jedoch der vermeintliche Verletzer und leugnet eine Rechtsverletzung, muss der Betreiber dies an den Abmahnenden wiederum weiterleiten, ebenfalls verbunden mit der Bitte zur Stellungnahme. Erhält der Betreiber von dessen Seite aus keine weitere Stellungnahme, kann der Betreiber die Äußerung auf seinen Webseiten stehen lassen; [100] wehrt sich der Abmahnende jedoch gegen die Stellungnahme des Verletzers, muss der Betreiber sich entscheiden, ob er quasi der Seite des Verletzers beitritt und sich notfalls verklagen lassen muss, oder ob er eine Vertragsverletzung gegenüber dem Verletzer riskiert (und damit ebenfalls in die Haftung genommen werden kann). Andere Möglichkeiten lässt das geltende System nicht zu – auch wenn der Provider damit letztlich doch zwischen Scylla und Charybdis landet.

50 Davon zu unterscheiden ist, ob der Provider auch verpflichtet, **ähnliche Persönlichkeitsrechtsverletzungen** in Zukunft zu unterbinden: Hier ist angesichts der für den Provider äußerst schwierig zu beurteilenden Rechtslage hinsichtlich der Abwägung zwischen den verschiedenen Grundrechten sowie der mangelnden Kenntnis der konkreten Kommunikationsvorgänge und -hintergründe eine enge Auslegung geboten. Gleiches gilt für unwahre Tatsachenbehauptungen, § 824 BGB. Nur wenn die Verletzungen offensichtlich gleich den zuvor inkriminierten Äußerungen sind,

---

[98] BGHZ 194, 339 Rn. 22 – Alone in the Dark; krit. dazu: Hoeren, MMR 2013, 188.
[99] BGH, NJW 2013, 3245 Rn. 36 – File-Hosting-Dienst.
[100] BGHZ 191, 219 Rn. 25 ff. = MMR 2012, 124 m. Anm. Hoeren; dazu Spindler, CR 2012, 176; Feldmann, K&R 2012, 113.

kann der Provider auf Unterlassung ähnlicher Verletzungen in Anspruch genommen werden; alles andere ginge über die ihm zumutbaren Prüfungspflichten hinaus.[101] Ähnlich ist die Rechtslage beim Recht am eigenen Bild nach §§ 22, 23 KUG, da auch dieses oftmals Interessenabwägungen voraussetzt, aber auch von einer Einwilligung abhängen kann, die der Kenntnis des Providers entzogen ist.

51 Auch einer **Störerhaftung für Facebook-Parties** oder Aufrufe zum Flash-Mob sind enge Grenzen gesetzt: Denn der Provider kann kaum selbst einschätzen, ob den Aufrufen ein realer Sachverhalt zu Grunde liegt, welche Interessen Dritter gefährdet werden können oder wie (z. B. im Fall der Flash-Streiks im Arbeitsrecht) die konkrete Interessenabwägung ausfallen kann. Daher wird ein Betreiber sozialer Netzwerke hier nur zur Unterlassung gleichartiger Aufrufe verpflichtet werden können, die fast identisch mit den inkriminierten Aufrufen sind.

52 Etwas intensiver fallen die Pflichten bei **Urheber-** oder anderen **Immaterialgüterrechtsverletzungen** aus, wenn die Rechtsinhaberschaft und die Berechtigung einfacher geprüft werden kann, erst recht wenn automatisierte Beschwerde und Rechtsverfolgungsmöglichkeiten zur Verfügung stehen. Hier ist der Provider eher gehalten, ähnliche Verletzungen zu verfolgen bzw. zu unterbinden.

53 Last but not least käme eine Haftung der Betreiber sozialer Netzwerke gegenüber Eltern in Betracht, wenn minderjährige Netzwerkteilnehmer Zugang zu jugendgefährdenden Inhalten haben. Allerdings gelangt auch eine solche Haftung nicht zum Zuge, da den Provider allenfalls rudimentäre Pflichten der Kontrolle treffen können, wiederum nur bezogen auf weitgehend identische Inhalte. Zudem müssten die Normen des JMStV aus deliktischer Sicht Schutzgesetze zugunsten der Eltern sein – was angesichts des intendierten Schutzes der Jugendlichen schwer zu begründen wäre. Allenfalls wäre denkbar, dass sie Schutzgesetze zugunsten der Jugendlichen selbst sind, deren Ansprüche durch die Eltern quasi als ein „Schutz vor sich selbst" geltend gemacht werden. Zivilrechtlich ist dies bislang ungeklärt, da die Jugendlichen selbst den Zugang zu diesen Inhalten suchen bzw. darin einwilligen. Entscheidend ist aber, dass selbst nach der einschlägigen Rechtsprechung im Bereich der elektronischen Handelsplattformen nur äußerst eingeschränkte Prüfungspflichten gelten. Davon zu unterscheiden sind vertragliche Ansprüche von Eltern gegen einen sozialen Netzwerkbetreiber, wenn nicht der Jugendliche selbst Vertragspartner des Netzwerkes geworden ist.[102]

---

[101] „Großzügige" bis keine Prüfpflichten: Kartal-Aydemir/Krieg, MMR 2012, 647 (651); entsprechend für Autocomplete-Funktion bei Suchmaschinen: Engels, MMR 2013, 535 (539 f.); offen gelassen bei Peifer/Becker, GRUR 2013, 751 (755); entsprechend für Internet-Foren: Nieland, NJW 2010, 1494 (1497): technisch unzumutbar; keine Prüfpflichten eines nicht-professionellen Forenbetreibers: OLG Düsseldorf, MMR 2006, 618 (620); ebenso, wegen der Schwierigkeit Suchbegriffe zu finden: KG, BeckRS 2009, 26813.

[102] Zum Vertragsrecht s. Bräutigam/v. Sonnleitner, Kap. 3 Rn. 98 ff.

5.4.2 Nutzer

Aber auch der Nutzer kommt als Störer in Betracht: Hat er selbst die Rechtsverletzungen begangen, ist er selbstverständlich nach den allgemeinen Regeln auch zur Unterlassung für die Zukunft verpflichtet. Handelt es sich dagegen um den bei sozialen Netzwerken eher seltenen Fall fremder Inhalte, hängt seine Haftung von den gleichen Kriterien ab wie die Störerhaftung der Netzwerkbetreiber, allerdings mit dem Unterschied, dass der Nutzer mit Aufrufen seines Profils in aller Regel bereits genaue Kenntnis von den fremden Inhalten erlangt, zudem oftmals die Verhältnisse etwa einer Kommunikation besser einschätzen kann und ihn daher wesentlich höhere Prüfungspflichten treffen als einen Netzwerkbetreiber. In der Regel dürfte der Nutzer im Grundsatz daher auch bei fremden Inhalten als Störer haften. **54**

Kann der Nutzer jedoch nicht die fremden Kommentare, Postings, Bilder etc. von seinem Profil entfernen, fehlt es ihm an der entsprechenden **Kontrollmöglichkeit**, die unabdingbare Voraussetzung für die Störerhaftung ist, da er sonst verpflichtet wäre, generell jedes Teilen oder jeden Kommentar abzuschalten, was im Lichte von Art. 5 Abs. 1 GG unverhältnismäßig wäre.[103] **55**

5.5 Sonstige Haftungsprivilegierungen

5.5.1 Gestaltungsmöglichkeiten, insbesondere Haftungsausschlussklauseln

Neben den gesetzlichen Haftungsprivilegierungen greifen nach allgemeinen Regeln auch vertragliche Haftungsausschluss- oder -begrenzungsklauseln bei sozialen Netzwerken ein.[104] Soweit diese nach §§ 305 ff. BGB zulässig sind, können sie sowohl die Haftung der Netzwerkbetreiber als auch der Nutzer beschränken. Allerdings kann die Haftung für die Verletzung von Kardinalpflichten allenfalls hinsichtlich der Höhe (voraussehbarer Schaden) begrenzt werden, nicht aber auf grobe Fahrlässigkeit[105] – insbesondere hinsichtlich der Sicherungspflichten als besonders wichtige Nebenpflichten entfällt daher weitgehend die Möglichkeit der Haftungsprivilegierung.[106] **56**

---

[103] Zutr. Stadler, Haftungsrisiko Facebook?, v. 10.4.2012, abrufbar unter: http://www.internet-law.de/2012/04/haftungsrisiko-facebook.html, der jedoch bereits die Diensteigenschaft ablehnt.

[104] Z. B. Facebook: Ziffer 16.3 AGB, abrufbar unter: https://www.facebook.com/terms/provisions/german/index.php; Twitter: Ziffer 11 AGB: abrufbar unter: https://twitter.com/tos; LinkedIn: Ziffer 5 und 6 der Nutzervereinbarungen, abrufbar unter: http://de.linkedin.com/legal/user-agreement?trk = hb_ft_userag; Xing: Ziffer 9 AGB, abrufbar unter: http://www.xing.com/terms.

[105] Christensen, in: Ulmer et al., AGB-Recht, § 309 Nr. 7 BGB, Rn. 39; BGHZ 96, 18 (26 f.) = NJW 1986, 1610; BGHZ 106, 259 (267) = NJW 1989, 582; BGHZ 120, 108 (122) = NJW 1993, 326; BGH, NJW 1996, 1407 (1407 f.).

[106] S. o. Fn. 466.

57 **Im Verhältnis der Nutzer untereinander** können die Haftungsbegrenzungsklauseln ebenfalls Wirkung entfalten, da alle Teilnehmer sich auf die gleichen Bedingungen eingelassen haben. Entsprechend den zu Auktionsplattformen entwickelten Grundsätzen[107] müssen sich die Teilnehmer daher den gleichen Bedingungen unterwerfen, einschließlich auch etwaiger Spielregeln oder zu beachtender Grundsätze.[108] Weitere Haftungsausschlüsse wie etwa § 708 BGB können dagegen nicht ins Feld geführt werden, da kein gesellschaftsvertragliches Verhältnis zwischen den Teilnehmern existiert; wohl aber können im Rahmen etwa der Interessenabwägung bei Äußerungsdelikten die auf einer Plattform vorherrschenden Kommunikationsstandards eine Rolle spielen, etwa wenn üblicherweise eine derbe oder deutliche Sprache gepflegt wird.

58 Selbstverständlich können vertragliche Haftungsreduzierungen nicht gegenüber Dritten eingreifen.

5.5.2 Minderjährige

59 Darüber hinaus greifen die üblichen Haftungsprivilegierungen ein, insbesondere im Deliktsrecht für Minderjährige nach §§ 827 ff. BGB; erst bei entsprechender Einsichtsfähigkeit kommen demnach Schadensersatzansprüche in Betracht. Gem. § 828 Abs. 1 BGB erreicht ein Minderjähriger diese erst mit Vollendung des siebenten Lebensjahres. Vom vollendeten siebenten bis zum vollendeten achtzehnten Lebensjahr besteht eine widerlegliche Vermutung dafür, dass der Minderjährige einsichtsfähig ist (§ 828 Abs. 3 BGB).

5.6 Haftung von Eltern und Aufsichtspersonen

60 Neben Minderjährigen und bei deren fehlender Deliktsfähigkeit anstelle von ihnen kann eine Schadensersatzhaftung der Aufsichtspersonen, insbesondere Eltern, nach § 832 BGB in Betracht kommen. Wie der BGH allerdings unlängst zu Recht festgehalten hat, dürfen an die Überwachungspflichten der Eltern keine überspannten Anforderungen gestellt werden.[109] Zwar muss immer der konkrete Charakter und die Eigenheiten des Minderjährigen beachtet werden,[110] aber bei einem gewöhnlich entwickelten 13-jährigen sind Kontrollen nur bei tatsächlichen Anhaltspunkten nötig;

---

[107] S. dazu: BGH, NJW 2011, 2643; Wagner/Zenger, MMR 2013, 343 (346 f.); Wiebe, in: Spindler/Wiebe, Internetauktionen und elektronische Marktplätze, 2. Aufl. 2005, Kap. 4 Rn. 120 ff.; Spindler, ZIP 2001, 809; LG Bonn, BeckRS 2012, 14820.

[108] Zu den vertragsrechtlichen Fragen s. Bräutigam/v. Sonnleitner, Kap. 3 Rn. 85 ff.

[109] BGH, NJW 2013, 1441 – Morpheus = CR 2013, 324 m. Anm. Brüggemann = GRUR 2013, 511 m. Anm. Schaub = K&R 2013, 326 m. Anm. Drücke = MMR 2013, 388 m. Anm. Hoffmann.

[110] Dies betonend Schaub, GRUR 2013, 511 (516).

es genügt im Übrigen, den Minderjährigen zu ermahnen und zu belehren.[111] Eine tatsächliche Kontrolle des Verhaltens würde dazu führen, dass der Minderjährige auf Schritt und Tritt überwacht werden müsste, was in der Regel unvereinbar mit der zu beachtenden wachsenden Selbstständigkeit des Kindes ist und auch in der Wertung von § 1626 Abs. 2 S. 1 BGB zum Ausdruck kommt.[112] Zudem ist die Gefährdung der Rechtsgüter Dritter, die durch eine Teilnahme eines Kindes an einer Tauschbörse entsteht, wesentlich geringer als bspw. die im Straßenverkehr.[113] Kontrollpflichten können aber bestehen, wenn der Minderjährige einen konkreten Anlass geboten hat,[114] vor allem bei Verstößen gegen das Verbot und entsprechender Auffälligkeit für die Eltern. Dies gilt erst recht für volljährige Familienangehörige.[115] Allerdings lässt die Rechtsprechung offen, ob dann verschärfte Kontrollpflichten gleich bei einem ersten Verstoß[116] oder erst bei nicht mehr gelegentlichen Verstößen eingreifen.[117]

Nichts anderes gilt auch für soziale Netzwerke und Rechtsverletzungen, die Minderjährige dort begehen. Auch hier können die Eltern allenfalls zu stichprobenartigen Überprüfungen im Rahmen ihrer Möglichkeiten gehalten sein; ein generelles Verbot etwa der Beteiligung an sozialen Netzwerken ist angesichts der gerade für jüngere Generationen überragenden Bedeutung dieser Kommunikationsplattformen kaum angemessen.[118] **61**

5.7 Kollisionsrecht und europäisches Recht (Herkunftslandprinzip)

Angesichts der Globalität auch von sozialen Netzwerken[119] kann schließlich kollisionsrechtlich fraglich sein, welche Rechtsordnung auf eine Rechtsverletzung anwendbar ist. Soziale Netzwerke werfen hier keine Besonderheiten auf, so dass sich die jeweilige Rechtsordnung nach den für das entsprechende Rechtsgebiet entwickelten Anknüpfungskriterien richtet, die hier nur summarisch dargelegt werden können: **62**

Für **Urheberrechtsverletzungen** ist für das Vervielfältigungsrecht (Upload von Dateien etc.) der Ort maßgeblich, an dem das neue Werkstück angefertigt wird. **63**

---

[111] BGH, NJW 2013, 1441 Rn. 24 – Morpheus; ein an Altersstufen ausgerichtetes abgestuftes System andenkend: Hilbig-Lugani, LMK 2013, 347217.
[112] BGH, NJW 2013, 1441 Rn. 26 – Morpheus; zust. Brüggemann, CR 2013, 327 (328).
[113] BGH, NJW 2013, 1441 Rn. 27 – Morpheus; m. krit. Anm. dazu: Hoffmann, MMR 2013, 388 (392); Rauer/Pfuhl, WRP 2013, 802 (803).
[114] BGH, NJW 2013, 1441 Rn. 25 – Morpheus; krit. Gooren, ZUM 2013, 479 (481).
[115] BGH W 2014, 2360 – Bearshare.
[116] Drücke, K&R 2013, 322 (327); wohl auch Gooren, ZUM 2013, 479 (481).
[117] Rauer/Pfuhl, WRP 2013, 802 (804): erst bei mehr als gelegentlichen Verstößen.
[118] Brüggemann, CR 2013, 327 (328); Thora, VersR 2013, 868 (869).
[119] So gibt es etwa bei Facebook keine territorialen Einschränkungen für Teilnehmer, auch wenn die Plattform je nach Land andere Sprachen verwendet etc.

Allerdings wäre dies gerade im Internet und bei sozialen Netzwerken eine unbefriedigende Lösung, erst recht in der Cloud, da der Ort der speichernden Server nicht vorhersehbar ist, so dass die jeweilige Rechtsordnung eher zufällig wäre. Stattdessen ist auf den Ort abzustellen, von dem der Vervielfältigungsvorgang aus gesteuert wird.[120] Für das öffentliche Zugänglichmachen (§ 19a UrhG) ist demgegenüber auf die Ausrichtung eines Angebotes auf einem bestimmten Adressatenkreis (bzw. dessen Rechtsordnung) abzustellen, was sich nach verschiedenen Kriterien wie verwandte Sprache etc. richten kann.[121]

64 Für **Persönlichkeitsrechtsverletzungen** kristallisiert sich inzwischen eine vergleichbare Anknüpfung heraus: Als Erfolgsort sieht der EuGH i. R. d. internationalen Prozessrechts gem. Art. 5 Abs. 3 EuGVVO hier den Ort an, an dem der Geschädigte den Mittelpunkt seiner Interessen hat, da der Schädiger in der Regel Kenntnis davon hat und zudem Zufälligkeiten damit verhindert werden.[122] Der Mittelpunkt der Interessen wird in der Regel am gewöhnlichen Aufenthaltsort liegen, kann aber auch in Ausnahmefällen in einem anderen Staat belegen sein, bspw. wenn der Betroffene dort seinem Beruf nachgeht.[123] Nur an diesem oder am Handelsort – der Niederlassung des Schädigers – kann der gesamte Schadensersatz, an allen anderen Orten von denen der Inhalt zugänglich ist, dagegen nur Ersatz für den Schaden verlangt werden, der dort auch wirklich entstanden ist (sog. „Mosaiklösung“).[124] Die Mosaikmethode verursacht aber Probleme, wenn man sie auf Unterlassungs- und Beseitigungsansprüche anwendet.[125] Denn hiernach könnte praktisch überall ein Unterlassungs- und Beseitigungsanspruch gerichtlich geltend gemacht werden.[126] Allerdings lässt sich dies durch eine einschränkende Auslegung von Art. 5 Abs. 3 EuGVVO auffangen, indem man für Unterlassungs- und Beseitigungsansprüche nicht die bloße Zugänglichkeit genügen lässt um einen Erfolgsort zu begründen.[127]

65 Schließlich wird für EU-Mitgliedstaaten das anwendbare Recht für Persönlichkeitsrechtsverletzungen durch das **Herkunftslandprinzip**, Art. 3 ECRL, überlagert,

---

[120] Dreier, in: Dreier/Schulze, UrhG, Vorb. §§ 120 ff. Rn. 33; Katzenberger, in: Schricker/-Loewenheim, UrhR, vor §§ 120 ff., Rn. 145; a. A. Hoeren, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 7.8 Rn. 16;

[121] EuGH, MMR 2013, 108 Rn. 39 ff. – Football Dataco = K&R 2013, 107; s. dazu auch Spindler, in: FS Schneider, 2014; Götting, LMK 2012, 337357, Reinholz, K&R 2013, 171.

[122] EuGH, NJW 2012, 137 Rn. 52 – eDate Advertising = JZ 2012,199 m. Anm. Hess = CR 2011, 808 m. Anm. Roth; dazu s. auch Spindler, AfP 2012, 114 (116); W.-H. Roth, IPrax 2013, 215 (221).

[123] EuGH, NJW 2012, 137 Rn. 49 – eDate Advertising; krit. hinsichtlich der Vorhersehbarkeit: Roth, IPrax 2013, 215 (221).

[124] EuGH, NJW 2012, 137 Rn. 52 – eDate Advertising = JZ 2012,199 m. Anm. Hess = CR 2011, 808 m. Anm. H.-P. Roth; Spindler, AfP 2012, 114 (116 f.); W.-H. Roth, IPrax 2013, 215 (221 f.).

[125] Spindler, AfP 2012, 114 (117).

[126] W.-H. Roth, IPrax 2013, 215 (223).

[127] So W.-H. Roth, IPrax 2013, 215 (223); s. auch Wagner, in: Stein/Jonas, ZPOArt. 5 EuGVVO, Rn. 169 und Leible, in: Rauscher, Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR, Art. 5 Brüssel I-VO, Rn. 92, die Art. 5 Abs. 3 EuGVVO nicht auf negatorische Ansprüche anwenden wollen.

wonach das jeweils günstigere Recht (ob Herkunftsland oder Empfangsstaat) anzuwenden ist.[128] Allerdings greift das Herkunftslandprinzip nur für kommerzielle Dienste, nicht dagegen für private Nutzer – die meisten Delikte im Rahmen sozialer Netzwerke kommen daher nicht in den Genuss des Herkunftslandprinzips, sondern unterfallen den allgemeinen oben dargelegten Regeln, mithin dem Erfolgsort des Geschädigten bzw. dessen Rechtsordnung ohne einen Günstigkeitsvergleich.[129]

5.8 Prozessuale Fragen – Beweis- und Darlegungslast, Auskunftsansprüche

66 Auch hinsichtlich der prozessualen Fragen ergeben sich keine Besonderheiten gegenüber den allgemeinen Regeln: der Geschädigte hat die ihm günstigen Tatsachen darzulegen und zu beweisen und umgekehrt für den Schädiger.[130] Lediglich für die Bereiche der Produkthaftung, z. B. bereitgehaltene Apps, und auch für die Verletzung von Sicherungspflichten kann mangels entsprechender Einblicke der Geschädigten in die Abläufe bei sozialen Netzwerkbetreibern eine Umkehr der Darlegungs- und Beweislast angenommen werden.[131]

67 Last but not least wird für Geschädigte oftmals das Problem bestehen, die Identität eines Schädigers auf sozialen Netzwerken festzustellen, da Nutzer häufig Synonyme gebrauchen, auch wenn viele AGB von Netzwerkbetreibern eine Pflicht zum Klarnamen statuieren.[132] Gegenüber den Netzwerkbetreibern besteht aber für Urheberrechtsverletzungen ein **Auskunftsanspruch** nach § 101 Abs. 2 Nr. 3 UrhG;[133] hat

---

[128] EuGH, NJW 2012, 137 Rn. 68; s. auch Spindler, AfP 2012, 114 (119 f.); W.-H. Roth, IPrax 2013, 226; Einzelheiten bei Spindler, in: Spindler et al., TMG, § 3 TMG (erscheint 2015).

[129] Altenhain, in: MüKo-StGB, § 3 TMG, Rn. 9; Pfeiffer et al., in: Spindler/Schuster, § 3 TMG Rn. 5; Gitter, in: Roßnagel, Recht der Telemediendienste, § 3 TMG, Rn. 17.

[130] BGH, NJW-RR 2010, 1378 (1379); NJW 2005, 2395 (2396); BGHZ 113, 222 (224 f.) = NJW 1991, 1052; BGHZ 116, 278 (288) = NJW 1992, 683; Prütting, in: MüKo-ZPO, § 286 Rn. 111; Foerste, in: Musielak, ZPO, § 286 Rn. 35; Saenger, in: Saenger, ZPO, § 286 Rn. 58.

[131] So für IT-Produkte: Spindler, Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010, S. 39 f.; s. ferner allgemein zur Beweislastumkehr: Spindler, in: Bamberger/Roth, § 823 Rn. 552 ff.; Wagner, in: MüKo-BGB, § 823 Rn. 684; BGHZ 80, 186 (196 f.) bestätigt in BGH, NJW 1996, 2507 (2508); VersR 1999, 456.

[132] Facebook: Ziffer 4 Erklärung der Rechte und Pflichten, abrufbar unter: https://www.facebook.com/legal/terms; LinkedIn: Ziffer 2 C Nutzervereinbarungen, abrufbar unter: http://de.linkedin.com/legal/user-agreement?trk=hb_ft_userag; Xing: Ziffer 2.2 AGB, abrufbar unter: http://www.xing.com/terms; s. auch Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, Band I, 2012, F 59.

[133] Entsprechend zu Host-Providern: OLG München, ZUM-RD 2012, 88; OLG Köln, ZUM-RD 2011, 350; Spindler, in: Spindler/Schuster, § 101 UrhG, Rn. 7; Dreier, in: Dreier/Schulze, UrhG, § 101 Rn. 10; Reber, in: BeckOK-UrhG, § 101 Rn. 3; s. ferner: Weber, Die Umsetzung der Enforcement-Richtlinie ins deutsche Recht, S. 109 ff., 340 ff.; Spindler/Weber, ZUM 2007, 257 (261).

allerdings der Netzwerkbetreiber nicht die Identität geprüft, muss der Geschädigte versuchen, über die verfügbaren Daten den Schädiger zurückzuverfolgen.

68 Für Persönlichkeitsrechte besteht derzeit kein ausdrücklicher vergleichbarer Auskunftsanspruch, was verfassungsrechtlich bedenklich ist. Hier muss in entsprechender Analogie bzw. verfassungskonformer extensiver Auslegung § 101 UrhG entsprechend angewandt werden, zumindest die bestehenden Auskunftsansprüche über § 242 BGB ausgedehnt werden, damit der Geschädigte nicht rechtlos steht.[134]

Literatur

Ahlberg, H., Götting, H.-P. (Hrsg.) (2013). *Beck'scher Online-Kommentar Urheberrecht* (Edition 2). München: C. H. Beck.

Bamberger, H. G., Roth, H. (Hrsg.) (2013a). *Beck'scher Online-Kommentar BGB* (Edition 28). München: C. H. Beck.

Bamberger, H. G., Roth, H. (Hrsg.) (2013b). *Bürgerliches Gesetzbuch*. 3. Aufl. München: C. H. Beck.

Baumgartner, U., Ewald, K. (2013). *Apps und Recht*. München: C.H. Beck.

Bentley, L. A. F., Derclaye, E. et al. (2013). University of Cambridge Faculty of Law Research Paper No. 6/2013, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220326.

Berberich, M. (2010). *Virtuelles Eigentum*. Tübingen: Mohr Siebeck.

Berger, A., Janal, R. (2004). Suchet und Ihr werdet finden? – Eine Untersuchung zu Störerhaftung und Auktionshäusern. *CR*, 917 ff.

Bräutigam, P. (2012). Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten. *MMR*, 635 ff.

Dreier, T., Leistner, M. (2013). Urheberrecht im Internet: die Forschungsherausforderungen. *GRUR*, 881 ff.

Dreier, T., Schulze, M. (2013). *Urheberrechtsgesetz*. 4. Aufl. München: C. H. Beck.

Ewert, J., von Hartz, N. (2009). Neue kostenrechtliche Herausforderungen bei der Abmahnung im Urheberrecht. *MMR*, 84 ff.

Foerste, U., von Westphalen, F. Graf (Hrsg.) (2012). *Produkthaftungshandbuch*. 3. Aufl. München: C. H. Beck.

Fromm, F. K., Nordemann, W. (Hrsg.) (2008). *Urheberrecht*. 10. Aufl. Stuttgart: Kohlhammer.

Fuhlrott, M., Fabritius, B. (2010). Zur Zulässigkeit von Flashmob-Aktionen. *EWiR*, 51 f.

Gabel, D. (2005). Die Haftung für Hyperlinks im Lichte des neuen UWG. *WRP*, 1102 ff.

Gola, P., Schomerus, R. (Hrsg.) (2012). *Bundesdatenschutzgesetz*. 11. Aufl. München: C. H. Beck.

Gooren, P. (2013). Internetnutzung und elterliche Aufsichtspflicht. *ZUM*, 479 ff.

Götting, H.-P. (Hrsg.) (2008). *Handbuch des Persönlichkeitsrechts*. München: C. H. Beck.

---

[134] Anders jedoch BGH NJW 2014, 2651 wegen Grenzen richterlicher Rechtsfortbildung; s. dazu Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen des 69. Deutschen Juristentages, Band I, F 58, F 111 f.; BGHZ 148, 26 (30) – Entfernung der Herstellernummer II; BGHZ 125, 322 (331) – Cartier-Armreif; BGH NJW 1995, 1965 (1966) – Schwarze Liste; OLG Dresden, ZUM-RD 2012, 536 (538 f.); LG Berlin, ZUM 2006, 430; Seitz, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 8 Rn. 71 ff.; abl. für Telemedien: OLG Hamm, ZUM-RD 2011, 684 (685); AG München, MMR 2011, 417; abl. für die Fälle der Störerhaftung Rixecker, in: MüKo-BGB, § 12 Rn. 253; zu den Voraussetzungen des Anspruchs s. Freund, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 53 Rn. 16 ff.; zum Verhältnis zu § 101 UrhG s. auch Amschewitz, WRP 2011, 301 ff.

Härting, N. (2012). Rotlichtgerüchte: Haftet Google? *K&R*, 633 ff.
Härting, N. (2013). Allgegenwärtige Prüfungspflichten für Intermediäre – Was bleibt noch nach „Kinderhochstühle" und „Autocomplete" von der Störerhaftung übrig? *CR*, 443 ff.
Heidrich, J., Forgó, N., Feldmann, T. (Hrsg.) (2011). *Heise Online-Recht – Der Leitfaden für Praktiker & Juristen*. Loseblatt (Stand: 3. EL Oktober 2011). Hannover: Heise.
Hoeren, T. (2009). 100 Euro und Musikdownloads – die Begrenzung der Abmahngebühren nach § 97a UrhG. *CR*, 378 ff.
Hoeren, T. (2013). Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht. *MMR*, 486 ff.
Hoeren, T., Sieber, U., Holznagel, B. (Hrsg.) (2012). *Handbuch Multimedia-Recht*. Loseblatt (Stand: 34. EL April 2013). München: C. H. Beck.
Joecks, W., Miebach, K. (Hrsg.) (2010). *Münchener Kommentar zum StGB*, Bd. 6/1. 2. Aufl. München: C. H. Beck.
Kartal-Aydemir, A., Krieg, R. (2012). Haftung von Anbietern kollaborativer Internetplattformen – Störerhaftung für User Generated Content? *MMR*, 647 ff.
Kilian, W., Heussen, B. (Hrsg.) (2012). *Computerrechts-Handbuch*. Loseblatt (Stand: 31. EL Mai 2012). München: C. H. Beck.
Krieger, S., Günther, J. (2010). Streikrecht 2.0 – Erlaubt ist, was gefällt!? *NZA*, 20 ff.
Kühl, K. (2011). *Strafgesetzbuch*. 27. Aufl. München: C. H. Beck.
Leible, S., Sosnitza, O. (2004). „3… 2… 1… meins!" und das TDG – Zur Haftung von Internetauktionshäusern für rechtswidrige Inhalte. *WRP*, 592 ff.
Leistner, M. (2010). Störerhaftung und mittelbare Schutzrechtsverletzung. *GRUR*, Beilage zu Heft 1, 1 ff.
Leistner, M. (2012). Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet. *ZUM*, 722 ff.
Loewenheim, U. (Hrsg.) (2010). *Handbuch des Urheberrechts*. 2. Aufl. München: C. H. Beck.
Maaßen, S. (2013). Neuregelung der Abmahnung im Urheberrecht – Analyse von § 97a UrhG-E. *GRUR-Prax*, 153 ff.
Malkus, M. (2010). Harry Potter und die Abmahnung des Schreckens – Die Höhe von Abmahngebühren bei Urheberrechtsverletzungen auf Tauschbörsen gem. § 97a Abs. 2 UrhG. *MMR*, 382 ff.
Matthies, U. (2004). *Providerhaftung für Online-Inhalte*. Baden-Baden: Nomos.
Meier, K., Wehlau, A. (1998). Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung. *NJW*, 1585 ff.
Meyer, S. (2013). Aktuelle Rechtsentwicklungen bei Suchmaschinen im Jahre 2012. *K&R*, 221 ff.
Musielak, H.-J. (Hrsg.) (2013). *Kommentar zur Zivilprozessordnung*. 10. Aufl. München: Vahlen.
Nieland, H. (2010). Störerhaftung bei Meinungsforen im Internet – Nachträgliche Löschungspflicht oder Pflicht zur Eingangskontrolle? *NJW*, 1494 ff.
Obergfell, E. I. (2013). Expansion der Vorbeugemaßnahmen und zumutbare Prüfpflichten von File-Hosting-Diensten. *NJW*, 1995 ff.
Ott, S. (2004). Die urheberrechtliche Zulässigkeit des Framing nach der BGH-Entscheidung im Fall „Paperboy". *ZUM*, 357 ff.
Ott, S. (2011). Die Entwicklung des Suchmaschinen- und Hyperlink-Rechts im Jahr 2010. *WRP*, 655 ff.
Peifer, K.-N. (2013). Persönlichkeitsrechte im 21. Jahrhundert – Systematik und Herausforderungen. *JZ*, 853 ff.
Rauer, N., Ettig, D. (2013). Zur urheberrechtlichen Zulässigkeit des Framing. *K&R*, 429 ff.
Rauer, N., Pfuhl, F. (2013). Anmerkung zum Urteil des BGH vom 15.11.2012 (I ZR 74; WRP 2013, 799). *WRP*, 802 ff.
Rauscher, T. (Hrsg.) (2011). *Europäisches Zivilprozess- und Kollisionsrecht*. München: Sellier.
Rauscher, T., Wax, P., Wenzel, J. (Hrsg.) (2013). *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*, Band. 1. 4. Aufl. München: C. H. Beck.

Rehder, B., Deinert, O., Callsen, R. (2012). Atypische Arbeitskampfformen der Arbeitnehmerseite – sozialwissenschaftliche Grundlagen und rechtliche Rahmenbedingungen. *ArbuR*, 103 ff.

Reinholz, F. (2013). Grenzüberschreitende Weiterverwendung von Daten aus geschützter Live-Fußball-Datenbank. *K&R*, 171 ff.

Rosenbaum, B., Tölle, D. (2013). Aktuelle rechtliche Probleme im Bereich Social Media – Überblick über die Entscheidungen der Jahre 2011 und 2012. *MMR*, 209 ff.

Roßnagel, A. (Hrsg.) (2013). *Beck'scher Kommentar zum Recht der Telemediendienste*. München: C. H. Beck.

Rössel, M. (2011). Filterpflichten des Providers im Lichte des EuGH – Eine Entlastung des I. Zivilsenats. *CR*, 589 ff.

Roth, H.-P. (2011). Verantwortlichkeit von Betreibern von Internet-Marktplätzen für Markenrechtsverletzungen durch Nutzer: L'Oréal gegen eBay – Gleichzeitig Anmerkungen zum EuGH-Urteil vom 12.07.2011 (Rs. C –324/09). *WRP*, 1258 ff.

Roth, W.-H. (2013). Persönlichkeitsschutz im Internet: Internationale Zuständigkeit und anwendbares Recht. *IPrax*, 215 ff.

Säcker, F. J., Rixecker, R. (Hrsg.) (2012). *Münchener Kommentar zum Bürgerlichen Gesetzbuch*. 6. Aufl. München: C. H. Beck.

Schack, H. (2013). *Urheber- und Urhebervertragsrecht*. 6. Aufl. Tübingen: Mohr Siebeck.

Schapiro, L. (2008). Die neuen Musiktauschbörsen unter „Freunden". *ZUM*, 273 ff.

Schönke, A., Schröder, H. (Hrsg.) (2010). *Strafgesetzbuch*. 28. Aufl. München: C. H. Beck.

Schöwerling, H. (2007). *E-Learning und Urheberrecht an Universitäten*. Wien: Verl. Medien und Recht.

Schricker, G., Loewenheim, U. (Hrsg.) (2010). *Urheberrecht*. 4. Aufl. München: C. H. Beck.

Sieber, U., Liesching, M. (2007). Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem Telemediengesetz. *MMR*, Beilage 8/2007, 1 ff.

Simitis, S. (Hrsg.) (2011). *Bundesdatenschutzgesetz*. 7. Aufl. Baden-Baden: Nomos.

Sobola, S., Kohl, K. (2005). Haftung von Providern für fremde Inhalte Haftungsprivilegierung nach § 11 TDG – Grundsatzanalyse und Tendenzen der Rechtsprechung. *CR*, 443 ff.

Spickhoff, A. (2011). Der Schutz von Daten durch das Deliktsrecht. In: S. Leible, M. Lehmann, H. Zech (Hrsg.), *Unkörperliche Güter im Zivilrecht*. Tübingen: Mohr Siebeck (S. 223 ff.).

Spieker, O. (2010). Verantwortlichkeit von Internetsuchdiensten für Persönlichkeitsrechtsverletzungen in ihren Suchergebnislisten. *MMR*, 727 ff.

Spindler, G. (2001). Vertragsabschluß und Inhaltskontrolle bei Internet-Auktionen – Zugleich eine Besprechung des Urteils des OLG Hamm vom 14 Dezember 2000, ZIP 2001, 291- ricardo-de. *ZIP*, 809 ff.

Spindler, G. (2002a). Verantwortlichkeit und Haftung für Hyperlinks im neuen Recht. *MMR*, 495 ff.

Spindler, G. (2002b). Das Gesetz zum elektronischen Geschäftsverkehr – Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip. *NJW*, 921 ff.

Spindler, G. (2004a). Hyperlinks und ausländische Glücksspiele – Karlsruhe locuta causa finita? *GRUR*, 724 ff.

Spindler, G. (Hrsg.) (2004b). *Vertragsrecht der Internet-Provider*. 2. Aufl. Köln: O. Schmidt.

Spindler, G. (2004c). Die Verantwortlichkeit der Provider für „Sich-zu-Eigen-gemachte" Inhalte und für beaufsichtigte Nutzer. *MMR*, 440 ff.

Spindler, G. (2005). Verantwortlichkeit eines Plattformbetreibers für fremde Inhalte. *JZ*, 3 ff.

Spindler, G. (2007a). *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären*, Studie im Auftrag des BSI, 2007, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile.

Spindler, G. (2007b). Das neue Telemediengesetz – Konvergenz in sachten Schritten. *CR*, 239 ff.

Spindler, G. (2011a). *Haftung und Versicherung im IT-Bereich: Karlsruher Forum 2010*. Karlsruhe: Verl. Versicherungswirtschaft.

Spindler, G. (2011b). Präzisierungen der Störerhaftung im Internet – Besprechung des BGH-Urteils „Kinderhochstühle im Internet". *GRUR*, 101 ff.

Spindler, G. (2011c). Europarechtliche Rahmenbedingungen der Störerhaftung im Internet – Rechtsfortbildung durch den EuGH in Sachen L'Oréal/eBay. *MMR*, 703 ff.
Spindler, G. (2011d). Der Schutz virtueller Gegenstände. *ZGE*, 129 ff.
Spindler, G. (2012a). Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung. In: Ständige Deputation des Deutschen Juristentages (Hrsg.), *Verhandlungen des 69. Deutschen Juristentages*, Band I.
Spindler, G. (2012b). Störerhaftung des Host-Providers bei Persönlichkeitsrechtsverletzungen – Impulse aus dem VI. Zivilsenat des BGH – zugleich Anmerkung zu BGH, Urt. v. 25.10.2011- VI ZR 93/10- Blogger. *CR*, 176 ff.
Spindler, G. (2012c). Kollisionsrecht und internationale Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet – die eDate-Entscheidung des EuGH. *AfP*, 114 ff.
Spindler, G. (2012d). Anmerkung zum Urteil des EuGH vom 24.11.2011 (C-70/10; JZ 2012, 308) – Zur Frage der generellen Filterpflicht für Internet-Access-Provider. *JZ*, 311 ff.
Spindler, G., Schmitz, P. (Hrsg.) (2014). *TMG – Telemediengesetz Kommentar*. 2. Aufl. München: C. H. Beck.
Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien*. 2. Aufl. München: C. H. Beck.
Spindler, G., Volkmann, C. (2003). Die zivilrechtliche Störerhaftung der Internet-Provider. *WRP*, 1 ff.
Spindler, G., Wiebe, A. (Hrsg.) (2005). *Internetauktionen und elektronische Marktplätze*. 2. Aufl. Köln: O. Schmidt.
Spindler, G., Schmitz, P., Geis, I. (Hrsg.) (2004). *Teledienstegesetz*. München: C. H. Beck.
Saenger, I. (Hrsg.) (2013). *Zivilprozessordnung*. 5. Aufl. Baden-Baden: Nomos.
Stadler, T. (2005). *Haftung für Informationen im Internet*. 2. Aufl. Berlin: Erich Schmidt.
Staudinger, J. von (2014). *Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen*. Berlin: Sellier-de Gruyter.
Stein, F., Jonas, M. (2013). *Kommentar zur Zivilprozessordnung*. 22. Aufl. Tübingen: Mohr Siebeck.
Ulmer, P., Brandner, E., Hensen, H.-D. (Hrsg.) (2011). *AGB-Recht*. 11. Aufl. Köln: Dr. Otto Schmidt.
Volkmann, C. (2005). *Der Störer im Internet*. München: C. H. Beck (zugl. Diss Göttingen 2004).
von Ungern-Sternberg, J. (2012). Urheberrechtliche Verwertungsrechte im Lichte des Unionsrechts. *GRUR*, 1198 ff.
Wandtke, A.-A., Bullinger, W. (Hrsg.) (2009). *Praxiskommentar zum Urheberrecht*. 3. Aufl. München: C. H. Beck.
Wiebe, A. (2012). Providerhaftung in Europa: Neue Denkanstöße durch den EuGH (Teil 1). *WRP*, 1182 ff.

Kapitel 6
Persönlichkeitsrechtliche Aspekte der Social Media

Ralf Müller-Terpitz

Inhalt

R. Müller-Terpitz (✉)
Inhaber des Lehrstuhls für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien, Universität Mannheim, Schloss Westflügel, 68131 Mannheim, Deutschland
E-Mail: mueller-terpitz@uni-mannheim.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_6

6.1 Einleitung

1 Social Media wie die Netzwerk- und Multimediaplattformen Facebook, Google+, Stayfriends, Xing, LinkedIn, YouTube, Instagram oder Flickr, Personal Publishing-Plattformen wie Blogger, die Wiki-Systeme sowie Instant Messaging-Dienstleistungen wie Twitter oder WhatsApp[1] ermöglichen soziale, kulturelle, politische oder auch wissenschaftliche Interaktionen zwischen ihren Nutzern. Insbesondere eröffnen sie die Möglichkeit, einfach und schnell eigene Inhalte – den sog. **„user generated content"** – auf solchen Plattform einzustellen und ihn dadurch einer unbeschränkten oder zuvor definierten Öffentlichkeit zugänglich zu machen.

2 Zu diesen Inhalten gehören typischerweise Meinungsäußerungen oder Tatsachenbehauptungen über Dritte, aber auch Bilder und Bewegtbilder, in denen Dritte dargestellt werden. Beeinträchtigungen oder gar Verletzungen der Persönlichkeitsrechte dieser Dritten sind damit programmiert. Zwar ist dieses Verhalten in vielen Fällen der Tätigkeit traditioneller Medien (Presse, Rundfunk) und der hieraus resultierenden Rechtsfragen vergleichbar. Es unterscheidet sich von diesen aber auch durch **Besonderheiten**: Zum einen erfolgt die Verbreitung der Inhalte nicht zwangsläufig durch professionelle Akteure, sondern zu einem Großteil durch Private („Laien"). Zumeist fehlt diesen die Erfahrung im Umgang mit Persönlichkeitsrechten der Betroffenen, nicht zuletzt, wenn es sich bei diesen Privaten – wie sehr häufig im Bereich der Social Media – um jugendliche Nutzer handelt. Mitunter ist die „generation of content" sogar auf eine gezielte Persönlichkeitsrechtsverletzung angelegt, etwa bei Inhalten, die bewusst auf einer „Mobbing-" oder „Pranger-Plattform"[2] gepostet werden. Zum anderen sind diese Inhalte über leistungsfähige Suchmaschinen leicht auffindbar und ubiquitär, d. h. von überall abrufbar, was die Erstellung von mehr oder wenig detaillierten Persönlichkeitsprofilen ermöglicht.[3] Des Weiteren stößt die Entfernung persönlichkeitsrechtsverletzender Inhalte aus dem Netz schnell an technische (Spiegeln von Inhalten auf verschiedenen Servern) oder rechtliche Grenzen (unterschiedliche Jurisdiktionsräume); auch kann es sich als schwierig erweisen, den für einen inkriminierten Inhalt Verantwortlichen zur Rechenschaft zu ziehen, da dieser möglicherweise anonym bleibt oder in einem anderen Staat beheimatet ist.

3 Vor diesem Hintergrund können Persönlichkeitsbeeinträchtigungen durch Social Media von stärkerer Intensität sein als bei traditionellen Medien. Dies führt zu der Frage, welche **Bedeutung** dem Persönlichkeitsrecht in sozialen Netzwerken zukommt, d. h. in welchem Umfang es geschützt ist und durch welche netzwerkspezifischen Verhaltensweisen es verletzt werden kann.

---

[1] Ausführlich zum Begriff der Social Media und seiner Systematisierung Hohlfeld/Godulla, Kap. 2, Rn. 21 ff.

[2] Als Beispiel kann hier auf die zwischenzeitlich gesperrten bzw. „gehackten" Plattformen „rottenneighbor" oder „iShareGossip" verwiesen werden.

[3] Vgl. EuGH, GRUR 2014, 895 (897, 900) – Google.

6.2 Grundrechtlicher Rahmen für persönlichkeitsrelevante Sachverhalte

6.2.1 Vorbemerkungen

Das Persönlichkeitsrecht gehört mittlerweile zum tradierten Bestand des Grundrechtekanons. Im Grundgesetz wird es als allgemeines Persönlichkeitsrecht durch **Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG** geschützt. In der Europäischen Menschenrechtskonvention (EMRK) findet es Niederschlag im Recht auf Achtung des Privatlebens aus Art. 8 Abs. 1 EMRK. Die EU-Grundrechtecharta (EU-GRC) hat diese Bestimmung wortgleich in ihren Art. 7 übernommen. **4**

In der Bundesrepublik Deutschland wurde das allgemeine Persönlichkeitsrecht zunächst durch die Rechtsprechung der Zivilgerichte entwickelt und als **„sonstiges Recht"** i. S. d. § 823 Abs. 1 BGB anerkannt. Dementsprechend können Verletzungen des allgemeinen Persönlichkeitsrechts zivilrechtliche Schadensersatzansprüche oder – über eine analoge Anwendung des § 1004 BGB – Beseitigungs- und Unterlassungsansprüche nach sich ziehen.[4] **5**

Erst später wurde dieses Recht auch vom **Bundesverfassungsgericht** (BVerfG) aus den Grundrechten hergeleitet.[5] Das zivil- und grundrechtliche Persönlichkeitsrecht ist weitgehend, aber nicht vollständig deckungsgleich[6]; der zivilrechtliche Schutz kann weiter reichen als der grundrechtliche und insbesondere auch das vermögenswerte Interesse der Persönlichkeit umfassen[7], da das Verfassungsrecht insoweit nur einen durch das einfache Recht und die Fachgerichtsbarkeit auszufüllenden Rechtsrahmen vorgibt. Tangiert ein Verhalten den Schutzbereich des grundrechtlichen Persönlichkeitsrechts, so ist jedoch im Regelfall auch das „sonstige Recht" i. S. d. § 823 Abs. 1 BGB beeinträchtigt. Die nachfolgenden Ausführungen konzentrieren sich deshalb auf die Grundrechtsposition. **6**

6.2.2 Mittelbare Drittwirkung des allgemeinen Persönlichkeitsrechts

Historisch betrachtet, wurden die Grundrechte als Abwehrrechte des Bürgers gegen den Staat konzipiert.[8] Eine **unmittelbare (Dritt-)Wirkung** dieser Grundrechte **7**

---

[4] Hierzu ferner Spindler, Kap. 5, Rn. 5.

[5] Vgl. BGHZ 13, 334 (338) – Leserbrief; BVerfGE 27, 1 (6 f.) – Mikrozensus; BVerfGE 54, 148 (153) – Eppler (dort auch erstmalig als allgemeines Persönlichkeitsrecht bezeichnet).

[6] Näher hierzu Jarass, NJW 1989, 857 (858).

[7] Vgl. BGH, NJW 2000, 2195 ff. – Marlene Dietrich. Demgegenüber vertritt das BVerfG die Auffassung, dass der verfassungsrechtliche Privatsphärenschutz aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht im Interesse einer Kommerzialisierung der eigenen Person gewährleistet ist (BVerfGE 101, 361 [385] – Caroline von Monaco I).

[8] Vgl. BVerfGE 7, 198 (204) – Lüth; 50, 290 (337) – Mitbestimmung; Dreier, in: Dreier, GG, Vorb. Art. 1 Rn. 84.

zwischen Privaten wird von der herrschenden Grundrechtsdogmatik demgegenüber abgelehnt. Hiergegen spricht nicht nur die Historie, der Wortlaut und die Systematik der Verfassung (vgl. Art. 1 Abs. 3 GG) sowie anderer Grundrechtskodifikationen (vgl. Art. 1 EMRK und Art. 51 Abs. 1 EU-GRC), sondern auch das Telos der Grundrechte: eine Interpretation als unmittelbar zwischen Privaten geltendes Recht veränderte ihren Charakter als Grund*recht* zu einer (dem anderen Privaten gegenüber obliegenden) Grund*pflicht*.[9]

8 Hieraus folgt indessen nicht, dass die Grundrechte – unter Einschluss des allgemeinen Persönlichkeitsrechts – keinen Einfluss auf Privatrechtsverhältnisse entfalteten. In seiner Lüth-Entscheidung[10] entwickelte das BVerfG vielmehr den bahnbrechenden Gedanken, dass Grundrechte verfassungsrechtliche Wertentscheidungen verkörpern, die in die Gesamtrechtsordnung ausstrahlen und insbesondere bei der Interpretation des einfachen Rechts zu berücksichtigen sind. Dieser gemeinhin als **„mittelbare Drittwirkung“** bezeichnete Mechanismus wurzelt letztlich in der Schutzfunktion der Grundrechte, aus der die Verpflichtung des Staates resultiert, die in den Grundrechten verkörperten Rechtsgüter und zum Ausdruck kommenden Wertentscheidungen gegen Übergriffe anderer Privater zu schützen.[11] Dieser Wirkmechanismus der Grundrechte ist nicht nur für den nationalen Rechtsraum anerkannt, sondern wurde auch von der internationalen Gerichtsbarkeit rezipiert.[12] Insbesondere erfordert dies, dass der Gesetzgeber rechtliche Regelungen zur Verfügung stellt, die es dem Betroffenen ermöglichen, sich gegen Persönlichkeitsrechtsverletzungen gerichtlich zur Wehr zu setzen.[13] Infolge des Umstands, dass das allgemeine Persönlichkeitsrecht als „sonstiges Recht“ i. S. d. § 823 Abs. 1 BGB anerkannt ist, kommt dem in weiten Teilen deckungsgleichen grundrechtlichen Persönlichkeitsrecht über den Hebel des Zivilrechts damit letztlich doch so etwas wie eine unmittelbare Drittwirkung zu.

6.2.3 Personaler Schutzbereich des allgemeinen Persönlichkeitsrechts

6.2.3.1 Natürliche und juristische Personen

9 Da sich onlinebasierte Sachverhalte nicht im rechtsfreien Raum ereignen, finden in dieser „virtuellen Welt“ die gleichen Rechtsgrundlagen und -prinzipien Anwendung

---

[9] Götting, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 3 Rn. 2; Jaeckel, Schutzpflichten, S. 40 ff.

[10] BVerfGE 7, 198 (204 ff.).

[11] Herdegen, in: Maunz/Dürig, GG, Art. 1 Abs. 3 Rn. 64 f.

[12] Vgl. zuletzt etwa EGMR, Beschluss v. 12.6.2014, Az. 40454/07, Rn. 45 m.w.N. Der EGMR spricht insoweit von „positive obligations“ der Mitgliedstaaten, die er von ihren (rein abwehrrechtlichen) „negative obligations“ abgrenzt. Allg. zur Schutzpflichtendogmatik nach dem Europa- und Unionsrecht Jaeckel, Schutzpflichten, S. 133 ff. m.w.N.

[13] Meyer-Ladewig, in: EMRK, Art. 8 Rn. 2 ff.

wie in der „analogen“. Von daher genießen **natürliche Personen** auch in Social-Media-Kontexten den Schutz des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, und zwar unabhängig von ihrer Staatsangehörigkeit. Ferner kann dem postmortalen Persönlichkeitsrecht, welches das BVerfG (ausschließlich) aus Art. 1 Abs. 1 GG herleitet[14], eine – wenn auch mit der Zeit verblassende – grundrechtliche Relevanz für den Schutz von Verstorbenen zukommen. Zu denken ist hier etwa an Plattformen wie Facebook, auf denen verstorbene Personen „virtuell weiter existieren“.[15]

10 Seit jeher umstritten hingegen ist die Frage, ob das allgemeine Persönlichkeitsrecht auch auf **juristische Personen** erstreckt werden kann, soweit es um Eigenschaften oder Beziehungen – etwa den Schutz des Achtungsanspruchs eines Wirtschaftsunternehmens – geht, die nicht nur natürlichen Personen wesenseigen sind.[16] Der Bundesgerichtshof (BGH) stützt den grundrechtlichen Schutz insoweit nicht auf Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, sondern auf Art. 12 Abs. 1 i. V. m. Art. 19 Abs. 3 GG oder – so namentlich in seinen frühen Entscheidungen[17] – lediglich auf Art. 2 Abs. 1 GG ohne Rekurs auf die Menschenwürdegarantie. Die Zivilgerichte sprechen in diesem Zusammenhang bisweilen auch von einem Persönlichkeitsrecht des Unternehmens, welches aber nicht umfassend ausgestaltet, sondern auf einzelne Aspekte wie den Schutz des guten Rufs oder das Recht am eigenen Namen konzentriert wird, woraus eine nur „beschränkte Wirkungskraft“ dieses Rechts resultiert.[18] Mitunter rekurriert die Rechtsprechung hier auch allein auf das zivilrechtliche Persönlichkeitsrecht, d. h. auf ein Recht i. S. d. § 823 Abs. 1 BGB. In einer neueren Entscheidung zur Verunglimpfung eines Unternehmens durch eine Umweltschutzorganisation hat der BGH die schutzwürdigen unternehmerischen Belange schließlich auf Art. 2 Abs. 1 und Art. 12 Abs. 1 GG gestützt.[19]

11 Eine Gegenauffassung verankert das **„Unternehmenspersönlichkeitsrecht“** wie bei natürlichen Personen in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[20] Dieser Ansatz begegnet allerdings Bedenken, da die Würdegarantie, welche vom BVerfG zur Schutzbereichsverstärkung des allgemeinen Persönlichkeitsrechts herangezogen wird, unstreitig nur auf natürliche Personen Anwendung findet. Jedenfalls die Verbindungskonstruktion mit Art. 1 Abs. 1 GG vermag deshalb nicht zu überzeugen.

---

[14] Locus classicus: BVerfGE 30, 173 (194) – Mephisto. Aus jüngerer Zeit vgl. BVerfG-K, NJW 2001, 594 – Willy-Brandt-Gedenkmünze; NJW 2001, 2957 (2958 f.) – Wilhelm Kaisen.
[15] Vgl. Martini, JZ 2012, 1145 ff.
[16] Vgl. Ziegelmayer, GRUR **?** , 761 ff.
[17] Vgl. insbesondere BGH, NJW 1975, 1882 ff.
[18] Vgl. BGHZ 78 (274 ff.); 91, 117 ff.; 98, 94 (97 f.).
[19] BGH, NJW 2008, 2110 (2112).
[20] Vgl. OLG Hamburg, NJOZ 2007, 2696 (2699). Ebenso Wronka, Persönlichkeitsrecht, S. 99 ff.

Doch auch ein allein aus Art. 2 Abs. 1 GG hergeleitetes allgemeines Persönlichkeitsrecht des Unternehmens[21] stößt in der zivil-[22] wie verfassungsrechtlichen[23] Literatur mehrheitlich auf Ablehnung. Folgt man dieser Auffassung, wird eher die Berufsfreiheit als Schutzinstrument gegen Beeinträchtigungen der unternehmerischen Sphäre ins Feld zu führen sein.[24] Dessen ungeachtet kann festgehalten werden, dass alle Ansätze einen vergleichbar starken Schutz des Unternehmenspersönlichkeitsrechts zur Folge haben.

6.2.3.2 Grundrechtsmündigkeit

12 Da soziale Medien besonders intensiv von Jugendlichen und damit **minderjährigen Personen** (vgl. § 2 BGB) genutzt werden, stellt sich die Frage, inwiefern diese durch das allgemeine Persönlichkeitsrecht geschützt sind. Diese Frage wird unter dem Topos der Grundrechtsmündigkeit diskutiert. Dem Begriff werden dabei zwei Bedeutungen zugeschrieben: Zum Teil wird mit ihm die Frage adressiert, ob jemand fähig ist, Grundrechtsträger zu sein. Allerdings wird er auch verwendet, um festzustellen, ob einem Minderjährigen das Recht zusteht, seine Grundrechte selbstständig auszuüben und prozessual durchzusetzen.[25] Da davon auszugehen ist, dass (jedenfalls) geborene Personen des uneingeschränkten Schutzes der Grundrechte (unter Einschluss des allgemeinen Persönlichkeitsrechts) teilhaftig sind, ist der Begriff der Grundrechtsmündigkeit vorliegend ausschließlich im letztgenannten Sinne zu verstehen. Inwiefern ein Minderjähriger zur eigenverantwortlichen Ausübung und prozessualen Wahrnehmung des allgemeinen Persönlichkeitsrechts in der Lage ist, bedarf jedoch einer am Einzelfall orientierten Betrachtung. Gegebenenfalls muss er dieses Recht mithilfe seiner gesetzlichen Vertreter geltend machen.[26]

6.2.3.3 Virtuelle Persönlichkeiten

13 Unter virtuellen Persönlichkeiten – auch als **Avatare** bezeichnet – sind Figuren zu verstehen, die Menschen oder menschenähnlichen (Fabel-)Wesen nachempfunden sind. Mangels der Eigenschaft, eine natürliche Person zu sein, besteht für derartige Avatare kein grundrechtlicher Persönlichkeitsschutz, wohl aber für den Menschen,

---

[21] Dafür aus verfassungsrechtlicher Sicht z. B. Beyerbach, Unternehmensinformation, S. 137 ff.
[22] Vgl. z. B. Rixecker, in: MüKo-BGB, § 12 Rn. 22 ff.; Kau, Persönlichkeitsschutz, S. 25 ff. A.A. allerdings Brändel, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 3; Kraft, in: Forkel/Kraft, FS Hubmann, S. 201 (215 ff.).
[23] Glück, Recht auf informationelle Selbstbestimmung, S. 95 f.; Kloepfer/Schärdel, JZ 2009, 453 (457); Schmitt Glaeser, in: Isensee/Kirchhof, HStR VI, § 129 Rn. 88.
[24] So offenbar auch Kunig, Jura 1993, 595 (599).
[25] Vgl. Rüfner, in: Isensee/Kirchhof, HStR IX, § 196 Rn. 9.
[26] Kunig, in: v. Münch/Kunig, GG, Art. 2 Rn. 39.

den sie repräsentieren oder möglicherweise ähnlich sind.[27] Mangels persönlichkeitsrechtlichen Schutzes sind diese Figuren deshalb nicht beleidigungsfähig, wohl aber die Spieler, die hinter ihnen stehen.[28] Ab einer gewissen Schöpfungshöhe (vgl. § 2 UrhG) können derartige virtuelle Persönlichkeiten im Übrigen urheberrechtlichen Schutz genießen.[29]

6.2.4 Sachlicher Schutzbereich des allgemeinen Persönlichkeitsrechts

6.2.4.1 Vorbemerkungen

Das allgemeine Persönlichkeitsrecht ist nicht ausdrücklich in der Verfassung verankert, sondern wird vom BVerfG aus einer Kombination des Art. 2 Abs. 1 mit Art. 1 Abs. 1 GG hergeleitet und dementsprechend als **„unbenanntes Grundrecht"** qualifiziert. Seine Aufgabe ist es, „die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die konkreten Freiheitsgarantien nicht abschließend erfassen lassen".[30] **14**

Zur besseren Handhabung dieses unbestimmten und entwicklungsoffenen Grundrechts hat das BVerfG **spezielle Ausprägungen** des allgemeinen Persönlichkeitsrechts anerkannt bzw. im Laufe seiner Rechtsprechung entfaltet.[31] Diese lassen sich ihrerseits auf einer übergeordneten Ebene in Rechte der Selbstbestimmung, Rechte der Selbstbewahrung und Rechte der Selbstdarstellung kategorisieren.[32] Als geschützte Ausprägungen sind vorliegend von Relevanz: **15**

6.2.4.2 Schutz der Privat-, Geheim- und Intimsphäre

Die engere persönliche Lebenssphäre des Einzelnen ist insbesondere durch seine Privat-, Geheim- und Intimsphäre gekennzeichnet. Dies eröffnet ihm einen unverzichtbaren **Raum autonomer Selbstentfaltung** nach innen.[33] In thematischer Hinsicht handelt es sich hierbei um Angelegenheiten, die vom Grundrechtsträger einer öffentlichen Erörterung oder Zurschaustellung entzogen zu werden pflegen. In räumlicher Hinsicht gehört zur Privatsphäre ein Rückzugsbereich des Einzelnen, der ihm insbesondere im häuslichen, aber auch außerhäuslichen Bereich die Möglichkeit **16**

---

[27] Vgl. insoweit auch BVerfGE 87, 209 (225) – Tanz der Teufel, wonach der Begriff „Mensch" nicht auf menschenähnliche Wesen erstreckt werden kann.
[28] Vgl. Klickermann, MMR 2007, 766 (768).
[29] Vgl. erneut Klickermann, MMR 2007, 766 (768).
[30] BVerfGE 34, 269 (281) – Soraya; 54, 148 (153) – Eppler.
[31] Vgl. BVerfGE 54, 148 (153 f.); Murswiek, in: Sachs, GG, Art. 2 Rn. 68 ff. Für das Zivilrecht vgl. insofern BGH, NJW 2000, 2195 ff.
[32] So Pieroth et al., Grundrechte, Rn. 391 ff.
[33] Vgl. Dreier, in: Dreier, GG, Art. 2 I Rn. 70.

des Zu-Sich-Selbst-Kommens und der Entspannung sichert.[34] Nach ständiger verfassungsgerichtlicher Rechtsprechung gewährt das allgemeine Persönlichkeitsrecht dem Einzelnen darüber hinaus einen **Kernbereich höchstpersönlicher, privater Lebensgestaltung**, einen unantastbaren Bereich zur Entfaltung seiner Persönlichkeit, der wegen seiner besonderen Nähe zur Menschenwürde absolut geschützt und einer Einschränkung durch Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes nicht zugänglich ist. Zu diesem Kernbereich gehört insbesondere die Intimsphäre, d. h. Ausdrucksformen der Sexualität und sexuellen Identität.[35] Anhand des Einzelfalls ist zu beurteilen, ob ein Sachverhalt zu diesem absolut geschützten Kernbereich gehört. Maßgebliche Kriterien können dabei sein, ob der Betroffene diesen Bereich geheim halten will[36] oder ob er nach seinem Inhalt höchstpersönlichen Charakters ist[37] und in welcher Art bzw. Intensität er die Sphäre anderer oder die Belange der Gemeinschaft berührt.[38]

6.2.4.3 Schutz der persönlichen Ehre

17 Das allgemeine Persönlichkeitsrecht schützt des Weiteren die persönliche Ehre.[39] Hierunter ist das Erscheinungsbild einer Person in der sozialen Gemeinschaft zu verstehen. Der grundrechtliche Schutz soll sicherstellen, dass dieses Erscheinungsbild nicht negativ dargestellt wird. Von daher werden insbesondere der **soziale Geltungs- und Achtungsanspruch** des Einzelnen sowie seine soziale Identität gegen unwahre Tatsachenbehauptungen geschützt.[40] Einfachgesetzlich wird der Ehrenschutz u. a. durch die §§ 185 ff. StGB konkretisiert und sichergestellt.[41]

6.2.4.4 Recht am eigenen Bild

18 Speziell in den Medien unter Einschluss sozialer Netzwerke kommt dem Recht am eigenen Bild eine besondere Bedeutung zu. Es räumt dem Betroffenen Einfluss- und Entscheidungsmöglichkeiten über das Anfertigen und die Verwendung von (Bewegt-) Bildern, auf denen er abgebildet ist, ein.[42] Einfachgesetzlich wird dieses Recht durch die **§§ 22 ff. KUG** ausgestaltet und geschützt.

---

[34] BVerfGE 101, 361 (382) – Caroline von Monaco I; BVerfGE 120, 180 (199) – Caroline von Monaco II.
[35] BVerfGE 109, 279 (313) – großer Lauschangriff; 119, 1 (29 f.) – Esra.
[36] BVerfGE 80, 367 (373) – Tagebuch.
[37] BVerfGE 109, 279 (313) – großer Lauschangriff.
[38] BVerfGE 34, 238 (246); BGH, NJW 2012, 767 (767).
[39] Vgl. BVerfGE 54, 148 (154) – Eppler; BVerfGE 99, 185 (193) – Scientology; BVerfGE 114, 339 (346) – Stolpe. Allg. dazu Glaser, NVwZ 2012, 1432 ff.
[40] Murswiek, in: Sachs, GG, Art. 2 Rn. 74.
[41] Ausführlich dazu Esser, Kap. 7, Rn. 38 ff.
[42] BVerfGE 101, 361 (381) – Caroline von Monaco I.

6.2.4.5 Recht am eigenen Wort

Das allgemeine Persönlichkeitsrecht schützt des Weiteren das Recht am nicht öffentlich gesprochenen oder geschriebenen Wort. Aus diesem Recht folgt insbesondere das **Verbot der unbefugten Aufzeichnung** und Publikation solcher Äußerungen. Verstöße hiergegen haben strafrechtliche Relevanz (vgl. § 201 StGB).[43] **19**

Zudem schützt dieses **Recht gegen Entstellungen oder Unterschiebungen** von Äußerungen (Falschzitate).[44] Eine Beeinträchtigung kann auch dadurch erfolgen, dass dem Einzelnen Äußerungen zugeschrieben werden, die er so nicht gemacht hat oder die er so nicht verstanden wissen will.[45] Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG schützt deshalb nicht nur gegen behauptete Äußerungen, sondern auch gegen unrichtige, verfälschte, entstellte Wiedergaben oder den Eindruck, dass keine andere Interpretation einer Äußerung möglich sei.[46] Dieser Schutzfunktion kann sogar absolute Wirkung zukommen, da die Kommunikationsgrundrechte (Art. 5 Abs. 1 GG) prinzipiell keinen Schutz für unrichtige, untergeschobene oder verfälschte Äußerungen gewähren.[47] **20**

6.2.4.6 Recht am eigenen Namen

Des Weiteren umfasst Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG das Recht am eigenen Namen. Denn der Name eines Menschen ist Ausdruck seiner Identität sowie Individualität und begleitet die Lebensgeschichte seines Trägers, die unter dem Namen als zusammenhängende erkennbar wird.[48] Einfachgesetzlich erfährt dieses Namensrecht eine Konkretisierung durch **§ 12 BGB**. **21**

6.2.4.7 Recht auf informationelle Selbstbestimmung

Unter den modernen Bedingungen der **Datenverarbeitung** setzt laut BVerfG die freie Entfaltung der Persönlichkeit den Schutz des Einzelnen gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz – dem gerade im Hinblick auf Social Media eine kaum zu unterschätzende Bedeutung zukommt – ist daher ebenfalls vom Schutzbereich des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[49] **22**

---

[43] Ausführlich hierzu Esser, Kap. 7, Rn. 121 ff.
[44] Vgl. BVerfGE 34, 269 (282) – Soraya; BVerfGE 54, 148 (155) – Eppler; BVerfGE 82, 236 (269) – Schubart; Di Fabio, in: Maunz/Dürig, GG, Art. 2 Abs. 1 Rn. 199.
[45] Vgl. BGH, NJW 2011, 3516 (3516) – Das Prinzip Arche Noah.
[46] Diederichsen, AfP 2012, 217 (217 f.).
[47] Vgl. BVerfGE 54, 208 (217 f.) – Böll; BVerfGE 82, 236 (269) – Schubart.
[48] Vgl. BVerfGE 84, 9 (22); 97, 391 (399); 109, 256 (266).
[49] Locus classicus: BVerfGE 65, 1 (42) – Volkszählung.

23 Das BVerfG hat dieses Recht zuletzt um die Gewährleistung der **Vertraulichkeit und Integrität informationstechnischer Systeme** erweitert[50], wobei die Notwendigkeit für eine solche spezielle Verbürgung jedoch im Unklaren bleibt. Beide Ausprägungen des allgemeinen Persönlichkeitsrechts berühren die Thematik des Datenschutzes in sozialen Netzwerken. Dieser ist in Kap. 4 ein eigenständiger Beitrag gewidmet.

6.2.5 Europarechtliche Einflüsse

24 Der Schutz des allgemeinen Persönlichkeitsrechts in medialen Kontexten wird seit geraumer Zeit stark durch das Europarecht beeinflusst. Zu nennen ist hier **Art. 8 Abs. 1 EMRK**, der das Privat- und Familienleben des Einzelnen schützt.[51] Der Begriff des Privatlebens ist nach Auffassung des EGMR weit (i. S. v. umfassend) zu verstehen und soll – ähnlich wie Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – einer abschließenden Definition deshalb nicht zugänglich sein. Ihm unterfalle die körperliche und geistige Integrität einer Person, Aspekte ihrer körperlichen und sozialen Identität, ihr Name, ihre geschlechtliche Identität und sexuelle Ausrichtung sowie ihr Sexualleben als solches. Die Vorschrift schützt nach ständiger Rechtsprechung des Gerichtshofs ferner das Recht auf Entwicklung der Persönlichkeit sowie das Recht, Beziehungen zu anderen Personen und zur Außenwelt herzustellen bzw. zu entwickeln.[52] Art. 8 Abs. 1 EMRK schützt deshalb u. a. das Recht am eigenen Bild und den guten Ruf.[53] Gerade die *Caroline*-Rechtsprechung des EGMR zum Recht am eigenen Bild hat die deutsche Rechtsprechung zum Persönlichkeitsschutz in den Medien nachhaltig verändert und der früheren Rechtsprechung deutscher Zivilgerichte zu den sog. „absoluten" und „relativen" Personen der Zeitgeschichte ein Ende bereitet.[54]

25 Für den unionsrechtlichen Bereich statuiert **Art. 7 EU-GRC** eine wortgleiche Verbürgung, welche neben Art. 8 EU-GRC (Schutz personenbezogener Daten) erst

---

[50] BVerfGE 120, 274 ff. – Online-Durchsuchung. Näher hierzu Roßnagel/Schnabel, NJW 2008, 3534 ff.; Hirsch, NJOZ 2008, 1907 ff.; Hoeren, MMR 2008, 365 ff.; Bartsch, CR 2008, 613 ff.; Peilert, in: Menzel/Müller-Terpitz, Verfassungsrechtsprechung, S. 851 ff.

[51] S. o. Rn. 4.

[52] EGMR, NJW 2004, 2505 (2507); NJW 2011, 3773, je m.w.N.

[53] Vgl. EGMR, NJW 2004, 2647 ff. – Caroline von Monaco I; EGMR, NJW 2012, 1053 ff. – Caroline von Monaco II; EGMR, Beschluss v. 12.6.2014, Az. 40454/07, Rn. 44.

[54] Vgl. insofern BGH, NJW 1996, 1128 ff. – Caroline von Monaco, im Wesentlichen bestätigt durch BVerfGE 101, 361 ff. – Caroline von Monaco I. Zusammenfassend zur alten BGH-, BVerfG- und EGMR-Rspr. etwa: Fiedler, in: Menzel/Müller-Terpitz, Verfassungsrechtsprechung, S. 658 ff.; Herrmann, in: Gersdorf/Paal, Informations- und Medienrecht, S. 799 ff.; Lederer, Bildberichterstattung, S. 19 ff., je m.w.N.

unlängst im Kontext datenschutzrechtlicher Löschungsansprüche gegen Suchmaschinenbetreiber eine bedeutsame Rolle gespielt hat.[55] Aufgrund der Kollisionsregelung in Art. 52 Abs. 3 EU-GRC hat der EuGH bei der Interpretation dieses Grundrechts der Judikatur des EGMR Rechnung zu tragen.

6.3 Persönlichkeitsrechtlich relevante Sachverhalte in Social Media

6.3.1 Verursacher von Beeinträchtigungen des Persönlichkeitsrechts

26 Beeinträchtigungen des Persönlichkeitsrechts in sozialen Netzwerken können durch unterschiedliche Akteure verursacht werden. In Betracht kommen hier zunächst die grundrechtlich unmittelbar gebundenen **staatlichen Institutionen**. Gegen solche Beeinträchtigungen stehen dem Betroffenen die üblichen öffentlich-rechtlichen Schutzmechanismen zur Verfügung, d. h. insbesondere die in den Grundrechten sowie im Rechtsstaatsprinzip wurzelnden Unterlassungs- und Folgenbeseitigungsansprüche.[56]

27 Rein quantitativ betrachtet, werden die meisten Persönlichkeitsrechtsbeeinträchtigungen indes durch **Private** verursacht. Hiergegen stehen dem Betroffenen vor allem zivilrechtliche Schutzansprüche, etwa in Gestalt eines Unterlassungsanspruchs (§ 1004 BGB analog i. V. m. § 823 Abs. 1 BGB) oder eines auf immateriellen Schadensersatz gerichteten deliktischen Anspruchs aus § 823 BGB, zur Verfügung.[57] Daneben stehen dem Betroffenen aber auch strafrechtliche Reaktionsmöglichkeiten, insbesondere in Gestalt einer Strafanzeige (vgl. z. B. § 194 StGB), zur Verfügung.[58]

28 Beeinträchtigungen erfolgen allerdings nicht nur durch die unmittelbar handelnden Akteure, die für ihre persönlichkeitsrelevanten Äußerungen über Dritte

---

[55] Vgl. EuGH, GRUR 2014, 895 ff. – Google.

[56] Zu diesen Anspruchsgrundlagen, ihren Voraussetzungen sowie ihrer prozessualen Geltendmachung vgl. statt Vieler Maurer, Verwaltungsrecht, § 30.

[57] Daneben sind – je nach Konstellation – auch Berichtigungsansprüche, deliktische Ansprüche auf Ersatz eines materiellen Schadens, Herausgabe- oder Gegendarstellungsansprüche denkbar. Näher zu diesen Ansprüchen und ihren Voraussetzungen: Fechner, Medienrecht, 4. Kap. Rn. 98 ff.; Söder, in: Gersdorf/Paal, Informations- und Medienrecht, S. 687 ff. S. ferner Spindler, Kap. 5, Rn. 5 und Beyerbach, Kap. 9, Rn. 75 f. Mangels Anspruchsgrundlage hat der von einer negativen Bewertung in einem Bewertungsportal Betroffene allerdings keinen Anspruch gegen den Portalbetreiber auf Erteilung einer Auskunft zu den Kontaktdaten des Verfassers der Bewertung; vgl. hierzu LG München I, Urt. v. 3.7.2013, Az. 25 O 23782/12, JurPC Web-Dok. 2/2014, abrufbar unter http://www.jurpc.de/jurpc/show?id=20140002 und nunmehr auch BGH, NJW 2014, 2651 ff.; Lauber-Rönsberg, MMR 2014, 10 ff. Die Unterlassungs- und Löschungsansprüche gegen den Host Provider bzw. strafrechtliche Ermittlungsbefugnisse bleiben davon allerdings unberührt.

[58] Allg. zu strafrechtlichen Fragen in Bezug auf Social Media Esser, Kap. 7.

nach Maßgabe der jeweils einschlägigen Haftungsgrundlagen stets voll verantwortlich sind.[59] Auch die **Transporteure** solcher Äußerungen, d. h. insbesondere die Betreiber von Social Media-Plattformen, tragen zu solchen Beeinträchtigungen zumindest mittelbar bei. Ihre Verantwortlichkeit ist spezialgesetzlich in den haftungsprivilegierenden Tatbeständen der §§ 8 bis 10 TMG geregelt.[60]

6.3.2 Fallgruppen von Beeinträchtigungen des Persönlichkeitsrechts

6.3.2.1 Äußerungen über andere Personen

29 Vor allem Äußerungen, welche in sozialen Netzwerken über andere Personen getätigt werden, können zu einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts führen. Staatlicherseits ist dies etwa der Fall, wenn die Polizei über den Stand eines Ermittlungsverfahrens auf einer Social-Media-Plattform berichtet oder über diesen Weg ein Diskussionsforum zu einer Straftat eröffnet, in dem die Nutzer konkrete Verdächtigungen gegen andere, namentlich benannte Personen aussprechen und diskutieren können.[61] Das Öffentlich-Machen des Umstands, dass ein Ermittlungsverfahren gegen einen bestimmten Beschuldigten eingeleitet wurde, stellt stets einen schweren Eingriff in dessen allgemeines Persönlichkeitsrecht dar. **Polizei und Staatsanwaltschaft** müssen insoweit die widerstreitenden Interessen des Beschuldigten einerseits sowie der Medien und Öffentlichkeit andererseits gegeneinander abwägen. Es ist insbesondere darauf zu achten, dass die aus Art. 6 Abs. 2 EMRK folgende Unschuldsvermutung zu jedem Zeitpunkt des Verfahrens gewährleistet bleibt. Zumeist betrifft dies nicht die Frage des „Ob", sondern des „Wie" der Veröffentlichung, vor allem unter dem Gesichtspunkt einer sog. identifizierenden Berichterstattung über den Beschuldigten. Oberste staatliche Handlungsmaxime ist insoweit Zurückhaltung bei der Preisgabe personenbezogener Daten.[62]

30 Zwischen **Privaten** können ehrenrührige Äußerungen in einem Blog Beeinträchtigungen des Persönlichkeitsrechts zur Folge haben, etwa wenn dort öffentlich Gerüchte oder Behauptungen verbreitet werden („F nutzt diese Visa-Karte im Wesentlichen zur Begleichung von Sex-Club Rechnungen").[63] Persönlichkeitsbeeinträchtigungen können sich zudem aus öffentlich zugänglichen Bonitätseinschätzungen über eine Person ergeben.[64] Das Gleiche gilt für Formulierungen von Hyperlinks.[65]

---

[59] Vgl. insoweit den in § 7 Abs. 1 TMG zum Ausdruck kommenden allgemeinen Rechtsgedanken.
[60] Für Einzelheiten hierzu s. Spindler, Kap. 5, Rn. 30 ff.
[61] So die Konstellation in OLG Celle, MMR 2008, 180 ff. Zur Nutzung sozialer Medien als polizeiliches Fahndungsinstrument s. ferner Esser, Kap. 7, Rn. 370 f.
[62] Allg. hierzu Glaser, NVwZ 2012, 1432 (1436); Gounalakis, NJW 2012, 1473 (1473).
[63] Vgl. BGH, MMR 2012, 124 m. Anm. Hoeren – www.blogspot.com; Diederichsen, AfP 2012, 217 (223); Ladeur/Gostomzyk, NJW 2012, 710 (714).
[64] Vgl. BGH, MMR 2011, 409 ff.; Diederichsen, AfP 2012, 217 (217).
[65] Vgl. Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 823 Rn. 17.

Auch **Beleidigungen und Schmähkritik** stellen nach ständiger Rechtsprechung der Zivilgerichte Beeinträchtigungen des allgemeinen Persönlichkeitsrechts dar. Dies gilt selbstverständlich auch für derartige Äußerungen in sozialen Netzwerken.[66] Beleidigungen i. S. d. § 185 StGB, d. h. Werturteile über den Betroffenen gegenüber Dritten, welche im geschützten Bereich eines sozialen Netzwerks (konkret: Facebook) gepostet werden, sind ebenfalls als persönlichkeitsrechtsrelevante Äußerungen anzusehen. Vom Beleidigungstatbestand ausgenommen sind lediglich vertrauliche Äußerungen im Familienbereich – eine Voraussetzung, die auf den geschützten Bereich von Facebook nicht zutrifft.[67] **31**

Persönlichkeitsbeeinträchtigende Äußerungen können sich zudem aus **Wikipedia-Beiträgen** ergeben, auch wenn sich diese Web 2.0-Plattform als eine zu Neutralität verpflichete Enzyklopädie versteht und sich dementsprechende Regeln zum Umgang mit Persönlichkeitsrechten gegeben hat: So sollen die Autoren persönliche Meinungsäußerungen unterlassen und Quellen nach objektiven und ausgewogenen Kriterien auswählen bzw. darstellen.[68] Von daher besteht die projektinterne Pflicht, alle Aussagen durch bereits veröffentlichte „Sekundärquellen" und nicht durch persönliches Wissen oder persönliche Erfahrung zu belegen.[69] Zusätzlicher Schutz wird durch das Administratorensystem sichergestellt. Ein absoluter Schutz durch zeitlich nicht beschränkte Bearbeitungssperren – etwa um Beiträge über zeitgenössische Personen zu verhindern – wird von Wikipedia demgegenüber abgelehnt, da dies gegen das Prinzip der freien Inhalte verstieße und eine Weiterentwicklung sowie Aktualisierung der Artikel verhinderte.[70] **32**

6.3.2.2 Einstellen von (Bewegt-)Bildern ohne Einwilligung

Werden **(Bewegt-)Bilder oder Bildnisse** einer Person auf Social-Media-Plattformen eingestellt, liegt eine öffentliche Zurschaustellung im Sinne des KUG vor; dies eröffnet den Anwendungsbereich dieses Gesetzes.[71] Ein Einstellen im vorbeschriebenen Sinne ist zu bejahen, wenn das Bildnis entweder auf einem Server des Verantwortlichen zum Abruf bereitgehalten wird oder im Rahmen eines Frames bzw. Inline Links als Inhalt einer anderen Webseite erscheint.[72] Das OLG München lässt für eine Veröffentlichung sogar die bloße Linksetzung auf eine Webseite und das dort enthaltene Bild genügen.[73] **33**

---

[66] Vgl. LG Berlin, ZUM 2012, 997 ff.
[67] Vgl. AG Bergisch Gladbach, BeckRS 2011, 24506. S. ferner AG Bad Segeberg, BeckRS 2013, 18801 sowie Esser, Kap. 7, Rn. 43 ff.
[68] Dilling, ZUM 2013, 380 (382).
[69] Dilling, ZUM 2013, 380 (382).
[70] Dilling, ZUM 2013, 380 (384).
[71] Zur Reichweite des für das KUG maßgeblichen Bildnis-Begriffs vgl. Engels, in: BeckOK Urheberrecht, § 22 KUG Rn. 20.
[72] Vgl. Feldmann, in: Heise Online-Recht, B. II C. II. 4. b).
[73] Vgl. OLG München, MMR 2007, 659.

34 Für die öffentliche Zurschaustellung im vorstehend skizzierten Sinne statuiert § 22 KUG den Grundsatz einer die Beeinträchtigung ausschließenden **Einwilligung**. Diese kann ausdrücklich oder konkludent erteilt werden. Bei Minderjährigen ist insoweit auf die Einsichtsfähigkeit abzustellen, welche sich auch an den Besonderheiten des jeweiligen sozialen Netzwerks zu orientieren hat. Hinzutreten muss die Einwilligung des gesetzlichen Vertreters.[74] Der Widerruf der Einwilligung ist grundsätzlich jederzeit möglich und kann auch explizit vorbehalten werden.[75] Auch eine Befristung der Einwilligung oder eine Beschränkung auf bestimmte Gegenstände ist zulässig.[76] Eine (ausdrückliche) Einwilligung wird u. a. bei Zahlung eines Entgelts an den Betroffenen vermutet. Sie gibt zugleich Aufschluss über den konkreten Verwendungszweck. Speziell für die Einwilligung in die Zurschaustellungen von Bildnissen auf Social Media-Plattformen gilt deshalb, dass sich der Betroffene mit seiner Einverständniserklärung zur öffentlichen Zugänglichmachung auf einer nicht zugriffsbeschränkten Website zugleich damit einverstanden erklärt, dass das Bildnis mit den Möglichkeiten des Internets wahrnehmbar gemacht wird, also über Suchmaschinen aufgefunden und im Rahmen sog. „thumbnails" (Vorschaubildern) von diesen wiedergegeben werden darf.[77]

35 Im Übrigen ist gemäß § 23 Abs. 1 KUG unter den dort genannten Voraussetzungen eine Verbreitung und Veröffentlichung des Bildnisses auch ohne Einwilligung möglich, sofern hierdurch keine „berechtigten Interessen" des Abgebildeten oder – im Todesfall – seiner Angehörigen verletzt werden (§ 23 Abs. 2 KUG).[78] Der insoweit bedeutsame Rechtfertigungstatbestand des **„Bildnisses aus dem Bereiche der Zeitgeschichte"** (§ 23 Abs. 1 Nr. 1 KUG) bedarf nach der neuen, auf den EGMR zurückzuführenden BGH-Rechtsprechung einer eingehenden und abwägenden Prüfung, welche das oberste Zivilgericht als „abgestuftes Schutzkonzept" umschreibt: Auf der **ersten Stufe** dieses Konzepts ist zu analysieren, ob es sich bei dem in Rede stehenden (Bewegt-)Bild um ein Bildnis aus dem Bereich der Zeitgeschichte i. S. d. § 23 Abs. 1 Nr. 1 KUG handelt. Der Begriff der Zeitgeschichte ist dabei weit zu verstehen und umfasst aufgrund des Informationsbedarfs der Öffentlichkeit nicht nur Vorgänge von historisch-politischer Bedeutung, sondern ganz allgemein das Zeitgeschehen, also alle Fragen von allgemein-gesellschaftlichem Interesse. Der Begriff „Zeitgeschichte" wird mithin vom Interesse der Öffentlichkeit in Wechselwirkung mit den Medien determiniert und kann sich auch auf unterhaltende Beiträge („Infotainment") beziehen.

36 Dieses Informationsinteresse besteht allerdings nicht schrankenlos. Vielmehr wird der Einbruch in die persönliche Sphäre des Abgebildeten durch den Grundsatz der Verhältnismäßigkeit begrenzt. Die Anwendung des § 23 Abs. 1 Nr. 1 KUG erfordert deshalb eine einzelfallbezogene Abwägung zwischen den Rechten der Abgebildeten nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. Art. 8 Abs. 1 EMRK einerseits und

---

[74] Näher dazu Ohly, AfP 2011, 428 (434); Piltz, Soziale Netzwerke, S. 253 ff. Für die vertragsrechtlichen Aspekte vgl. Bräutigam/von Sonnleithner, Kap. 4, Rn. 98 ff.

[75] S. erneut Ohly, AfP 2013, 428 (433 f.); Piltz, Soziale Netzwerke, S. 261 ff.

[76] Härting, CR 2009, 21 (26).

[77] Feldmann, in: Heise Online-Recht, B. II C II. 4. c).

[78] Ausführlich zu den §§ 22, 23 KUG im Kontext sozialer Netzwerke Piltz, Soziale Netzwerke, S. 192 ff.

den Rechten der Medien aus Art. 5 Abs. 1 GG bzw. Art. 10 Abs. 1 EMRK andererseits. Wegen der auch dienenden Funktion der Medienfreiheiten für den Prozess öffentlicher Meinungsbildung und für die Meinungsfreiheit der Bürger haben Äußerungen in den bzw. durch die Medien allerdings zunächst die (widerlegliche) Vermutung der Zulässigkeit für sich, auch wenn sie die Rechtssphäre anderer berühren. Für das Zurücktreten dieser Vermutung bleibt dann wenig Raum, wenn die Berichterstattung einen Beitrag zu **Fragen von allgemeinem Interesse** leistet. Als Abwägungskriterien stellt der BGH insbesondere auf folgenden Gesichtspunkt ab: Steht das Bildnis in einem Kontext, welcher der ernsthaften und sachbezogenen Erörterung einer Angelegenheit (auch soweit sie die „Normalität des Alltagslebens" von „Prominenten" betrifft) dient, oder steht die bloße Befriedigung der Leserneugier auf private Angelegenheiten im Vordergrund? Diese Gewichtung ist im Konfliktfall nicht den Medien vorbehalten, sondern obliegt den Gerichten. Laut BGH haben diese wegen des Zensurverbots aus Art. 5 Abs. 1 S. 3 GG allerdings von einer inhaltlichen Bewertung (etwa als wertvoll oder wertlos, seriös oder unseriös) abzusehen und sich auf die Prüfung zu beschränken, in welchem Ausmaß der Bericht einen **Beitrag für die öffentliche Meinungsbildung** zu erbringen imstande ist. Hinzu kommt, dass der Informationswert einer Bildberichterstattung – soweit das Bild nicht schon als solches eine für die öffentliche Meinungsbildung bedeutsame Aussage enthält – im Kontext der dazugehörenden Wortberichterstattung zu ermitteln ist; der begleitende Bericht darf sich dabei allerdings nicht darauf beschränken, lediglich einen Anlass für die Abbildung von Personen zu schaffen, ohne dass die Berichterstattung einen Beitrag zur öffentlichen Meinungsbildung erkennen lässt. Über „Personen des öffentlichen Interesses" („personnages publics/public figures"), also insbesondere Prominente, darf dabei in größerem Umfang berichtet werden als über „gewöhnliche" Personen („personnages ordinaires/ordinary persons"), sofern die Nachricht einen hinreichenden Informationswert mit Orientierungsfunktion im Hinblick auf eine die Allgemeinheit interessierende Sachdebatte aufweist und keine schwerwiegenden Interessen des Betroffenen entgegenstehen. In noch stärkerem Maße gilt dies für Personen des politischen Lebens („personnages politiques/politicians")[79], an denen in einem demokratischen Gemeinwesen generell ein überragendes Informationsinteresse besteht.[80]

Auf einer **zweiten Stufe** schließlich ist im Rahmen des § 23 Abs. 2 KUG zu prüfen, **37**
ob trotz Vorliegens der Voraussetzungen des § 23 Abs. 1 Nr. 1 KUG ein „berechtigtes Interesse" des Abgebildeten der Verbreitung und Zurschaustellung des Bildnisses entgegensteht. In diesem Kontext können etwa der Anlass und die Umstände berücksichtigen werden, unter denen eine Aufnahme entstanden ist. „Unerträgliche Bespitzelung" (Heimlichkeit) oder die Drangsalierung des Betroffenen (beharrliche Nachstellung) können hier ebenso zu einem Ausschluss der Veröffentlichung führen

[79] Vgl. zuletzt EGMR, Beschluss v. 12.6.2014, Az. 40454/07, Rn. 49 ff.

[80] Aus der kaum noch zu überschauenden Rspr. und Lit. vgl. BGH, NJW 2007, 1977 ff. – St. Moritz; BGH, NJW 2008, 3138 ff. – Sabine Christiansen auf Mallorca; BGH, NJW 2011, 746 ff. – Rosenball in Monaco. S. ferner BVerfGE 120, 180 ff. – Caroline von Hannover II; BVerfG-K, NJW 2012, 756 ff.; Frenz, NJW 2012, 1039 ff.; Herrmann, in: Gersdorf/Paal, Informations- und Medienrecht, S. 803 ff.

wie die Darstellung von Einzelheiten der Privatsphäre (örtliche Abgeschiedenheit; „Momente der Entspannung oder des Sich-Gehen-Lassens außerhalb der Einbindung in die Pflichten des Berufs und des Alltags“) oder die Darstellung des Umgangs mit Kindern. Im Unterschied zu § 23 Abs. 1 Nr. 1 KUG obliegt die Beweislast für das Vorliegen dieser tatbestandlichen Voraussetzungen allerdings dem Betroffenen.[81]

38 Die Beeinträchtigung des Persönlichkeitsrechts durch Bilder wiegt nach Auffassung der Rechtsprechung im Übrigen meist schwerer als eine reine **Wortberichterstattung**. Entsprechend werden an die Veröffentlichung von Bildern zumeist strengere Anforderungen geknüpft als an die Publikation eines Texts: „Während die Veröffentlichung eines Bildes von einer Person grundsätzlich eine rechtfertigungsbedürftige Beschränkung ihres allgemeinen Persönlichkeitsrechts begründet, die unabhängig davon ist, ob die Person in privaten oder öffentlichen Zusammenhängen und in vorteilhafter oder unvorteilhafter Weise abgebildet ist, ist dies bei personenbezogenen Wortberichten nicht ohne Weiteres der Fall. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bietet hier nicht schon davor Schutz, überhaupt in einem Bericht individualisierend benannt zu werden, sondern nur in spezifischen Hinsichten“, also etwa in Bezug auf den Schutz rein privater oder intimer Belange des Betroffenen.[82]

6.3.2.3 Einstellen von (Bewegt-)Bildern durch den Abgebildeten selbst

39 Werden (Bewegt-)Bilder vom Abgebildeten selbst auf Social-Media-Plattformen eingestellt, wirft dies die Frage auf, ob hierin eine Einwilligung in das Kopieren und Weiterverwenden solcher Bilder durch Dritte zu sehen ist.[83] Hier muss im **Einzelfall** geprüft werden, ob dies gewollt ist und wie weit eine Einwilligung möglicherweise reicht.[84] Im Zweifel ist von Folgendem auszugehen: Verweist jemand per Hyperlink von seiner Seite auf ein (Bewegt-)Bild, liegt hierin regelmäßig keine Beeinträchtigung des Rechts am eigenen Bild, da hinsichtlich solcher Verweise von einer konkludenten Einwilligung des Betroffenen ausgegangen werden kann. Anders ist dies bei der Übernahme des Bildnisses in eine fremde Website oder seine Verwendung (Verlinkung) in einem zweifelhaften Umfeld (z. B. Werbung für eine Pornoseite) zu beurteilen.[85] Wird dieses Bild in ein journalistisch-redaktionell gestaltetes Angebot übernommen, hat dies ebenfalls grundsätzlich keine Rechtsverletzung zur Folge; dies

---

[81] Eingehend zu § 23 Abs. 2 KUG Herrmann, in: Gersdorf/Paal, Informations- und Medienrecht, S. 806 ff. m.w.N.

[82] BVerfG, MMR 2012, 338 (339) – Ochsenknecht, unter Berufung auf BVerfG, ZUM-RD 2010, 657. So auch BGH, NJW 2011, 744 (745) – Rosenball. Vgl. ferner Feldmann, in: Heise Online-Recht, B. II C. II. 4.; Härting/Schätzle, ITRB 2009, 39 (40).

[83] Vgl. hierzu Seitz, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 60 Rn. 76; Petershagen, NJW 2011, 705.

[84] Härting, CR 2009, 21 (26); Seitz, in: Götting et al., Handbuch des Persönlichkeitsrechts, § 60 Rn. 76.

[85] Libertus, ZUM 2007, 621 (622).

insbesondere dann nicht, wenn der Einstellende das Bild erkennbar für eine Weiterbenutzung durch Dritte online gestellt hat (etwa unter der Rubrik „Pressefoto“ oder in einem berufsbezogenen Kontext).

6.3.2.4 Identitätsmissbrauch und „Fake-Accounts“

Typische Erscheinungsformen des Identitätsmissbrauchs oder -diebstahls im Online-Bereich sind die Nutzung fremder Adress- oder fremder Kreditkartendaten, die Nutzung eines fremden E-Mail-Accounts oder das sog. **„Spoofing“**, d. h. der Verschleierung der eigenen Identität in einem Online-Netzwerk.[86] Ein „Fake-Account“ wird beispielsweise angelegt, um die eigene Identität zu verschleiern, andere Personen gezielt zu „mobben“ oder wirtschaftlich zu schädigen.[87] Durch diese Verhaltensweisen können das Namensrecht (§ 12 BGB) und, sofern in diesem Zusammenhang Bilder hochgeladen werden, das Recht am eigenen Bild beeinträchtigt sein. Werden beim Posten einem bestimmten Namensgeber Äußerung untergeschoben, liegt zudem eine Verletzung des Rechts am eigenen Wort vor.[88] **40**

6.3.2.5 Abgabe von Bewertungen über Bewertungsplattformen

Bewertungsplattformen ermöglichen öffentlich einsehbare Bewertungen von Personen, Produkten oder Dienstleistungen. Bekannte Beispiele hierfür sind die Webseiten **„spickmich.de“**[89] und **„meinprof.de“**.[90] Im Dienstleistungsbereich haben sich solche Plattformen vor allem in Gestalt medizinischer Portale wie etwa „jameda.de“ etabliert, die eine Bewertung der ärztlichen Dienstleistungsqualität ermöglichen.[91] **41**

Solche Portale können zu einer Beeinträchtigung des **allgemeinen Persönlichkeitsrechts** oder der **Berufsfreiheit** des Betroffenen führen, da sein Recht auf persönliche wie berufliche Selbstdarstellung durch negative Bewertungen empfindlich beeinträchtigt zu werden vermag. Verschärfend kommt in diesem Kontext hinzu, dass solche Bewertungen zumeist anonym abgegeben werden können. Sie sind deshalb auch kaum auf ihren Wahrheitsgehalt überprüfbar und erschweren es dem Bewerteten, direkt und überzeugend auf sie zu replizieren. **42**

---

[86] Vgl. Borges, in: Borges et al., Identitätsdiebstahl, S. 15.
[87] Vgl. Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 17 ff.
[88] Zu diesen Rechten vgl. o. Rn. 18 ff.
[89] Vgl. hierzu die Grundsatzentscheidung BGH, MMR 2009, 608 ff.
[90] Ausführlich zu diesen Plattformen Kamp, Personenbewertungsportale, S. 3 ff.; Weigl, Meinungsfreiheit, S. 180 ff.
[91] Allg. zum Thema medizinische Bewertungsprotale Lacher, Ärztliche Leistungen S. 117 ff.

6.3.2.6 Anprangerungen im Online-Bereich

43 Online-Anprangerungen erfolgen nicht selten über Plattformen der Social Media, da diese aufgrund ihrer Reichweite und ihrer kommunikativen Möglichkeiten für derartige Ausdrucksformen gut geeignet sind. So werden in den USA beispielsweise über das Internet einsehbare **Register über Sexualstraftäter** und deren Wohnorte publiziert.[92]

44 Online-Anprangerungen beeinträchtigen einerseits den sozialen Wert- und Achtungsanspruch des Betroffenen nach außen und sind deshalb **im hohen Maße persönlichkeitsrelevant**. Der öffentliche Druck, der von solchen Anprangerungen auszugehen vermag, kann zu einer erheblichen Verhaltensänderung beim Betroffenen führen, bis hin zum Wegzug aus einer bestimmten Region oder in – allerdings seltenen – Extremfällen, insbesondere bei psychisch labilen Personen, zum Suizid des Betroffenen. Aber auch Anprangerungen gegen kommerziell tätige Unternehmen vermögen diese zwecks Vermeidung von Imageverlusten zu einer Verhaltensänderung zu bewegen.[93] Andererseits können – dies zeigt gerade das letztgenannte Beispiel – durch solche Anprangerungen auch Missstände im öffentlichen oder privaten Bereich aufgedeckt werden.

45 Soziale Netzwerke eignen sich ferner zum **Anprangern einer unangemessenen Verhaltensweise**. Ein solches unangemessenes Verhalten kann beispielsweise darin bestehen, dass das „Stalking" (beharrliche Verfolgen) eines „Stalkers" durch die betroffene Person über eine Social-Media-Plattform publik gemacht wird[94] oder Videosequenzen über ein Fehlverhalten ins Internet gestellt werden.[95] Problemtisch an einer solchen Vorgehensweise kann jedoch sein, dass die Unschuldsvermutung zugunsten der Betroffenen ein Stück weit ausgehebelt wird. Denn im Internet werden Dinge oft ohne Nachweis behauptet, wodurch der Anschein entsteht, das unangemessene Verhalten des Betroffenen habe sich tatsächlich so ereignet.[96]

46 Eine weitere Art der Online-Anprangerung ist der sog. **„Shitstorm"**. Dieser zielt darauf ab, das Ansehen und die Ehre seines Opfers zu beschädigen. Entsprechend definiert ihn der Duden als einen „Sturm der Entrüstung in einem Kommunikationsmedium des Internets, der zum Teil mit beleidigenden Äußerungen einhergeht".[97] Adressat kann eine natürliche oder juristische Person sein. Nicht selten soll durch einen solchen „Shitstorm" der Betroffene zu einer Verhaltensänderung bewegt

---

[92] Vgl. hierzu die Webseite des US-Justizministeriums http://www.nsopw.gov/en.

[93] Vgl. insoweit Dörnhöfer, in: Bielefeldt, Nothing to hide, S. 114.

[94] So im Fall der Leichtathletin Ariane Friedrich, die den Namen und die Adresse eines Mannes, der ihr eine anzügliche E-Mail nebst Foto seines Genitals schickte, über Facebook publik machte. Vgl. hierzu Spiegel-Online v. 22.4.2012. Allg. zur Strafbarkeit des sog. „Cyber-Stalkers" Esser, Kap. 7, Rn. 167 ff.

[95] So im Fall des sog. „Dog Poop Girl", das die Hinterlassenschaften ihres Hundes nicht wegräumte und dabei gefilmt wurde. Nach Einstellung dieser Videosequenz sah sie sich Anfeindungen im Internet ausgesetzt.

[96] Vgl. Dörnhöfer, in: Bielefeldt, Nothing to hide, S. 115; Wienen, ITRB 2012, 160 (161).

[97] Abrufbar unter www.duden.de. S. ferner Voskamp/Kipker, DuD 2013, 787 (788 f.). Zu Fragen der Strafbarkeit vgl. Esser, Kap. 7, Rn. 42.

werden. Er kann zudem auf traditionelle Medien überschwappen und dort zum Gegenstand einer Berichtserstattung werden.[98]

„Cyber-Mobbing“, auch als „Cyber-Bullying“, „Cyber-Stakling“ oder „Internet-Mobbing“ bezeichnet, richtet sich gemeinhin gegen in der Öffentlichkeit unbekannte Personen.[99] Eine allgemein gültige Definition für diese Form des Mobbings existiert nicht. Zumindest herrscht aber Einigkeit über den Umstand, dass das Mobbing gekennzeichnet ist durch „negative kommunikative Handlungen (von einer oder mehreren Personen), die gegen eine (oder mehrere) Person(en) gerichtet sind und die sehr oft und über einen längeren Zeitraum hinweg vorkommen“.[100] Gerade im Rahmen von sozialen Netzwerken ist die Mobbing-Hemmschwelle aufgrund der Möglichkeit zu anonymem Handeln sowie aufgrund der Tatsache, dass man die Reaktion des Opfers nicht beobachten muss, also aus der Ferne operiert, stark heruntergesetzt. Allerdings sind viele „Cyber-Bullies“ auch im realen Leben Opfer derartiger Anfeindungen, viele Jugendliche zugleich Täter und Opfer. Ferner ist zu berücksichtigen, dass „traditionelles Mobbing“ viel weiter verbreitet ist als „Cyber-Bullying“. Verglichen mit herkömmlichen Formen des Mobbings spielen derartige Vorfälle entgegen ihrer öffentlichen Wahrnehmung und Diskussion (insbesondere in der Folge spektakulärer und zugleich tragischer Suizidfälle) von daher eine wohl eher untergeordnete Rolle.[101] 47

Dessen ungeachtet bestehen auch **Unterschiede des virtuellen zum realen Mobbing**. So hat der VGH Mannheim mit Recht festgestellt, dass Beleidigungen gegenüber Mitschülern im Internet ein besonderes Augenmerk geschuldet sei, da sie dort „von allen Nutzern [. . .] zur Kenntnis genommen werden“ könnten. Gerade der Einsatz des Internets, die damit verbundene unkontrollierbare Verbreitung und der Umstand, dass selbst nach Löschung Inhalte vielfach nicht mehr vollständig aus dem Netz zu entfernen sind („Das Netz vergisst nichts!“), begründe ein erhebliches und zu sanktionierendes Fehlverhalten.[102] „Cyber-Mobbing“ stellt folglich eine tiefgreifende Beeinträchtigung des allgemeinen Persönlichkeitsrechts des Betroffenen dar. 48

6.3.2.7 Beeinträchtigungen des postmortalen Persönlichkeitsschutzes

Der mit der Zeit verblassende postmortale Persönlichkeitsschutz ist insbesondere darauf gerichtet, den Verstorbenen vor unwahren Behauptungen, vor Herabsetzungen und Erniedrigungen sowie vor **groben Entstellungen** seines Lebensbilds 49

---

[98] Glaser, NVwZ 2012, 1432 (1432).
[99] Glaser, NVwZ 2012, 1432 (1432).
[100] Vgl. Duden, Das Fremdwörterbuch, Stichwort: „mobben/Das Mobbing“. Da Mobbing über einen längeren Zeitraum hinweg erfolgt, ist der Shitstorm als einmaliges, heftiges Ereignis tendenziell keine Form des Mobbings. Zum Begriff s. erneut Voskamp/Kipker, DuD 2013, 787 (788) sowie Esser, Kap. 7, Rn. 41.
[101] Vgl. Sticca et al., Journal of Community and Applied Social Psychology 2013, 52 ff.
[102] VGH Mannheim, NVwZ-RR 2011, 647.

und seiner Lebensleistung zu schützen. Wie das AG Berlin-Charlottenburg in der *Tron*-Entscheidung feststellt hat, verletzt die namentliche Nennung einer mit 26 Jahren verstorbenen Person auf einer Wikipedia-Seite diese allerdings nicht in ihrem postmortalen Persönlichkeitsrecht.[103]

6.3.2.8 Beeinträchtigungen durch Suchmaschinen

50 Suchmaschinen wie z. B. Google, Bing, Yahoo oder Ask lassen sich zwar nicht als Social-Media-Plattformen im eingangs (Rn. 1) skizzierten Sinne qualifizieren; sie sind im vorliegenden Kontext aber dennoch von Relevanz, da sie auf persönlichkeitsrelevante Beeinträchtigungen in sozialen Netzwerken hinführen. Dies wirft die Frage auf, inwiefern auch der Suchmaschinenbetreiber für solche Beeinträchtigungen zur Verantwortung gezogen werden kann. Die Rechtsprechung zu dieser Frage hat sich in jüngerer Zeit teils spektakulär entwickelt: So nimmt der BGH[104] mittlerweile an, dass die Ergebnisse der **Suchergänzungsfunktion** eigene Inhalte des Suchmaschinenbetreibers darstellen, für die der Betreiber gemäß § 7 Abs. 1 TMG voll verantwortlich ist. Denn der Nutzer – so der BGH – entnehme den Autocomplete-Vorschlägen einen hinreichend konkreten Aussagengehalt, der sich nicht lediglich in der Information erschöpfe, dass vorherige Nutzer den Begriff in Kombination mit anderen Begriffen gesucht hätten.[105] Vielmehr werde ein inhaltlicher Bezug zu dem vom Nutzer eingegebenen Suchbegriff erwartet. Dem Nutzer würden von den Suchmaschinen nicht irgendwelche Vorschläge unterbreitet, sondern möglichst inhaltlich weiterführende. Daher erwarte der suchende Nutzer, dass ihm die Vorschläge hilfreich sein könnten, weil die angebotenen Kombinationen inhaltlich Bezüge widerspiegelten.[106] Der Suchmaschinenbetreiber sei daher für solche Ergänzungsvorschläge verantwortlich und hafte für daraus resultierende Persönlichkeitsverletzungen[107], wenn er es nach Hinweis des Betroffenen unterlasse, künftige Verletzungen zu verhindern.[108]

51 Ähnlich gelagert war der Fall des KG Berlin.[109] Dieser betraf **„Snippets“** (Schnipsel)[110], durch welche der – unzutreffende – Eindruck vermittelt wurde, dass im Internet Nacktaufnahmen einer bestimmten Person existierten. Das Gericht sah hierin eine Persönlichkeitsrechtsverletzung. Dahinter steht die zutreffende Annahme,

---

[103] Vgl. AG Berlin-Charlottenburg, Beschluss v. 9.2.2006, Az. 218 C 1001/06, abrufbar über juris. Zum Themenkomplex s. ferner Martini, JZ 2012, 1145 ff.

[104] BGH, NJW 2013, 2348 (2348 Rn. 12).

[105] BGH, NJW 2013, 2348 (2349).

[106] BGH, NJW 2013, 2348 (2349).

[107] Bspw. die Verbindung des Namens der Ehefrau eines ehemaligen Spitzenpolitikers mit den Themen Prostitution und Escort.

[108] BGH, NJW 2013, 2348 (2350). Dazu auch Bamberger, in: BeckOK-BGB, § 12 Rn. 139b; Hager, in: Staudinger, BGB, Eckpfeiler des Zivilrechts, T. § 3, VI., Rn. 329. Zu Fragen der Verantwortlichkeit von Suchmaschinenbetreibern s. ferner Spindler, Kap. 5, Rn. 26.

[109] KG Berlin, MMR 2006, 817 (817).

[110] = kurzer Textauszug aus einer Webseite, der auf der Ergebnisseite einer Suchmaschine angezeigt wird.

dass durch die „Schnipsel-Technik“ ein eigener Aussagegehalt generiert zu werden vermag.[111] Von daher kann die Zusammenfassung bzw. Verkürzung der verlinkten Seite den Rahmen der Kernaussage der Ursprungsseite sprengen. Wenn die verkürzt zusammenfassende Darstellung im Snippet derart sinnentstellend ist, dass ihr ein eigener Unrechtsgehalt zukomme, könne dies eine Persönlichkeitsrechtsverletzung begründen. Anders hatten dies allerdings das OLG Hamburg[112] und das OLG Stuttgart[113] bewertet.

Einen anderen Sachverhalt hatte das LG Mönchengladbach zu entscheiden[114]: **52**
Dort ging es um den Fall, dass bei Eingabe des Klägernamens unter den Suchergebnissen ein **Link** zu einem Blogeintrag erschien, durch den der Kläger in seinem Persönlichkeitsrecht verletzt wurde. Weder im Hyperlink noch in den „Snippets“ oder in der Suchergänzungsfunktion, also irgendwo auf der Seite des Suchmaschinenbetreibers, fand sich indes ein Hinweis auf die Persönlichkeitsverletzung auf der anderen Webseite. Das LG hielt die Klage gegen den Suchmaschinenbetreiber dementsprechend für unbegründet, da sich die Suchmaschine auf das reine Bereitstellen von Suchergebnissen beschränke. Sie verbreite keine Äußerungen, sondern liste nur auf.[115] Selbst wenn man das anders sähe, seien nur widerrechtliche Äußerungen untersagt. Hier müsse aber abgewogen werden. Der Nutzer der Suchmaschine verlasse sich darauf, dass die Ergebnisse seiner Suche „neutral“, also nicht redaktionell bearbeitet wurden. Würde man dies ändern, sähe sich die Suchmaschine dem Vorwurf der Zensur ausgesetzt.[116] Zudem wäre beim Vorgehen gegen nur eine Suchmaschine die verletzende Äußerung im Internet immer noch vorhanden und auch noch über andere Suchmaschinen bzw. direkt durch Eingabe der URL auffindbar.[117]

Diese Sichtweise dürfte durch eine aktuelle Entscheidung des **EuGH** allerdings **53**
nunmehr überholt sein: Auf Vorlage eines spanischen Gerichts hatte der EuGH eine vergleichbare Konstellation am Maßstab der Datenschutzrichtlinie[118] zu prüfen. Insoweit erklärte er den Suchmaschinenbetreiber – konkret: Google – zunächst zu einer verantwortlichen datenverarbeitenden Stelle i. S. dieser Richtlinie.[119] Sodann hielt er den territorialen Anwendungsbereich der Richtlinie für eröffnet, obschon die eigentliche Datenverarbeitung auf Servern in den USA erfolgt.[120] Auch verneinte er die Notwendigkeit, dass sich der Betroffene zunächst an die unmittelbar datenverarbeitende Stelle wenden müsse.[121] Auf die Frage, ob der Inhalt, auf den verlinkt wird, rechtmäßig oder unrechtmäßig im Netz steht, soll es nach Auffassung des

---

[111] KG Berlin, MMR 2010, 495 (496).
[112] OLG Hamburg, MMR 2010, 490 (492).
[113] OLG Stuttgart, CR 2009, 187 (187 f.).
[114] LG Mönchengladbach, ZUM-RD 2014, 46 ff.
[115] LG Mönchengladbach, ZUM-RD 2014, 46 (48).
[116] LG Mönchengladbach, ZUM-RD 2014, 46 (48).
[117] LG Mönchengladbach, ZUM-RD 2014, 46 (48 f.).
[118] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Abl. EG Nr. L 281/31.
[119] EuGH, GRUR 2014, 895 (897) – Google.
[120] EuGH, GRUR 2014, 895 (898) – Google.
[121] EuGH, GRUR 2014, 895 (901) – Google.

EuGH ebenfalls nicht ankommen.[122] Vielmehr müsse der Suchmaschinenbetreiber nunmehr eine Abwägungsentscheidung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse der Öffentlichkeit vornehmen[123], an deren Ende zugunsten des durch den Link Betroffenen ein **„Recht auf Vergessenwerden"** stehen kann. Die zunächst euphorisch begrüßte Entscheidung erweist sich bei näherer Betrachtung als problematisch: Möglicherweise stärkt sie über Gebühr das Privatheitsinteresse der Betroffenen und schädigt damit zugleich den für eine offene Gesellschaft essentiellen „free flow of information". Als weltweit operierende Anbieter werden Suchmaschinenbetreiber die skizzierten Abwägungsentscheidungen zwischen den privaten und öffentlichen Interessen möglicherweise nicht mit der gebotenen Sorgfalt vornehmen können bzw. wollen. Hieraus könnte die Gefahr erwachsen, dass beanstandete Links ohne nähere oder nach nur oberflächlicher Prüfung gelöscht werden, insbesondere wenn es darum geht, Prozessrisiken zu minimieren („Im Zweifel für die Löschung"). Eine sachgerechtere Lösung könnte demgegenüber darin bestehen, Suchmaschinenbetreiber nach dem Vorbild des § 8 TMG als privilegierte, d. h. nicht verantwortliche Access Provider einzustufen.[124] Personen, die sich durch Inhalte in ihrem Persönlichkeitsrecht verletzt fühlen, müssten diese Frage dann zunächst mit dem unmittelbar Verantwortlichen klären. Eine subsidiäre Inanspruchnahme des Suchmaschinenbetreibers – etwa wenn jener aus rechtlichen oder tatsächlichen Gründen nicht erreichbar sein sollte – muss daneben allerdings möglich bleiben.[125]

6.4 Schranken des allgemeinen Persönlichkeitsrechts

6.4.1 Vorbemerkungen

54 Auch wenn das BVerfG das allgemeine Persönlichkeitsrecht aus einer Kombination der Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG herleitet, folgt daraus nicht, dass dieses Grundrecht absolute Geltung beansprucht, d. h. unbeschränkbar ist. Vielmehr unterliegt es – wie auch die in Art. 2 Abs. 1 GG verankerte allgemeine Handlungsfreiheit – einem **Gesetzesvorbehalt**, den das BVerfG seit seiner *Elfes*-Entscheidung[126] vor allem in der „verfassungsmäßen Ordnung", d. h. in jedem formell und materiell ordnungsgemäß zustande gekommenen Gesetz radiziert.[127]

---

[122] EuGH, GRUR 2014, 895 (902) – Google.
[123] EuGH, GRUR 2014, 895 (902) – Google.
[124] In diese Richtung schon der Generalanwalt Jääskinen, Schlussanträge vom 25.06.2013, Rs. C-131/12, insb. Rn. 38 und 84 ff.
[125] Zum Google-Urteil des EuGH vgl. ferner Hornung, Kap. 4, Rn. 24 ff.
[126] BVerfGE 6, 32 ff.
[127] Vgl. BVerfGE 6, 32 (41) – Elfes; 80, 367 (373) – Tagebuchaufzeichnungen.

Dessen ungeachtet spielt die Inbezugnahme des Art. 1 Abs. 1 GG allerdings nicht nur für die oben[128] dargestellte Schutzbereichs-, sondern auch für die Schrankenebene eine bedeutsame Rolle: Denn je stärker eine staatliche oder private Maßnahme den Persönlichkeitskern einer Person tangiert, desto höher sind die Anforderungen an eine Rechtfertigung dieser Beeinträchtigung. Zur Operationalisierung dieses Systems einer „kommunizierenden Röhre" rekurrieren das BVerfG wie auch der BGH auf die sog. **„Sphärentheorie"**: Nach dieser ist die Intimsphäre eines Menschen, also insbesondere der auf seine sexuelle Identität und Selbstbestimmung bezogene Lebensbereich, stets absolut, d. h. eingriffsresistent geschützt. Dem vorgelagert ist die sog. Privatsphäre, d. h. ein räumlich abgegrenzter Ort, der als privat gilt. Einschränkungen dieser Sphäre bedürfen eines besonders gewichtigen Grundes. In der Sozialsphäre schließlich tritt der Mensch selbst in die Öffentlichkeit bzw. in Kontakt zu seinen Mitmenschen. Beschränkungen bzw. Beeinträchtigungen dieser Sphäre sind am ehesten möglich, sofern sie in verhältnismäßiger Weise der Realisierung eines legitimen öffentlichen oder privaten Belangs dienen.[129] **55**

Freilich handelt es sich bei diesem Modell nur um eine **grobe Orientierung**. Denn die Grenzen dieser Sphären sind fließend, was eine Zuordnung des relevanten Sachverhalts mitunter erschwert. So kann etwa auch über sexuelle Vorgänge in den Medien berichtet werden, wenn der Betroffene dazu selbst Details in die Öffentlichkeit getragen hat[130] oder wenn es um die Frage geht, ob ein US-amerikanischer Präsident die Öffentlichkeit über sein Verhältnis zu einer Praktikantin bewusst angelogen hat. Im Übrigen können Beschränkungen des allgemeinen Persönlichkeitsrechts zum Schutze der folgenden Rechtsgüter erforderlich sein: **56**

6.4.2 Meinungsfreiheit

Das in Art. 5 Abs. 1 S. 1 Alt. 1 GG verankerte „Jedermannsgrundrecht" der Meinungsfreiheit schützt grundsätzlich nur **Meinungsäußerungen** (= Werturteile), nicht hingegen **Tatsachenmitteilungen** (= wertneutrale, dem Beweis zugängliche Informationen). Meinungen sind durch die subjektive Beziehung des Einzelnen zum Inhalt seiner Aussage geprägt. Für sie ist das Element der Stellungnahme und des Dafürhaltens kennzeichnend.[131] Insofern lassen sich Meinungsäußerungen auch nicht als wahr oder unwahr qualifizieren. Ausnahmsweise werden Tatsachenmitteilungen **57**

---

[128] Rn. 9 ff.

[129] Vgl. BVerfGE 80, 367 (373 ff.) – Tagebuchaufzeichnungen; 90, 145 (171 f.) – Cannabis; 119, 1 (29 f.) – Esra. Näher zur Sphärentheorie Weigl, Meinungsfreiheit, S. 111 ff.; Wieczorek, Persönlichkeitsrecht, S. 217 ff., je m.w.N.

[130] Vgl. insoweit BGH, NJW 2012, 767 (768) – Berichterstattung über Mitwirkung in kommerziellen Pornofilmen.

[131] Eine solche wertende Stellungnahme liegt etwa auch bei der Einschätzung der Bonität einer Person vor; vgl. BGH, NJW 2011, 2204; Diederichsen, AfP 2012, 217 (217).

aber dann durch Art. 5 Abs. 1 S. 1 GG geschützt, wenn sie zugleich die Grundlage einer Meinungsäußerung bilden. Dies gilt allerdings nicht für bewusst unwahre Tatsachenbehauptungen („Auschwitz-Leugnung") oder bewusst falsche Zitate.[132]

58 Auf den **Wert einer Meinungsäußerung** (wertvoll oder wertlos), polemische Zuspitzung („Damals: Holocaust – heute: Babycaust"), Gefährlichkeit oder Harmlosigkeit, Begründetheit bzw. Grundlosigkeit, Vernünftigkeit (Rationalität) bzw. Emotionalität kommt es dementsprechend ebenfalls nicht an; es muss sich auch nicht um eine politische Meinungsäußerung handeln. Der Einzelne ist ferner rechtlich nicht verpflichtet, die der Verfassung zugrunde liegenden Wertentscheidungen persönlich zu teilen (kein Zwang zu Werteloyalität). Geschützt sind deshalb auch Äußerungen, die auf eine grundlegende Änderung der politischen Ordnung gerichtet sind. Auch rechtsradikales oder nationalsozialistisches Gedankengut fällt deshalb grundsätzlich unter den Schutzbereich des Art. 5 Abs. 1 S. 1 GG. Die Verfassung vertraut insoweit auf bürgerliches Engagement, den freien politischen Diskurs sowie die Bildung und Erziehung an den Schulen (Art. 7 Abs. 1 GG), um derartigem Gedankengut entgegenzutreten (= weites Schutzbereichsverständnis).[133] Religiöse oder weltanschauliche Äußerungen hingegen werden durch den spezielleren und vorbehaltlos gewährleisteten Art. 4 Abs. 1 GG erfasst.[134]

59 Nicht nur das Äußern, sondern auch das Verbreiten von Meinungen wird durch Art. 5 Abs. 1 GG geschützt.[135] Deshalb sind auch die **Anbieter sozialer Medien** von seinem Schutzbereich umfasst. Auf europarechtlicher Ebene folgt dieser Schutz aus Art. 10 Abs. 1 EMRK.

60 Auf sozialen Plattformen spielt zudem die Möglichkeit **anonymer Äußerungen oder Bewertungen** eine große Rolle. Bewertungsplattformen wie Spickmich.de oder MeinProf.de stehen exemplarisch hierfür. Hierbei ist zu berücksichtigen, dass das Recht auf Äußerung und Verbreitung einer Meinung nicht von der Identitätspreisgabe des Äußernden abhängt.[136] Anonymität per se führt folglich nicht zur Unzulässig- oder Schutzlosigkeit einer Äußerung, da sonst – gerade im Hinblick auf kritische Äußerungen – die Gefahr einer Selbstzensur bestünde.[137] Mit einem offenen Kommunikationsprozess, der das Fundament jeder freiheitlich-demokratischen Grundordnung bildet, wäre dies nicht zu vereinbaren. Der BGH hat in seiner wegweisenden Spickmich-Entscheidung deshalb zu Recht festgestellt, dass offenen und anonymen Äußerungen grundsätzlich das gleiche Gewicht zukommt.[138] In beiden Fällen ist mithin der Schutzbereich der Meinungsfreiheit eröffnet.

---

[132] Vgl. BVerfGE 54, 208 (219) – Böll; Bethge, in: Sachs, GG, Art. 5 Rn. 27 m.w.N.
[133] BVerfGE 124, 300 (320 f.) – Wunsiedel.
[134] Vgl. BVerfGE 32, 98 (107). Speziell für den Online-Bereich s. Luch/Schulz, MMR 2013, 88 (88 f.).
[135] Schulze-Fielitz, in: Dreier, GG, Art. 5 I, II Rn. 67.
[136] Spindler, Persönlichkeitsschutz im Internet, F 25.
[137] Wienen, ITRB 2013, 114 (115).
[138] BGH, ZUM 2009, 753 (758).

Auch das **Setzen eines Hyperlinks** kann durch die Meinungsfreiheit geschützt sein. Der BGH hat dies für einen im Internet veröffentlichten, seinem übrigen Inhalt nach dem Schutz der Meinungsfreiheit unterfallenden Beitrag bejaht, in den elektronische Verweise (Links) auf fremde Internetseiten in der Weise eingebettet wurden, dass sie einzelne Angaben des Beitrags belegen oder diese durch zusätzliche Informationen ergänzen sollten. Die Verlinkung diene hier dem Leser dazu, weitere Informationen und Belege zu beschaffen. Das Setzen eines Hyperlinks ist dabei immer dann unproblematisch, wenn auch der Inhalt, auf den verwiesen wird, rechtmäßig ist. Ist dieser Inhalt rechtswidrig, kann das Setzen des Hyperlinks dennoch zulässig sein, z. B. wenn ein überwiegendes Informationsinteresse besteht und der Verfasser sich den verlinkten Inhalt nicht zu eigen macht.[139] **61**

6.4.3 Informationsfreiheit

Gemäß Art. 5 Abs. 1 S. 1 Alt. 2 GG darf sich jeder aus **allgemein zugänglichen Quellen** ungehindert unterrichten. Ob eine Quelle allgemein zugänglich ist, bestimmt der Inhaber bzw. Kontrolleur dieser Quelle.[140] Bei Social-Media-Angeboten, die sich an eine breite (Internet-)Öffentlichkeit richten, ist diese Voraussetzung zumeist zu bejahen. Angebote wie Facebook, Spickmich.de oder MeinProf.de stellen deshalb im Grundsatz allgemein zugängliche Quellen gemäß Art. 5 Abs. 1 S. 1 GG dar. Entsprechende Rezipientenfreiheiten resultieren aus Art. 10 Abs. 1 EMRK und Art. 11 Abs. 1 EU-GRC, welche – in Ergänzung zur nationalen Verbürgung – einen „free flow of information" auch zwischen den Mitgliedstaaten, also international, sicherstellen sollen. **62**

6.4.4 Medienfreiheit

Der **Begriff** „Medienfreiheit" ist kein (verfassungs-)rechtlicher, sondern ein deskriptiver. Er umfasst die Mediengattungen Rundfunk, Presse, Film und Online, deren Grenzen im Zuge des technischen und hierdurch bedingten inhaltlichen Konvergenzprozesses fließend geworden sind.[141] Demgegenüber differenziert Art. 5 Abs. 1 S. 2 GG nach wie vor zwischen den Mediengattungen Presse, Rundfunk und Film, was dem Entstehungszeitpunkt (1948/1949) dieses Grundrechts geschuldet ist. In modernen Grundrechtskodifikationen hingegen hat der in den 1990er Jahre eingesetzte Konvergenzprozess mittlerweile auch textuell seinen Niederschlag gefunden.[142] **63**

---

[139] BGH, GRUR 2011, 513 (515).
[140] Vgl. BVerfGE 90, 27 (32); Bethge, in: Sachs, GG, Art. 5 Rn. 54.
[141] Vgl. Fechner, Medienrecht, 3. Kap. Rn. 101; Weigl, Meinungsfreiheit, S. 93.
[142] Vgl. insoweit Art. 11 Abs. 2 EU-GRC, der allgemein die „Freiheit der Medien" schützt, ohne zwischen verschiedenen Mediengattungen zu differenzieren.

64 Welchen Schutz der Online-Bereich unter Einschluss sozialer Netzwerke im Grundgesetz genießt, ist dementsprechend umstritten. Zum Teil wird aus der Enumeration des Art. 5 Abs. 1 S. 2 GG ein einheitliches **Grundrecht der Medienfreiheit** deduziert und zur Begründung auf den erwähnten Konvergenzprozess verwiesen und eine Parallele zur Interpretation des Art. 12 Abs. 1 GG als einheitliches Grundrecht der Berufsfreiheit gezogen.[143] Eine solche Sichtweise begegnet allerdings Bedenken, da Art. 5 Abs. 1 S. 2 GG die dort genannten Mediengattungen Presse, Rundfunk und Film nicht beispielhaft, sondern abschließend aufzählt. Hieran anknüpfend wird zudem eine „Freiheit der Internetdienste" postuliert, welche über das Internet vermittelte Kommunikationsinhalte, die an einen unbestimmten Personenkreis verbreitet werden, schützen soll.[144] Auch die Verortung dieses Internetgrundrechts im geltenden Verfassungsrecht bleibt allerdings unklar.

65 Eine weitere Auffassung plädiert für ein funktionales und nicht technisches Verständnis des **Pressebegriffs**.[145] Da es nach diesem technologieneutralen Ansatz auf eine stoffliche Verkörperung der publizierten Inhalte nicht ankommen soll, werden auch alle presseähnlichen Online-Angebote unter den Pressebegriff subsumiert.[146] Demnach würden publizistische Wortbeiträge in Kombination mit (Stand-)Bildern dem grundrechtlichen Schutz des Art. 5 Abs. 1 S. 2 Alt. 1 GG unterfallen. Diese Sichtweise verdient Zustimmung im Hinblick auf die sog. „funktionellen Surrogate" traditioneller Printmedien, also insbesondere ihre elektronischen „Eins-zu-Eins"-Ausgaben („e-paper"). Im Übrigen wirft sie jedoch neue Abgrenzungsschwierigkeiten hinsichtlich der Frage auf, wann der Äquivalenzbereich zum traditionellen Printmedium verlassen wird, d. h. ab wann insbesondere eingebettete Bewegtbildanteile einem Online-Angebot seine Presseähnlichkeit nehmen. Indem der Ansatz versucht, Online-Inhalte am Maßstab traditioneller Mediengattungen zu kategorisieren, trägt er der Eigenart des Internets – seiner technischen wie inhaltlichen Konvergenz – nicht hinreichend Rechnung. Im vorliegenden Kontext kommt hinzu, dass es sich bei einer Vielzahl von Inhalten sozialer Netzwerke gar nicht um journalistisch-redaktionell gestaltete Angebote im Sinne des Pressebegriffs handelt. Für die Frage, welchen grundrechtlichen Schutz Social Media genießen, ist dieser Ansatz – wenn überhaupt – deshalb nur partiell weiterführend.

66 Die wohl herrschende Auffassung kategorisiert die in Art. 5 Abs. 1 S. 2 GG enumerierten Mediengattungen deshalb primär anhand technischer Gesichtspunkte. Der Begriff **„Rundfunk"** soll sich demnach nicht nur auf das traditionelle lineare Medium Rundfunk i. S. d. (engen) einfachgesetzlichen Rundfunkbegriffs[147] beziehen,

---

[143] Vgl. Fechner, Medienrecht, 3. Kap. Rn. 101 f.

[144] Vgl. Holznagel/Schumacher, in: Kloepfer, Netzneutralität, S. 47 ff.

[145] Fiedler, AfP 2011, 15 ff.

[146] Zur Definition des Begriffs „presseähnliche Angebote" vgl. § 2 Abs. 2 Nr. 20 RStV. Der Vertrag versteht hierunter „nicht nur elektronische Ausgaben von Printmedien, sondern alle journalistisch-redaktionell gestalteten Angebote, die nach Gestaltung und Inhalt Zeitungen oder Zeitschriften entsprechen."

[147] Vgl. hierzu die Definition in § 2 Abs. 1 RStV. Der Begriff „Rundfunk" wird dort definiert als „ein linearer Informations- und Kommunikationsdienst; er ist die für die Allgemeinheit und zum

sondern in einem (weiten) verfassungsrechtlichen Verständnis meinungsbildungsrelevante (publizistische) Darbietungen aller Art umfassen, welche an die Allgemeinheit gerichtet sind und mittels einer elektronischen Infrastruktur übertragen werden. Eine solche erweiterte Interpretation des verfassungsrechtlichen Rundfunkbegriffs steht zudem im Einklang mit der Rechtsprechung des BVerfG, welches stets die Offenheit des Rundfunkbegriffs für neue technische Entwicklungen betont.[148] Andererseits zwingt dieser Ansatz nicht dazu, die verfassungsgerichtliche Sonderdogmatik der „dienenden Rundfunkfreiheit" pauschal auf den Internet-Bereich zu extendieren, da das Gericht diese Dogmatik wegen der von ihm postulierten Besonderheiten des Leitmediums Fernsehen und Hörfunk (Aktualität, Breitenwirkung und Suggestivkraft) bislang lediglich auf diese traditionellen Rundfunkmedien beschränkt.[149] Diese unterschiedliche Reichweite des verfassungs- und einfachrechtlichen Rundfunkbegriffs spiegelt sich denn auch im derzeitigen RStV wider, der in den §§ 2 ff. RStV strenge Anforderungen an den traditionellen Rundfunk formuliert, wohingegen (publizistische) Online-Medien gemäß §§ 54 ff. RStV lediglich weniger einschneidende, presseähnliche Restriktionen zu beachten haben. Vor diesem Hintergrund können sich zahlreiche soziale Netzwerke auf den Schutz der Rundfunkfreiheit aus Art. 5 Abs. 1 S. 2 Alt. 2 GG berufen, da sie aufgrund ihrer Gestaltung (Stichwort: Bewertungsportale) oder ihrer internen Plattform-Vernetzung ein Agenda-Setting vornehmen oder Informationen redaktionell aufbereiten, mithin publizistisch tätig sind, und sich an eine nicht näher bestimmbare Öffentlichkeit richten. Zudem weisen auch etliche Inhalte solcher Plattformen, wie insbesondere Blogs oder Wiki-Beiträge, meinungsbildende Relevanz auf und werden deshalb ebenfalls durch die Rundfunkfreiheit geschützt.[150]

Dies führt zu der weiteren, bislang wenig beachteten Frage, inwiefern die Betreiber sozialer Netzwerke unter räumlichen Gesichtspunkten als grundrechtsfähig anzusehen sind. Zwar fällt – wie vorstehend ausgeführt – der Betrieb deutschsprachiger Blog- oder Wikipedia-Seiten grundsätzlich in den sachlichen Schutzbereich der Rundfunkfreiheit. Nicht selten handelt es sich bei den Anbietern solcher Seiten allerdings um außereuropäische Unternehmen. **Ausländische juristische Personen** genießen gemäß Art. 19 Abs. 3 GG allerdings prinzipiell keinen materiellen Grundrechtsschutz[151]; auch ist die „community" der (Blog- oder Wiki-)Autoren nicht rechtsfähig. Im Einzelfall mag allerdings eine inländische Mitbetreiberin – etwa **67**

zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen." Hierzu zählen das Fernsehen und der Hörfunk.

[148] Vgl. insofern BVerfGE 74, 297 (350) – Baden-Württemberg; 83, 238 (299) – WDR-Gesetz.

[149] Vgl. insoweit aus jüngerer Zeit BVerfGE 121, 30 (50 f.) – Beteiligung von Parteien am Rundfunk; BVerfG, Urt. v. 25.03.2104, Az. 1 BvF 1/11 u. a. Rn. 33 f. – ZDF-Staatsvertrag.

[150] Näher zum Vorstehenden Beyerbach, Kap. 9, Rn. 5 ff. und 13 ff. S. ferner Bethge, in: Sachs, GG, Art. 5 Rn. 90 ff.; Bloch, Meinungsvielfalt, S. 89 ff.; Degenhart, CR 2011, 231 ff. Kühling, in: Gersdorf/Paal, Art. 5 GG, Rn. 73 ff., je m.w.N.

[151] Anderes gilt nur für Unternehmen mit Sitz in der EU. Für diese stellt nach einer jüngeren Entscheidung des BVerfG (E 129, 78 ff.) die Erstreckung der Grundrechtsberechtigung eine aufgrund des Anwendungsvorrangs der Grundfreiheiten im Binnenmarkt (Art. 26 Abs. 2 AEUV) und des

Wikimedia Deutschland e. V. – als Verantwortliche und damit Grundrechtsberechtigte in Betracht kommen.[152] Das OLG Stuttgart hat hierzu angemerkt: „Ob sich die Beklagte selbst auf Art. 5 Abs. 1 GG berufen kann, erscheint hingegen sehr fraglich: ausländische juristische Personen können sich in europarechtskonformer Ausweitung des Anwendungsbereichs des Art. 19 Abs. 3 Grundgesetz auf die Grundrechte (mit Ausnahme der justiziellen Grundrechte) nur berufen, wenn sie ihren Sitz in einem Mitgliedstaat der Europäischen Union haben (BVerfG NJW 2011, 3428 Tz. 69 ff.), was auf die Beklagte nicht zutrifft. Dennoch wird in der Literatur angesichts des Umstands, dass das deutschsprachige Angebot von ‚Wikipedia' ganz überwiegend von deutschen Nutzern eingestellt wird und sich in erster Linie an diese richtet, ein Schutz der Beklagten über Art. 5 Abs. 1 GG befürwortet, weil der einzige unmittelbare Anknüpfungspunkt im Ausland der Sitz der Beklagten als verantwortlichem Anbieter sei, der den notwendigen Server bereitstelle (Strauß, ZUM 2006, 277, 279; ohne nähere Begründung die Anwendbarkeit von Art. 5 Abs. 1 Grundgesetz bejahend LG Tübingen ZUM-RD 2013, 345 Rn. 28 in Juris). Die Frage kann letztlich dahinstehen [. . .]."[153]

6.4.5 Kunstfreiheit

68 An dem durch Art. 5 Abs. 3 S. 1 GG vorbehaltlos verbürgten Schutz der Kunstfreiheit kann insbesondere die Art und Weise einer Darstellung von Social Media-Inhalten partizipieren. Insoweit kommen insbesondere künstlerisch gestaltete **Videoclips, Fotografien** oder sonstige **grafische Darstellungen**, aber auch satirische Beiträge in Betracht.[154] Für den europäischen Bereich findet sich eine gleichlautende Verbürgung in Art. 13 EU-GRC.

6.4.6 Wirtschaftliche Betätigungsfreiheit

69 Dem Betrieb sozialer Netzwerke liegt des Weiteren ein Geschäftsmodell zugrunde, weshalb sich Plattformbetreiber im Netz unternehmerisch betätigen. Folglich können sie sich auf den Schutz der wirtschaftlich relevanten Grundrechte, also insbesondere die **unternehmerische Betätigungsfreiheit** (Art. 12 Abs. 1 GG) und die **Eigentumsfreiheit** (Art. 14 Abs. 1 GG), berufen.[155] Im supranationalen Kontext der EU sind zudem die entsprechenden Verbürgungen der Grundrechte-Charta (Art. 16

allgemeinen Diskriminierungsverbots wegen der Staatsangehörigkeit (Art. 18 AEUV) vertraglich veranlasste Anwendungserweiterung des deutschen Grundrechtsschutzes dar.

[152] Vgl. Dilling, ZUM 2013, 380 (388).

[153] OLG Stuttgart, NJW 2014, 423 (425).

[154] Hierzu ferner Luch/Schulz, MMR 2013, 88 (89).

[155] Näher hierzu Weigl, Meinungsfreiheit, S. 89 ff. S. ferner Luch/Schulz, MMR 2013, 88 (91).

und Art. 17 EU-GRC) sowie die Dienstleistungsfreiheit (Art. 56 AEUV) zu beachten. Die Gegenleistung, welche die Plattformbetreiber für ihre zumeist entgeltfreien Social-Media-Angebote erhalten, besteht zumeist in der Preisgabe personenbezogener Daten, welche sie für personenbezogene Zwecke, insbesondere in Gestalt von Werbung, nutzen. Gerade für diesen Wirtschaftszweig gilt: Daten sind die neue Währung des Internets.

6.4.7 Versammlungsfreiheit

Vereinzelt findet sich schließlich die Auffassung, dass bei **gemeinschaftlich vertretenen Überzeugungen** – etwa im Rahmen eines über Social-Media-Plattformen initiierten „Shitstorms“[156] – eine Versammlung i. S. d. Art. 8 Abs. 1 GG vorliegen könne. Denn in diesem Fall „[. . .] bildeten sich z. B. Meinungsfraktionen heraus, die eine gemeinsame Überzeugung innerhalb von Beiträgen und Beitragskommentaren sichtbar gemeinsam und geschlossen vertraten und sich damit als eine Versammlung i. S. d. Art. 8 GG qualifizierten.“[157] **70**

Die Bundesregierung ist dem mit Recht entgegengetreten und stellt hierzu fest, dass eine Versammlung i. S. d. grundrechtlichen Verbürgung die gleichzeitige körperliche Anwesenheit mehrerer Personen an einem Ort erfordert. Mangels Körperlichkeit sind sog. **virtuelle Versammlungen** auf Social-Media-Plattformen im Rahmen sonstiger internetbasierter Angebote deshalb keine Versammlungen im verfassungsrechtlichen Sinne.[158] Hieraus folgt, dass die Teilnehmer einer Versammlung gleichzeitig anwesend sein müssen und ihre Handlungen synchron zu erfolgen haben. Das Posten von Kommentaren in einem sozialen Netzwerk ist deshalb eher vergleichbar mit Debatten in einer Tageszeitung, in der mit zeitlichem Abstand aufeinander Bezug nehmende Beiträge oder Leserbriefe veröffentlicht werden.[159] Solche Vorgänge sind durch Art. 2 Abs. 1 oder Art. 5 Abs. 1 GG, nicht aber durch Art. 8 Abs. 1 GG geschützt.[160] **71**

6.5 Schranken-Schranken des allgemeinen Persönlichkeitsrechts

6.5.1 Vorbemerkungen

Zwar findet das allgemeine Persönlichkeitsrecht prinzipiell in den vorstehend (Rn. 54 ff.) skizzierten Grundrechten seine Schranke. Eine Beschränkung des allgemeinen **72**

---

156 S. o. Rn. 46.
157 Schwenke, K&R 2012, 305 (307).
158 BT-Drs. 17/10379, S. 11 (zu Nr. 19).
159 Möhlen, MMR 2013, 221 (229 Fn. 124).
160 Luch/Schulz, MMR 2013, 88 (90).

Persönlichkeitsrechts durch diese Grundrechtspositionen ist allerdings nur gerechtfertigt, wenn diese ihrerseits bestimmten begrenzenden Anforderungen – den sog. „Schranken-Schranken" – genügt. Die bedeutsamste Schranken-Schranke stellt dabei der aus Art. 19 Abs. 2 GG und dem Rechtsstaatsprinzip (Art. 20 Abs. 2 und 3 GG) herzuleitende **Verhältnismäßigkeitsgrundsatz** dar.[161]

73 Im Zivilrecht – dem wohl wichtigsten Schutzinstrument des allgemeinen Persönlichkeitsrechts[162] – sind diese Gesichtspunkte im Rahmen der **Rechtswidrigkeit einer persönlichkeitsbeeinträchtigenden Maßnahme** zu berücksichtigen: So kann der Betroffene die Unterlassung eines Übergriffs in sein Persönlichkeitsrecht nur verlangen, wenn er nicht zur Duldung dieser Beeinträchtigung verpflichtet ist (vgl. § 1004 Abs. 2 BGB).[163] Auch löst eine solche Beeinträchtigung einen (materiellen oder immateriellen) Schadensersatzanspruch nur aus, wenn der Eingriff schuldhaft und rechtswidrig erfolgt (vgl. § 823 Abs. 1 BGB). Anders als bei den in § 823 Abs. 1 BGB explizit aufgeführten Rechtsgütern wird die Rechtswidrigkeit des Verhaltens durch die Beeinträchtigung von Persönlichkeitsinteressen dabei nicht indiziert, sondern muss durch eine Interessenabwägung konturiert und für den Einzelfall konkretisiert werden.[164] Im Rahmen der Rechtswidrigkeit ist deshalb zu erörtern, ob es für die Beeinträchtigung des Persönlichkeitsrechts einen rechtfertigenden Grund gibt, der insbesondere aus einer der vorstehend skizzierten Grundrechtspositionen des Äußernden resultieren kann. Freilich muss dieses Grundrecht das Persönlichkeitsrecht des Betroffenen auch überwiegen. Im Rahmen dieser Abwägungsentscheidung ist dabei den nachstehend skizzierten Besonderheiten sozialer Netzwerke Rechnung zu tragen.

6.5.2 Hochrangigkeit der Kommunikationsfreiheiten

74 Bei der Abwägung des allgemeinen Persönlichkeitsrechts mit den vorstehend skizzierten Grundrechten kommt insbesondere der Meinungs-, Informations- und Medienfreiheit (d. h. den Kommunikationsfreiheiten) eine zentrale Bedeutung zu, und zwar sowohl in publizistisch-professionellen als auch in privaten Kontexten. Das BVerfG misst den Kommunikationsfreiheiten für die individuelle Persönlichkeitsentfaltung, aber auch für das demokratische Gemeinwesen und seine gedeihliche Entwicklung eine **„schlechthin konstituierende" Bedeutung** bei. Dieser überragenden „wertsetzenden Bedeutung" der Kommunikationsgrundrechte ist im Rahmen

---

[161] Näher zur Herleitung und zum Inhalt dieses Grundsatzes BVerfGE 7, 377 (409 ff.); Hillgruber, in: Isensee/Kirchhof, HStR IX, § 201 Rn. 51 ff.

[162] S. hierzu o. Rn. 5 und 27.

[163] Aufgrund der gesetzlichen Ausgestaltung des Unterlassungsanspruchs obliegt der Nachweis der Duldungspflicht des Betroffenen (und damit der mangelnden Rechtswidrigkeit) dabei dem Äußernden. Sie gibt dem Störer eine Einwendung, welche verhindert, dass der Anspruch überhaupt entsteht; vgl. Fritzsche, in: BeckOK-BGB, § 1004 Rn. 98.

[164] Wagner, in: MüKo-BGB, § 823 Rn. 242.

des Verhältnismäßigkeitsprinzips gebührend Rechnung zu tragen (Wechselwirkungslehre).[165] So hat der BGH etwa erst jüngst festgestellt, dass die Kommunikationsfreiheit eines Bewertungsportalbetreibers höher zu bewerten sei als das Recht auf informationelle Selbstbestimmung eines Arztes auf Löschung seiner Basisdaten aus diesem Portal.[166] Nur bei eindeutigem Überwiegen persönlichkeitsrechtlicher Belange vermögen sich diese gegenüber den Kommunikationsfreiheiten durchzusetzen. Ansonsten gilt: „Im Zweifel für die Meinungsfreiheit".

Solche Zweifel können sich insbesondere aus mehrdeutigen, d. h. **interpretationsoffenen Äußerungen** ergeben („Soldaten sind Mörder"). Die Gerichte sind in derartigen Konstellationen gehalten, eine dem Äußernden günstige Deutungsvariante für ihrer Abwägungsentscheidung zugrunde zu legen und so den Kommunikationsfreiheiten zum Durchbruch zu verhelfen.[167] Das BVerfG hat diese Abwägungsdirektive, die von den Gerichten zunächst auf alle Entscheidungssituationen appliziert wurden, zwischenzeitlich jedoch restringiert und auf solche Konstellationen beschränkt, in denen es um eine nachträgliche Sanktion kommunikativen Verhaltens in Gestalt einer strafrechtlichen Verurteilung oder eines Schadensersatzanspruchs (§§ 185 ff. StGB, §§ 823 Abs. 1 und 2 BGB) geht. Für zukunftsgerichtete Unterlassungsansprüche hingegen ist das Gericht zwischenzeitlich von dieser Linie abgerückt: In solchen Konstellationen muss der Äußernde den Inhalt seiner mehrdeutigen Aussage nunmehr klarstellen. Tut er dies nicht, ist zu prüfen, ob eine nicht fernliegende Deutungsvariante zu einer rechtswidrigen Beeinträchtigung des Persönlichkeitsrechts führt. Es gilt also der Grundsatz: „Im Zweifel für das Persönlichkeitsrecht".[168] **75**

Zu überzeugen vermag diese Differenzierung freilich nicht: Sie schränkt den offenen Meinungskampf, der für eine demokratische und durch plurale Wertvorstellungen geprägte Gesellschaft unverzichtbar ist, zu sehr ein. Prima vista mag es einleuchten, bei mehrdeutigen Äußerungen zwischen der Art der gerichtlichen Auseinandersetzung (nachträgliche oder zukunftsgerichtete Sanktionierung) zu unterscheiden. Das BVerfG lässt sich insoweit offensichtlich von der Vorstellung leiten, dass ein Unterlassungsanspruch weit weniger in die Grundrechtssphäre des Äußernden eingreift als eine nachträgliche, repressive Sanktion mit ggf. einschneidender belastender Wirkung (strafgerichtliche Verurteilung, Verurteilung zu Schadensersatz). Dies verkennt jedoch, dass auch ein Unterlassungsbegehren zu erheblichen Prozess- und Anwaltskosten für den Äußernden führen kann. Äußert er sich polemisch oder zugespitzt („Damals: Holocaust – heute: Babycaust"), um Gehör im vielstimmigen Meinungskampf zu finden, geht der Äußernde mithin in jeder Konstellation ein erhebliches Risiko ein. Realisiert sich dieses Risiko bei Unterlassungsbegehren für ihn eher als in Straf- oder Schadensersatzkonstellationen, beeinflusst (i. S. v. moderiert) dies zwangsläufig sein generelles Äußerungsverhalten, **76**

[165] Locus classicus zum Vorstehenden: BVerfGE 7, 198 (208 f.) – Lüth.
[166] BGH, Urt. v. 23.09.2014, Az. VI ZR 358/139
[167] Grundlegend insoweit BVerfGE 93, 266 ff. – Soldaten sind Mörder.
[168] Vgl. BVerfGE 114, 339 ff. – Stolpe; BVerfG-K, NJW 2006, 3769 (3772 f.) – Babycaust.

zumal sich die Betroffenen durch die Wahl des geltend gemachten Rechtsschutzes auf diese Differenzierung und die durch sie bewirkte Verteilung des Prozessrisikos einzustellen vermag. Letzteres kann indes nicht im gesamtgesellschaftlichen Interesse liegen.[169] Von daher sollte der Grundsatz **„Im Zweifel für die Meinungsfreiheit"** für alle Rechtsschutzkonstellationen Geltung beanspruchen.

77 In der Rechtsprechung geklärt hingegen ist, dass bei Meinungsäußerungen mit würdeverletzendem Charakter, bei **Schmähkritik**[170] und **Formalbeleidigungen**, d. h. unangemessenen Ausdrucksweisen, die Meinungsfreiheit stets hinter das Persönlichkeitsrecht zurückzutreten hat.[171] Sie begründen einen Anspruch auf Ersatz des immateriellen Schadens (§ 253 Abs. 2 BGB), wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in andere Weise befriedigend aufgefangen werden kann. Dies gilt auch für derartige Äußerungen in sozialen Netzwerken.[172]

6.5.3 Bedeutung des (Vor-)Verhaltens der Betroffenen

78 Auch das (Vor-)Verhalten des Betroffenen kann für den Abwägungsvorgang von Relevanz sein, insbesondere in Konstellationen der **„Rede und Gegenrede"** bzw. des **„Gegenschlags"**.[173] Von daher kann es etwa gerechtfertigt sein, in sozialen Medien identifizierend über strafbare Sachbeschädigungen bzw. Randale von Jugendlichen zu berichten, sofern sich dieser Bericht auf wahre Tatsachen stützt und das bisherige Verhalten der Betroffenen einen legitimen Anlass für eine solche Berichterstattung bietet. Im konkreten Fall war laut BVerfG der Schutz des allgemeinen Persönlichkeitsrechts insbesondere deshalb verringert, weil „die Kläger (. . .) über das Fernsehen die Öffentlichkeit unstreitig oft gesucht, ein Image als ‚Junge Wilde' gepflegt und ihre Idolfunktion kommerziell ausgenutzt [. . .] und so ihre Person selbst in die Öffentlichkeit gestellt haben." Der Bericht war deshalb nach Auffassung des Gerichts geeignet, eine öffentliche Debatte in Gang zu setzen, weshalb trotz der Minderjährigkeit der Betroffenen die Meinungs- bzw. Medienfreiheiten ihr Persönlichkeitsrecht überwogen.[174]

---

[169] Kritisch wie hier: Fiedler, in: Menzel/Müller-Terpitz, Verfassungsrechtsprechung, S. 771 ff.; Hochhut, NJW 2007, 192 ff.; a. A. Seitz, NJW 2003, 3523 ff.

[170] Hierbei handelt es sich um Äußerungen, die primär auf eine Herabsetzung der betroffenen Person, nicht aber auf eine geistige Auseinandersetzung in der Sache zielen.

[171] Vgl. statt Vieler OLG Köln, AfP 2009, 156 ff.; Feldmann, in: Heise Online-Recht, B. II; C. II. 3. aa).

[172] Vgl. LG Berlin, ZUM 2012, 997 ff.

[173] Feldmann, in: Heise Online-Recht, B. II.; C. II. 3. bb) (2).

[174] BVerfG, MMR 2012, 338 (339 f.) – Ochsenknecht. Die Zivilgerichte hatten dies wegen der Minderjährigkeit der Betroffenen noch anders bewertet.

6.5.4 Minderjährige in sozialen Netzwerken

Soziale Netzwerke werden zu einem großen Teil von Minderjährigen genutzt. Diese Personengruppe zeichnet sich dadurch aus, dass sie aufgrund mangelnder (Lebens-) Erfahrung **leicht beeinflussbar** ist. Auch dieser Umstand ist bei entsprechenden Abwägungsentscheidungen gebührend in Rechnung zu stellen.[175] Entsprechend betont das BVerfG, dass das junge bzw. jugendliche Alter besonders in Erwägungen zur Intensität des Persönlichkeitsschutzes einzubeziehen ist. Kinder und Jugendliche bedürfen eines besonderen Schutzes, weil sie sich zu eigenverantwortlichen Personen erst noch entwickeln müssen. Minderjährige bis zur Vollendung des 14. Lebensjahres gelten dabei als besonders schutzwürdig, weil sie sich in einer für die Persönlichkeitsentwicklung höchst bedeutsamen Phase (Pubertät) befinden, in der sie als „Suchende" für äußere Einflüsse besonders anfällig sind. Von daher dürfen sie auch nicht ohne Weiteres „ins Licht der Öffentlichkeit gezerrt" werden.[176] Wie vorstehend (Rn. 78) bereits skizziert, genügt es jedoch nicht den verfassungsrechtlichen Vorgaben, eine Regelvermutung dahingehend zu postulieren, dass jedes Informationsinteresse an Kindern oder Jugendlichen hinter ihrem Anonymitätsinteresse zurückzustehen hat.[177] **79**

Minderjährige können dabei – etwa in Fällen des sog. „Cyber-Mobbings" oder „Cyber-Bullyings"[178] – nicht nur Opfer von Persönlichkeitsbeeinträchtigungen sein, sondern auch als **Täter** solcher Beeinträchtigungen in Erscheinung treten. Dabei sind sowohl Übergriffe in das Persönlichkeitsrecht anderer Minderjährige, aber auch von Erwachsenen denkbar. Über letztere Konstellation hatte der BGH etwa im **Spickmich-Urteil**[179] zu entscheiden. Er hob diesen Aspekt bei seiner Abwägung denn auch gesondert hervor: Es sei für jedermann erkennbar, dass es sich bei den Lehrerbewertungen auf dem Bewertungsportal spickmich.de um Aussagen von minderjährigen Schülern handele. Die Erhebung der Daten entspreche nach Vielfalt und Qualität nicht den Anforderungen an eine aussagekräftige Lehrerevaluation, weshalb der BGH im Ergebnis eine Beeinträchtigung des Persönlichkeitsrechts der Lehrer verneinte. **80**

6.5.5 Offene und anonyme Äußerungen

Zwar fallen – wie gesehen (Rn. 60) – sowohl offene als auch anonyme Äußerungen in den Schutzbereich der **Meinungsfreiheit**. Die Anonymität des Äußernden kann allerdings auf der Schrankenebene Bedeutung erlangen: Während für offene Äußerungen **81**

---

[175] Vgl. Köhler, Persönlichkeitsrechte im Social Web, S. 85.
[176] Vgl. BGH, ZUM 2013, 682 (683); BVerfGE 119, 1 (24) – Esra.
[177] Vgl. erneut BVerfG, MMR 2012, 338 (339) – Ochsenknecht.
[178] S. o. Rn. 47.
[179] BGH, MMR 2009, 608 ff.

insoweit die allgemeinen und zum Teil vorstehend skizzierten Abwägungsgesichtspunkte greifen, ist dies bei anonymen Äußerungen im Grundsatz nur dann der Fall, wenn die Anonymität erst die Voraussetzung für den Freiheitsgebrauch sicherstellt. Besteht hingegen ein gewichtiges öffentliches Interesse an der Identifikation des Äußernden oder widerfährt dem Betroffenen durch die Anonymität ein schwerwiegender Nachteil, ist dieser Äußerungsform in Relation zum Persönlichkeitsrecht ein anderes, sprich geringeres Gewicht beizumessen.[180]

6.5.6 Weltweite Abrufbarkeit

82 Im Unterschied zu Druckerzeugnissen mit einer quantitativ und räumlich begrenzten Auflage oder zu lediglich regional ausgestrahlten Rundfunkangebote zeichnen sich Internetmedien unter Einschluss sozialer Netzwerke durch den Umstand aus, dass die dort publizierten personenbezogenen Inhalte **weltweit abrufbar** und über **Suchmaschinen** zumeist leicht erschließbar sind.[181] Prima facie scheint dies im Online-Bereich für eine höhere Eingriffsintensität persönlichkeitsrelevanter Sachverhalte und für eine Verschiebung der Abwägungsgewichte zugunsten des Persönlichkeitsrechts zu sprechen.

83 Einer solchen **Pauschalisierung** ist allerdings mit Vorsicht zu begegnen: Denn die Größe des Leser- bzw. Adressatenkreises ist für sich genommen noch kein hinreichender Grund, um bei der Abwägung zwischen Persönlichkeitsrechten einerseits und der Meinungs- bzw. Informationsfreiheit in sozialen Netzwerken andererseits eo ipso andere Maßstäbe anzulegen als bei Offline-Publikationen oder bei einer Kommunikation in geschlossenen Nutzergruppen. Die Meinungs- und Informationsfreiheit gilt für Medien mit hohem Verbreitungsgrad genauso wie für solche mit einem nur begrenzten Adressatenkreis. Allein aus der größeren Reichweite eines Mediums lässt sich deshalb nicht automatisch schlussfolgern, dass dem Persönlichkeitsrecht stets ein stärkeres Gewicht zukommen muss als bei Offline-Publikationen.[182]

84 Die Ubiquität und leichte Auffindbarkeit persönlichkeitsrelevanter Inhalte wird zudem durch den Umstand relativiert, dass der Informationszugang – anders als

---

[180] Allg. hierzu Bernreuther, in: Leible, Innovation und Recht, S. 164 ff. Restriktiver demgegenüber Graef, ZUM 2009, 759 (761), dem zufolge bei der Abwägung stets berücksichtigt werden müsse, welche Art der Äußerung – offen oder anonym – vorliege.

[181] Vgl. Gounalakis/Klein, NJW 2010, 566 (567).

[182] So mit Recht Härting, CR 2009, 21 (23). S. ferner BVerfGE 119, 1 (25) – Esra, wo das Gericht bereits die Erkennbarkeit einer realen Person hinter einer fiktiven (Roman-)Figur durch einen „näheren Bekanntenkreis“ für die Annahme einer Persönlichkeitsrechtsbeeinträchtigung ausreichen lässt. Anders mag dies bei der Bemessung des (immateriellen) Schadensersatzes infolge einer Persönlichkeitsrechtsverletzung zu bewerten sein. Dort ist nach st. Rspr. des BGH die Reichweite der Persönlichkeitsbeeinträchtigung für die Entschädigungshöhe sehr wohl von Relevanz; vgl. insoweit BGH, ZUM-RD 2014, 145 m. Anm. Stender-Vorwachs, GRUR-Prax 2014, 134 und Haug, K&R 2014, 235. Ebenso OLG Bamberg v. 10.04.2013–3 U 282/12 (Juris); AG Schwerin v. 30.11.2012–14 C 424/11 (Juris).

bei traditionellen (Push-)Medien wie Fernsehen oder Hörfunk – einer gezielten Abfrage durch den Nutzer und dementsprechend einer nutzerseitigen Informationsselektion bedarf. Hinzukommen können teilnehmerdefinierte Begrenzungen des Informationszugangs und der Kommunikation, wie sie gerade für Social Media kennzeichnend sind.[183] Dieser Abruf- bzw. **„Pull"-Charakter** des Internets schränkt die Informationsverbreitung und damit die Intensität der Persönlichkeitsbeeinträchtigung tendenziell wieder ein.[184] Dies kann vor allem dann von Relevanz sein, wenn es sich um Persönlichkeitsbeeinträchtigungen von Personen handelt, die weder weltweit noch national, regional oder lokal „im Rampenlicht der Öffentlichkeit" stehen. Demgegenüber ist zu berücksichtigen, dass Nutzer sozialer Netzwerke über die technisch einfache Möglichkeit verfügen, Inhalte zu teilen, so dass Informationen über solche Plattformen mitunter schnell verbreitet werden können. Auch sind Persönlichkeitsbeeinträchtigungen mittels leistungsfähiger Suchmaschinen im Netz zumeist für längere Zeit auffindbar und ermöglichen so die Erstellung von Persönlichkeitsprofilen.[185]

Vor diesem Hintergrund bedarf es stets einer wertenden **Betrachtung des Einzelfalls**, in die alle vorstehend skizzierten Gesichtspunkte abwägend einzubeziehen sind. Im Übrigen bleibt abzuwarten, welche Bedeutung in diesem Kontext dem „Recht auf Vergessenwerden", das der EuGH in Bezug auf Suchmaschinenindizes erst unlängst bejaht hat[186], für den Schutz des Persönlichkeitsrechts zukommen wird. **85**

6.6 Fazit und Ausblick

Bereits im Jahre 2001 stellte das **BVerfG** fest, dass die Nutzung des damals erst im Aufbau befindlichen und daher mit erheblichen Rechtsunsicherheiten verbundenen Internets mit neuartigen, Dritte gezielt in ihren grundrechtlichen Positionen beeinträchtigenden Aktivitäten verbunden sei.[187] An dieser Einschätzung hat sich bis heute nichts geändert – im Gegenteil. **86**

Die Vorstellung, dass sich Nutzer sozialer Netzwerke wirksam **selbst regulieren und kontrollieren** könnten, erscheint dabei illusorisch. Eher ist zu beobachten, dass sich persönlichkeitsbeeinträchtigende Informationen durch solche Netzwerke schnell verbreiten, statt zügig richtig gestellt oder korrigiert zu werden.[188] Auch die von US-amerikanischen Gerichten vereinzelt vertretene Auffassung, Online-Nutzer **87**

[183] Vgl. Bruns, AfP 2011, 421 (422).
[184] Vgl. insoweit auch BGH ZUM 2011, 647 ff., ZUM-RD 2011, 296 ff., ZUM 2013 399 ff., die u. a. aus diesen Gründen eine identifizierende Wortberichterstattung über Straftäter in Online-Archiven von Tageszeitungen grundsätzlich für zulässig erachten, auch wenn der Betroffene seine Strafe bereits verbüßt und dementsprechend einen ebenfalls in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG wurzelnden Anspruch auf Resozialisierung hat.
[185] Vgl. erneut EuGH, GRUR 2014, 895 (897, 900) – Google.
[186] Vgl. o. Rn. 53.
[187] BVerfGE 104, 65 (74) – Schuldnerspiegel.
[188] Vgl. Ladeur/Gostomzyk, NJW 2012, 710 (714).

seien sich darüber im Klaren, dass das Internet nicht als „seriöses Medium“ bewertet werden könne und nähmen Persönlichkeitsbeeinträchtigungen deshalb nicht so ernst, vermag in dieser Pauschalität nicht zu überzeugen.[189]

88 Zur Verbesserung des Schutzes der Persönlichkeit wird vor diesem Hintergrund die Einrichtung von sog. **„Cyber-Courts“** diskutiert. Hierbei handelt es sich um private Schieds- oder Beschwerdestellen, die im Konfliktfall vermittelnd tätig werden können.[190] In seinem „blogspot.com“-Urteil hat der BGH bereits ein Verfahren beschrieben, das an einen solchen „Cyber-Court“ erinnert.[191] Zudem könnte man die Haftungsfreistellung eines Service Providers davon abhängig machen, dass solche „Cyber-Courts“ eingerichtet werden. Jeder Nutzer müsste sich dann verpflichten, sich dieser Schiedsstelle zu unterwerfen. Zudem könnten sachverständige Dritte, etwa Bürgerrechtsgruppen oder mit Persönlichkeitsrechtsfragen vertraute Personen (Rechtsanwälte, Journalisten etc.), an solchen Verfahren beteiligt werden.[192]

89 Freilich darf dieser Mechanismus der (regulierten) Selbstregulierung in sozialen Netzwerken[193] nicht dazu führen, den Zugang zu staatlichen Gerichten zu erschweren oder gar zu vereiteln. Es kann sich hierbei nur um eine freiwillige, **optionale Möglichkeit** des Rechtsschutzes für die Nutzer handeln. Von daher könnte sie über das Potential verfügen, die effektive Durchsetzung des Persönlichkeitsrechts zu verbessern und die staatlichen Gerichte zu entlasten, insbesondere wegen der nur geringen Zugangshürden zu diesem (unentgeltlichen) Instrument. Freilich bleiben Fragen offen, die – nach Möglichkeit auf europäischer Ebene – gesetzlich geregelt werden sollten: So ist etwa zu klären, für welche Plattformen eine Verpflichtung zur Errichtung solcher „Cyber-Courts“ bestehen soll und wie die „Richter“ für diese Schiedsstelle zu bestellen sind. Auch das Verhältnis zur staatlichen Gerichtsbarkeit wäre klarzustellen.

---

[189] Vgl. Ladeur/Gostomzyk, NJW 2012, 710 (714) unter Verweis auf Surpreme Court of the State of Delaware, Doe No. 1 v. Cahill, Urt. v. 05.10 2005, S. 26 f., abrufbar unter https://www.eff.org/files/filenode/Doe_v_Cahill/doe_v_cahill_decision.pdf.

[190] Glaser, NVwZ 2012, 1432 (1437).

[191] Vgl. Ladeur/Gostomzyk, NJW 2012, 710 (715) unter Verweis auf BGH, NJW 2012, 148 ff. Dort geht der Gerichtshof von einer Verpflichtung zur Löschung eines beanstandeten Eintrags (erst) dann aus, wenn auf der Grundlage der Stellungnahme des für den Eintrag (konkret: ein Blog) Verantwortlichen und einer etwaigen Replik des Betroffenen unter Berücksichtigung ggf. erforderlicher Nachweise von einer Verletzung des Persönlichkeitsrechts auszugehen ist. Die Schiedsstelle ist hier freilich kein Neutraler, sondern das Unternehmen (Host Provider) selbst, welches den Speicherplatz für den inkriminierten Eintrag zur Verfügung stellt.

[192] Näher zum Ganzen Ladeur/Gostomzyk, NJW 2012, 710 (715). Kritisch demgegenüber Glaser, NVwZ 2012, 1432 (1438) mit weiteren Vorschlägen.

[193] Allg. dazu Roßnagel, in: Bieber et al., Soziale Netzwerke, S. 271 ff.

Literatur

Ahlberg, H., Götting, H.-P. (2014). *Beck'scher Online-Kommentar Urheberrecht*. München: C.H. Beck (Stand Februar 2014).

Bamberger, H. G., Roth, H. (2014). *Beck'scher Online-Kommentar BGB*. München: C.H. Beck (Stand Mai 2014).

Bartsch, M. (2008). Die Vertraulichkeit und Integrität informationstechnischer Systeme als sonstiges Recht nach § 823 Abs. 1 BGB. *CR*, 613 ff.

Bernreuther, F. (2012). Anonymer Meinungsangriff und gestörte Kommunikationsparität. In S. Leible (Hrsg.), *Innovation und Recht im Internet*. Stuttgart: Boorberg.

Beyerbach, H. (2012). *Die geheime Unternehmensinformation. Grundrechtlich geschützte Betriebs- und Geschäftsgeheimnisse als Schranke einfachrechtlicher Informationsansprüche*. Tübingen: Mohr Siebeck.

Bieber, C., Eifert, M., Groß, T. & Lamla, J. (2009). *Soziale Netzwerke in der digitalen Welt. Das Internet zwischen egalitärer Teilhabe und ökonomischer Macht*. Frankfurt am Main (u. a.): Campus Verlag.

Bielefeldt, H. u. a. (Hrsg.) (2011). *Nothing to hide – nothing to fear? Datenschutz – Transparenz – Solidarität, Jahrbuch Menschenrechte 2011*. Wien (u. a.): Böhlau.

Bloch, A. (2013). *Meinungsvielfalt contra Medienmacht*. Berlin: Logos.

Borges, G., Schwenk, J., Stuckenberg C.-F. & Wegener, C. (2011). *Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte*. Berlin (u. a.): Springer.

Bruns, A. (2011). Persönlichkeitsschutz im Internet – Medienspezifisches Privileg oder medienpersönlichkeitsrechtlicher Standard? *AfP*, 421 ff.

Degenhart, C. (2011). Verfassungsfragen der Internet-Kommunikation, *CR*, 231 ff.

Diederichsen, A. (2012). Aktuelle Rechtsprechung des BGH zum Persönlichkeitsschutz. *AfP*, 217 ff.

Dilling, O. (2013). Persönlichkeitsschutz durch Selbstregulierung in der Wikipedia. *ZUM*, 380 ff.

Dörnhöfer, S. (2011). Am digitalen Pranger. In H. Bielefeldt (Hrsg), *Nothing to hide – nothing to fear? Jahrbuch Menschenrechte 2011*. Wien (u. a.): Böhlau.

Dreier, H. (Hrsg.) (2013). *Grundgesetz Kommentar* Band 1: Art. 1-19 GG. 3. Aufl. Tübingen: Mohr Siebeck.

Fechner, F. (2012). *Medienrecht*. 13. Aufl. Tübingen: Mohr Siebeck.

Fiedler, C. (2011), Technologieneutrale Pressefreiheit. *AfP*, 15 ff.

Frenz, W. (2012). Konkretisierte Abwägung zwischen Pressefreiheit und Persönlichkeitsschutz. *NJW*, 1039 ff.

Gersdorf, H., Paal, B. P. (Hrsg.) (2014). *Informations- und Medienrecht Kommentar*. München: C. H. Beck.

Glaser, A. (2012). Grundrechtlicher Schutz der Ehre im Internetzeitalter. *NVwZ*, 1432 ff.

Glück, O. (2005). *§24c KWG und das Recht auf informationelle Selbstbestimmung Eine Untersuchung der Verfassungsmäßigkeit des automatisierten Abrufs von Kontoinformationen*. Frankfurt am Main (u. a.): Peter Lang.

Götting, H.-P., Schertz, C., Seitz, W. (2008). *Handbuch des Persönlichkeitsrechts*. München: C.H. Beck.

Gounalakis, G. (2012). Verdachtsberichterstattung durch den Staatsanwalt. *NJW*, 1473 ff.

Gounalakis, G., Klein, C. (2010). Zulässigkeit von personenbezogenen Bewertungsplattformen. *NJW*, 566 ff.

Graef, R. O. (2009). Lehrerbewertung in einem Schülerportal – „spickmich.de". *ZUM*, 759 ff.

Habersack, M. (Hrsg.) (2013). *Münchener Kommentar zum Bürgerlichen Gesetzbuch. Kommentar*, Bd. 5: Schuldrecht – Besonderer Teil III, herausgegeben von F. J. Säcker und R. Rixecker. 6. Aufl. München: C. H. Beck.

Hager J., in: *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen. Band: Eckpfeiler des Zivilrechts*. 5. Aufl. 2014. München/Saarbrücken: Beck, Sellier – de Gruyter, JURIS.

Härting, N. (2009). „Prangerwirkung“ und „Zeitfaktor“. *CR*, 21 ff.
Härting, N., Schätzle, D. (2010). Rechtsverletzungen in Social Networks. *ITRB*, 39 ff.
Haug, S. (2014). Geldentschädigung bei Persönlichkeitsrechtsverletzung im Internet. *K&R*, 235 ff.
Heidrich, J., Forgó, N., Feldmann, T. (2011). *Heise Online-Recht*, Loseblatt (Stand: 3. EL Oktober 2011). Hannover: Heise.
Hirsch, B. (2008). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822. *NJOZ*, 1907 ff.
Hochhut, M. (2007), Schatten über der Meinungsfreiheit – Der „Babycaust“-Beschluss des BVerfG bricht mit der „Vermutung für die Zulässigkeit der freien Rede“. *NJW*, 192 ff.
Hoeren, T., Sieber, U., Holznagel, B. (Hrsg.) (2013). *Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs*, Loseblatt (Stand: 34. EL April 2013). München: C.H. Beck.
Hoeren, T. (2008). Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“? *MMR*, 356 ff.
Holznagel, B., Schumacher, P. (2011). Kommunikationsfreiheiten und Netzneutralität. In M. Kloepfer (Hrsg.), *Netzneutralität in der Informationsgesellschaft* (S. 47 ff.). Berlin: Duncker & Humblot.
Jaeckel, L. (2001). *Schutzpflichten im deutschen und europäischen Recht. Eine Untersuchung der deutschen Grundrechte, der Menschenrechte und Grundfreiheiten der EMRK sowie der Grundrechte und Grundfreiheiten der Europäischen Gemeinschaft*. Baden-Baden: Nomos Verlag.
Jarass, H. D. (1989). Das allgemeine Persönlichkeitsrecht im Grundgesetz. *NJW*, 857 ff.
Kamp, J. (2013). *Personenbewertungsportale. Eine datenschutzrechtliche und äußerungsrechtliche Untersuchung unter besonderer Berücksichtigung des Lehrerbewertungsportals spickmich.de*. München: C.H. Beck.
Kau, W. (1989). *Vom Persönlichkeitsschutz zum Funktionsschutz. Persönlichkeitsschutz juristischer Personen des Privatrechts in verfassungsrechtlicher Sicht*. Heidelberg: Müller.
Klickermann, P. H. (2007). Virtuelle Welten ohne Rechtsansprüche? *MMR*, 766 ff.
Kloepfer, M., Schärdel, F. (2009). Grundrechte für die Informationsgesellschaft – Datenschutz und Informationszugangsfreiheit ins Grundgesetz? *JZ*, 453 ff.
Köhler, C. M. (2011). *Persönlichkeitsrechte im Social Web – verlorene Grundrechte? Der Lehrer am Pranger in der virtuellen Welt*. Hamburg: Verlag Dr. Kovač.
Kraft, A. (1985). Gedanken zum allgemeinen Persönlichkeitsrecht juristischer Personen. In: H. Forkel, A. Kraft (Hrsg.), *Beiträge zum Schutz der Persönlichkeit und ihrer schöpferischen Leistungen. Festschrift für Heinrich Hubmann zum 70. Geburtstag*, (S. 201 ff.). Frankfurt am Main: Metzner.
Kunig, P. (1993). Der Grundsatz informationeller Selbstbestimmung. *Jura*, 595 ff.
Lacher, J. (2012). *Rechtliche Grenzen der Kommunikation über ärztliche Leistungen: Arztwerberecht, Ärzte-Rankings, Arztbewertungsportale*. Hamburg: Verlag Dr. Kovač.
Ladeur, K.-H., Gostomzyk, T. (2012). Der Schutz von Persönlichkeitsrechten gegen Meinungsäußerungen in Blogs. *NJW*, 710 ff.
Lauber-Rönsberg, A. (2014). Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet. Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen. *MMR*, 10 ff.
Lederer, B. (2009). *Quo vadis Bildberichterstattung? Eine Standortbestimmung im Spannungsfeld zwischen nationaler und europäischer Rechtsprechung*. München: Utz.
Leible, S. (Hrsg.) (2012). *Innovation und Recht im Internet*. Stuttgart (u. a.): Boorberg.
Libertus, M. (2007). Die Einwilligung als Voraussetzung für die Zulässigkeit von Bildnisaufnahmen und deren Verbreitung. *ZUM*, 621 ff.
Luch, A. D., Schulz, S. E. (2013). Die digitale Dimension der Grundrechte. *MMR*, 88 ff.
Martini, M. (2012). Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet. *JZ*, 1145 ff.

Maunz, T., Dürig, G. (2013). *Grundgesetz Kommentar*, Loseblatt (Stand: 70. EL Dezember 2013). München: C.H. Beck.
Maurer, H. (2011). *Allgemeines Verwaltungsrecht*. 18. Aufl. München: C.H. Beck.
Menzel, J., Müller-Terpitz, R. (Hrsg.) (2011). *Verfassungsrechtsprechung*. 2. Aufl. Tübingen: Mohr Siebeck.
Meyer-Ladewig, J. (2011). *Europäische Menschenrechtskonvention: EMRK, Handkommentar*. 3. Aufl. Baden-Baden: Nomos.
Möhlen, C. (2013). Das Recht auf Versammlungsfreiheit im Internet. *MMR*, 221 ff.
von Münch, I., Kunig, P. (Hrsg.) (2012). *Grundgesetz Kommentar*. Bd. 1: Präambel, Art. 1–69. 6. Aufl. München: C. H. Beck.
Münchener Kommentar zum Bürgerlichen Gesetzbuch → siehe unter Säcker.
Ohly, A. (2011). Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht? *AfP*, 428 ff.
Petershagen, J. (2011). Der Schutz des Rechts am eigenen Bild vor Hyperlinks. *NJW*, 705 ff.
Pieroth, B., Schlink, B., Kingreen, T. & Poscher, R. (2013). *Grundrechte Staatsrecht II*. 29. Aufl. Heidelberg: C.F. Müller.
Piltz, C. (2013). *Soziale Netzwerke im Internet – Eine Gefahr für das Persönlichkeitsrecht?* Frankfurt am Main: Peter Lang.
Roßnagel, A., Schnabel, C. (2008). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht. *NJW*, 3534 ff.
Roßnagel, A. (2009). Persönlichkeitsentfaltung zwischen Eigenverantwortung, gesellschaftlicher Selbstregulierung und staatlicher Regulierung. In C. Bieber, M. Eifert, T. Groß & J. Lamla (Hrsg.), *Soziale Netzwerke in der digitalen Welt*. Frankfurt am Main (u. a.): Campus Verlag.
Rüfner, W. (2011). Grundrechtsträger. In J. Isensee, P. Kirchhof (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland, B and IX: Allgemeine Grundrechtslehren*. 3. Aufl. (§ 196, S. 731 ff.). Heidelberg: C. F. Müller.
Sachs, M. (2011). *Grundgesetz. Kommentar*. 6. Aufl. München: C.H. Beck.
Säcker, F. J. (Hrsg.) (2012). *Münchener Kommentar zum Bürgerlichen Gesetzbuch. Kommentar*, Bd. 1: Allgemeiner Teil, herausgegeben von F. J. Säcker und R. Rixecker. 6. Aufl. München: C.H. Beck.
Schmitt Glaeser, W. (2001). Schutz der Privatsphäre. In J. Isensee, P. Kirchhof (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland, B and VI: Freiheitsrechte*. 2. Aufl. (§ 129, S. 41 ff.). Heidelberg: C. F. Müller.
Schwenke, T. (2012). Das virtuelle Hausrecht als Abwehrmaßnahme gegen „Shitstorms" innerhalb von Social Media Plattformen. *K & R*, 305 ff.
Seitz, W. (2003). Meinungsfundamentalismus. Von „Babycaust" und „rechtswidrigen Abtreibungen". *NJW*, 3523 ff.
Spindler, G. (2012). Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung. Gutachten F für den 69. Deutschen Juristentag München 2012. In: *Verhandlungen des 69. Deutschen Juristentages*. Beck. München: C.H. Beck.
Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien*. 2. Aufl. München: C.H. Beck.
Staudingers Kommentar zum BGB⟶ siehe Hager.
Stender-Vorwachs, J. (2014), Geldentschädigung wegen Persönlichkeitsrechtsverletzung im Internet. *GRUR-Prax*, 134.
Sticca, F., Perren, S., Ruggieri, S. & Alsaker, F. (2013). Longitudinal Risk Factors for Cyberbullying in Adolescence. *Journal of Community and Applied Social Psychology* 23 (1), 52 ff.
Voskamp, F., Kipker, D. (2013). Virtueller Pranger Internet. *DuD*, 787 ff.
Weigl, M. (2011). *Meinungsfreiheit contra Persönlichkeitsschutz am Bespiel von Web 2.0-Applikationen*. Hamburg: Verlag Dr. Kovač.
Wienen, A. V. (2012). Prangerwirkung von Onlineveröffentlichungen. *ITRB*, 160 ff.
Wieczorek, M. (2013). *Persönlichkeitsrecht und Meinungsfreiheit im Internet*. Frankfurt a. M.: Lang.
Wronka, G. (1972). *Das Persönlichkeitsrecht juristischer Personen*. Diss. Bonn 1972.

Kapitel 7
Strafrechtliche Aspekte der Social Media

Robert Esser

Inhalt

R. Esser (✉)
Inhaber des Lehrstuhls für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht sowie Wirtschaftsstrafrecht; Leiter der Forschungsstelle Human Rights in Criminal Proceedings (HRCP), Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: robert.esser@uni-passau.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_7

7.1 Einleitung

1 Der Einfluss des Internet auf das tägliche Leben hat in den letzten Jahren stetig zugenommen. In vielen Bereichen des Privat- und Berufslebens, in der Schule oder auch im Studium ist ein Austausch über dieses Medium kaum noch wegzudenken. Vor allem die Nutzung sozialer Netzwerke bietet eine bis vor wenigen Jahren nicht vorhandene „Kommunikations-Plattform" für Gleichgesinnte. Rund 76 % der deutschen Internetnutzer sind mittlerweile Mitglied in einem sozialen Netzwerk.[1] Innerhalb dieser Netzwerke erfolgt ein reger, oft gedankenloser Datenaustausch. Sensible personenbezogene Informationen und Daten werden freiwillig preisgegeben. Als „Gegenleistung" erhält man personenbezogene Informationen über andere Nutzer, die man auf herkömmlichen Austauschwegen gar nicht oder erst später erfahren hätte.[2]

2 Soziale Netzwerke stellen ohne Zweifel eine Bereicherung für Internetnutzer dar; von ihnen lässt sich in vielfältiger Weise profitieren, etwa durch ihre Nutzung als kostenlose Werbeplattform für Politiker, Prominente oder Unternehmen.[3] Aber es mehren sich auch die Bedenken. So darf nicht übersehen werden, dass auch das Internet und vor allem die Spezifika sozialer Netzwerke die Begehung von Straftaten auf sehr vielfältige Art und Weise fördern oder gar hervorrufen. Bei der Kriminalität im Internet geht es primär um Angriffe gegen die Integrität von IT-Systemen, den heimlichen Zugriff auf (betriebs-)interne Daten oder die Nutzung des Internet selbst als Tatwerkzeug für die Begehung von Alltagskriminalität (z. B. Betrugshandlungen, § 263 StGB).[4] Neuartige kriminelle Phänomene, nicht selten organisiert von

---

[1] Vgl. Viefhues, MMR-Aktuell 2011, 322686 (http://www.beck-online.beck.de); hierzu auch: Wernert, Internet-Kriminalität, S. 15.

[2] Vgl. Beukelmann, NJW 2012, 2617 (2618). Soweit sich ein detailliertes Profil einer Person durch die Nutzung einer Suchmaschine wie z. B. „Google" und deren Verlinkungen auf Drittseiten ergibt, hat der EuGH entschieden, dass der Betroffene einen Antrag an den Suchmaschinenbetreiber stellen kann, der nach sorgfältiger Abwägung zwischen dem Recht auf Privatsphäre des Einzelnen und dem Recht auf Information der Öffentlichkeit bei überwiegendem Interesse des Betroffenen die Daten zu löschen hat, EuGH, Urt. v. 13.4.2014 – C-131/12, Rn. 80, 92, 99.

[3] Vgl. hierzu: Zehn Jahre Facebook, SZ Nr. 27 v. 3.2.2014, S. 40.

[4] Zur Internetkriminalität allgemein: Sieber, Straftaten und Strafverfolgung im Internet, 2012; Eisele, Computer- und Medienstrafrecht, 2013; Marberth-Kubicki, Computer- und Internetstrafrecht, 2010; zu Cyberbedrohungen in der Praxis: Gräfin von Brühl/Brandenburg, ITRB 2013, 260.

Banden[5] begangen, sind etwa die Versendung von E-Mails, durch die das Opfer dazu veranlasst werden soll, einen Vorschuss auf eine angebliche ihm zustehende Geldtransaktion zu leisten, das „Erschleichen" von Passwörtern oder sonstiger personenbezogener Daten, mit denen anschließend Missbrauch betrieben wird (sog. „**Phishing**"; „Diebstahl der Persönlichkeit"), das gezielte Ausspähen von Personen in sozialen Netzwerken zum anschließenden Datenabzug (sog. „**Spare-Infection**") oder die Errichtung von Onlineportalen ohne ein dahinter tatsächlich bestehendes Unternehmen, durch die das Opfer zu einem Kauf von Waren veranlasst werden soll, die später nie versandt werden.[6]

Bei kriminellem Verhalten speziell in sozialen Netzwerken geht es zumeist um **3**
Straftaten aus dem zwischenmenschlichen Bereich und um Schutzrechtsverletzungen. Da die Begehungsformen häufig in erheblichem Maße Persönlichkeitsrechte[7] von Mitmenschen (Ehre, Privatsphäre[8]) betreffen, darf gerade die Störqualität eines strafrechtlich relevanten Verhaltens in sozialen Netzwerken für das geordnete Zusammenleben in einer Gesellschaft keinesfalls unterschätzt werden. Soziale Netzwerke bieten ein beträchtliches Maß an Anonymität und die Möglichkeit, mit Personen, nicht direkt (real) miteinander in Kontakt zu treten. Es kann daher zu Begegnungen und Entäußerungen kommen, die im „echten" Leben aufgrund der dort vorhandenen **sozialen Kontroll- und Feedback-Mechanismen** so nicht stattgefunden hätten (Prägung von Verhalten durch Nichtreaktion).[9] Gerade ehrverletzende Äußerungen (Beleidigungen; Rn. 43 ff.) und Straftaten gegen die persönliche Freiheit (bis hin zu Morddrohungen, Rn. 194) gehen im virtuellen Raum der sozialen Netzwerke leichter von statten als dies im realen Leben der Fall wäre, weil man häufig die unmittelbare

[5] Zum Aufwärtstrend dieser Kriminalitätsform auch auf internationaler Ebene, *Thomas de Maizière* zitiert nach Fuchs, Kriminalistik 2014, 174 (175).

[6] Vgl. Beukelmann, NJW 2012, 2617 (2618); Der unsichtbare Feind, SZ Nr. 14 v. 18./19.1.2014, S. 54; zu den daraus resultierenden Herausforderungen für das Technikrecht: Hilgendorf, JZ 2012, 825 (828); vgl. Koalitionsvertrag der Regierungsparteien CDU, CSU und SPD, Dezember 2013, 18. LegPeriode, http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile&v=2, S. 147, wonach eine zentrale Stelle für Phishing und ähnliche Delikte zur Verbesserung der Prävention und Erleichterung der Ermittlungen eingerichtet werden soll. Zur Verbrechensverabredung mit einem unbekannten Chatpartner vgl. BGH, NStZ 2011, 570 m. Anm. Weigend; hierzu auch Piazena, Das Verabreden, Auffordern und Anleiten zur Begehung von Straftaten unter Nutzung der Kommunikationsmöglichkeiten des Internets, S. 407 ff.

[7] Vgl. Piltz, Soziale Netzwerke im Internet: zu soziale Netzwerken als Gefahr für das Persönlichkeitsrecht aus zivil- und öffentlichrechtlicher Sicht.

[8] Kritisch zum Umgang mit der Privatsphäre im heutigen Zeitalter: Schertz/Höch, Privat war gestern. Wie Medien und Internet unsere Werte zerstören.

[9] Vgl. nur SZ v. 2.8.2010 (abrufbar unter: http://www.sueddeutsche.de/digital/trickreicher-hackerangriff-ein-kurzes-heisses-leben-1.982586) zum Fall „Robin Sage" (USA 2010), wodurch Mitglieder der US-Armee, des Geheimdienstes sowie Angestellte der Sicherheitsunternehmen und Auftragnehmern des Weißen Hauses höchst sensible und vertrauliche Informationen an den hinter dem Fakeprofil stehenden Hacker preisgegeben haben. Hierzu auch Günther, ArbRAktuell 2013, 223 (224).

Reaktion Betroffener nicht wahrnimmt. Das führt letztlich zur Entstehung normabweichender Wertevorstellungen im Netz, die sich in sozialen Netzwerken u. a. in einem speziellen „Umgangston“ ausdrücken.

4 Als kriminalitätsfördernd dürfte sich auch der Umstand auswirken, dass das Netzwerk (scheinbar) einen **virtuellen Schutzwall** um den Täter aufbaut. Dieser fühlt sich vor seinem Rechner „allein“, sprich unbeobachtet und geht davon aus, nicht erkannt zu werden. Neben dieser trügerischen Sicherheit bieten soziale Netzwerke aufgrund der bereitgestellten Technik (**Tatgelegenheit**) eine leichte und letztlich unbegrenzte Möglichkeit zur Verbreitung illegaler Daten und Schriften (vgl. § 11 Abs. 3 StGB; Rn. 88). Durch mangelnde Zugangsbarrieren und die dadurch bedingte „große Offenheit“ können sämtliche Inhalte schnell und unkompliziert auf das jeweilige Profil hochgeladen werden; dies eröffnet die Gefahr ebenso wie die bewusste Möglichkeit von strafrechtlich relevanten Urheberrechtsverstößen (Rn. 196).

5 Soziale Netzwerke bieten daher ohne Zweifel eine nicht zu unterschätzende Plattform für eine Vielzahl strafrechtlich relevanter Rechtsverstöße. Andererseits können solche Netzwerke auch zur **Prävention und Aufklärung von Straftaten** beitragen, weil die mit ihnen verbundenen Such- und Kontrollfunktionen ermittlungstechnische Verbesserungen und Fortschritte für die Strafverfolgungsbehörden bieten. Polizeidienststellen weisen in Aufklärungskampagnen längst nicht mehr nur auf das Gefahrenpotential sozialer Netzwerke hin. Einige Dienststellen auf Länderebene, darunter die Polizeidirektion Hannover als Vorreiter, nutzen sehr intensiv die Möglichkeiten solcher Netzwerke bei der Kriminalitätsbekämpfung, etwa in Form der Verbreitung von Fahndungsaufrufen, der Einbeziehung der Allgemeinheit in Ermittlungen und der Verbesserung der Verfolgungsintensität- und -qualität.[10] Eine weitere, bis vor wenigen Jahren nicht existente strafprozessuale Aufklärungsmaßnahme stellt der **Einsatz „virtueller Ermittler“** dar (Rn. 325 ff.). Dieser ermittelt verdeckt innerhalb sozialer Netzwerke und kann so an Informationen bezüglich tatverdächtiger Personen, ihres Umfeldes einschließlich einer möglichen Beziehung zu mutmaßlichen Opfern von Straftaten gelangen, die den Strafverfolgungsbehörden bei herkömmlichen Ermittlungsmaßnahmen nicht bekannt würden. In Hinblick auf diese prozessuale Thematik ist jedoch zu klären, wie diese Einsatzmöglichkeiten rechtlich einzuordnen sind, ob sie überhaupt rechtlich zulässig sind und welche Gefahren und Risiken (Datenschutz, Tatprovokation) damit verbunden sind.

Im Folgenden werden die Möglichkeiten und Gefahren sozialer Netzwerke aus der Perspektive des Strafrechts analysiert.

7.2 Anwendbarkeit deutschen Strafrechts

6 Die Nutzung sozialer Netzwerke erfolgt ohne Rücksicht auf nationale Grenzen. Eine Strafbarkeit nach deutschem Strafrecht wegen eines bestimmten Verhaltens in sozialen Netzwerken und eine damit verbundene Zuständigkeit deutscher

[10] Vgl. http://de-de.facebook.com/PolizeiHannover. Hierzu: Kolmey, DRiZ 2013, 242 ff.; May/Arnd, Kriminalistik 2013, 384 ff.; Beukelmann, NJW 2012, 2617 (2619).

Strafverfolgungsbehörden kommt allerdings nur in Betracht, wenn materiell deutsches Strafrecht auf den Sachverhalt angewendet werden kann.[11]

Nach dem **Territorialitätsprinzip** ist deutsches Strafrecht anwendbar, wenn die Tat im Inland begangen ist (§ 3 StGB). Wann eine Inlandstat vorliegt, regelt § 9 StGB. Konkret stellt sich die Frage nach dem Ort der Begehung eines möglicherweise strafrechtlich relevanten Handelns. Begangen ist eine Tat gemäß § 9 Abs. 1 StGB dort, wo ihr Handlungs- oder Erfolgsort liegt (Ubiquitätstheorie).[12] Bei über das Internet begangenen Straftaten handelt es sich nicht selten um sog. Distanzdelikte, bei denen beide Orte regelmäßig auseinanderfallen. **7**

Der **Handlungsort** ist bei einem Begehungsdelikt dort anzunehmen, wo der Täter eine auf die Tatbestandsverwirklichung gerichtete Tätigkeit im Ausführungsstadium der Tat erbringt.[13] Bei einem Auftreten in sozialen Netzwerken wäre dies z. B. das Einloggen und die Eingabe bzw. das Hochladen von Inhalten in das Nutzerprofil. Teilweise wird im Schrifttum auch der Server-Standort zum Handlungsort gezählt,[14] was in technischer Hinsicht und mangels Bestimmbarkeit nicht überzeugend ist.[15] **8**

Bei einem Handlungsort im Ausland wird das deutsche Strafrecht daher regelmäßig nur anwendbar sein, wenn der **Erfolgsort** im Inland liegt. Tatsächlich ist der Erfolgsort schon angesichts des Übertragungsmediums Internet häufig nur schwer zu bestimmen, zumal es sich bei den in Frage kommenden Delikten meist nicht um klassische Erfolgsdelikte handelt. **9**

Gerade bei **abstrakten Gefährdungsdelikten** wie § 130 StGB,[16] die also nicht den Eintritt eines konkreten Erfolges verlangen, lässt sich kein Erfolgsort konstruieren.[17] Ausgehend vom Wortlaut des § 9 Abs. 1 Alt. 3 StGB („an dem der zum Tatbestand gehörende Erfolg eingetreten ist“) entsteht der Eindruck, dass die Vorschrift zumindest für Gefährdungsdelikte nicht anwendbar ist.[18] **10**

Für den speziellen Fall eines „**abstrakt-konkreten**“ **Gefährdungsdelikts**, bei dem zwar die Schaffung einer abstrakten Gefahr ausreicht, die Eignung zu ihrer Herbeiführung aber anhand des konkreten Einzelfalls bestimmt werden muss, hat der BGH für den Fall der Verbreitung der sog. Auschwitz-Lüge vom Ausland **11**

---

[11] Zu den erheblichen Problemen, die sich dem deutschen Strafanwendungsrecht bei der Behandlung der Internetkriminalität stellen, vgl. zusammenfassend: Safferling, Internationales Strafrecht, § 3 Rn. 25 ff.

[12] Eser in: Schönke/Schröder, StGB, § 9 Rn. 3; Ambos, Internationales Strafrecht, § 1 Rn. 17; Safferling, Internationales Strafrecht, § 3 Rn. 16.

[13] Rackow, in: BeckOK-StGB, § 9 Rn. 2, zu den Unterlassungsdelikten Rn. 9 ff.

[14] Cornils, JZ 1999, 394 (396).

[15] Vgl. Safferling, Internationales Strafrecht, § 3 Rn. 26; Derksen, NJW 1997, 1878 (1880); siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 160 ff., zu diesem und weiteren Ansätzen, den Handlungsort zu bestimmen.

[16] Vgl. auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 167 ff., auch zum Streitstand bzgl. der Deliktsqualität des § 201a StGB.

[17] Ambos, in: MüKo-StGB, § 9 Rn. 27 ff.

[18] So etwa Hilgendorf, NJW 1997, 1873 (1876); Satzger, NStZ 1998, 112 (113 ff.); a. A. Sieber, NJW 1999, 2065 (2067 ff.); BGHSt 46, 212 (221 ff.) = NStZ 2001, 305 mit zustimmenden Anm. Hörnle = MMR 2001, 228 und m. krit. Anm. Clauß.

aus über das Internet entschieden, dass § 9 Abs. 1 Alt. 3 StGB anwendbar und Erfolgsort i. S. d. Vorschrift derjenige Ort sei, an dem die konkrete Tat ihre Gefährlichkeit im Hinblick auf das im Tatbestand umschriebene Rechtsgut entfalten könne.[19] Zusätzlich verlangt der BGH jedoch mit Blick auf den völkerrechtlichen Nichteinmischungsgrundsatz,[20] dass ein „völkerrechtlich legitimierender Anknüpfungspunkt" vorliegt.[21] Dies bedeutet nichts anderes, als dass die Tat zumindest irgendeinen „spezifischen Inlandsbezug"[22] haben muss. Bei dem zu beurteilenden Sachverhalt lag dieser Inlandsbezug nach Ansicht des BGH darin, dass die Tat ein gewichtiges inländisches Rechtsgut betraf und zudem „objektiv einen besonderen Bezug auf das Gebiet der Bundesrepublik Deutschland" aufwies.[23] Bei einem tatbestandsrelevanten Handeln (z. B. nach § 126 StGB – Störung des öffentlichen Friedens durch Androhung von Straftaten) im Ausland, müsse demnach wenigstens eine konkrete Eignung zur Störung des öffentlichen Friedens im Inland vorliegen.[24] Ob diese Rechtsprechung auf *alle* abstrakten Gefährdungsdelikte übertragbar ist,[25] scheint äußerst fraglich.

12 Um dennoch bei abstrakten Gefährdungsdelikten zu einer Anwendbarkeit deutschen Strafrechts zu gelangen, hat die Rechtsprechung den Handlungsbegriff drastisch erweitert und dahingehend verstanden, dass eine „inländische" Handlung schon dann vorliegt, wenn der Täter im Ausland eine Körperbewegung tätigt, die im Inland Auswirkungen hat.[26]

13 Auch das **aktive Personalitätsprinzip** kann bei Handlungen in sozialen Netzwerken die Anwendbarkeit deutschen Strafrechts begründen. Das gilt etwa für § 126 StGB, der tatbestandlich nicht nur den öffentlichen Frieden in Deutschland schützt, so dass insbesondere über § 7 Abs. 2 Nr. 1 StGB grundsätzlich auch eine Strafbarkeit für Taten in Betracht kommt, die lediglich den öffentlichen Frieden im Ausland betreffen.[27]

14 Nach dem in § 5 StGB verankerten **Schutzprinzip** gilt das deutsche Strafrecht auch für die dort aufgezählten wichtigen inländischen Rechtsgüter, unabhängig davon, wo die Tat begangen wurde. Überwiegend handelt es sich bei den aufgezählten

---

[19] BGHSt 46, 212 (221). Vgl. dazu auch Eisele, Computer- und Medienstrafrecht, § 3 Rn. 10 ff.
[20] Grundlegend dazu der Lotus-Fall des StIGH (Entscheidung v. 7.9.1927, Series A No. 10). Dazu auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 182 f.
[21] BGHSt 46, 212 (224).
[22] Eisele, Computer- und Medienstrafrecht, § 3 Rn. 16.
[23] BGHSt 46, 212 (224). Kritisch dazu Ambos in: MüKo-StGB, § 9 Rn. 35. Zustimmend: Safferling, Internationales Strafrecht, § 3 Rn. 30.
[24] Rackow in: BeckOK-StGB, § 126 Rn. 23, kritisch gegenüber einer derart weiten Auslegung: Fischer, StGB, § 126 Rn. 6.
[25] Zweifel hegt insoweit zu Recht: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 185 f.
[26] KG, NJW 1999, 3500 (3502): „Eine teilweise Verwirklichung der Handlung im Inland liegt auch vor, wenn Wirkungen des Verhaltens, die nach der tatbestandlichen Handlungsbeschreibung als deren Bestandteil zu betrachten sind, dort eintreten." Ähnlich Werle/Jeßberger, JuS 2001, 35 (39).
[27] Rudolphi/Stein, in: SK-StGB, § 126 Rn. 6; zum insoweit vergleichbaren § 125 StGB: OLG Celle, NJW 2001, 2734 (Landfriedensbruch eines Deutschen im Ausland).

Tatbeständen um Staatsschutzdelikte sowie Delikte, die einen Auslandsbezug aufweisen und sich gegen eine Person richten, die im Bundesgebiet wenigstens ihren Wohnsitz hat (**sog. passives Personalitätsprinzip**, z. B. bei Kindesentführung, § 5 Nr. 6a StGB). In § 5 Nr. 8 StGB sind Straftaten gegen die sexuelle Selbstbestimmung (§§ 174 Abs. 1, 3; 176–176b; 182 StGB) aufgeführt, die nicht selten über Kontakte in sozialen Netzwerken vorbereitet werden. Diese sind in den Fällen des § 174 Abs. 1, 3 StGB dann strafbar, wenn sowohl Täter und Opfer Deutsche sind und bei §§ 176–176b, 182 StGB dann, wenn der Täter Deutscher ist. Unmittelbar die Kontaktaufnahme über soziale Netzwerke für spätere sexuelle Handlungen betrifft § 176 Abs. 4 Nr. 3 StGB (sog. „**Grooming**", siehe Rn. 18, 114 ff.). Damit unterfallen jedoch nicht alle aus der Richtlinie 2011/93/EU vom 13.12.2011[28] (vgl. hierzu Rn. 18) und den auf der Ebene des Europarates geschlossenen Konventionen vom 25.10.2007[29] und 11.5.2011[30] resultierenden Straftatbestände der deutschen Gerichtsbarkeit. Ein im April 2014 vorgelegter Referentenentwurf (RefE) des BMJV[31] über ein Gesetz zur Änderung des Strafgesetzbuchs will gerade diese europäischen Vorgaben zum Sexualstrafrecht umsetzen und dementsprechend den Katalog von § 5 StGB erweitern. Künftig soll sich die Anwendbarkeit deutschen Strafrechts in § 5 Nr. 8 StGB-E auch auf die Straftaten nach §§ 174 Abs. 1, 2, 4; 177–179 StGB erstrecken, wobei es nicht länger gemäß § 5 Nr. 8a StGB auf die deutsche Staatszugehörigkeit und den Lebensmittelpunkt des Opfers in Deutschland zum Zeitpunkt der Tat ankommen soll.[32]

15 § 6 StGB schützt auf der Grundlage des Weltrechtsprinzips – ähnlich dem Schutzprinzip (§ 5 StGB) – bestimmte **international geschützte Rechtsgüter** unabhängig von dem Ort, an dem die Tat begangen wurde. Im Bereich der sozialen Netzwerke besonders relevant ist § 6 Nr. 6 StGB, der für die Verbreitung pornographischer Schriften nach §§ 184a; 184b Abs. 1, 3; 184c Abs. 1, 3 StGB (sog. harte Pornographie) weltweit deutsches Recht für anwendbar erklärt.[33] Auch im Fall des Weltrechtsprinzips ist – nach allerdings umstrittener Auffassung – erforderlich, dass aufgrund des

---

[28] Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates v. 13.12.2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. EU Nr. L 335 v. 17.12.2011, S. 1 (berichtigt in: ABl. EU Nr. L 18 v. 21.1.2012, S. 7 [früher RL 2011/92/EU]).

[29] Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch v. 25.10.2000 (CETS 201).

[30] Übereinkommen des Europarates zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt v. 11.5.2011 (CETS 210).

[31] Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht, Bearbeitungsstand 28.4.2014, http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/Gesetz-Aenderung-StGB-Umsetzung-europaeischer-Vorgaben-zum-Sexualstrafrecht.html?nn=3433226 (Stand: 8.5.2014); zwischenzeitlich ist der Gesetzentwurf der Bundesregierung ergangen, BT- Drucksache 18/2601 v. 23.09.2014.

[32] RefE (Fn. 31), S. 23 f.

[33] Ambos, Internationales Strafrecht, § 3 Rn. 106 hält die Norm für völkerrechtswidrig, da die Bundesrepublik völkerrechtlich nicht (mehr) ermächtigt sei, die Verbreitung harter Pornographie

völkerrechtlichen Nichteinmischungsgrundsatzes (s. o.) ein gewisser Inlandsbezug der Tat besteht.[34] Dies gilt mindestens bei den Taten, die nicht vom völkerrechtlichen Weltrechtsprinzip umfasst sind, also solchen, die keine universell anerkannten Rechtsgüter verletzen. Nur bei Letzteren kann der völkerrechtliche Nichteinmischungsgrundsatz unangewendet bleiben, weil alle Staaten an der Verfolgung eines bestimmten Delikts (z. B. der Piraterie) Interesse haben.[35] Für die Internetstraftaten bedeutet dies, dass zumeist ein innerstaatlicher Anknüpfungspunkt zu fordern sein wird; schließlich ist etwa die strafrechtliche Bekämpfung der Verbreitung „harter" Pornographie nicht vom völkerrechtlichen Weltrechtsprinzip umfasst.

7.3 Internationale Rahmenbedingungen und Pönalisierungspflichten

7.3.1 Europäische Union

7.3.1.1 Rahmenbeschlüsse und Richtlinien

16 Auf der Ebene der EU hatte bereits der Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über **Angriffe auf Informationssysteme**[36] die wachsende Besorgnis über Terroranschläge auf Informationssysteme zum Ausdruck gebracht. Solche werden zunehmend auch über das Internet organisiert, mitunter auch über soziale Netzwerke. Die unionsweite Angleichung des Strafrechts im Bereich der Angriffe auf Informationssysteme, um eine möglichst effiziente polizeiliche und justizielle Zusammenarbeit bei Straftaten in Verbindung mit Angriffen auf Informationssysteme sicherzustellen, wird durch die Richtlinie 2013/40/EU[37] weiter vorangetrieben.

17 Der **Rahmenbeschluss 2008/913/JI** des Rates vom 28.11.2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von **Rassismus und Fremdenfeindlichkeit**[38] verpflichtet die Mitgliedstaaten dazu, rassistische und fremdenfeindliche Taten, die vorsätzlich begangen werden, unter Strafe zu stellen (Art. 1). Da die Taten (Art. 1 lit. a) auch durch öffentliches Verbreiten begangen werden können (Art. 1 lit. b) oder bereits von vornherein eine öffentliche Handlungsweise

weltweit nach deutschem Strafrecht zu bestrafen. Werle/Jeßberger, in: LK-StGB, § 6 Rn. 88 plädieren für eine völkerrechtskonforme Auslegung.

[34] So auch BGHSt 45, 65 (66) = NStZ 1999, 396 m. Anm. *Ambos* = JZ 1999, 1176 m. Anm. Werle = JR 2000, 202 m. Anm. Lagodny/Nill-Theobald; BGH, StV 1999, 240.

[35] So auch Ambos, in: MüKo-StGB, § 6 Rn. 4; ders., § 3 Rn. 93, 102; Werle/Jeßberger, in: LK-StGB, § 6 Rn. 34 f.; a. A. Eser, in: Schönke/Schröder, StGB, § 6 Rn. 1.

[36] ABl. EU Nr. L 69 v. 16.03.2005, S. 67.

[37] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. EU Nr. L 218 v. 14.8.2013, S. 8.

[38] ABl. EU Nr. L 328 v. 6.12.2008, S. 55; zur Umsetzung auf nationaler Ebene: KOM (2014) 27 v. 27.1.2014.

voraussetzen, können sie auch über soziale Netzwerke oder Informationssysteme begangen werden (was insoweit auch Art. 9 bestätigt; siehe hierzu § 130 StGB, Rn. 31). Die gerichtliche Zuständigkeit des Mitgliedsstaates muss auch dann begründet sein, wenn die Tat ganz oder teilweise in seinem Hoheitsgebiet im Rahmen eines Informationssystems begangen wird (Art. 9 I lit. a, II), soweit der Täter physisch im Hoheitsgebiet anwesend ist (Art. 9 II lit. a) oder die Handlungen Inhalte betreffen, die sich in einem in seinem Hoheitsgebiet betriebenen Informationssystem befinden (Art. 9 II lit. b).

18 Die nach dem Inkrafttreten des Vertrags von Lissabon aufgelegte **Richtlinie 2011/93/EUI** des Europäischen Parlaments und des Rates vom 13.12.2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie [...][39] verpflichtet die Mitgliedstaaten dazu, schwere Formen des sexuellen Missbrauchs und der sexuellen Ausbeutung unter Strafe zu stellen. Dazu gehören insbesondere die besonderen Formen, die durch Informations- und Kommunikationstechnologien – wie etwa über soziale Netzwerke – erleichtert werden (ErwG Nr. 12), wie etwa die Kontaktaufnahme zu Kindern für sexuelle Zwecke (Art. 6 I; sog. „**Grooming**"; vgl. § 176 IV Nr. 3 StGB; Rn. 14, 109). Ebenso ist der wissentliche Zugriff auf Kinderpornografie mittels Informations- und Kommunikationstechnologie unter Strafe zu stellen (Art. 5 Abs. 3; ErwG Nr. 18). Art. 5 III sieht dafür eine Freiheitsstrafe im Höchstmaß von mindestens einem Jahr vor. Neben der Kinderpornografie (Art. 2 lit. c.) sowie der Kinderprostitution (Art. 2 lit. d) umfasst die RL auch die pornografische Darbietung als Live-Zurschaustellung mittels Informations- und Kommunikationstechnologie (Art. 2 lit. e). Von der RL 2011/93/EU erfasste Straftaten, die mittels Informations- und Kommunikationstechnologie verübt werden, auf die der Zugriff aus dem Hoheitsgebiet eines Mitgliedstaates erfolgt, sollen unter dessen gerichtliche Zuständigkeit fallen, unabhängig davon, ob sich die Technologie im Hoheitsgebiet befindet (Art. 17 Abs. 3). Art. 25 verpflichtet die Mitgliedstaaten dazu, Websites, die Kinderpornografie enthalten oder verbreiten, zu entfernen (Art. 25 Abs. 1) und stellt die Sperre solcher Websites in das Ermessen der Staaten (Art. 25 Abs. 2).

7.3.1.2 Europol – European Cybercrime Center

19 Das Europäische Polizeiamt (Europol) in Den Haag hat ein **European Cybercrime Center (ECC)** eingerichtet, das am 11.1.2013 die Arbeit aufgenommen hat. Im Mittelpunkt seiner Tätigkeit stehen die Bekämpfung der bandenmäßigen Begehung von Cyberkriminalität, insbesondere des gewerbsmäßigen Internetbetrugs, der sexuellen Ausbeutung von Kindern im Internet sowie von Cyberattacken auf Informations- und Datensysteme. Die zentrale Speicherung aller Informationen bzgl. Cyberkriminalität gehört zu den Hauptaufgaben des Zentrums. Es soll die EU-Staaten bei der

[39] ABl. EU Nr. L 335 v. 17.12.2011, S. 1, berichtigt in ABl. EU Nr. L 18 v. 21.1.2012, S. 7.

Verfolgung der Kriminalität im Netz, insbesondere auch durch die Entwicklung neuer technischer Möglichkeiten, unterstützen. Das ECC hat die Gefahren, die soziale Netzwerke in sich bergen, erkannt und will sich auch dieser Bedrohungslage künftig verstärkt zuwenden.[40]

Am 1.9.2014 haben Europol und das BKA, unterstützt von anderen internationalen Experten die Arbeit in der **„Joint Cybercrime Action taskforce" (J-CAT)** in Den Haag aufgenommen, mit der alle Formen von Cybercrime effektiv bekämpft werden sollen (BT-Drucks. 18/2674).

7.3.2 Europarat

20 Auf der Ebene des Europarates verpflichtet das **Übereinkommen über Computerkriminalität v. 23.11.2001 (ETS 185)** die Staaten u. a. zu einem strafrechtlichen Vorgehen gegen computerbezogene (Art. 7–8; computerbezogene Fälschung/Betrug) und inhaltsbezogene Straftaten (Art. 9 – Kinderpornographie) sowie gegen Straftaten in Zusammenhang mit einer Verletzung des Urheberrechts und verwandter Schutzrechte (Art. 10; siehe hierzu: § 106 UrhG; Rn. 193).

21 Nach dem **Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art v. 28.1.2003 (ETS 189)** ist innerstaatlich das Verbreiten oder anderweitige Öffentlich-Verfügbar-Machen rassistischen oder fremdenfeindlichen Materials über ein Computersystem (Art. 3 Abs. 1), die Drohung, eine schwere Straftat zu begehen, gerichtet mittels eines Computersystems gegen eine Person oder eine Personengruppe (Art. 4), die öffentliche Beleidigung einer Person oder einer Personengruppe mittels eines Computersystems (Art. 5) sowie die Leugnung, grobe Verharmlosung, Billigung oder Rechtfertigung von Völkermord oder Verbrechen gegen die Menschlichkeit durch das Verbreiten oder anderweitiges Öffentlich-Verfügbar-Machen von Material über ein Computersystem (Art. 6) unter Strafe zu stellen.

22 Das **Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch v. 25.10.2007 (CETS 201)** verlangt die Pönalisierung von Handlungen, mit denen sich eine Person rechtswidrig und wissentlich Zugang zu Kinderpornografie durch Informations- und Kommunikationstechnologie verschafft (Art. 20 Abs. 1 *lit.* f).

---

[40] Umfassend hierzu: First Year Report, abrufbar unter: https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf. Zur erfolgreichen Aufnahme der Koordinierungsfunktion *Thomas de Maizière*, zitiert nach Fuchs, Kriminalistik 2014, 174 (175).

7.4 Kriminalitätslagebild/Polizeiliche Kriminalstatistik

Der vom Bundeskriminalamt (BKA) herausgegebenen Polizeilichen Kriminalstatistik (PKS) für das Jahr 2013[41] ist zu entnehmen, dass knapp 257.486 Verdachtsfälle von Straftaten im Zusammenhang mit der Nutzung des Tatmittels Internet verzeichnet wurden, wobei diese Deliktsgruppe hauptsächlich **Betrugsdelikte** umfasst. Dies bedeutet einen Anstief von 12,2 % gegenüber dem Jahr 2012. Die Verbreitung pornographischer Schriften (§ 184 StGB) über das Internet stief gegenüber dem Jahr 2012 von rund 5.000 Fälle auf 6.600 Fälle. Im Vergleich zum Vorjahr ist allerdings mit etwa 13.740 Fällen im Jahr 2013 ein leichter Rückgang des Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB) von rund 10,8 % zu verzeichnen.[42] Straftaten im Zusammenhang mit der Verletzung von Urheberrechtsbestimmungen machten lediglich 7 % der gesamten im Jahr 2013 verzeichneten Verdachtslagen unter Nutzung des Tatmittels Internet aus.[43] Im Vergleich zum Vorjahr bedeutet dies einen Anstieg von 5,5 %. **23**

Die Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) nahm um 24,6 % auf knapp 900 Fälle zu. Bei den Beleidigungsdelikten (§§ 185 ff. StGB) ist ein leichter Anstieg um 3,0 % auf rund als 223.000 Fälle festzustellen.[44] Allerdings ist in diesen Bereichen kein spezifischer Zusammenhang mit der Nutzung des Internet durch die PKS ausgewiesen. **24**

Unter diesem Gesichtspunkt ist insgesamt kritisch anzumerken, dass die PKS 2013 lediglich einzelne Tatbestände bzw. eher abstrakt bezeichnete Deliktsgruppen anführt. Dies hat zudem als Verdachtslage zur Folge, dass aus der **Ausgangsstatistik durch die Polizei** nicht ersichtlich ist, in welchem konkreten Zusammenhang die Delikte registriert wurden. Eine eindeutige Aussage über die Zu- oder Abnahme der im Zusammenhang mit sozialen Netzwerken begangenen Straftaten lässt sich daher auf der Grundlage der PKS 2013 erst recht nicht treffen. Ein Hinweis auf die strafrechtliche Relevanz sog. neuer Medien findet sich allerdings hinsichtlich der **Präventionsarbeit** im Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK).[45] **25**

---

[41] Aufrufbar unter www.bka.de/nn_193486/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html

[42] PKS 2013 (Fn. 41), S. 9.

[43] PKS 2013 (Fn. 41), S. 17.

[44] PKS 2013 (Fn. 41), S. 73.

[45] PKS 2013 (Fn. 41), S. 14.

7.5 Materielle Straftatbestände

7.5.1 Störung des öffentlichen Friedens (§ 126 StGB)

26 § 126 StGB untersagt die Androhung bzw. Vortäuschung der Begehung bestimmter schwerwiegender Straftaten in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören. Die Norm schützt nach h.M. den **öffentlichen Frieden**.[46] Dessen Störung verlangt eine allgemeine Beunruhigung der deutschen Bevölkerung, zumindest jedoch einer nicht unerheblichen Personenzahl.[47] Da es sich bei der Norm nicht um ein konkretes Gefährdungsdelikt handelt, ist es nicht erforderlich, dass der öffentliche Friede durch die Handlung des Täters tatsächlich gestört wird. Richtiger Ansicht nach reicht „die generelle Gefährlichkeit einer konkreten Tat" aus (zu daraus resultierenden Problemen in Hinblick auf die Anwendbarkeit deutschen Strafrechts siehe Rn. 6 ff.).[48]

27 Keine Besonderheiten ergeben sich bei einer Tatbegehung im Internet hinsichtlich der beiden Tathandlungsalternativen, dem **Androhen** (Ankündigung einer Katalogtat, auf deren Verwirklichung der Täter Einfluss zu haben vorgibt;[49] Absatz 1) bzw. **Vortäuschen** (intendiertes Erregen oder Unterhalten eines Irrtums, dass die Begehung einer Katalogtat bevorstehe;[50] Absatz 2) einer der in § 126 Abs. 1 Nr. 1–7 StGB genannten Straftaten, solange die geforderte Störung des öffentlichen Friedens als Wirkung in der Öffentlichkeit nahe liegt.[51]

28 Der Tatbestand fordert weiterhin die **konkrete Eignung** der Tathandlung, den öffentlichen Frieden zu stören.[52] Eine nicht ernst zu nehmende Äußerung ist schon tatbestandlich nicht erfasst.[53]

29 Die Tathandlung selbst muss nicht öffentlich erfolgen, es kann vielmehr das Handeln gegenüber einer einzelnen Person genügen, wenn nach den konkreten Umständen damit zu rechnen ist, dass die Ankündigung einer **breiteren Öffentlichkeit** bekannt wird.[54] Das ist insbesondere dann anzunehmen, wenn die Ankündigung gegenüber einem nicht näher eingegrenzten Kreis von Personen, von denen Diskretion nicht zu erwarten ist, oder gegenüber einem unmittelbar Betroffenen erfolgt, wenn anzunehmen ist, dass dieser sich (etwa aus Sorge um das mutmaßliche Opfer,

---

[46] Rackow, in: BeckOK-StGB, § 126 Rn. 5.
[47] BGH, NStZ-RR 2011, 109; AG Wolfratshausen, StV 2013, 709.
[48] Schäfer, in: MüKo-StGB, § 126 Rn. 5 f. (m.w.N. zum Meinungsstreit).
[49] Ostendorf, in: NK-StGB, § 126 Rn. 13.
[50] Lackner/Kühl, StGB, § 126 Rn. 3.
[51] Schäfer, in: MüKo-StGB, § 126 Rn. 12.
[52] BGHSt 46, 212 (218).
[53] Schäfer, in: MüKo-StGB, § 126 Rn. 30.
[54] BGHSt 29, 26 (27) = BGH, NJW 1979, 1992.

Empörung oder Wichtigtuerei) an die Öffentlichkeit wendet.[55] So ist die **Ankündigung eines Amoklaufs** im Netzwerk *Facebook*, und sei dieser auch nur unbestimmt, grundsätzlich geeignet, den öffentlichen Frieden zu stören.[56]

Mit Ausnahme des Vortäuschens (Absatz 2; dieses muss wider besseres Wissen erfolgen), genügt bei § 126 StGB hinsichtlich aller Merkmale des objektiven Tatbestands **bedingter Vorsatz**.[57] Ein entsprechender Nachweis kann scheitern, wenn der Handelnde davon ausgegangen ist, dass lediglich eine bestimmte Zahl von Personen („Freunden"), die unbeschränkten Zutritt zur Seite eines sozialen Netzwerks haben, den tatbestandlich relevanten Eintrag lesen und nicht an dritte Personen weitergeben. Unklar bleibt, ab wie vielen Personen mit einer Zugangsmöglichkeit von einer erheblichen Anzahl auszugehen ist.[58] **30**

7.5.2 Volksverhetzung (§ 130 StGB)

§ 130 StGB vereint fünf weitgehend selbstständige Delikte. Nach § 130 Abs. 1 StGB wird derjenige bestraft, der in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, zum Hass gegen bestimmte nationale, rassische, religiöse oder ethnische Gruppen aufruft (Nr. 1) oder diese öffentlich verächtlich macht (Nr. 2). § 130 Abs. 2 StGB stellt den Aufruf zum Hass gegen bestimmte Gruppen mittels Schriften[59] (Nr. 1) oder durch die Verbreitung über Rundfunk, Medien- und Teledienste[60] (Nr. 2) unter Strafe. § 130 Abs. 3 StGB betrifft die sog. **Holocaust-/Auschwitzlüge**, also das öffentliche Billigen, Verleumden oder Verharmlosen des von den Nationalsozialisten in der Zeit von 1933–1945 begangenen Völkermordes (vgl. § 6 VStGB) in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören. § 130 Abs. 4 StGB stellt das öffentliche Billigen, Verherrlichen oder Rechtfertigen der nationalsozialistischen Gewaltherrschaft unter Strafe, wenn dadurch der öffentliche Friede in einer die Würde der Opfer verletzenden Weise gestört wird.[61] § 130 Abs. 5 StGB untersagt das Verbreiten von Erklärungen des Inhalts von § 130 Abs. 3, 4 StGB mittels Schriften. **31**

---

[55] BGHSt 34, 329 (332) = BGH, NJW 1987, 1898; BGH, NStZ 2010, 570.

[56] LG Aachen, Kriminalistik 2013, 169 = BeckRS 2012, 24704: Ein 15 Jähriger (J) hatte auf Facebook folgenden Eintrag eingestellt: „Leute die ich so gar nicht leiden kann, haben fb (Facebook), wenn die mir fa (Freundschaftsanfragen) schicken, lauf ich Amok". Das AG als Vorinstanz hatte den J zur Ableistung von 20 Stunden Sozialdienst verurteilt. Das LG verneinte den erforderlichen Vorsatz für den Öffentlichkeitsbezug der Tat (siehe Rn. 30). Siehe ferner: AG Wolfratshausen, StV 2013, 709.

[57] Sternberg-Lieben in: Schönke/Schröder, StGB, § 126 Rn. 12.

[58] Vgl. Sieber, FD-StrafR 2012, 340802; im Fall des LG Aachen (Fn. 56): 40 Personen; AG Wolfratshausen (Fn. 56): 25–35 Personen.

[59] Zum Vorschlag des BMJV, den Singular „Schrift" zu verwenden, vgl. Art. 1 Nr. 5 RefE (Fn. 31), S. 28.

[60] Nach Art. 1 Nr. 5 RefE (Fn. 31), S. 29 soll künftig auf die Tathandlung des „Öffentlichen Zugänglichmachens" abgestellt werden.

[61] Nach § 130 Abs. 5 S. 2 StGB-E des RefE (Fn. 31), S. 29, soll auch das Zugänglichmachen von Inhalten nach § 130 Abs. 3, 4 StGB via Rundfunk oder Telemedien strafbar sein.

Der RefE des BMJV vom April 2014 sieht zudem in § 130 Abs. 6 StGB-E künftig die Strafbarkeit des Versuchs vor.[62]

32 Der Tatbestand wurde in jüngerer Zeit durch die Umsetzung des **Rahmenbeschlusses 2008/913/JI zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit vom 28.11.2008**[63] und des **Zusatzprotokolls zum Übereinkommen des Europarates über Computerkriminalität**[64] verändert. Als Folge davon ist er rahmenbeschluss- bzw. völkerrechtskonform auszulegen.[65]

33 Gegen § 130 StGB wurden und werden immer wieder verfassungsrechtliche Bedenken geäußert, da die Vorschrift einen rechtfertigungsbedürftigen Eingriff in die Meinungsfreiheit (Art. 5 Abs. 1 GG) darstellt.[66]

34 § 130 Abs. 1 und 3 StGB stellen nach h. M. **abstrakt-konkrete Gefährdungsdelikte** dar („geeignet ist, den öffentlichen Frieden zu stören"; dazu bereits Rn. 26), während § 130 Abs. 2 StGB ein abstraktes Gefährdungsdelikt und § 130 Abs. 4 StGB ein Erfolgsdelikt darstellt („wer ... den öffentlichen Frieden ... stört"). Da die von § 130 StGB erfassten Rechtsgüter bei Weitem nicht in allen Staaten der Erde einen vergleichbaren strafrechtlichen Schutz genießen, kommt es immer wieder zu schwierigen Fragen bzgl. der Anwendbarkeit deutschen Strafrechts. Dies ist insbesondere der Fall, wenn die Tat über das Internet begangen wird.[67]

35 Im Hinblick auf soziale Netzwerke bestehen besondere Problemfelder – neben der Anwendbarkeit deutschen Strafrechts – vor allem bei der Bestimmung der **Geeignetheit zur Störung** des öffentlichen Friedens bei § 130 Abs. 1, 3 StGB. Zwar ist die Verbreitung von volksverhetzenden Aussagen über das Internet dazu grundsätzlich geeignet, da die Aussagen einer größeren Öffentlichkeit zur Kenntnis gelangen (vgl. Rn. 29).[68] Allerdings würde das Tatbestandsmerkmal gänzlich konturenlos, wenn man allein die Erreichbarkeit der Aussage für die deutsche Bevölkerung über das Internet ausreichen ließe. Vielmehr ist zusätzlich zu fordern, dass weitere Umstände hinzutreten, die die Aussage geeignet erscheinen lassen, den öffentlichen Frieden zu stören.[69]

---

[62] Vgl. Art. 1 Nr. 5 RefE (Fn. 31), S. 30.
[63] ABl. EU Nr. L 328 v. 6.12.2008, S. 55 (vgl. 7.3.1, Rn. 17).
[64] Vom 28.1.2003, ETS Nr. 189.
[65] Vgl. zur Änderung des § 130 StGB umfassend: Hellmann/Gärtner, NJW 2011, 961.
[66] Vgl. etwa Bertram, NJW 2005, 1476 (1477 f.); Überblick über den Meinungsstand bei Krauß in: LK-StGB, § 130 Rn. 19 ff.
[67] Vgl. etwa BGHSt 46, 212 – Verbreitung der Auschwitzlüge über das Internet vom Ausland aus. Umfassend zur Anwendbarkeit deutschen Strafrechts bei volksverhetzenden Aussagen, die über das Internet vom Ausland verbreitet werden, Morozinis, GA 158 (2011), 475 (483 ff.).
[68] BGHSt 46, 212 (219 f.).
[69] Vgl. BGH, NStZ 2007, 216 (217) für ein Pamphlet mit rechtsextremem Inhalt, dessen Inhalt nach Ansicht des BGH vom aufgeklärten Teil der Bevölkerung nicht in der Weise ernstgenommen werden konnte, dass daraus eine Störung des öffentlichen Friedens zu resultieren vermochte.

Weiterhin besteht auch im Rahmen von § 130 StGB die Problematik des von der Rechtsprechung vertretenen spezifischen **Verbreitungsbegriffes** bei Internetstraftaten (vgl. Rn. 98).[70] **36**

7.5.3 Öffentliche Aufforderung zu Straftaten (§ 111 StGB)

Nach § 111 Abs. 1 StGB wird – im Falle der späteren Begehung einer entsprechenden rechtswidrigen Tat (§ 11 Nr. 5 StGB) – wie ein Anstifter (§ 26 StGB) bestraft, wer öffentlich (vgl. Rn. 83) oder durch das Verbreiten (Rn. 83) von Schriften (§ 11 Abs. 3 StGB; Rn. 88)[71] zu dieser Tat aufgefordert hat.[72] Die Norm stellt eine unselbständige (d. h. an die Begehung der späteren Tat) anknüpfende Form der Teilnahme dar, deren Normierung notwendig ist, weil die tatgegenständliche Aufforderung aufgrund der Art der Begehung häufig nicht die engen Voraussetzungen der Anstiftung (§ 26 StGB) erfüllt.[73] In sozialen Netzwerken kann die Norm vor allem bei Aufrufen zur Billigung oder Förderung von Straftaten eine Rolle spielen („Unterstützerappell"), speziell im Fall des Aufrufs zur „**Lynchjustiz**".[74] **37**

7.5.4 Beleidigungsdelikte (§§ 185 ff. StGB)

7.5.4.1 Spezifika von ehrverletzenden Handlungen im Internet

Die Beleidigungsdelikte (14. Abschnitt des StGB) stellen eine der Deliktsgruppen dar, die durch das Internet in den letzten Jahren zunehmend an Bedeutung gewonnen haben. Insbesondere die ohne Rücksicht auf nationale Grenzen erfolgende Nutzung der größten sozialen Netzwerke Facebook und Twitter, sowie im deutschsprachigen Raum Studi.vz bzw. das Anfang 2013 eingestellte Schüler.vz als zentrale Kommunikationsplattformen im Internet, stellen die Straftatbestände der §§ 185, 186 und 187 **38**

---

[70] Dieser wird in Anbetracht der quantitativ stärkeren Bedeutung der §§ 184 ff. StGB für eine Begehung über soziale Netzwerke dort dargestellt (siehe Rn. 98).

[71] Die ebenfalls vorgesehene Begehungsweise „*in einer Versammlung*" ist für soziale Netzwerke irrelevant.

[72] Bleibt die Aufforderung ohne Erfolg, so wird der Auffordernde ebenfalls bestraft (§ 111 Abs. 2 S. 1 StGB). Die Strafe darf dann aber nicht schwerer sein als die, die für den Fall angedroht ist, dass die Aufforderung Erfolg hat (§ 111 Abs. 2 S. 2 StGB mit Verweis auf Absatz 1).

[73] Hierzu: Krey/Esser, Strafrecht Allgemeiner Teil, Rn. 1052 (Konkretisierung der Person des Täters und der Haupttat); Ostendorf et al., NStZ 2012, 529 (532).

[74] Vgl. hierzu: Ostendorf et al., NStZ 2012, 529 (531); OLG Celle, NStZ 2013, 720 m. Anm. Jahn, JuS 2014, 463 (Eintragung in eine Unterstützerliste eines Aufrufs – „Schottern" von Gleisanlagen aus Anlass eines Castortransportes, § 316b Abs. 1 Nr. 1 StGB – auf einer frei zugänglichen Internetseite).

StGB vor neue Herausforderungen. Für das Phänomen ehrverletzender Äußerungen im Internet wurde der spezielle Begriff des „**Flamings**“ geschaffen.[75]

39 Der Grund für die zunehmende Zahl an ehrverletzenden Äußerungen im Internet dürfte vor allem in den Besonderheiten der Kommunikation über dieses Medium liegen.[76] Ein persönliches Aufeinandertreffen der Kommunikationspartner – wie in mündlichen Gesprächen üblich – und eine damit verbundene Hemmung vor ehrverletzenden Äußerungen findet im Internet regelmäßig nicht statt. Diese **scheinbare** „**Heimlichkeit**“ und „**Barrierefreiheit**“ des Internet reduziert die Hemmschwelle zur Begehung von Beleidigungsdelikten in Foren und sozialen Netzwerken offenbar erheblich.[77] Oft bedarf es nur eines (unbedachten) Mausklicks, um die betreffende Botschaft abzuschicken oder zu „posten“. Dies erfolgt meist von zu Hause oder einer ähnlich vertrauten Umgebung aus, die das Bewusstsein für die Begehung einer strafrechtlich relevanten Ehrverletzung herabsetzt. Weiterhin vermittelt die vermeintliche Anonymität des Internet[78] vielen Inhabern eines Accounts bei einem sozialen Netzwerk eine trügerische Sicherheit vor Strafverfolgung. Dies führt dazu, dass viele User die teilweise weitreichenden Konsequenzen ihres Handelns nicht bedenken.

40 Hinzu kommen neben den Besonderheiten des Internet als Begehungsplattform auch **gesellschaftliche Entwicklungen**. In modernen Gesellschaften lässt sich längst nicht mehr eindeutig festlegen, wann eine Aussage den Tatbestand eines Beleidigungsdelikts erfüllt und wann nicht.

41 Ein eng mit den Beleidigungstatbeständen – aber auch mit den Delikten der Nachstellung (§ 238 StGB; „Cyberstalking“, Rn. 167) und Nötigung (§ 240 StGB; Rn. 188 ff.) – verknüpftes Problemfeld ist das sog. **Cybermobbing** (auch als Online-Mobbing oder **Cyberbullying** bezeichnet).[79] Dieser kriminologische Begriff umschreibt das

---

[75] Dazu Fawzi, Cyber-Mobbing, S. 38.

[76] So auch Brodowski, JR 2013, 513 (514).

[77] Dazu auch Krischker, JA 2013, 488 (489); Heckmann, NJW 2012, 2631 (2632); Brodowski, JR 2013, 513 (514: „erhöhte Gefährdungslage durch wahrgenommene Entpersonalisierung“).

[78] Vgl. hierzu auch: LG Duisburg, Beschl. v. 6.11.2012 – 32 Qs-245 UJs 89/11-49/12 (Ordnungsgeldfestsetzung gegen den Mitarbeiter eines Klinikbewertungsportals zur Erzwingung der Bekanntgabe des Urhebers einer beleidigenden Äußerung; kein Zeugnisverweigerungsrecht nach § 53 Abs. 1 S. 3 StPO).

[79] Gut ein Viertel der jugendlichen Internetnutzer gibt an, Personen zu kennen, die bereits Opfer von Cybermobbing geworden sind, ein Fünftel sogar, selber zu den Opfern von Beleidigungen zu zählen (Medienpädagogischer Forschungsverbund Südwest, JIM-STUDIE 2010, Jugend, Information, (Multi-) Media, S. 48 – http://www.mpfs.de/fileadmin/JIM-pdf10/JIM2010.pdf). Zu höheren Werten gelangt das Forschungsprojekt „Cybermobbing an Schulen“: Pressemitteilung vom 25.7.2013 (ein Drittel der befragten Schüler betroffen/ Täter oft auch Opfer), vgl. https://www.uni-hohenheim.de/news/rache-im-netz-4. Gleiches gilt für die aktuelle JIM-STUDIE 2013, wonach bereits Zweidrittel der Befragten Personen kennen, die über das Internet „fertig gemacht“ worden sind (Medienpädagogischer Forschungsverbund Südwest/ JIM-STUDIE 2013, Jugend, Information, (Multi-) Media, S. 46 – http://www.mpfs.de/fileadmin/JIM-pdf13/JIMStudie2013.pdf); hierzu auch Bündnis gegen Cybermobbing e. V., Gefangen im Netz. Nach Fawzi, Cyber-Mobbing, S. 38 ff., handelt es sich beim Cyberstalking nur um eine Form des Cybermobbings; dort auch zu anderen Formen. Speziell zur Verletzung des Allgemeinen Persönlichkeitsrechts, vgl. Schliesky/Hoffmann *u. a.*, Schutzpflichten und Drittwirkung im Internet, S. 129 ff.

Phänomen, bei dem Personen – in der Regel anonym – auf Internetplattformen oder in sozialen Netzwerken oder unter Zuhilfenahme sonstiger moderner Kommunikationsformen wie SMS massiv beleidigt oder belästigt oder bloßgestellt werden.[80] Die Wirkung des Cybermobbings ist gegenüber dem herkömmlichen Mobbing größer, weil etwaige Bemerkungen nicht nur dauerhaft elektronisch gespeichert sind, sondern auch einfacher und schneller einem wesentlich größeren Adressatenkreis zugänglich gemacht werden können.[81] Der folgende Abschnitt geht auf die Herausforderungen ein, vor denen die Beleidigungsdelikte der §§ 185 ff. StGB angesichts der durch das Internet hervorgebrachten Besonderheiten stehen.

Ein spezielles Phänomen ehrverletzender Äußerungen über soziale Netzwerke **42**
stellen die sog. „**Shitstorms**" dar, eine massenhaft öffentlich geäußerte Kritik an einem Zustand, vom Duden als „Sturm der Entrüstung in einem Kommunikationsmedium des Internets, der zum Teil mit beleidigenden Äußerungen einhergeht"[82] definiert.[83] Ein öffentlichkeitswirksamer Fall eines solchen „Shitstorms" über *Facebook* erlebte etwa der Kölner Zoo nach dem tragischen Tod einer Tierpflegerin aufgrund eines Tigerangriffs im August 2012.[84] Vor Shitstorms sind auch Unternehmen nicht gefeit. So traf es in der Vergangenheit u. a. die Drogeriekette *Schlecker*[85], den Elektronik-Großkonzern *Dell*[86] und einige Banken.[87]

---

[80] Zu Definitionsversuchen vgl. Fawzi, Cyber-Mobbing, S. 31 ff.; siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 112 ff., 116 ff., auch zu Erscheinungsformen; zum speziellen Phänomen des Lehrermobbings: Beck, MMR 2008, 77.

[81] Auer-Reinsdorff, FPR 2012, 434 (437); Fawzi, Cyber-Mobbing, S. 66 ff., zu den Merkmalen des Cybermobbings gegenüber herkömmlichem Mobbing (Einsatz von Internet/Handy, Anonymität/Unsichtbarkeit/Distanz, Dauerhaftigkeit, größere Reichweite, geringere Unterstützungsmöglichkeiten auf Seiten des Opfers, Wehrlosigkeit); ähnlich Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 109 ff.; vgl. ferner den Roman Cybermob, Mobbing im Internet von Clay (mit einer Aufstellung von Hilfsangeboten für Betroffene).

[82] Http://www.duden.de.

[83] Laut einer Umfrage des Hightech-Verbandes BITKOM aus dem Jahr 2012 sind vor allem Unternehmen schlecht auf derartige „Angriffe" eingerichtet; rund 45 % verfügten laut dieser Studie nicht über einen Aktionsplan als Reaktionsmechanismus (BITKOM, Pressemitteilung v. 17.8.2012; https://www.bitkom.org/de/presse/74532_73173.aspx.

[84] Der Zoo-Direktor hatte den Tiger zur Rettung der Pflegerin erschossen, was große Empörung auslöste. Die zum Teil wüsten Beschimpfungen entluden sich größtenteils über die Facebook-Seite des Kölner Zoos.

[85] Der Slogan der Drogeriekette Schlecker „For You. Vor Ort" sorgte aufgrund seines Sprachenmischmasch für harsche Kritik. Als ein Unternehmenssprecher entgegnete, dies spreche exakt den durchschnittlichen Schlecker-Kunden an, entlud sich auf zahlreichen Plattformen der Ärger über dieses Marketingkonzept; siehe Zeit online v. 18.6.2012, http://www.zeit.de/news/2012-06/18/internet-hintergrund-bekannte-shitstorm-faelle-18151403.

[86] Der Proteststurm gegenüber dem Computer-Hersteller Dell und schlechtem Kundenservice im Jahr 2005 gilt als einer der ersten seiner Art und trägt den bildhaften Namen „Dell Hell"; siehe Zeit online v. 18.6.2012, http://www.zeit.de/news/2012-06/18/internet-hintergrund-bekannte-shitstorm-faelle-18151403; siehe dazu auch Wais, in Die Welt v. 19.2.2013, http://www.welt.de/print/welt_kompakt/webwelt/article113733638/Marken-im-Auge-des-Shitstorms.html.

[87] Teilweise folgen diese Shitstorms ihren eigenen Gesetzen. In einem TV-Spot für die ING-DiBA aß Basketball-Profi *Dirk Nowitzki* eine Scheibe Wurst. Wütende Vegetarier protestierten im Internet über diesen angeblichen Skandal. Allerdings drehte sich in diesem Fall die Stimmung

7.5.4.2 Beleidigung (§ 185 StGB)

43 Der objektive Tatbestand des § 185 StGB setzt eine Verletzung der Ehre einer anderen Person durch die vorsätzliche Kundgabe von Missachtung, Geringschätzung oder Nichtachtung voraus, sog. **Formalbeleidigung**.[88] Die Kundgabe der Missachtung kann dabei sowohl unmittelbar gegenüber der betreffenden Person erfolgen als auch vermittelt werden, etwa durch einen Dritten.

44 Erfasst werden von § 185 StGB sowohl **Werturteile als auch ehrverletzende Tatsachenbehauptungen**. Erfolgt die Kundgabe einer ehrverletzenden Tatsache, so sind im Fall der Äußerung gegenüber einem Dritten die §§ 186, 187 StGB einschlägig.

45 Eine besondere Form der Erklärung schreiben die §§ 185 ff. StGB nicht vor, erfasst sind daher auch die in sozialen Netzwerken üblichen Äußerungsformen, wie Pinnwandeinträge, persönliche Nachrichten etc.[89] Allein die Tatsache, dass eine Äußerung über das Internet und dort innerhalb eines sozialen Netzwerks erfolgt, beeinflusst ihren etwaig beleidigenden Charakter also nicht.

46 Schwierigkeiten bereitet in der Praxis häufig die Frage, welcher **Erklärungsgehalt** einer Aussage beizumessen ist. Bedeutung erlangt in dieser Hinsicht insbesondere die durch die Strafbarkeit von Beleidigungen gegebene Einschränkung der Meinungsäußerungsfreiheit aus Art. 5 Abs. 1 S. 1 GG.[90] Unter dem Gesichtspunkt einer verfassungskonformen Auslegung der Beleidigungstatbestände kann heute manches über einen Mitmenschen behauptet und geäußert werden, was noch vor Jahren die Grenze der Strafbarkeit überschritten hätte.

47 Das **BVerfG** hat in zahlreichen Urteilen allgemein geltende Maßstäbe zur Ermittlung des objektiven Erklärungssinns einer Äußerung festgelegt: „[...] Weder die subjektive Absicht des sich Äußernden noch das subjektive Verständnis der von der Äußerung Betroffenen [sind maßgeblich], sondern der Sinn, den sie nach dem Verständnis eines unvoreingenommenen und verständigen Publikums hat. Dabei ist stets vom **Wortlaut** der Äußerung auszugehen. Dieser legt ihren Sinn aber nicht abschließend fest. Er wird vielmehr auch von dem **sprachlichen Kontext**, in dem die umstrittene Äußerung steht, und den **Begleitumständen**, unter denen sie fällt, bestimmt, soweit diese für die Rezipienten erkennbar waren. Die isolierte Betrachtung eines umstrittenen Äußerungsteils wird daher den Anforderungen an eine zuverlässige Sinnermittlung regelmäßig nicht gerecht“[91].

48 Letztlich lässt sich keine pauschale Aussage darüber treffen, wann eine Äußerung ehrverletzenden Charakter hat. Es muss vielmehr eine **Einzelfallbetrachtung**

---

zugunsten der Privatbank und den protestierenden Vegetariern selbst wurde in Internetforen ein Proteststurm entgegengeschleudert, siehe Zeit online v. 18.6.2012, http://www.zeit.de/news/2012-06/18/internet-hintergrund-bekannte-shitstorm-faelle-18151403.

[88] Vgl. nur Fischer, StGB, § 185 Rn. 4.

[89] Siehe nur Krischker, JA 2013, 488 (489); Fischer, StGB, § 185 Rn. 7. Zur Beleidigung durch die Verbreitung von Bildaufnahmen: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 96 ff.

[90] Hierzu ausführlich Brodowski, JR 2013, 513 (514 ff.).

[91] BVerfG, NStZ 1996, 26 (27).

unter Berücksichtigung der jeweiligen Besonderheiten des Falles erfolgen.[92] Dabei spielt neben dem Ort der Begehung (soziale Netzwerke) eine Rolle, welcher sozialen Schicht, Region, Nationalität, Altersgruppe usw. der mutmaßliche Täter angehört; entscheidend ist, wie ein verständiger Dritter die Aussage verstehen durfte.[93] Möglich ist aber die Unterscheidung in eine innere Ehre als ein dem Menschen als Träger von Werten zukommender Achtungsanspruch sowie eine äußere Ehre, die den „guten Ruf", das Ansehen und das Image einer Person in seinem sozialen Umfeld und der Gesellschaft beschreibt.[94] Das Einstellen („Zur-Schau-Stellen") von Bildern einer Person im Internet hat grundsätzlich nur dann (den erforderlichen) ehrverletzenden Charakter, wenn damit eine „Herabsetzung" bzw. „Verachtung" der Person verbunden ist.[95]

Ist nach dieser Betrachtung keine eindeutige Zuordnung der Äußerung als ehrverletzend möglich, ist ihr Erklärungsgehalt durch **Auslegung** zu ermitteln.[96] Bereits im „herkömmlichen" Begehungsfeld der Beleidigung, also im nicht-virtuellen Raum, bereitet diese Einordnung Schwierigkeiten. Das Internet, insbesondere die auf spontane, „freundschaftliche" aber durchaus ggf. auch auf „abgegrenzte" Kommunikation („Gruppen") ausgerichteten sozialen Netzwerke verstärken diese Probleme weiter. Das liegt vor allem daran, dass eine Reihe von Begleitumständen bzw. Auslegungshilfen (Mimik, Gestik, Tonfall etc.), die bei einer mündlichen Äußerung zur Bestimmung ihres beleidigenden Charakters durch einen verständigen Dritten herangezogen werden können, im Internet nicht zur Verfügung stehen. **49**

Da soziale Netzwerke eine Reihe von **Besonderheiten in der Kommunikation** mit sich bringen (kein persönliches Gegenübertreten der Kommunikationspartner, vermeintliche Anonymität, herabgesetzte Hemmschwelle etc.), sind maßgeblich diese zur Auslegung heranzuziehen. Ein Beispiel dafür sind die sog. **Emoticons**. Als solche bezeichnet man aus Satzzeichen und Buchstaben zusammengesetzte „Gefühlssymbole", die bei der Kommunikation über das Internet genutzt werden, um die fehlenden Möglichkeiten der eben hinsichtlich einer mündlichen Kommunikation genannten Umstände zu ersetzen.[97] Die früher weitgehend tatsächlich nur aus Satzzeichen bestehenden Emoticons werden heute zunehmend durch Smileys ersetzt, die eine Bewertung des Erklärungsgehaltes einer Äußerung in den meisten Fällen erleichtern.[98] **50**

---

[92] BVerfGE 85, 1 (18); 93, 266 (295 f.); vgl. auch LG München I, Urt. v. 15.1.2014 – 25 O 16238/13 (Schmähkritik durch Bewertung eines Arztes in einem Onlineportal).
[93] Fischer, StGB, § 185 Rn. 8.
[94] Ostendorf et al., NStZ 2012, 529 (534).
[95] Vgl. Beck, MMR 2008, 77 (80).
[96] Näheres bei Hilgendorf, in: LK-StGB, § 185 Rn. 17.
[97] Hilgendorf et al., Rn. 523.
[98] Neben den herkömmlichen statischen *Smileys* gibt es inzwischen bewegte bzw. sich bewegende *Emoticons*. Sogar auf staatlich geförderten Internetseiten für Kinder und Jugendliche (BMF SFJ) werden bereits junge Internetnutzer an die Bedeutung dieser Symbole herangeführt, vgl. z. B. http://www.blinde-kuh.de/smiley/tabelle.html.

51 Weiterhin ist der in sozialen Netzwerken übliche Umgangston bzw. der dort angewandte **Kommunikationsstandard** zu beachten, wobei allerdings ein beleidigender Umgangs- und Umgebungston die betreffenden Personen nicht grundsätzlich von jeglichen Beleidigungen freispricht.[99] Die (bereits den Tatbestand der Beleidigung ausschließende) **Sozialadäquanz** der Aussagen von zumeist jungen Internetnutzern unterscheidet sich oft erheblich von dem dieser „Kultur" nicht angehörenden Personen.[100] Ein rauer Umgangston in sozialen Netzwerken ist eher die Regel als die Ausnahme und kann als „sozialadäquat" angesehen werden.[101] Nicht mehr umfasst werden sollten hingegen Äußerungen, die weit über das „Ziel", die sozialadäquate „Frotzelei" hinausschießen. Zeigt ein auf einem sozialen Netzwerk hochgeladenes Foto beispielsweise einen missglückten Kochversuch und schreibt der Ersteller des Beitrags selbst darunter, dass er „zu dumm zum Kochen sei", ist die Erwiderung eines Dritten („nicht nur dazu") noch vom Grundtenor der Selbstironie gedeckt. Wird hingegen ein persönlicher Angriff vorgenommen, der nur in losem Kontext zu dem eingestellten Beitrag steht („Du bist sowieso ein Idiot, schau dir nur etc. . . ."), ist diese Form der Diffamierung nicht mehr von einer (konkludenten) Einwilligung gedeckt. Wer demnach den Vorwand nutzt, um gegen andere auszuteilen (**Schmähung**), ist nicht mehr schutzwürdig.[102]

52 Anstelle der Verortung des Problems im Bereich der Sozialadäquanz kommt – ebenfalls auf Tatbestandsebene – die Annahme eines **tatbestandsausschließenden Einverständnisses** in Betracht. Von einem solchen Einverständnis ist dort auszugehen, wo die tatbestandliche Verhaltensbeschreibung ein Handeln oder Unterlassen ohne Zustimmung des Betroffenen voraussetzt.[103] Wann ein solches Einverständnis vorliegt, ist strittig. Notwendig sei mehr als ein bloßes „Dulden, Geschehenlassen oder tatsächliches Nichthindern", gleichwohl muss die Rechtsgutsverletzung nicht „herbeigewünscht" werden.[104] Wer bewusst Schmähungen provoziert, ist mit dem Gros der erzeugten Reaktionen auch einverstanden. In dieser Konstellation scheint die Annahme eines bereits tatbestandlich zu verneinenden „ehrenrührigen" Reaktionsverhaltens gegenüber einer von der h. M. erst auf Rechtfertigungsebene (Einwilligung, Rn. 61) vorgenommenen Lösung vorzugswürdig.

53 Die **Kundgabe der Äußerung**, also die Kommunikation eines gedanklichen Inhalts und die Kenntnisnahme durch eine andere Person,[105] wird dagegen meist kein Problem darstellen. Die führenden sozialen Netzwerke Facebook, Twitter oder

---

[99] Vgl. Hilgendorf et al., Rn. 524; Krischker, JA 2013, 488 (489).
[100] Hilgendorf, ZIS 2010, 208 (212).
[101] Vgl. zur Sozialadäquanz bei Sportwettkämpfen: BayObLG, NJW 1999, 372 (373) mit zust. Anm. Otto, JR 1999, 124; zu beleidigenden Äußerungen über Unternehmen vgl. Härting, ZWH 2014, 45 f.
[102] Hardtung, in: MüKo-StGB, § 228 Rn. 36, bezogen auf Sportarten.
[103] Baumann et al., Strafrecht AT, § 17 Rn. 93; Gropp, Strafrecht AT, § 6 Rn. 59; Krey/Esser, Strafrecht AT, Rn. 655 f.
[104] Hirsch, in: LK-StGB, vor § 32 Rn. 111.
[105] Hilgendorf in: LK-StGB, § 185 Rn. 10. Zur dogmatisch interessanten Abgrenzung von Täterschaft und Teilnahme im Falle des „Likens" oder „Teilens" beleidigender Inhalte: Krischker, JA 2013, 488 (490 ff.).

Studi.vz sind gerade darauf ausgelegt, dass ihre Nutzer ihre Gedanken öffentlich verbreiten und stellen entsprechende Plattformen, wie etwa die Chronik bei Facebook, zur Verfügung. Bei der Veröffentlichung eines Beitrags kann dieser bei Facebook und studi.vz von allen befreundeten Usern (und bei entsprechenden Privatsphäre-Einstellungen sogar noch von einem größeren Personenkreis) gelesen werden, bei Twitter entsprechend von allen „Followern".

54 Natürlich muss der Nutzer eines sozialen Netzwerks nicht jede Nachricht öffentlich machen. Äußerungen können auch auf einen **abgrenzbaren Personenkreis** beschränkt werden. Es besteht etwa die Möglichkeit, private Nachrichten an eine oder mehrere Personen zu verschicken oder im Rahmen eines Chatprogramms miteinander zu kommunizieren. Doch auch bei diesen Kommunikationsformen wird der Inhalt der jeweiligen Nachricht unmittelbar an den ausgewählten Personenkreis weitergeleitet, also kundgetan.

55 Zu beachten sind in diesem Kontext jedoch die Besonderheiten hinsichtlich der Kundgabe gegenüber Familienmitgliedern, Lebenspartnern oder engen Freunden. Ein auf engste Vertrauensverhältnisse beschränkter sog. **beleidigungsfreier Raum** führt im Ergebnis dazu, dass etwaige in ihm getätigte ehrverletzende Äußerungen nicht als Beleidigungen angesehen werden.[106] Teilweise wird zur strafrechtlichen Einordnung dieser Privilegierung im Hinblick auf Art. 6 GG eine teleologische Reduktion des § 185 StGB gefordert,[107] teils wird dieser Aspekt auf Rechtfertigungsebene mit einem Verweis auf die Figur der „Wahrnehmung berechtigter Interessen" (vgl. § 193 StGB)[108] behandelt. Letztlich kann eine genaue Erörterung dieses Problems dahinstehen, da die Privilegierung ungeachtet ihrer genauen Verortung als solche bei sozialen Netzwerken nicht einschlägig ist. Ihr Grund liegt in der Annahme, dass jeder Mensch ein Anrecht auf eine strafrechtsfreie Sphäre persönlicher Kommunikation hat, in deren Rahmen Äußerungen nicht sozial kontrolliert und sanktioniert werden sollen.[109] Diesen Raum auf den in sozialen Netzwerken bestehenden „Freundeskreis" auszuweiten, erscheint höchst fraglich. Zum einen besteht hier kein Schutz durch Art. 6 Abs. 1 GG, der sich auf Ehe und Familie beschränkt.[110] Zum anderen weisen die im Internet bestehenden Kontakte kaum jemals eine auch nur in Ansätzen vergleichbare Intimität bzw. Vertraulichkeit auf. Vielmehr handelt es sich in den meisten Fällen um flüchtige Bekanntschaften, alte Schulfreunde, Nachbarn, Arbeitskollegen, Kommilitonen etc. Eine etwaige Privilegierung ist aus diesem Grund abzulehnen.

56 Der von §§ 185, 15 StGB geforderte **Vorsatz** für die Kundgabe einer ehrverletzenden Äußerung setzt voraus, dass sich der Betroffene darüber **bewusst** ist, dass seine Äußerung nach außen dringt und von Adressaten bzw. Dritten wahrgenommen

---

[106] Fischer, StGB, § 185 Rn. 12.
[107] Lackner/Kühl, StGB, § 185 Rn. 9; Regge, in: MüKo-StGB, vor §§ 185 ff., Rn. 58 ff.; Brodowski, JR 2013, 513 (516).
[108] Hilgendorf, in: LK-StGB, § 185 Rn. 14.
[109] Fischer, StGB, § 185 Rn. 12; Hilgendorf, in: LK-StGB, § 185 Rn. 13.
[110] Ebenso Hilgendorf, ZIS 2010, 208 (210).

werden kann. Bereits hinsichtlich dieses Prüfungspunktes bestehen aufgrund der Besonderheiten des Mediums Internet Probleme. Die über das Internet in sozialen Netzwerken kommunizierte Beleidigung unterscheidet sich von der „herkömmlichen“ (von Angesicht zu Angesicht kommunizierten) Beleidigung vor allem darin, dass sie zumeist in einem sehr privaten Umfeld in den Umlauf gebracht wird. Die meisten User sozialer Netzwerke agieren vom heimischen PC aus und sind sich angesichts dieser vertrauten Umgebung und der damit verbundenen vermeintlich „heimlichen“ Atmosphäre möglicherweise nicht bewusst, dass sie gerade eine beleidigende Äußerung kundtun.[111]

57 Tatsächlich wird der Vorsatz aber kaum je bestritten werden können. Immerhin genügt für den subjektiven Tatbestand des § 185 StGB **dolus eventualis**. Ein beschuldigter User wird im Regelfall nur sehr schwer begründen können, dass er es nicht einmal **billigend in Kauf genommen hat**, dass seine objektiv ehrverletzende Äußerung nach außen treten könnte. Vielmehr liegt der Sinn sozialer Netzwerke gerade darin, eine mehr oder weniger breite Öffentlichkeit in Form des dort vertretenen „Freundeskreises“ mit den vom Provider bereitgestellten Kundgabeformen zu erreichen, wie etwa durch „Posts“ bei Facebook.[112]

58 Auch bei **privaten Kundgabeformen**, wie etwa dem Verschicken persönlicher Nachrichten oder dem Chatten, ist den Nutzern durchaus bewusst, dass diese den gewünschten Empfänger erreichen, sobald der entsprechende Mausklick getätigt wird. Zwar ist die Kommunikation über das Internet deutlich anfälliger für ein versehentliches Fehlverhalten, etwa in Form eines „Vertippens“ oder „Verklickens“, sodass Nutzer entsprechende Schutzbehauptungen aufstellen könnten. Sämtliche soziale Netzwerke stellen aber ausreichende Möglichkeiten zur Verfügung, eventuell nicht beabsichtigte Äußerungen wieder zurückzunehmen bzw. zu löschen, sodass sich selbst in diesen Fällen die Verneinung eines Vorsatzes zur Kundgabe schwerlich begründen lässt.

59 Weiterhin muss sich der Vorsatz auch auf die Tatsache beziehen, dass die Äußerung nach ihrem objektiven Sinn eine **Missachtung** darstellt.[113] Hier ergeben sich außer der bereits oben erläuterten Problematik der Ermittlung des Sinngehalts einer beleidigenden Aussage letztlich keine Besonderheiten.

60 Hinsichtlich der Prüfungsebene der **Rechtswidrigkeit** eines tatbestandlich relevanten Verhaltens (zum vorrangig zu prüfenden Ausschluss von Äußerungen über das Tatbestandsmerkmal der Sozialadäquanz bzw. eines tatbestandsausschließenden Einverständnisses bereits oben Rn. 52) können sich bei der Begehung von Beleidigungsdelikten in sozialen Netzwerken Fragen in Bezug auf das Vorliegen einer rechtfertigenden Einwilligung und des besonderen Rechtfertigungsgrundes der Wahrnehmung berechtigter Interessen, § 193 StGB, ergeben.

61 Dass die Nutzer sozialer Netzwerke bzw. des Internet allgemein im Vorhinein in gegen sie gerichtete Beleidigungen einwilligen, wird man nicht annehmen können.

---

[111] Das Problem wirft auch Hilgendorf, ZIS 2010, 208 (210) auf.
[112] So auch Hilgendorf, ZIS 2010, 208 (210).
[113] Fischer, StGB, § 185 Rn. 17.

Eine **rechtfertigende Einwilligung** liegt deshalb nur im Einzelfall bei Zusammentreffen der allgemeinen Voraussetzungen[114] und der folgenden Konstellation vor: Ein Nutzer stellt Bilder, Videos oder sonstige Inhalte aus eigenem Antrieb auf das Nutzerprofil seines sozialen Netzwerks online und diese werden dann im Nachhinein in einem von ihm nicht vorhergesehenen (beleidigenden) Kontext wiederverwendet.[115] Obwohl dieser Fall auf den ersten Blick recht exotisch und nach einer Ausnahme klingt, wird er in der Praxis nicht selten vorliegen. Die wenigsten Nutzer sozialer Netzwerke sind sich im Klaren darüber bzw. verlieren den Überblick darüber, welche und in welchem Umfang von ihnen eingestellte Daten und Bilder für andere Nutzer und vor allem die Betreiber des sozialen Netzwerks frei zugänglich und nutzbar sind.

Ebenso liegen Fälle, in denen ein Nutzer bewusst peinliche oder zumindest dis- **62**
kutable Inhalte auf Plattformen lädt (Partyfotos, Sport, Alltagsmissgeschicke) und durch eigenes Kommentierverhalten Dritte sogar bewusst dazu animiert, seinen Beitrag ironisch, abschätzig oder überspitzt zu kommentieren, um so entsprechend größere Aufmerksamkeit der Netzgemeinde zu erlangen. Es erscheint denkbar, in der Bereitstellung des provokanten Beitrags eine **konkludente Einwilligung** in entsprechende Diffamierungen zu sehen.

An eine (konkludente) Einwilligung ist in den zuvor genannten Fällen deshalb **63**
zu denken, weil jeder Nutzer vor seinem Beitritt in das jeweilige soziale Netzwerk dessen **Allgemeine Geschäftsbedingungen** (AGB) akzeptieren muss und diese oftmals Klauseln enthalten, die es den Betreibern faktisch möglich machen, die von Nutzern zur Verfügung gestellten Inhalte für beinahe jeden Zweck zu nutzen.[116] Damit die Akzeptanz von AGB beim Eintritt in ein soziales Netzwerk tatsächlich eine Einwilligung im strafrechtlichen Sinn begründen kann, müssten die allgemein anerkannten Voraussetzungen einer Einwilligung vorliegen. Der Betreffende muss befugt sein, über das entsprechende Rechtsgut zu verfügen und fähig sein, in dessen Verletzung einzuwilligen. Ferner muss er die Einwilligung ausdrücklich oder konkludent zum Tatzeitpunkt frei von Willensmängeln erklärt und der Täter in Kenntnis der Einwilligung gehandelt haben.[117] In den meisten Fällen wird der Inhalt von AGB aufgrund ihres Umfangs nicht vollumfänglich gelesen; vielmehr wird oft nur ein „**Häkchen**“ als Erklärung allgemeiner Zustimmung gesetzt. In Anlehnung an die Voraussetzungen der Einwilligung beim ärztlichen Heileingriff (siehe jetzt: §§ 630e ff. BGB) kann eine solche Erklärung nicht ausreichen, um eine rechtfertigende Einwilligung zu begründen. Es genügt gerade nicht, dem Betroffenen nur die Möglichkeit der Kenntnisnahme etwaiger Risiken durch die Aushändigung komplexer AGB zu eröffnen, sondern dieser muss durch eine effektive Aufklärung in Kenntnis der tatsächlichen Sachlage in die Beeinträchtigung seiner Ehre einwilligen. Die Einwilligung muss sich außerdem auf eine zumindest ansatzweise konkretisierte zukünftige Rechtsgutsverletzung beziehen. Dies dürfte bei möglichen Beleidigungen

[114] Vgl. dazu Krey/Esser, Strafrecht AT, Rn. 663 ff.
[115] Hilgendorf, ZIS 2010, 208 (214).
[116] Siehe Hilgendorf, ZIS 2010, 208 (214).
[117] Krey/Esser, Strafrecht AT, Rn. 663 ff.

über das Internet kaum jemals der Fall sein. Selbst in der oben geschilderten besonderen Konstellation kann somit von dem Vorliegen einer strafrechtlichen Einwilligung nicht ausgegangen werden.[118]

64 Weiterhin ist an eine mögliche Rechtfertigung über die Figur der **Wahrnehmung berechtigter Interessen** (§ 193 StGB) zu denken. Sie stellt eine Möglichkeit dar, der Vielzahl kultureller und in Bezug auf die Besonderheiten der Umgangsformen in sozialen Netzwerken (s. o.) subkulturellen Besonderheiten gerecht zu werden und somit eine ausufernde Ausweitung der Strafbarkeit von Beleidigungsdelikten zu verhindern.[119] Insbesondere im Hinblick auf Kollisionen mit **grundrechtlich geschützten Positionen**, wie etwa der Kunstfreiheit aus Art. 5 Abs. 3 S. 1 GG, hat § 193 StGB allerdings eine eigenständige Bedeutung weitgehend verloren; der Regelungsgehalt der Norm wird vielmehr durch die grundrechtlichen Normen konsumiert.[120]

65 Im Rahmen der **Schuld** ergeben sich hinsichtlich Beleidigungen in sozialen Netzwerken im Wesentlichen keine Besonderheiten. Einzig die Möglichkeit eines **Verbotsirrtums** nach § 17 StGB erscheint erwähnenswert. Hier kann auf die Argumentation eines eventuell fehlenden Vorsatzes zur Kundgabe mit der Besonderheit verwiesen werden (Rn. 56), dass der Nutzer sich zwar im Klaren darüber ist, dass er die entsprechende Äußerung getätigt hat, aber nicht darüber, dass eine solche virtuelle Interaktion eine nach § 185 StGB strafbare Beleidigung darstellt, die Rechtsgutsverletzung als solche also nicht als Unrecht erkennt.[121] In der überwiegenden Zahl der Fälle wird ein solcher Verbotsirrtum jedoch vermeidbar sein.[122] Das gilt zumindest dann, wenn die betreffende Äußerung für den Täter erkennbar ausschließlich Personen erreicht, die sich im Geltungsbereich des deutschen Strafrechts befinden und somit auch das deutsche Beleidigungsrecht zur Anwendung kommt. Das ist etwa dann der Fall, wenn bei Facebook, Twitter oder studi.vz im Rahmen einer (Gruppen-)Nachricht nur in Deutschland befindliche Personen angesprochen werden.

66 Schwieriger ist die Lage allerdings zu bewerten, wenn die Äußerung mittels der **Pinnwand-Funktion** bei Facebook (hier dann Chronik) oder studi.vz „gepostet“ bzw. bei Twitter „getwittert“, und so dem gesamten Kreis der vorhandenen Kontakte (der Personenkreis ist jeweils abhängig von der individuellen Privatsphäre-Einstellung) zugänglich gemacht wird, die verschiedenen Rechtsordnungen und vor allem Kulturkreisen zuzuordnen sind. Zwar ist bei den wortbasierten Funktionen der sozialen Netzwerke auch hier kaum vorstellbar, dass eine bestimmte Äußerung in einer anderen Rechtsordnung als Beleidigung aufgefasst wird, ohne dass dies der jeweilige User erkennt, weil sie im eigenen Kulturkreis etwa nicht beleidigend ist. Im Gegensatz zur Bewertung der **Vermeidbarkeit des Verbotsirrtums** im nationalen Kontext wird ein solcher im letzteren Fall dennoch häufiger als unvermeidbar einzustufen sein, weil der Handelnde sich entweder bereits der Tatsache nicht bewusst

---

[118] Zum Ganzen: Hilgendorf, ZIS 2010, 208 (214).
[119] Hilgendorf, ZIS 2010, 208 (214).
[120] Hilgendorf in: LK-StGB, § 193 Rn. 4 ff.
[121] Etwa Valerius, NStZ 2003, 341 (346); siehe auch Krischker, JA 2013, 488 (489).
[122] Hilgendorf, ZIS 2010, 208 (211).

ist, dass er den Rechtskreis einer fremden Rechtsordnung berührt oder ihm deren Rechtssätze unbekannt sind.[123]

Die Beleidigung (§ 185 StGB) wird (grundsätzlich) nur auf **Antrag** verfolgt (§ 194 Abs. 1 S. 1 StGB) – mit einer Ausnahme für Angehörige bestimmter verfolgter Gruppen (§ 194 I 2 StGB) – eine gerade in sozialen Netzwerken durchaus vorkommende Konstellation. Richtet sich die Tat gegen einen Amtsträger (z. B. Lehrer), einen für den öffentlichen Dienst besonders Verpflichteten oder gegen einen Soldaten der Bundeswehr, so hat auch der Dienstvorgesetzte ein Antragsrecht (§ 194 Abs. 3 S. 1 StGB). **67**

7.5.4.3 Überlegungen für eine Reform des Beleidigungstatbestandes

Die neuartigen Phänomene der Kommunikation über soziale Netzwerke haben Zweifel dahingehend aufkommen lassen, ob die aktuelle Fassung des Beleidigungstatbestandes diesen Spezifika noch in ausreichendem Maße gerecht wird. **68**

Für Überlegungen zur Einführung eines **neuen Qualifikationstatbestandes** der „Beleidigung im Internet“,[124] d. h. eines speziell auf internettypische Begehungsweisen zugeschnittenen Tatbestandes bzw. eines Regelbeispiels[125], sprechen die diversen Besonderheiten des Mediums Internet als Kommunikationsforum. Konkret könnte die Ausgestaltung eines solchen Qualifikationstatbestandes entweder an die Verbreitung ehrenrühriger Äußerungen über das Internet anknüpfen, um die besondere Verwerflichkeit der Handlung zu unterstreichen, oder aber – in Anlehnung an § 192 StGB – an die Tatsache, dass die Verbreitung der Information öffentlich geschieht.[126] So knüpfen auch die Straftatbestände der §§ 111, 130 und 164 StGB strafbegründend bzw. strafschärfend an die öffentliche Begehungsweise an. **69**

Durch Äußerungen im Internet wird naturgemäß eine deutlich **breitere Öffentlichkeit** erreicht, als dies etwa bei einer persönlichen Auseinandersetzung mit der entsprechenden Person der Fall wäre.[127] Je nach Sachlage können durch einen einfachen Eintrag bei Facebook oder Twitter u. U. innerhalb von Sekunden Millionen von Menschen erreicht werden. Eine ehrverletzende Äußerung wird jedoch nicht nur von vornherein einem deutlich größeren Personenkreis zugänglich gemacht, sondern sie bleibt in aller Regel auch erheblich länger, wenn nicht sogar zeitlich unbegrenzt, im Netz erhalten. An aktuellen Fällen, die aufzeigen, in welchem Umfang Daten auf unkontrollierte Art und Weise im Internet kursieren, mangelt es nicht. **70**

2011 wollte ein Wiener Jurastudent von Facebook Auskunft darüber erhalten, welche Daten von ihm bei Facebook vorhanden waren.[128] Als Ergebnis bekam er 1.200 **71**

---

[123] Valerius, NStZ 2003, 341 (346), allerdings vor allem zur Verbreitung der Auschwitz-Lüge über das Internet von einem ausländischen Provider aus.
[124] Hilgendorf, EWE 2008, 403 (410).
[125] Dazu Krischker, JA 2013, 488 (493).
[126] Beck, MMR 2009, 736 (740).
[127] Beck, MMR 2009, 736 (738 f.).
[128] http://www.zeit.de/digital/datenschutz/2011-09/facebook-daten-herausgabe.

DIN-A4-Seiten zugeschickt, die zu großen Teilen Daten enthielten, von denen er der Ansicht war, sie längst gelöscht zu haben. Zu bedenken ist, dass es sich in diesem Fall um ein soziales Netzwerk handelte, das ein vollkommen legales Geschäftsmodell darstellt und ein Interesse daran hat oder zumindest haben sollte, Missbrauch zu verhindern. Es lässt sich nur erahnen, welche Probleme es in der Praxis bereiten wird, das Internet von Daten zu säubern, die auf illegale Weise eingestellt wurden. In diesen Fällen wird es oftmals schon an einem passenden Ansprechpartner fehlen, der die entsprechenden Server betreibt und die Daten löschen könnte. Soweit es sich um Verlinkungen durch Suchmaschinen zu Informationen oder Seiten Dritter handelt, hat der Betroffene das **Recht gegenüber dem Suchmaschinenbetreiber**, dass – nach Abwägung seiner Rechte mit dem Recht der Öffentlichkeit auf Information – solche Verlinkungen bei überwiegendem persönlichen Interesse (Zeitablauf/Unrichtigkeit der Daten) gelöscht werden.[129]

72 Es fragt sich jedoch, ob allein die **Besonderheiten der „Dauerhaftigkeit" des Internet** bereits ausreichen, einen derart erhöhten Unrechtsgehalt einer ehrverletzenden Äußerung anzunehmen, dass der bestehende Strafrahmen des Beleidigungstatbestandes (§ 185 StGB) zur Ahndung nicht mehr ausreicht.[130]

73 Auf der anderen Seite hätte die Einführung eines Qualifikationstatbestandes der „Beleidigung im Internet" im Ergebnis eine erhebliche Verschärfung der Strafbarkeit von Beleidigungsdelikten zur Folge. Vor allem im Hinblick auf die deutlich herabgesetzte Hemmschwelle zur Begehung des Delikts im Internet besteht die Gefahr einer der ultima-ratio-Funktion des Strafrechts widersprechenden **Ausweitung der Strafbarkeit („Überkriminalisierung")**.[131] Es ist zumindest anzudenken, ob nicht weniger einschneidende Mittel und Methoden zur Verfügung stehen, um die mit dem Internet und der Nutzung sozialer Netzwerke verbundenen Probleme auf andere Art und Weise einzudämmen. Zu denken wäre in diesem Zusammenhang etwa an eine **stärkere Inpflichtnahme der Provider**.[132] Das entspräche auch den Vorgaben des BVerfG, wonach der durch Art. 5 Abs. 1 S. 1 GG geschützten Meinungsfreiheit überragende gesellschaftliche Bedeutung zuzumessen ist und der Verhältnismäßigkeitsgrundsatz in besonderem Maße bei der Auslegung der §§ 185 ff. StGB zu beachten ist. Bezogen auf die Beleidigungsdelikte bedeutet das für die Auslegung mehrdeutiger Äußerungen, die verschiedene, teilweise nicht strafrechtlich relevante Interpretationen zulassen, dass der Tatrichter nur dann von einer zur Verurteilung führenden Deutung der Norm ausgehen darf, wenn er *alle* nicht strafbaren Auslegungsmöglichkeiten ausgeschöpft hat.[133]

---

[129] EuGH, Urt. v. 13.5.2014 – C-131/12, Rn. 80, 92 ff.
[130] So Beck, MMR 2009, 736 (739).
[131] Hilgendorf, EWE 2008, 403 (410).
[132] Hilgendorf, EWE 2008, 403 (410); siehe auch den Koalitionsvertrag zwischen CDU, CSU und SPD (Fn. 6), S. 148.
[133] BVerfG, NJW 1994, 2943 (2944); Däubler, AiB 2014, 26 (27) bzgl. Kündigungsrecht.

7.5.4.4 Kompensationsgrundsatz (§ 199 StGB)

Zu erinnern ist diesem Zusammenhang auch an den für sämtliche Delikte des 14. Abschnitts des StGB geltenden und speziell in § 199 StGB zum Ausdruck kommenden Kompensationsgrundsatz, der eine in das Ermessen des Gerichts gestellte Straffreiheit für die Fälle wechselseitiger Beleidigungen vorsieht. Hinter der Norm steht der Gedanke, dass im Falle von *unmittelbar* („auf der Stelle") erwiderten Beleidigungen das Strafbedürfnis häufig so weit reduziert sein dürfte, dass eine umfassende Bestrafung der Täter im Ergebnis nicht notwendig erscheint. Dies ergibt sich daraus, dass der Ersttäter bereits eine Übelzufügung durch die erwiderte Beleidigung des Zweittäters erfahren hat, während das Verhalten des Zweittäters durch die vorhergehende Provokation des Ersttäters weniger schwer wiegt.[134] **74**

§ 199 StGB setzt daher mindestens zwei strafbare, also rechtswidrig und schuldhaft begangene Beleidigungen i. S. d. §§ 185 ff. StGB voraus sowie eine **Wechselseitigkeit** derselben. Die zeitlich später erfolgte Beleidigung muss also eine Erwiderung der früher geäußerten Beleidigung sein, wobei eine ausdrückliche Bezugnahme genauso wenig wie eine persönliche Identität zwischen Erst- und Zweittäter (etwa: Erwiderung der Beleidigung einer dem Täter nahe stehenden Person) erforderlich ist. Weiterhin muss die Erwiderung „auf der Stelle" erfolgen. Darunter ist ein psychischer bzw. reaktiver Zusammenhang in einem engen zeitlichen Rahmen zu verstehen.[135] **75**

Besondere Bedeutung erlangt § 199 StGB bei Beleidigungsdelikten im Internet bzw. in sozialen Netzwerken, weil die dort typischen Begehungsformen seine Einschlägigkeit in vielen Fällen begünstigen werden. Sämtliche über soziale Netzwerke eröffnete Kommunikationswege fördern wechselseitige Beleidigungen, indem sie den Nutzer unmittelbar darauf aufmerksam machen, dass eine Äußerung in seiner Chronik (Facebook) oder auf seiner Wall (Twitter) oder Pinnwand (studi.vz) gepostet wurde und diesen somit fast schon zu einer unmittelbaren Gegenreaktion aufrufen, gar provozieren. Das gilt ebenso für die von allen sozialen Netzwerken bereitgestellten Chat- bzw. Nachrichtenprogramme. Stets ist darauf zu achten, ob tatsächlich eine Wechselseitigkeit der Handlungen vorliegt. Erfolgt die beleidigende Gegenäußerung erst nach einer gewissen Überlegungszeit, ist § 199 StGB nicht einschlägig. Hier kann die „Wechselseitigkeit" der Vorgänge nur unter allgemeinen Strafzumessungserwägungen berücksichtigt werden. **76**

Praktisch relevant ist erneut der bereits geschilderte Fall der „**provozierten Entgleisungen**" (Rn. 51). Bewusst selbstdiffamierende Inhalte werden in der Absicht hochgeladen, andere Nutzer zu spöttischen Kommentaren zu verleiten. Insgesamt verspricht sich der Urheber davon eine gesteigerte Aufmerksamkeit in der Forum-Community. Problematisch ist hierbei insbesondere das Merkmal der Wechselseitigkeit sowie die etwaige Einordnung als tatbestandsausschließendes Einverständnis oder als rechtfertigende Einwilligung. Ein Beitrag, der bewusst auf **77**

---

[134] Zum Ganzen: Hilgendorf, in: LK-StGB, § 199 Rn. 1; Krey/Hellmann, Strafrecht BT, Rn. 516.
[135] Zu den Voraussetzungen: Hilgendorf, in: LK-StGB, § 199 Rn. 2 ff.

eigene Unzulänglichkeiten anspielt (Bilder von Alltagsmissgeschicken, Unfällen, schlechten Leistungen im Sport oder im Zwischenmenschlichen) berührt zunächst selbstbestimmt die Sphäre des Urhebers. Wenn nun, angeregt und auch vom Urheber intendiert, weitere Kommentare, Bilder oder sonstige Beiträge diese Diffamierung verstärken, ist fraglich, ab wann der strafrechtserhebliche Bereich beginnt bzw. ob überhaupt – unter dem Aspekt der Strafwürdigkeit – eine zu pönalisierende Handlung vorliegen kann.

78 Jedenfalls ist nicht anzunehmen, dass die Verstärkung durch Dritte von gegenüber sich selbst geäußerten ehrenrührigen Behauptungen unter die Wechselseitigkeit i. S. d. § 199 StGB fällt. Es fehlt bereits am Aspekt der „ausgleichenden Gerechtigkeit", da die „Eigenbeleidigung" selbst nicht strafbewährt ist und somit kein Platz für eine Kompensation des Unrechts gegeben ist.

7.5.4.5 Zivilrechtlicher Kontext der Beleidigungsdelikte

79 Unabhängig von einer strafrechtlichen Verantwortlichkeit (§§ 185 ff. StGB) ergibt sich für den Kundgebenden aus dem Deliktsrecht (neben § 823 Abs. 1 BGB) speziell aus § 823 Abs. 2 BGB auch die Gefahr einer **zivilrechtlichen Haftung**. Die Norm des § 823 Abs. 2 BGB setzt die Verletzung eines Schutzgesetzes voraus. Als solches gilt jede Rechtsnorm i. S. d. Art. 2 EGBGB; als Schutzgesetz kommen jedoch nur solche Normen in Betracht, deren Schutz zumindest auch auf bestimmte Rechtsgüter oder Interessen des Einzelnen zielt.[136] Die überwiegende Mehrheit der Normen des StGB lassen sich unter den Begriff des Schutzgesetzes subsumieren, so auch die Beleidigungsdelikte der §§ 185 ff. StGB.[137] Hinsichtlich der Voraussetzungen des § 823 Abs. 2 BGB ergeben sich nur wenige Besonderheiten. Neben der Schutzgesetzeigenschaft müssen die tatbestandlichen Voraussetzungen der §§ 185 ff. StGB vorliegen. Das bei § 823 Abs. 2 BGB erforderliche Verschulden muss sich nicht auf das Entstehen des entsprechenden Schadens bzw. Erfolges erstrecken, sondern allein auf die Schutzgesetzverletzung.[138] Nach ganz überwiegender Auffassung ist der Wortlaut des § 823 Abs. 2 BGB als Gesamtverweisung auf sämtliche im StGB geltenden Formen der Schuld zu verstehen, so dass sich letztlich auch hier keine Besonderheiten ergeben.[139]

80 Hinsichtlich der **Beweislast** kommt grundsätzlich der im Zivilrecht geltende Grundsatz zur Anwendung, dass der mutmaßlich Geschädigte verpflichtet ist, die Voraussetzungen für einen Anspruch aus § 823 Abs. 2 BGB darzulegen und ggf. zu beweisen. Dies gilt allerdings nicht, wenn das Schutzgesetz selbst besondere Beweislastregeln enthält, wie dies gerade bei den Beleidigungsdelikten zum Teil der Fall ist. Dazu gehört die faktische Beweislastumkehr (objektive Bedingung der Strafbarkeit)

---

[136] Teichmann, in: Jauernig, BGB, § 823 Rn. 44.
[137] Wagner, in: MüKo-BGB, § 823 Rn. 423; Spindler, in: BeckOK-BGB, § 823 Rn. 175. Siehe auch LG Berlin, ZUM 2012, 997 (8.000 € für fortgesetzte Beleidigungen in sozialen Netzwerken).
[138] Wagner, in: MüKo-BGB, § 823 Rn. 434.
[139] Spindler, in: BeckOK-BGB, § 823 Rn. 164.

in Bezug auf die Wahrheit einer vom Schädiger verbreiteten ehrenrührigen Tatsache (§ 186 StGB, Rn. 82 f.) oder die Beweisregel des § 190 StGB.[140]

Darüber hinaus können ehrverletzende Äußerungen gegenüber dem Arbeitgeber diesen zu einer **außerordentlichen Kündigung** berechtigen.[141] **81**

7.5.4.6 Üble Nachrede (§ 186 StGB)

Im Gegensatz zu § 185 StGB stellt § 186 StGB nur das Behaupten und Verbreiten **nicht erweislicher Tatsachen**, die einen Angriff auf die Ehre des Betroffenen darstellen, unter Strafe. Die vom Täter behauptete Tatsache muss geeignet sein, die betroffene Person verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen. Hinsichtlich der Begehungsweise und der Besonderheiten bei der Nutzung des Mediums Internet ergeben sich letztlich keine Abweichungen zu den Ausführungen bei § 185 StGB. Bei Äußerungen in sozialen Netzwerken dürfte es sich in den meisten Fällen um Werturteile und nicht um Tatsachen handeln, sodass § 186 StGB in einer deutlich geringeren Anzahl von Fällen einschlägig sein wird. **82**

Handelt es sich aber im konkreten Fall um eine unwahre Tatsachenbehauptung, kann auch die **Qualifikation des § 186 2. Hs StGB** einschlägig sein. Diese setzt eine öffentliche oder durch Schriften verbreitete Begehungsweise voraus. **Öffentlich** wird die Tat verübt, wenn das Behaupten oder Verbreiten ein nach Zahl und Zusammensetzung unbestimmter oder ein nicht durch eine spezifische Beziehung verbundener größerer, wenn auch bestimmter Personenkreis unmittelbar wahrnehmen kann.[142] Auch in sozialen Netzwerken können unwahre Tatsachenbehauptungen einem unbestimmten Personenkreis zugänglich gemacht werden, wenn der Nutzer sein Profil nicht beschränkt. Selbst wenn eine Einschränkung der Personen erfolgt, die auf das Nutzerprofil zugreifen können, wird es sich in aller Regel um einen größeren Personenkreis handeln, mit dem der Nutzer zum Großteil in keiner engeren Beziehung steht (bei Twitter dürfte das sogar immer der Fall sein). Für die Annahme einer öffentlichen Begehungsweise reicht das nach der oben genannten Definition bereits aus. Weiterhin könnte man auch an das Vorliegen der dritten Qualifikationsalternative des „**Verbreitens von Schriften**“ denken. Die Definition des **83**

---

[140] Wagner, in: MüKo-BGB, § 823 Rn. 483.

[141] LAG Hamm, ZD 2013, 93; Bezeichnung des Arbeitgebers als „Menschenschinder“ und „Ausbeuter“ in Facebook; außerordentliche Kündigung gerechtfertigt (auch in Berufsausbildungsverhältnissen und im Lichte des Grundrechts der Meinungsfreiheit wegen Schwere der Ehrverletzung, Schmähung, Formalbeleidigung). Siehe auch ArbG Duisburg, NZA-RR 2013, 18 (fristlose Kündigung wegen Beleidigung von Kollegen via facebook); ArbG Dessau-Roßlau, BeckRS 2012, 69099 (Kündigung wegen Betätigung des „Gefällt-mir-Bottons“ bezüglich einer beleidigenden Äußerung via Facebook); ArbG Hagen, BeckRS 2012, 71401 (Post über Vorgesetzten als „kleiner Scheißhaufen“, „Wichser“, „faules Schwein“, für 36, teils betriebsinterne, Freunde einsehbar); vgl. auch Bauer/Günther, NZA 2013, 67; Scheid/Sigle, ArbRAktuell 2013, 341083; Däubler, AiB 2014, 26; zu sog. „Social Media Guidelines“ zur Prävention und zum verantwortlichen Umgang der Arbeitnehmer mit sozialen Medien, vgl. Günther, ArbRAktuell 2013, 223 (224 f.).

[142] Hilgendorf, in: LK-StGB, § 186 Rn. 13.

Tatbestandsmerkmals „Verbreiten von Schriften“ ist jedoch presserechtlich geprägt und setzt somit voraus, dass die Schrift einem größeren Personenkreis körperlich zugänglich gemacht wird und eben nicht nur, wie im Internet zwangsläufig nötig, ihrem Inhalt nach.[143] Der BGH hatte allerdings in einem Urteil zum früheren § 184 Abs. 3 Nr. 1 StGB festgestellt, dass diese enge Interpretation des Verbreitens auf Publikationen im Internet nicht anwendbar ist; stattdessen wird auf die Übertragung von Daten abgestellt.[144] Im Schrifttum ist dieser Ansatz bislang überwiegend auf Kritik gestoßen.[145] Unabhängig von der genauen Definition des Verbreitens von Schriften im Internet dürfte jedoch in nahezu allen Fällen die erste Qualifikationsalternative („öffentlich“) einschlägig sein (s. o.).

7.5.4.7 Verleumdung (§ 187 StGB)

84 Vom Tatbestand der üblen Nachrede unterscheidet sich die Verleumdung objektiv in der Hinsicht, dass die Unwahrheit der behaupteten oder verbreiteten Tatsachen objektives Tatbestandsmerkmal ist und dass die Variante der Kreditgefährdung hinzutritt. Subjektiv muss der Täter **wider besseres Wissen** handeln, *dolus eventualis* genügt also nicht. Ansonsten ergeben sich keine Besonderheiten; auch hier können Qualifikationstatbestände einschlägig sein.

7.5.5 Straftaten gegen die sexuelle Selbstbestimmung/Verbreitung pornographischer Schriften (§§ 184–184d StGB)

85 Ein großer Teil des Internet besteht mittlerweile aus Material mit sexuellem, oftmals pornographischem Inhalt, das mangels effektiver Sperrvorrichtungen zumeist frei verfügbar ist – auch für Kinder und Jugendliche. Diese **permanente Präsenz sexualisierter Bilder** hat erhebliche Auswirkung auf die Alltags- und Gesprächskultur von jungen Menschen. Die Sprache von Jugendlichen enthält zunehmend sexualisierte Begriffe. Die sexuellen „Vorgaben“ des Internet führen zu einem Anpassungsverhalten und mangels Erfüllbarkeit der Erwartungen nicht selten zu Frustrationen im Alltag.

86 Die u.a. dem Schutz junger Menschen vor schädlichen sexuellen Einflüssen dienenden §§ 184 ff. StGB stellen den Umgang mit pornographischen Schriften in Form verschiedener Tathandlungen unter Strafe. Dabei unterscheidet das Gesetz zwischen „einfachen“ **pornographischen Schriften** (§ 184 StGB) und „harten“ pornographischen Schriften in Form der **Gewalt- und Tierpornographie (§ 184a StGB)** bzw. **Kinderpornographie (§ 184b StGB)** mit entsprechend höherer Strafandrohung.

---

[143] Lenckner/Eisele, in: Schönke/Schröder, StGB, § 186 Rn. 20.
[144] BGH, NJW 2001, 3558 (3559).
[145] Vgl. die Darstellung des Meinungsspektrums bei: Hilgendorf et al., Rn. 409 ff. Vgl. auch Bornemann, MMR 2012, 157.

Infolge der rasanten technischen Neuerungen der letzten Jahrzehnte hat sich das Internet zu einer Plattform für die Begehung dieser Straftatbestände entwickelt.

Soziale Netzwerke sind geradezu prädestiniert, die Verwirklichung der §§ 184 ff. StGB zu fördern; sie ermöglichen den Kontakt zwischen sich oftmals unbekannten Personen und werden dabei überwiegend von jungen Menschen (davon ein Großteil Kinder und Jugendliche) genutzt. Mehrere Faktoren, die eine Begehung von „**Verbreitungsdelikten**" im Internet allgemein begünstigen (gesteigerte Anonymität, einfache Zugänglichkeit, unbegrenzbare Verbreitungsmöglichkeiten), führen somit dazu, dass soziale Netzwerke auch für diese Delikte als „Tatort" in Betracht kommen. **87**

7.5.5.1 Zentrales Tatbestandsmerkmal: Pornographische Schriften

Gemeinsames Tatobjekt der §§ 184 ff. StGB sind die sog. pornographischen Schriften. In der Praxis verhältnismäßig wenig Probleme bereitet die Einordnung von Darstellungen in sozialen Netzwerken als „**Schriften**". Durch den Verweis auf § 11 Abs. 3 StGB stellen sämtliche Tatbestände klar, dass den „klassischen" Schriften Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleichstehen. Das Einstellen und Abrufen von pornographischen Darstellungen kann dabei verschiedene „Schrift"-Merkmale erfüllen. **88**

Unter **Datenspeichern** sind sämtliche Speichermedien zur Aufzeichnung von Daten zu verstehen, die gedankliche Inhalte verkörpern, die nur unter Zuhilfenahme technischer Geräte abrufbar sind.[146] Nach überwiegender Ansicht fällt unter diesen Begriff auch der nicht permanente elektronische **Arbeitsspeicher**[147] sowie der als nicht permanenter Speicherort benutzte sog. *Cache*; dass der Cache automatisch und systembedingt wieder gelöscht wird, soll am (temporären) **Besitz** des Täters an den Inhalten nichts ändern.[148] Daher soll bereits das Anzeigen von Bildern auf dem Computerbildschirm als Verkörperung des Inhalts des Arbeitsspeichers unter den Begriff des Datenspeichers fallen.[149] Diese Ausweitung der §§ 184 ff. StGB erfolgte im Jahre 1997 durch das **Informations- und Kommunikationsdienste-Gesetz (IuKDG)**[150], um den durch das Internet begründeten Gefahren für den Kinder- und Jugendschutz (Markt/Nachfrage für den eigentlichen Missbrauch der Kinder und Jugendlichen) auf wirksame Weise begegnen zu können.[151] **89**

---

[146] Fischer, StGB, § 11 Rn. 36.

[147] Fischer, StGB, § 11 Rn. 36; BGH, NJW 2013, 2914 m. Anm. Hermann, StRR 2013, 431; OLG Hamburg, NJW 2010, 1893 m. Anm. Mintas; Eckstein, NStZ 2011, 18.

[148] OLG Hamburg, StV 2009, 469; AG Saarbrücken, Urt. v. 29.7.2009 – 115 Ds 87/09 (Feststellung eines Besitz-/Herrschaftswillens erforderlich). Zustimmend Gercke, ZUM 2010, 633 (641 f.).

[149] Fischer, StGB, § 11 Rn. 36a; OLG Hamburg, NJW 2010, 1893 = StV 2011, 99 = NStZ 2010, 704; zustimmend Eckstein, NStZ 2011, 18 (20), ders., ZStW 117 (2005), 107 (119 ff.); ablehnend Gercke, ZUM 2010, 633 (642 f.).

[150] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 22.7.1997, BGBl. I, S. 1870; dazu Engel-Flechsig et al., NJW 1997, 2981.

[151] Hilgendorf et al., Rn. 379.

90 Weiterhin ließe sich eine über das Internet in sozialen Netzwerken bereitgestellte bzw. aufgerufene Abbildung auch unter den Begriff der **Darstellung** subsumieren.

91 Um Kinderpornographie im Internet besser bekämpfen zu können, sieht der im Dezember 2013 zwischen den Regierungsparteien CDU, CSU und SPD geschlossene Koalitionsvertrag die Erweiterung des „veralteten Schriftenbegriff[s]" zu einem „**modernen Medienbegriff**" vor.[152]

92 Schwieriger ist dagegen die Definition des Begriffs der **Pornographie**. Nach überwiegender Auffassung versteht man darunter eine „Darstellung [...], die unter Ausklammerung sonstiger menschlicher Bezüge sexuelle Vorgänge in grob aufdringlicher Weise in den Vordergrund rückt und die in ihrer Gesamttendenz ausschließlich oder überwiegend auf sexuelle Stimulation angelegt ist, sowie dabei die im Einklang mit allgemeinen gesellschaftlichen Wertevorstellungen gezogenen Grenzen eindeutig überschreitet"[153]. Vielfach wird als Konkretisierung auf eine „*Objektformel*" zurückgegriffen und das Vorliegen von Pornographie demnach angenommen, wenn ein Mensch zum „bloßen auswechselbaren Objekt geschlechtlicher Begierde degradiert"[154] wird. Trotz dieser ausführlichen Definition wird eine abstrakte Aussage darüber, was nun Pornographie darstellt und was nicht, schwer fallen.[155] Der Verweis auf gesellschaftliche Wertevorstellungen setzt immer das Bestehen einheitlicher moralischer Wertevorstellungen voraus; solche lassen sich in modernen Gesellschaften jedoch nur sehr schwer festlegen, so dass über das Vorliegen von Pornographie letztlich nur unter Heranziehung der Umstände im Einzelfall entschieden werden kann.[156] Bei Zweifelsfällen ist in der Praxis nach dem Grundsatz „in dubio pro reo" zu verfahren.

7.5.5.2 Verbreitung pornographischer Schriften (§ 184 StGB)

93 Gemäß § 184 Abs. 1 Nr. 1 StGB macht sich strafbar, wer einer Person unter achtzehn Jahren pornographische Schriften[157] anbietet, überlässt oder zugänglich macht, also diese an minderjährige Personen verbreitet. Ein **Zugänglichmachen** liegt bereits dann vor, wenn dem Minderjährigen die konkrete Möglichkeit unmittelbarer

---

[152] Koalitionsvertrag zwischen CDU, CSU und SPD (Fn. 6), S. 145.

[153] Eisele, in: Schönke/Schröder, StGB, § 184 Rn. 8.

[154] Fischer, StGB, § 184 Rn. 7; Hörnle, in: MüKo-StGB, § 184 Rn. 17; OLG Düsseldorf, NJW 1974, 1474 (1475); OLG Karlsruhe, NJW 1987, 1957; KG, NStZ 2009, 446 (447); kritisch zu den Definitionsversuchen der Rechtsprechung: Laufhütte/Roggenbuck, in: LK-StGB, § 184 Rn. 4 ff.

[155] Vgl. umfassend zu den Definitionsschwierigkeiten: Laufhütte/Roggenbuck, in: LK-StGB, § 184 Rn. 4 ff.; bejahend für sog. „Pornomontagen", d. h. Videoklips mit einer Person (z. B. Lehrer) als Darsteller in einem fiktiven sexuellen Handlungsvorgang: Beck, MMR 2008, 77 (80).

[156] Zur Einordnung von Darstellungen als Pornographie vertiefend: Schreibauer, Das Pornographieverbot des § 184 StGB, 1999; Mahrenholz, ZUM 1998, 525; Schumann, in: FS Lenckner (1998), S. 565; Ladeur, AfP 2001, 471; Erdemir, MMR 2003, 628; Sieber, ZUM 2000, 89.

[157] Vgl. Art. 1 Nr. 13 RefE (Fn. 31), S. 28, 34, wonach anstelle des Plurals „Schriften" die Verwendung des Singulars „Schrift" vorgeschlagen wird. Eine inhaltliche Änderung soll damit nicht verbunden sein.

Kenntnisnahme für kurze oder längere Zeit eröffnet wird.[158] Bezogen auf soziale Netzwerke liegt diese Tatvariante bereits vor, wenn eine Datei in das Internet gestellt wird und dem Nutzer eine Zugriffsmöglichkeit eröffnet wird.[159] Bei sämtlichen sozialen Netzwerken dürfte das zumeist bereits der Fall sein, sobald der Minderjährige ein **Benutzerkonto** durch den Betreiber des sozialen Netzwerks zugewiesen bekommt *und* sich über dieses Konto anmeldet. Zwar ist ihm durch die Anmeldung nicht ohne Weiteres der Zugriff auf sämtliche Inhalte des sozialen Netzwerks möglich. Bei Facebook und studiVZ kann etwa auf Profile mit entsprechenden **Sicherheitseinstellungen** erst nach einer erfolgreich gestellten Freundschaftsanfrage zugegriffen werden; bei Twitter wird ein solcher Zugang erst ermöglicht, nachdem der Nutzer „Follower" der betreffenden Person geworden ist. Bei Facebook bleibt aber ein Zugriff auf sämtliche von Nutzern betriebenen Seiten durch eine einfache „Gefällt mir"-Angabe möglich. Eine Anmeldung bei Facebook kann bereits mit Vollendung des dreizehnten Lebensjahres erfolgen[160], bei dem im April 2013 geschlossenen Netzwerk schuelerVZ war eine Teilnahme erst ab einem Alter von zehn Jahren möglich. Die strengsten Anforderungen bestehen diesbezüglich bei studiVZ – hier erfolgt laut AGB eine Altersbeschränkung auf 16 Jahre. Eine weitergehende **Kontrolle des Alters** in Bezug auf bestimmte Inhalte erfolgt jedoch einheitlich bei allen sozialen Netzwerken – trotz Bestehens entsprechender technischer Möglichkeiten der Abfrage nicht.[161] Letztlich kann die Altersangabe der Nutzer auf keine Weise sicher überprüft werden, sodass davon auszugehen ist, dass nicht wenige Nutzer diesbezüglich unwahre Angaben machen und tatsächlich nicht einmal das von den Betreibern vorgegebene Mindestalter erreicht haben.

94 Mitunter wird sogar schon das **Setzen eines Links** auf der eigenen Homepage zu einer Website mit pornographischen Inhalten ausreichend sein, wenn sich der Betreiber die Inhalte als eigene zurechnen lassen muss. Diese Verlinkung wird in der Regel jedoch allenfalls den Tatbestand der Beihilfe erfüllen, weil ein Homepagebetreiber durch das schlichte Setzen eines Hyperlinks keine eigene Herrschaft über die Datenspeicherung hat.[162]

95 Eine tatsächliche Wahrnehmung der Inhalte durch ein Betrachten oder sogar Herunterladen der Inhalte muss aufgrund der Ausgestaltung von § 184 Abs. 1 Nr. 1 StGB als **abstraktes Gefährdungsdelikt** ebenso wenig erfolgen wie eine Individualisierung des Minderjährigen.[163]

---

[158] Fischer, StGB, § 184 Rn. 10; Laufhütte/Roggenbuck, in: LK-StGB, § 184 Rn. 18; BGH, NJW 1976, 1984.
[159] Fischer, StGB, § 184 Rn. 34.
[160] Vgl. dazu die Standards der Facebook-Gemeinschaft, Nr. 4 „Registrierung und Sicherheit der Konten": (5) „Du wirst Facebook nicht verwenden, wenn du unter 13 Jahre alt bist.", abrufbar unter www.facebook.de.
[161] Vgl. dazu Jandt/Roßnagel, MMR 2011, 637, die eine effektivere Altersüberprüfung in sozialen Netzwerken fordern.
[162] LG Karlsruhe, MMR 2009, 418 = NStZ-RR 2009, 309; Hörnle, in: MüKo-StGB, § 184 Rn. 48.
[163] Hilgendorf et al., Rn. 399 f.; Hörnle, in: MüKo-StGB, § 184 Rn. 28.

96 Zudem kommt eine Verwirklichung des **§ 184 Abs. 1 Nr. 2 StGB** in Betracht. Hiernach macht sich strafbar, wer pornographische Schriften an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, ausstellt, anschlägt, vorführt oder sonst zugänglich macht. Der RefE des BMJV vom April 2014 schlägt „zur redaktionellen Bereinigung" jedoch vor, künftig im Wortlaut des Gesetzes nur noch auf den Oberbegriff des „Öffentlichen-Zugänglichmachens" abzustellen.[164] Unter einem „**Ort**" ist dabei nach dem allgemeinen Sprachgebrauch eine Räumlichkeit zu verstehen, die körperlich betreten oder aufgesucht werden kann, womit das Internet selbst als möglicher Anknüpfungspunkt ausscheidet.[165] Es ist jedoch mit dem Wortlaut der Norm vereinbar, auf die Örtlichkeiten abzustellen, von denen aus auf das entsprechende Angebot zugegriffen werden kann, also etwa Schulen, Internet-Cafés oder private Computer mit einem Internetanschluss.[166]

97 Neben dem Anbieter pornographischer Inhalte kommt in diesen Fällen auf den ersten Blick eine weitere Personengruppe als Täter in Betracht: diejenigen, die den Minderjährigen den Zugriff auf den Computer ermöglichen, also etwa **Eltern, Lehrer** oder die **Betreiber von Internet-Cafés**.[167] Dies hätte jedoch eine unverhältnismäßige Ausweitung der Strafbarkeit zur Folge. Unter dem Gesichtspunkt des Bereitstellens eines Computers mit Internetzugang als **sozialadäquates Verhalten** (fehlende Strafwürdigkeit) ist daher eine Einschränkung der möglichen Strafbarkeit geboten. In Literatur und Rechtsprechung hat sich daher folgerichtig für die Annahme eines Tatbestandsausschlusses die Ansicht etabliert, dass hinsichtlich des Bereitstellens pornographischer Inhalte im Internet bzw. in sozialen Netzwerken das Bestehen einer Sicherung genügt, die eine effektive Barriere darstellt.[168] Es erscheint jedoch mehr als fraglich, dass allein die Sicherheitsvorkehrungen sozialer Netzwerke den Anforderungen einer „effektiven Barriere" genügen (vgl. Rn. 93). Eine solche Effektivität wurde bisher nicht einmal in den Fällen der Abfrage von Personalausweis- oder Kreditkartennummern angenommen.[169] Eine einfache Altersabfrage ohne weitergehende Kontrollen dürfte somit kaum ausreichend sein, um einen Tatbestandsausschluss zu bejahen. Auf der strafrechtlich sicheren Seite bewegt sich letztlich nur, wer auf den entsprechenden Computern ein **Filter-Programm** betreibt, das Seiten mit sexuellem Inhalt wirksam blockt.

---

[164] Art. 1 Nr. 13 RefE (Fn. 31), S. 28, 34.
[165] Hilgendorf et al., Rn. 401; Hörnle, in: MüKo-StGB, § 184 Rn. 33; Eisele, in: Schönke/Schröder, StGB, § 184 Rn. 241.
[166] Fischer, StGB, § 184 Rn. 11; Esser, GA 157 (2010), 65 (67 f.).
[167] Hilgendorf et al., Rn. 403; Eisele, in: Schönke/Schröder, StGB, § 184 Rn. 24.
[168] Eisele, in: Schönke/Schröder, StGB, § 184 Rn. 18 f., 23 f., 26 f.
[169] Eisele, in: Schönke/Schröder, StGB, § 184 Rn. 18.

7.5.5.3 Verbreitung gewalt- oder tierpornographischer Schriften (§ 184a StGB)

98 § 184a Abs. 1 Nr. 1 StGB stellt ein „Verbreiten" gewalt- oder tierpornographischer Schriften[170] unter Strafe. In sozialen Netzwerken dürften Verstöße gegen diese Norm eine deutlich geringere Bedeutung haben als solche gegen § 184 StGB. Ein Verbreiten setzt grundsätzlich eine körperliche Weitergabe voraus, also dass die pornographische Schrift vom Täter gegenständlich an einen größeren, von ihm nicht mehr individualisierbaren Personenkreis weitergegeben wird.[171] Eigentlich wäre somit das Einstellen pornographischer Inhalte in soziale Netzwerke nicht von der ersten Tatvariante umfasst, da bei der bloßen Bereitstellung von Daten in das Internet keine Verkörperung stattfindet, sondern ein reines *Zugänglichmachen* des Inhalts, welches von § 184a Abs. 1 Nr. 2 StGB erfasst wird (Rn. 100). Der BGH entschied jedoch im Jahr 2001, dass bei Veröffentlichungen im Internet ein „**spezifischer Verbreitungsbegriff**" gelten solle.[172] Danach soll ein Verbreiten im Internet bereits vorliegen, „wenn die Datei auf dem Rechner des Internetnutzers – sei es im (flüchtigen) Arbeitsspeicher oder auf einem (permanenten) Speichermedium – angekommen ist" (vgl. Rn. 89). Zur Begründung verweist der BGH auf die Gewährleistung eines effektiven Jugendschutzes im Internet und auf die Gleichstellung des Arbeitsspeichers mit Schriften i. S. d. § 11 Abs. 3 StGB. Das ebenfalls angeführte Argument einer angeblichen Schutzlücke in Bezug auf im Internet veröffentlichte pornographische Schriften vermag jedoch nicht zu überzeugen, da eine solche tatsächlich nicht besteht. Strafwürdige Sachverhalte und Inhalte, denen der BGH durch den weiten „Verbreitungsbegriff" begegnen will, lassen sich unter das Merkmal des „Zugänglichmachens" des § 184a Abs. 1 Nr. 2 StGB fassen.[173] Auch der Hinweis auf § 11 Abs. 3 StGB ist für die Annahme und Forderung eines weiten „Verbreitungsbegriffs" nicht überzeugend. Letztlich führt diese Argumentation zu einer diffusen Vermischung der Definition des Tatobjekts „Schrift" und der Tathandlung „Verbreiten".[174] Die schlichte Erfassung des körperlichen Arbeitsspeichers als „Schrift" ändert im Ergebnis nichts an der Tatsache, dass die auf ihm gespeicherten Daten weiterhin unkörperlich sind.[175] Vielmehr gebietet das Gesetz selbst eine genaue Unterscheidung, indem der Begriff des Verbreitens an die Weitergabe einer Schrift und der des Zugänglichmachens an die Weitergabe des Inhalts anknüpft.[176] Für die Praxis ist

---

[170] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 28, 35, wonach anstelle des Plurals „Schriften" die Verwendung des Singulars „Schrift" vorgeschlagen wird. Eine inhaltliche Änderung soll damit nicht verbunden sein.

[171] Eisele, in: Schönke/Schröder, StGB, § 184b Rn. 5, § 184a Rn. 5; Fischer, StGB, § 184b Rn. 8.

[172] BGHSt 47, 55 = NJW 2001, 3558 (3560) = JR 2002, 204 m. Anm. Lindemann/Wachsmuth = JZ 2002, 308 m. Anm. Kudlich = MMR 2001, 676 m. Anm. Gercke; zum identischen Begriff des Verbreitens i. R. d. § 184b Abs. 1 Nr. 1 StGB vgl. BGH, NStZ-RR 2014, 47; BGH, BeckRS 2013, 08218.

[173] So schon: Lindemann/Wachsmuth, JR 2002, 206 (207).

[174] Siehe: Kudlich, JZ 2002, 310 (311); Fischer, StGB, § 184 Rn. 35.

[175] Hilgendorf et al., Rn. 413; Eckstein, NStZ 2011, 18 (19 f.).

[176] Hilgendorf et al., Rn. 413.

es letztlich irrelevant, ob man dem Begriff des Verbreitens ein weites Verständnis zugrunde legt oder ob man die entsprechenden Handlungen unter den Begriff des Zugänglichmachens subsumiert.

99 Die Rechtsprechung ist indes dem Urteil des BGH von 2001 weitgehend gefolgt: Das OLG Hamburg hat 2010 entschieden, dass die mit dem Aufrufen von Internetinhalten verbundene automatische Zwischenspeicherung dieser Inhalte im Arbeitsspeicher des Computers ein Sich-Verschaffen i. S. v. § 184b StGB darstellt und damit spiegelbildlich auch ein Verbreiten des Inhalts.[177] Zur weiteren Entwicklung in der Rechtsprechung siehe unten bei § 184b StGB.

100 § 184a Abs. 1 Nr. 2 StGB setzt ein **Zugänglichmachen** (konkretisiert durch die speziellen Tatvarianten des Ausstellens, Anschlagens und Vorführens) [178] der tatbestandsrelevanten Schriften voraus, hier jedoch unter der Einschränkung der „**Öffentlichkeit**" desselben. Es muss also die Möglichkeit der Kenntnisnahme der pornographischen Schrift durch einen größeren, in seiner Zahl und Zusammensetzung unbestimmten Personenkreis bestehen.[179] Ein öffentliches Zugänglichmachen liegt bei dem Einstellen einer für alle nutzbaren Homepage in das Internet vor.[180] Soziale Netzwerke zeichnen sich dagegen gerade dadurch aus, dass ihre Inhalte eben nicht unbeschränkt von Jedermann eingesehen werden können, sondern dass zuvor eine Registrierung und Anmeldung bzw. weitere Schritte zu erfolgen haben (Freundschaftsanfrage, Follower etc.), um auf bestimmte Inhalte zugreifen zu können. Um das Tatbestandsmerkmal der Öffentlichkeit jedoch tatsächlich verneinen zu können, bedarf es weitergehender Beschränkungen als der, die derzeit von sozialen Netzwerken verlangt werden (vgl. hierzu die Ausführungen bei den Beleidigungstatbeständen, Rn. 55). Zu denken wäre in diesem Zusammenhang etwa an eine gänzlich ***geschlossene Benutzergruppe***, deren Zugangsdaten tatsächlich nur einem begrenzten Personenkreis zugänglich sind.[181] Wie aber erläutert, bleiben in sämtlichen sozialen Netzwerken etliche Inhalte für alle Nutzer einsehbar, ohne dass eine weitere auf den Inhalt bezogene Beschränkung erfolgt. Das Merkmal der Öffentlichkeit dürfte damit bei sämtlicher in sozialen Netzwerken einsehbarer Pornographie erfüllt sein.

---

[177] OLG Hamburg, NJW 2010, 1893 (1894 f.).

[178] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 35, 28, wonach auch hier künftig nur noch der Oberbegriff des „*Öffentlichen-Zugänglichmachens*" im Wortlaut des Gesetzes genannt werden soll.

[179] Hilgendorf et al., Rn. 407; Laufhütte/Roggenbuck, in: LK-StGB, § 184 Rn. 8.

[180] Fischer, StGB, § 184b Rn. 10.

[181] Hilgendorf et al., Rn. 408; Fischer, StGB, § 184b Rn. 10; Eisele, in: Schönke/Schröder, StGB, § 184b Rn. 6.

7.5.5.4 Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB)

101 Der Tatbestand des § 184b StGB untersagt es, Kinder als Darsteller für pornographische Schriften zu missbrauchen.[182] Insofern verbietet § 184b Abs. 1 StGB die Verteilung und § 184b Abs. 2 StGB den Besitz sowie die Verschaffung kinderpornographischer Schriften. § 184b Abs. 3 StGB enthält einen Qualifikationstatbestand bei gewerbs- bzw. bandenmäßiger Begehungsweise. Bislang ist die versuchte Begehung der Tat nicht strafbar. Da jedoch bereits bestimmte Vorbereitungshandlungen strafbar sind, soll nach dem RefE des BMJV vom April 2014 eine teilweise Versuchsstrafbarkeit eingeführt werden (§ 184b Abs. 4 StGB-E).[183]

102 Die Norm weist in ihrer Struktur und den geforderten Tatmodalitäten im Vergleich mit den §§ 184, 184a StGB im Wesentlichen keine Besonderheiten auf. Es gelten auch in Bezug auf soziale Netzwerke die dortigen Ausführungen (Rn. 93 ff.).

103 Zu beachten ist jedoch, dass die (Dritt-)Verschaffung kinderpornographischer Schriften nach § 184b Abs. 2, 4 StGB auf die Fälle begrenzt ist, in denen die Schriften ein **tatsächliches oder wirklichkeitsnahes Geschehen** wiedergeben. Durch dieses Merkmal sollen offensichtlich nicht der Wirklichkeit entsprechende Produkte wie Zeichnungen, Zeichentrickfilme oder Comics ausgeschlossen werden.[184] Der BGH hat mit Beschluss vom 19.3.2013 ausdrücklich klargestellt, dass auch die rein mit Worten beschreibende Wiedergabe eines tatsächlich erfolgten Kindesmissbrauchs in einer E-Mail nicht tatbestandsgemäß ist.[185] Hingegen sollen auch fiktive Darstellungen (Zeichnungen etc.) als wirklichkeitsnah eingestuft werden, wenn sie ein durchschnittlicher Betrachter als tatsächlich geschehen auffasst.[186] Der RefE des BMJV über ein Gesetz zur Änderung des Strafgesetzbuches aus April 2014 schlägt vor, dass sich nach § 184b Abs. 1 Nr. 3 StGB-E künftig auch strafbar machen soll, wer eine kinderpornographische Schrift, die ein tatsächliches Geschehen wiedergibt, herstellt. Anders als nach § 184b Abs. 2 StGB-E soll es dabei nicht auf die Absicht der späteren Verbreitung ankommen. Damit soll die Erfüllung der Vorgaben nach Art. 5 der EU-Richtlinie 2011/93/EU[187] und Art. 20 Abs. 1 lit. a der auf der Ebene des Europarates geschlossenen sog. Lanzarote Konvention (ETS 201)[188] klargestellt

---

[182] Zum Zweck vgl. Lackner/Kühl, StGB, § 184b Rn. 1; zu den verschiedenen Erscheinungsformen vgl. Wernert, Internet Kriminalität, S. 126 f.

[183] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 30, 36.

[184] Lackner/Kühl, StGB, § 184b Rn. 6; Ziegle, in: BeckOK-StGB, § 184b Rn. 6; vgl. auch BT-Drs. 12/4883, S. 8 zu § 184 Abs. 4 StGB a. F.

[185] BGH, NJW 2013, 2914 m. Anm. Herrmann, StRR 2013, 431; vgl. Lackner/Kühl, § 184b Rn. 6; Ziegler in: BeckOK-StGB, § 184b Rn. 6; Eisele, in: Schönke/Schröder, StGB, § 184b Rn. 11.

[186] Vgl. BT-Drs. 13/7934, S. 41; Lackner/Kühl, StGB, § 184b Rn. 6; Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 332; vgl. auch BGHSt 43, 366 (369 f.).

[187] ABl. EU Nr. L 335 v. 17.12.2011, S. 1, berichtigt in ABl. EU Nr. L 18 v. 21.1.2012, S. 7.

[188] Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch v. 25.10.2007.

werden. Da es hiernach nicht auf die Erfassung eines wirklichkeitsnahen Geschehens ankommt, soll darauf verzichtet werden.[189]

104 Zu beachten ist ferner, dass eine **sexuelle Handlung** wiedergegeben werden muss. Eine sexuelle Handlung „von" einem Kind liegt vor, wenn das Kind in einer unnatürlichen, sexualbezogenen Körperhaltung aktiv posiert und so der Fokus z. B. auf den Genitalbereich gelegt wird (sog. **Posing**).[190] Reine Nacktbilder von Kindern, die sie in einer natürlichen Körperhaltung beispielsweise am Strand oder im Planschbecken im Garten zeigen, erfüllen dagegen den Tatbestand nach geltender Rechtslage nicht.[191]

105 Der **Freistaat Thüringen** sieht darin eine Strafbarkeitslücke und hat deshalb dem Bundesrat am 5.3.2014 eine Entschließung zur Verschärfung der strafrechtlichen Regelungen zum Kinder- und Jugendschutz zugeleitet, wonach der **gewerbliche Handel mit reinen Nacktaufnahmen von Kindern und Jugendlichen** zukünftig unter Strafe gestellt werden soll. Zur Begründung wird angeführt, dass der kommerzielle Handel mit derartigen Nacktaufnahmen einen schweren Verstoß gegen die Menschenwürde der betroffenen Kinder und Jugendlichen darstelle.[192]

106 Auch das **Land Hessen** hat am 6.3.2014 an den Bundesrat eine Entschließung zur Ergreifung von Maßnahmen zur stärkeren Bekämpfung der Kinderpornografie im Internet und zum Schutz von Kindern und Jugendlichen vor sexueller Ausbeutung gerichtet. Danach erscheine es notwendig, jedenfalls **Bilder von nackten Kindern, die ohne jeden sinnstiftenden Kontext** allein auf die sexuelle Erregung des Betrachters abzielen, umfassend unter Strafe zu stellen. Es solle geprüft werden, ob bereits die kommerzielle Erstellung und die einschlägige Weiterverbreitung solcher Bilder unter Strafe zu stellen sei.[193] Es erscheint jedoch höchst fraglich, ob durch diese Vorschläge tatsächlich Strafbarkeitslücken geschlossen bzw. Abgrenzungsschwierigkeiten beseitigt werden können. Es besteht vielmehr die Gefahr, dass *neue* Abgrenzungsfragen geschaffen werden.[194]

107 Ebenso hat der **Freistaat Bayern** am 1.4.2014 im Bundesrat einen Gesetzesentwurf vorgelegt, der sich gegen die Strafbarkeitslücken bei bloßen Nacktaufnahmen

---

[189] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 35 f.

[190] Vgl. BGH, BeckRS 2014, 00753; BT-Drs. 16/3439, S. 9; Hörnle, in: MüKo-StGB, § 184b Rn. 17; Eisele, in: Schönke/Schröder, StGB, § 184b Rn. 3a; zu Abgrenzungsschwierigkeiten Braun/Keller, Kriminalistik 2014, 208 (209 f.); zu immer noch bestehenden Strafbarkeitslücken eingehend Röder, NStZ 2010, 113. Nach BGH, Beschl. v. 11.2.2014 – 1 StR 485/13, NJW 2014, 1829 = StRR 2014, 233 muss die Darstellung der sexuellen Handlung keinen „vergröbernd reißerischen Charakter" aufweisen.

[191] Hörnle, in: MüKo-StGB, § 184b Rn. 14; Eisele, in: Schönke/Schröder, § 184b Rn. 3a. Zur Anwendbarkeit des KUG: Janisch, Surfen im Graubereich, SZ Nr. 38 v. 15./16.2. 2014, S. 2. Kritisch zur Rechtfertigung des Durchsuchungsbeschlusses im Fall *Edathy*: Hoven, NStZ 2014, 361; ablehnend: Braun / Keller, Kriminalistik 2014, 283. Die Abgrenzung zu strafbewehrten Posing-Bildern fällt in der Praxis schwer: Zur Einteilung des Materials durch das BKA in kinder- und jugendpornographisches Material (erste Kategorie) und nichtpornographisches Material (zweite Kategorie), SZ Nr. 38 v. 15./16.2.2014, S. 2.

[192] Vgl. Antrag des Freistaats Thüringen, BR-Drs. 89/14.

[193] Vgl. Antrag des Landes Hessen, BR-Drs. 91/14.

[194] Kritisch auch Braun/Keller, Kriminalistik 2014, 209 (211 f.).

ohne primär sexualbezogene Handlung richtet.[195] Die „kinder- und jugendpornographischen Schriften" der §§ 184b, 184c StGB sollen demnach auch die „**aufreizende Darstellung der entblößten Genitalien oder des entblößten Gesäßes**" erfassen.[196]

108 Ein RefE des BMJV vom April 2014 über ein Gesetz zur Änderung des Strafgesetzbuches schlägt vor, „**die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in unnatürlich geschlechtsbetonter Körperhaltung**" in § 184b Abs. 1 Nr. 1 StGB-E aufzunehmen. Damit sollen die sog. Posing-Bilder ausdrücklich tatbestandlich erfasst werden. Darüber hinaus soll es jedoch in Abkehr zur bisherigen Rechtslage nicht mehr darauf ankommen, dass das Kind die entsprechende sexualbezogene Pose bewusst einnimmt, sondern es soll künftig allein die Körperhaltung des Kindes entscheidend sein. Damit werden beispielsweise auch schlafende oder spielende Kinder vom Schutzbereich der Norm erfasst.[197]

109 Erwähnenswert ist zudem die **Strafbarkeitsausweitung** in § 184b Abs. 4 StGB auf das **(vorsätzliche) Unternehmen des Sich-Verschaffens von Besitz an kinderpornographischen Schriften (Satz 1)** und auf den **Besitz** selbst (Satz 2). Der RefE des BMJV sieht jedoch vor, dass § 184b Abs. 3 StGB-E aufgrund der Einführung der Versuchsstrafbarkeit künftig nicht mehr als Unternehmensdelikt ausgestaltet sein soll.[198] Unter **Besitz** ist das Erlangen der tatsächlichen Verfügungsmacht zu verstehen.[199] Der Tatbestand soll nach überwiegender Ansicht bereits dann erfüllt sein, wenn ein Abspeichern der betreffenden Inhalte im Cache (Speicher) des Computers erfolgt.[200] Das soll sogar dann gelten, wenn der Cache später manuell oder automatisch wieder gelöscht wird.[201] Der Besitzwille des Angeklagten muss in diesem Falle allerdings gesondert festgestellt werden.[202]

110 Noch weitergehender begründet nach Ansicht des OLG Hamburg bereits das bewusste und gewollte Aufrufen von Internetseiten mit kinderpornographischem Inhalt das Unternehmen, sich Besitz i. S. v. § 184b Abs. 4 StGB zu verschaffen, da hiermit unweigerlich ein zumindest temporäres Abspeichern im Arbeitsspeicher des Computers verbunden sei, welches wiederum notwendiges Durchgangsstadium jeder Weiterverarbeitung sei und somit ein hohes Maß an Datenherrschaft mit sich bringe.[203] Nach dem Vorschlag des RefE des BMJV soll künftig gemäß § 184d Abs. 2 StGB-E auch der **Abruf kinder- bzw. jugendpornographischen Inhalts mittels**

---

[195] Vgl. Antrag des Freistaates Bayern, BR-Drs. 127/14, S. 1 f., 9 f.
[196] Antrag des Freistaates Bayern, BR-Drs. 127/14, S. 3.
[197] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 35.
[198] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 36.
[199] Fischer, StGB, § 184b Rn. 20.
[200] BGH, NStZ 2007, 95; Harms, NStZ 2003, 646 (650); Ziegler, in: BeckOK-StGB, § 184b Rn. 16.
[201] OLG Hamburg, StV 2009, 469.
[202] AG Saarbrücken, Urt. v. 29.7.2009 – 115 Ds 87/09; AG Backnang, Beschl. v. 13.1.2014 – 2Cs 27 Js 61608/13, StRR 2014, 195.
[203] OLG Hamburg, NJW 2010, 1893 (1896).

Telemedien strafbar sein.[204] In der Literatur ist diese Auffassung allerdings auf starke Kritik gestoßen; sie wird überwiegend als zu weitgehend abgelehnt.[205] In den Fällen des Speicherns im Cache bzw. Arbeitsspeicher dürfte es ohnehin regelmäßig an einem erforderlichen Vorsatz bezüglich des Besitzes der Schriften fehlen.[206]

7.5.5.5 Verbreitung, Erwerb und Besitz jugendpornographischer Schriften (§ 184c StGB)

111 Auch die Verbreitung, der Erwerb und der Besitz jugendpornographischer Schriften (bzgl. Handlungen von, an oder vor Personen von 14 bis 18 Jahren) kann je nach Sachlage mittels sozialer Netzwerke begangen werden. Tatbestandlich ergeben sich gegenüber §§ 184, 184a StGB keine Besonderheiten. Wie bei § 184b StGB ist auch hier das **Unternehmen der Besitzverschaffung** sowie der **Besitz** des Materials strafbar u.a. (§ 184c Abs. 4 StGB). Der RefE des BMJV vom April 2014 sieht die Herstellung jugendpornographischer Schriften ohne Verbreitungsabsicht gemäß § 184c Abs. 1 Nr. 3 StGB-E nur dann als strafbar an, wenn der Schrift ein *tatsächliches* jugendpornographisches Geschehen zugrunde liegt.[207] Darüber hinaus soll gemäß § 184c Abs. 5 StGB-E die Strafbarkeit des Versuchs eingeführt werden.[208]

112 In diesem Zusammenhang ist das unter Jugendlichen zu beobachtende Phänomen zu erwähnen, dem Partner im Laufe einer Liebesbeziehung eine **selbstgefertigte Intim-/Nacktaufnahme** des eigenen Körpers (meist per Handy) zukommen zu lassen (sog. **Sexting**).[209] Auch derartige Bildnisse werden mitunter nach dem Scheitern der Beziehung aus Enttäuschung oder Rache an Dritte weitergeleitet und damit verbreitet (§ 184c Abs. 1 Nr. 1 StGB) oder zugänglich gemacht (§ 184c Abs. 1 Nr. 2 StGB). Die Privilegierung gemäß § 184c Abs. 1 2 StGB greift insofern nicht ein. Zudem kommt eine Strafbarkeit iSv § 201a Abs. 3 StGB in Betracht (Rn. 133 ff.).

---

[204] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 39 f.

[205] Fischer, StGB, § 184b Rn. 21b; Eisele, in: Schönke/Schröder, StGB, § 184b Rn. 15a, zustimmend dagegen Eckstein, NStZ 2011, 18. Ähnlich bereits ders., ZStW 117 (2005), 107 (117 ff.); a. A. Braun/Keller, Kriminalistik 2014, 209 (211) (Bejahung von „Besitz" jedenfalls, wenn der Nutzer über das Angebot im Internet bei Aufruf frei verfügen kann).

[206] Vgl. dazu AG Saarbrücken, Urt. v. 29.7.2009 – 115 Ds 87/09.

[207] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 38.

[208] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 39.

[209] Frommel, in: NK-StGB, Vor §§ 174 Rn. 1. Der Begriff setzt sich zusammen aus „Sex" und „texting". Vgl. hierzu Berendsen, Sexting unter Jugendlichen, Ich will was von dir sehen, FAZ v. 17.2.2014, abrufbar unter: http://www.faz.net/aktuell/gesellschaft/sexting-unter-jugendlichen-ich-will-was-von-dir-sehen-12804044.html. Zum Pendant „Revenge Porns" unter Erwachsenen, vgl. Wernert, Internet Kriminalität, S. 20.

7.5.5.6 Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste (§ 184d StGB)

113 Bieten soziale Netzwerke die Möglichkeit, Inhalte live per Webcam zu veröffentlichen, kann Pornographie i. S. d. §§ 184–184c StGB auch in Echtzeit übertragen werden. Der Schriftenbegriff gemäß § 11 Abs. 3 StGB ist dann mangels Verkörperung nicht erfüllt. Allerdings stellt § 184d StGB gerade die **Verbreitung** (zum Begriff Rn. 98) derartiger „Live-Darbietungen" durch Rundfunk, Medien- oder Teledienste (zum Begriff „Telemedien"[210] Rn. 280) unter Strafe.[211] Die Verbreitung weicher Pornographie (§ 184 Abs. 1 StGB) in Echtzeit via Medien- oder Teledienste ist nach § 184d Abs. 1 Satz 2 StGB hingegen straflos, wenn sichergestellt ist, dass sie Personen unter achtzehn Jahren nicht zugänglich ist. Der RefE des BMJV von April 2014 sieht in § 184e StGB-E vor, dass künftig auch die Veranstaltung bzw. der Besuch von kinder- sowie jugendpornographischen Live-Darbietungen unter Strafe steht.[212]

7.5.5.7 Sexueller Missbrauch von Kindern/Anbahnung sexueller Kontakte zu Minderjährigen (§ 176 Abs. 4 Nr. 3 StGB)

114 Die Kontaktaufnahme zu Kindern über das Internet mit dem Zweck, einen späteren sexuellen Kontakt oder Missbrauch vorzubereiten, ist ein seit mehreren Jahren zu beobachtendes Phänomen, das insbesondere durch die Anonymität sozialer Netzwerke begünstigt wird (vgl. ErwG Nr. 19 der EU-Richtlinie 2011/93/EU; Rn. 18)[213]. § 176 Abs. 4 Nr. 3 StGB stellt das sog. „**Cyber-Grooming**" unter Strafe, d. h. eine im Vorfeld von sexuellem Missbrauch stattfindende absichtliche Kontaktaufnahme des Täters zu seinem späteren Opfer.[214] Die Vorschrift wurde mit dem Ziel geschaffen, bereits Anbahnungshandlungen seitens des Täters, insbesondere Verabredungen mit Kindern in Chatrooms, zu unterbinden.[215] Diese sind vom Anwendungsbereich der Norm umfasst, da der auch hier verwendete Begriff der Schriften (Rn. 88) auch nur vorübergehende elektronische Datenspeicher wie etwa den Arbeitsspeicher umfasst und somit im Ergebnis die gesamte über Chatprogramme erfolgende Internetkommunikation.

---

[210] Vgl. zum Begriff auch Art. 1 Nr. 14 RefE (Fn. 31), S. 39.
[211] Vgl. BT-Drs. 15/350 v. 28.1.2003, S. 21; Lackner/Kühl, § 184d Rn. 3; Ziegler, in: BeckOK-StGB, § 184d Rn. 3. Nach Art. 1 Nr. 14 RefE (Fn. 31), S. 29, 39 soll die Tathandlung des „Verbreitens" durch die des „Öffentlich-Zugänglichmachens" ersetzt werden.
[212] Vgl. Art. 1 Nr. 14 RefE (Fn. 31), S. 42.
[213] ABl. EU Nr. L 335 v. 17.12.2011, S. 1, berichtigt in ABl. EU Nr. L 18 v. 21.1.2012, S. 7.
[214] Fischer, StGB, § 176 Rn. 1; vgl. auch Hube, Kriminalistik 2011, 71; umfassend zur Regelung: Eisele, in: FS Heinz (2012), S. 697 ff.
[215] Ziegler, in: BeckOK-StGB, § 176 Rn. 24; kritisch dazu Eisele, in: FS Heinz, S. 697 (701); Duttge et al., NJW 2004, 1065 (1067 f.).

115 Zur Umsetzung von Art. 6 Abs. 1 der Richtlinie 2011/93/EU[216] (hierzu Rn. 18) und Art. 23 der Lanzarote-Konvention (ETS 201)[217] sieht der RefE des BMJV zur Änderung des Strafgesetzbuches die Erweiterung des Tatbestandes um die Möglichkeit des **Einwirkens „mittels Informations- und Kommunikationstechnologie"** vor. Das Erfordernis der kurzzeitigen Zwischenspeicherung soll damit aufgegeben werden, so dass künftig auch solche Fälle erfasst sein sollen, in denen die Informationsübertragung ausschließlich über Datenleitungen, wie etwa Telefonleitungen erfolgt.[218]

116 Bedeutung erlangt die Norm im Hinblick auf soziale Netzwerke, weil diese regelmäßig neben der Nutzung von Profilen und Seiten auch **Chatprogramme als Kommunikationsform** anbieten. Die zur Anwendung kommenden Schriften selbst müssen keinen pornographischen Inhalt haben oder sexuellen Bezug aufweisen, vielmehr will das Gesetz bereits solche Handlungen erfassen, die Kinder durch „Tricks" oder Täuschungen zu einem Treffen außerhalb des Chatrooms veranlassen.[219] Der Sexualbezug erfolgt erst auf der subjektiven Ebene, indem der Täter mit der Absicht handeln muss, das Kind zu sexuellen Handlungen an oder vor dem Täter oder einem Dritten oder zur Duldung derselben zu bringen.[220] Ein Einwirken setzt eine Einflussnahme seitens des Täters und eine Kenntnisnahme der Schriften seitens des Kindes voraus.[221] Der tatsächliche sexuelle Übergriff kann im Anschluss nicht nur außerhalb des Chatrooms erfolgen, sondern auch dadurch, dass das Kind dem Täter Bilder des eigenen Körpers zusendet (sog. „Sexting"; Rn. 112).

117 Verurteilungen auf der Grundlage von § 176 Abs. 4 Nr. 3 StGB sind selten. Grund hierfür dürfte sein, dass sich häufig schwerere Straftaten (§§ 176 Abs. 1, 2; 177 StGB) an das sog. „Grooming" anschließen und auf Verfolgungsebene insoweit meist eine **Teileinstellung** (§ 154 StPO) erfolgt.[222]

---

[216] ABl. EU Nr. L 335 v. 17.12.2011, S. 1, berichtigt in ABl. EU Nr. L 18 v. 21.1.2012, S. 7.

[217] Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch v. 25.10.2000.

[218] Vgl. RefE (Fn. 31), S. 17, 33.

[219] Eisele, in: Schönke/Schröder, StGB, § 176 Rn. 14; Renzikowski, in: MüKo-StGB, § 176 Rn. 39; Eisele, in: FS Heinz, S. 697 (699, 704 f.). A.A. Wolters, in: SK-StGB, § 176 Rn. 24b, der eine „objektive Sexualbezogenheit" fordert. Vgl. auch LG Düsseldorf, StraFo 2013, 70 (71), das einen Anfangsverdacht verneint, da „die Emails keinerlei eindeutigen pornographischen Inhalt aufweisen". Zustimmend dazu: Popp, jurisPR-ITR 15/2013 Anm. 2.

[220] Fischer, StGB, § 176 Rn. 14a; vgl. den Sachverhalt bei LG Düsseldorf, StraFo 2013, 70.

[221] Renzikowski, in: MüKo-StGB, § 176 Rn. 38; Hörnle, in: LK-StGB, § 176 Rn. 91.

[222] Vom AG Kempten wurde im April 2013 ein Student wegen sexuellen Missbrauchs (vorbereitet durch „Grooming") verurteilt, weil er über Facebook Kontakt zu Mädchen im Alter unter 14 Jahren hergestellt und diese via Webcam genötigt hatte, sexuelle Handlungen an sich vorzunehmen; er hatte gedroht, bereits gefertigte Aufnahmen an Dritte weiterzuleiten (vgl. http://www.antenne.de/Dreieinhalb-Jahre-Haft-fuer-sexuellen-Missbrauch-von-Kindern__nachrichten_670115_news.html).

7.5.6 Gewaltdarstellung (§ 131 StGB)

118 Soziale Medien bieten auch eine Plattform für die Veröffentlichung gewaltverherrlichender Schriften. Praxisrelevant sind dabei vor allem politisch motivierte Darstellungen wie etwa die Enthauptung eines US-Bürgers durch Mitglieder des Terrornetzwerks *Al Qaida*[223] oder auch Aufnahmen von besonders roher Gewaltpornographie[224]. § 131 StGB[225] will derartigen aggressionssteigernden exzessiven Gewaltdarstellungen entgegenwirken und den öffentlichen Frieden schützen.[226] Gemäß § 131 Abs. 1 S. 1 StGB sind jedoch nur solche Schriften i. S. v. § 11 Abs. 3 StGB tatbestandsgemäß, die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt. Es kommt nicht darauf an, ob es sich um ein reales, wirklichkeitsnahes oder fiktives Geschehen handelt. Ausschlaggebend ist, dass nicht allein die Auswirkungen, sondern die Vornahme von derartig grausamen oder sonst unmenschlichen Gewalttaten am Opfer dargestellt werden.[227] Der bloße Besitz von derartigen Gewaltdarstellungen ist nicht tatbestandsgemäß.[228] Die Erfüllung des objektiven Tatbestands verlangt vielmehr eine Adressierung des Materials an dritte Personen i. S. d. Tathandlungen, die bereits von den §§ 184 ff. StGB bekannt sind (vgl. Rn. 98 ff.). In subjektiver Hinsicht muss der Täter zumindest mit dolus eventualis handeln.[229] Ähnlich wie § 184d StGB stellt auch § 131 Abs. 2 StGB die Verbreitung gewaltverherrlichenden Materials via Rundfunk, Medien- oder Telediensten (vgl. Rn. 280 ff.) unter Strafe.

---

[223] BGH, BeckRS 2013, 01320 (Verlinkung des Films in einem Forum).

[224] Vgl. hierzu LG Kiel, BeckRS 2010, 26923; zum Phänomen „Happy Slapping" („fröhliches Schlagen") und der Verbreitung des Videos im Internet vgl. St v. 16.5.2014; Wernert, Internet Kriminalität, S. 124.

[225] Zu geplanten Änderungen vgl. Art. 1 Nr. 5 RefE (Fn. 31), S. 30.

[226] BGH, NStZ 2000, 307 (308); Eisele, Computer- und Medienstrafrecht, § 31 Rn. 138; Rackow, in: BeckOK-StGB, § 131 Rn. 5.

[227] OLG Stuttgart, MMR 2006, 387, 390 (Lichtbilder von Kannibalismus); Fischer, StGB, § 131 Rn. 5.

[228] Vgl. LG Kiel, BeckRS 2010, 26923 (Besitz gewaltverherrlichenden, kinderpornographischen Materials).

[229] Bei § 131 Abs. 1 Nr. 4 StGB ist zudem eine Verwendungsabsicht notwendig.

7.5.7 Verletzung des persönlichen Lebens- und Geheimbereichs

7.5.7.1 Allgemeines

119 Der Leitgedanke der §§ 201 ff. StGB ist der **Schutz der Privat- und Intimsphäre**. Die freie Entfaltung der Persönlichkeit kann nur angemessen gewährleistet werden, wenn dem Einzelnen sowohl gegenüber dem Staat als auch gegenüber der Gesellschaft ein individueller Freiraum eingeräumt wird.[230]

120 Diesem Prinzip tragen die §§ 201, 201a StGB Rechnung, indem sie einerseits die Vertraulichkeit des Wortes gewährleisten und andererseits den höchstpersönlichen Lebensbereich vor unbefugten Bildaufnahmen schützen. Gerade in einer von Fortschritt und Digitalisierung geprägten Gesellschaft werden aufgrund der fortschreitenden Neuerungen und einfachen Nutzungsmöglichkeiten diverser technischer Geräte sowie des Internet Rechtsgutsverletzungen in diesen Bereichen zunehmend wahrscheinlich.

7.5.7.2 Verletzung der Vertraulichkeit des Wortes (§ 201 StGB)

121 § 201 StGB schützt die Unbefangenheit mündlicher Äußerungen und das Vertrauen auf die Flüchtigkeit des nichtöffentlich gesprochenen Wortes.[231] Dabei kommt es im Kern auf die gesprochene Äußerung eines Gedankens an,[232] wobei nicht nur Gespräche „im Privaten" sondern auch Äußerungen im beruflichen Zusammenhang erfasst werden.[233]

122 Der objektive Tatbestand umfasst **vier Begehungsweisen**. Strafbar macht sich, wer das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt, eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht, das nicht zu seiner Kenntnis bestimmte nichtöffentliche Wort mit einem Abhörgerät abhört oder es im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

123 Kennzeichnend für alle Begehungsformen ist das Merkmal der **Nichtöffentlichkeit des „gesprochenen Wortes"**. Nichtöffentlich ist eine Äußerung, wenn sie nicht an die Allgemeinheit gerichtet und für Außenstehende nicht oder nicht ohne besondere Mühe wahrnehmbar ist.[234] Hierunter fallen zum Beispiel private Unterhaltungen oder Kommentare in einem geschlossenen, d. h. individuell begrenzten Kreis.[235] Wenn der Betroffene jedoch bewusst in der Öffentlichkeit ein Gespräch so führt,

---

[230] Lenckner/Eisele, in: Schönke/Schröder, StGB, vor § 201 Rn. 2.
[231] Vgl. Wessels/Hettinger, Strafrecht BT, Rn. 525.
[232] Vgl. Lackner/Kühl, StGB, § 201 Rn. 2.
[233] Für den Fall des „Lehrermobbing": Beck, MMR 2008, 77 (78).
[234] Wessels/Hettinger, Strafrecht BT, Rn. 527.
[235] Bejahend für Kommunikation im Schulunterricht: Beck, MMR 2008, 77 (79).

dass Dritte ohne Weiteres davon Kenntnis nehmen können, sind solche Äußerungen als faktisch öffentlich zu qualifizieren.[236]

Die Vorschrift setzt ein unbefugtes Handeln voraus. **Unbefugt** handelt dabei nicht, wer die Zustimmung des Betroffenen für sein Handeln erhalten hat. Eine solche Befugnis ist nach h. M. ein Rechtfertigungsgrund.[237] **124**

Praktische Anwendung findet § 201 StGB im Hinblick auf soziale Netzwerke am häufigsten bei Jugendlichen bzw. jungen Erwachsenen, die mithilfe eines Aufnahmegeräts ein von der Norm geschütztes Wort verbreiten. Nach der JIM-STUDIE 2012 besitzen 96 % der 12- bis 19-jährigen ein Handy. Davon hat inzwischen jeder zweite Jugendliche ein **Smartphone**, das über einen Internetzugang und erweiterte Funktionalitäten verfügt.[238] Ein solches Smartphone ist regelmäßig mit Foto-, Bild- und Tonaufnahmefunktionen ausgestattet sowie einer unmittelbaren Zugangsmöglichkeit zu sozialen Netzwerken. **125**

Hinsichtlich einer strafrechtlichen Relevanz ist zunächst an die Tonaufnahme- und Wiedergabefunktion eines Smartphones zu denken. Das gesprochene Wort eines anderen ist i. S. v. § 201 Abs. 1 Nr. 1 StGB auf einen **Tonträger aufgenommen**, wenn eine akustische Wiedergabe möglich ist. Dies ist bei Tonbändern, USB-Sticks oder Festplatten der Fall.[239] Bei einem Smartphone werden die gesprochenen Worte digitalisiert als Datei auf dem Speichermedium des Geräts – ähnlich wie bei einer Festplatte – abgespeichert. Danach kann das gesprochene Wort jederzeit vom Gerät selbsttätig wiedergegeben werden. Ein Smartphone (in seiner Funktion als Aufnahme- und Speichermedium) erfüllt folglich die Eigenschaft eines Tonträgers i. S. v. § 201 StGB. **126**

Wer mit einem Smartphone oder einem ähnlichen Gerät in der Schule, am Arbeitsplatz[240] oder in seiner Freizeit unbefugt ein privates Gespräch aufnimmt, macht sich nach § 201 Abs. 1 Nr. 1 StGB strafbar. Solche Aufnahmen lassen sich in der Regel schnell und einfach herstellen. Selbst wenn der Täter das Gerät vor den Augen anderer zur Aufnahme benutzt, wird kaum einer der Beteiligten sein Verhalten richtig deuten können, da es auch mit einem gewöhnlichen Gebrauch – z. B. dem Schreiben einer SMS – verwechselt werden kann. **127**

Weiterreichende strafrechtliche Konsequenzen für das Opfer hat ein anschließendes **Zugänglichmachen** der aufgenommenen Worte gegenüber einem Dritten (§ 201 Abs. 1 Nr. 2 StGB) bzw. ein **öffentliches Mitteilen** dieser Worte (§ 201 Abs. 2 S. 1 Nr. 2 StGB) in einem sozialen Netzwerk, da hier die Gefahr besteht, dass weitere **128**

---

[236] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201 Rn. 9.

[237] Fischer, StGB, § 201 Rn. 10; Kargl, in: NK-StGB, § 201 Rn. 22 ff.; siehe auch BGHSt 31, 304 (306); a. A. etwa Lackner/Kühl, StGB, § 201 Rn. 9.

[238] Medienpädagogischer Forschungsverbund Südwest, JIM-STUDIE 2012, Jugend, Information, (Multi-) Media, S. 52 (http://www.mpfs.de/fileadmin/JIM-pdf12/JIM2012_Endversion.pdf). Hier wird der Umgang von 12- bis 19-Jährigen mit verschiedenen Medien analysiert, darunter auch deren Medienbesitz und Handynutzung.

[239] Vgl. Lackner/Kühl, StGB, § 201 Rn. 3.

[240] Speziell zur Strafbarkeit von Polizeibeamten vgl. Willert, in: Willert/Bohrer, Soziale Netzwerke, S. 90, 100 ff.

Personen Kenntnis vom Wortinhalt nehmen und sich die Nachricht auf diese Weise unkontrolliert verbreitet. Der Tatbestand des § 201 Abs. 1 Nr. 2, Abs. 2 Nr. 2 StGB kann dabei schon dann erfüllt sein, wenn nur einzelne Äußerungen in ihrem wesentlichen Inhalt veröffentlicht werden.[241]

129 **Öffentlich mitteilen** i. S. v. § 201 Abs. 2 S. 1 Nr. 2 StGB bedeutet, das Aufgenommene oder Abgehörte für einen nach Zahl und Individualität unbestimmten oder für einen nicht durch persönliche Beziehungen innerlich verbundenen größeren bestimmten Kreis von Personen zugänglich zu machen.[242] In Anlehnung an das Merkmal des Öffentlichmachens einer Anklageschrift i. S. v. § 353d StGB[243] und der öffentlichen Begehungsweise bei § 186 StGB[244] fällt das unerlaubte Verbreiten eines nicht für die Öffentlichkeit bestimmten Wortes in sozialen Netzwerken demnach unter eine öffentliche Mitteilung, wenn der Täter die Nachricht für alle in dem Netzwerk registrierten Benutzer zugänglich macht. In diesem Fall ist der Personenkreis nicht mehr überschaubar; jedem Nutzer wird eine potentielle Einsichtsmöglichkeit gewährt. Doch selbst wenn die Nachricht lediglich mit den Kontakten des Täters geteilt wird, ist eine Strafbarkeit zu bejahen, da Statusmeldungen über den Kreis des Täters in sozialen Netzwerken typischerweise verbreitet werden können. Dass die Kontrolle des Personenkreises nicht mehr seinem Macht- und Einflussbereich unterliegt, dürfte der Verbreitende regelmäßig mit einkalkulieren.

130 Als **Täter** kommen sowohl der Aufnehmende selbst als auch ein Dritter in Betracht. Wie Letzterer Kenntnis von der Aufnahme erlangt hat, ist nicht von Bedeutung.[245] Auch ein Dritter, der vom Aufnehmenden einen detaillierten Bericht über eine Aufnahme erhalten hat und diesen anschließend in einem sozialen Netzwerk preisgibt, kann sich also strafbar machen.

131 Weiterhin gilt für § 201 Abs. 2 S. 1 Nr. 2 StGB eine Tatbestandseinschränkung auf **Mitteilungen, die geeignet sind, berechtigte Interessen eines anderen zu beeinträchtigen** (§ 201 Abs. 2 S. 2 StGB). Das Ziel dieser Bagatellklausel ist es, belanglose Äußerungen über alltägliche Themen aus dem Schutzbereich des Absatzes 2 auszuklammern.[246]

132 Eine Strafbarkeit nach § 201 StGB kann sich im Kontext sozialer Netzwerke ferner aus Absatz 1 Nr. 2 StGB ergeben. Eine der Tathandlungen besteht hier darin, dass die **Aufnahme einem Dritten zugänglich gemacht** wird. Dies ist dann der Fall, wenn diesem durch Übergabe der Gebrauch i. S. d. Abspielens ermöglicht wird oder ihm lediglich die Möglichkeit verschafft wird, von der akustischen Reproduktion Kenntnis zu nehmen; eine Kopie der Aufnahme ist dabei ausreichend. Dies wird z.

---

[241] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201 Rn. 25.

[242] Lackner/Kühl, StGB, § 201 Rn. 7.

[243] Vgl. zum *Öffentlichmachen* der Anklageschrift: Perron, in: Schönke/Schröder, StGB, § 353d Rn. 46 (abzulehnen bei Weitergabe an einen zahlenmäßig kleinen, dem Täter bekannten Kreis; anders dagegen wenn das Handeln auf eine *Weiterverbreitung* angelegt ist).

[244] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 186 Rn. 19.

[245] Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201 Rn. 24; Kargl, in: NK-StGB, § 201 Rn. 19.

[246] Kargl, in: NK-StGB, § 201 Rn. 20; vgl. auch Lackner/Kühl, StGB, § 201 Rn. 8.

B. bei einem Versenden der Datei per E-Mail bejaht.[247] Im Umkehrschluss muss dies aber erst Recht für den Fall gelten, dass der Täter die aufgenommenen Worte als Datei zum Abspielen oder Abrufen in einem sozialen Netzwerk veröffentlicht. Dabei ist es unerheblich, ob der Verwender die Aufnahme vorher selbst hergestellt hat. Erfasst ist auch ein Dritter, der lediglich zufällig den Besitz erlangt hat.[248] Ein tatbestandsrelevantes Handeln in sozialen Netzwerken liegt demnach vor, wenn der Täter oder ein Dritter entweder den wesentlichen Inhalt des Wortes auf seinem Profil zugänglich macht oder er bzw. ein Dritter die entsprechende Audiodatei auf sein Profil hochlädt.

7.5.7.3 Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB)

Während § 33 Abs. 1 KUG (Rn. 150 ff.) (erst) die Verbreitung und öffentliche Zur-Schau-Stellung eines Bildnisses ohne Einwilligung des Betroffenen schützt, können das bloße Herstellen eines Bildes und die Weitergabe eines solchen an Dritte tatbestandlich unter § 201a StGB fallen.[249] Der Gesetzgeber hat mit der Einführung des § 201a StGB ins StGB auf Entwicklungen reagiert, die sich im Bereich der **Video- und Bildertechnik** abgezeichnet haben. Es soll damit speziell auf das schnelle und unbemerkte Fotografieren und Verbreiten von Bildern im Internet reagiert werden.[250] Geschütztes Rechtsgut ist der höchstpersönliche Lebensbereich.[251] **133**

Strafbar macht sich, wer von einer anderen Person,[252] die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt **Bildaufnahmen** herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. Nach Absatz 2 wird ebenso bestraft, wer die Bildaufnahme gebraucht oder einem Dritten zugänglich macht. **134**

Absatz 3 hingegen bezieht sich auf eine befugt hergestellte Bildaufnahme in den geschützten Räumlichkeiten und untersagt es, diese Aufnahmen wissentlich unbefugt einem Dritten zugänglich zu machen und dadurch den höchstpersönlichen Lebensbereich des Abgebildeten zu verletzen. **135**

---

[247] Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201 Rn. 17; Graf, in: MüKo-StGB, § 201 Rn. 27.

[248] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201 Rn. 17.

[249] Erst mit dem 36. StRÄndG v. 30.7.2004 – § 201a StGB (BGBl. I S. 2012) wurde ein solches Verhalten unter Strafe gestellt. Zu den Vorarbeiten siehe: BT-Drucks. 15/2466 v. 10.2.2004 und 15/2995 v. 28.4.2004.

[250] Vgl. BT-Drs. 15/1891, S. 6. Siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 99.

[251] Ausführlich zum geschützten Rechtsgut: Kargl, in: NK-StGB, § 201a Rn. 2 f.

[252] Zum geschützten Personenkreis: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 260 ff.

136 Eine **Wohnung** i. S. d. Vorschrift ist das Zentrum des höchstpersönlichen Lebensbereichs. Dazu zählen auch fremde Wohnungen, Gäste- und Hotelzimmer.[253] Einbezogen sind Nebenräume (Dachboden, Keller), nicht jedoch vom Wohnbereich abgetrennte Kellerräume, Tiefgaragen oder Gärten.[254] Ein gegen Einblick besonders geschützter Raum liegt vor, wenn ein Sichtschutz besteht und der Betroffene deshalb seine Intimsphäre offenlegen kann (z. B. Duschen, Solarien, Umkleidekabinen, Garten mit hohem Sichtschutz).[255]

137 Keine Bildaufnahmen sind Gemälde, Zeichnungen, Karikaturen oder Bilder, die von einem Computer generiert wurden.[256]

138 Weiterhin ist es nach den Absätzen 1–3 erforderlich, dass der **höchstpersönliche Lebensbereich** verletzt wird. Die Gesetzesbegründung[257] sieht hierin den Bereich **privater Lebensführung** (etwa Tod, Krankheit, Sexualität, Tatsachen aus dem Familienleben), der Schutz vor dem Einblick Außenstehender verdient. Der Ort einer Dienst-/Berufsausübung fällt üblicherweise nicht darunter.[258] Neutrale Handlungen in einer geschützten Räumlichkeit werden in der Regel nicht vom höchstpersönlichen Lebensbereich betroffen sein.[259] Beim Merkmal „Unbefugt" sei auf die obigen (Rn. 124 ff.) Ausführungen verwiesen.

139 Im Hinblick auf soziale Netzwerke sind Absatz 2 und Absatz 3 des § 201a StGB von besonderer Relevanz. Nach Absatz 2 ist eine **Bildaufnahme gebraucht**, wenn die technischen Möglichkeiten eines Bildträgers z. B. durch Speichern oder durch Sichtbarmachen genutzt werden. Hier ist es nicht von Bedeutung, ob der Täter selbst oder ein Dritter von der Aufnahme Gebrauch macht.[260] Als logische Folge ist der Tatbestand schon dann erfüllt, wenn ein Dritter, dem alle Umstände der (Vor-)tat bewusst sind, in einem sozialen Netzwerk ein Bild herunterlädt, das nach Absatz 1 unbefugt hergestellt wurde. Das bloße **Beobachten** eines solchen Bildes in einem sozialen Netzwerk ist im Umkehrschluss straflos, hier erfolgt kein derartiger Archivierungsvorgang.[261]

140 Einem **Dritten zugänglich gemacht** ist die Aufnahme, wenn diesem der Zugriff auf das nach Absatz 1 hergestellte Bild z. B. durch Übergabe oder Ablegen der

---

[253] Vgl. BT-Drs. 15/2995 v. 28.4.2004, S. 5. Ausführlich Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 270 ff.

[254] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201a Rn. 6.

[255] Vgl. Kargl, in: NK-StGB, § 201a Rn. 5; siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 278 ff.

[256] Vgl. Lackner/Kühl, StGB, § 201a Rn. 2. Zum Begriff auch: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 257 ff., S. 268 ff., zur Frage, ob eine Erkennbarkeit der abgebildeten Person gegeben sein muss.

[257] BT-Drs. 15/2466 v. 10.2.2004, S. 5.

[258] Allgemein Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 291 ff.; Beck, MMR 2008, 77 (78; ablehnend für die „Schule" im Fall des „Lehrermobbing" mit einzelnen Räumlichkeiten, etwa Umkleideraum oder Toilette, als Ausnahme).

[259] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201a Rn. 9.

[260] Vgl. Kargl, in: NK-StGB, § 201a Rn. 9; Lackner/Kühl, StGB, § 201a Rn. 6; Valerius, in: LK-StGB, § 201a Rn. 24; Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 287 ff.

[261] Siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 286.

Datei auf einem Server oder die Kenntnisnahme z. B. durch Vorführen eines Films ermöglicht wird; eine tatsächliche Kenntnisnahme ist nicht erforderlich.[262] Wenn also eine unbefugt hergestellte Aufnahme i. S. d. Absatzes 1 in ein soziales Netzwerk hochgeladen wird, ist die Aufnahme ab Speicherung und damit erfolgender Anzeige auf dem Profil einem Dritten zugänglich gemacht.

Von Absatz 3 werden die Fälle erfasst, in denen das Bild zwar **befugt hergestellt** wurde, aber dann **unbefugt, d. h. ohne ausdrücklich erteilte Einwilligung, einem Dritten zugänglich gemacht** und dadurch der höchstpersönliche Lebensbereich des Abgebildeten verletzt wird.[263] Mögliche Konstellationen sind das Hochladen und Einstellen eines mit Einwilligung aufgenommenen intimen Fotos des Partners oder einer anderen vertrauten Person in ein soziales Netzwerk. Praktisch relevant ist in diesem Bereich der Fall, dass der spätere Täter während einer Lebens-/Liebesbeziehung zunächst befugt intime Aufnahmen seines Partners (in einer von § 201a StGB geschützten Räumlichkeit) herstellt und diese Aufnahme nach dem Scheitern der Beziehung (meist aus Rache) später an einen Dritten versendet oder ins Internet (etwa in einem sozialen Netzwerk) einstellt.[264] Der Fall ist nicht anders zu beurteilen, wenn die intime Nacktaufnahme vom späteren Opfer selbst gefertigt und dem späteren Täter übermittelt worden ist (sog. **Sexting**; Rn. 112). Der Wortlaut von § 201a Abs. 3 StGB setzt nicht voraus, dass „ein anderer" die Bildaufnahme hergestellt hat. Damit steht Art. 103 Abs. 2 GG einer derartigen Auslegung nicht entgegen. Zudem hat das Opfer das Bild zwar selbst verschickt, jedoch hat es die Aufnahme damit nur einer bestimmten Person und nicht einem unbestimmten Personenkreis zugänglich gemacht. Eine generelle Einwilligung in das Zugänglichmachen an dritte Personen ist beim Sexting folglich nicht gegeben. **141**

Der Täter muss stets **wissentlich unbefugt** handeln, d. h. positiv wissen und nicht nur damit rechnen, bei dem Zugänglichmachen ohne Befugnis des Betroffenen zu handeln.[265] **142**

Wenn der Täter eine Bildaufnahme zunächst herstellt und sie anschließend in ein soziales Netzwerk hochlädt, liegt nur **eine Tat** vor, denn bei den § 201a Abs. 1 und 2 StGB handelt es sich um unselbstständige Tatbestandsalternativen.[266] **143**

Gemäß § 205 Abs. 1 S. 1 StGB werden nach § 201 Abs. 1 und 2 und § 201a StGB begangene Taten nur auf **Antrag** verfolgt. **144**

Die Vorschrift des § 201a StGB ist derzeit **Gegenstand von Reformbestrebungen**, im Zusammenhang mit der Diskussion über die Erweiterung der Strafbarkeit bei Nacktaufnahmen (von Kindern). **145**

---

[262] Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201a Rn. 15; Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 289 f.

[263] Vgl. Kargl, in: NK-StGB, § 201a Rn. 10, 15; Hoyer, in: SK-StGB, § 201a Rn. 32 ff. (auch zur strittigen Auslegung des „wissentlich unbefugten Zugänglichmachens").

[264] Vgl. auch Valerius, in: LK-StGB, § 201a Rn. 27.

[265] Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201a Rn. 21.

[266] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, § 201a Rn. 22.

146 Der Gesetzesantrag, den der **Freistaat Bayern** am 1.4.2014 im Bundesrat vorgelegt hat,[267] sieht für § 201a StGB die Schaffung eines neuen Absatzes 4 vor, der den entgeltlichen oder im Rahmen eines Tauschsystems erfolgenden Handel mit Bildaufnahmen, die die Nacktheit von Kindern zur Schau stellen, unter Strafe stellt.[268] Ebenso soll nach dem bayerischen Vorschlag allgemein der Strafrahmen des § 201a StGB um ein Jahr angehoben werden und der Straftatbestand als Offizialdelikt ausgestaltet werden.[269]

147 Der im April 2014 vorgelegte RefE des BMJV sieht eine **Ausweitung des Anwendungsbereichs** von § 201a StGB auf bloßstellende Bildaufnahmen, unabhängig vom Ort ihrer Aufnahme, sowie von unbefugten Bildaufnahmen von unbekleideten Personen vor. Dazu soll § 201a Abs. 1 S. 2 StGB-E eingefügt werden: „*Ebenso wird bestraft, wer unbefugt eine bloßstellende Bildaufnahme von einer anderen Person oder unbefugt eine Bildaufnahme von einer unbekleideten anderen Person herstellt oder überträgt*“.[270] Bloßstellende Bildaufnahmen sollen beispielsweise gegeben sein, wenn sie „*betrunkene Personen auf dem Heimweg*“ oder „*Opfer einer Gewalttat, die verletzt und blutend auf dem Boden liegen*“[271] zeigen, es sich also allgemein um Aufnahmen handelt, „die die abgebildete Person in peinlichen oder entwürdigenden Situationen oder in einem solchen Zustand zeigen, und bei denen angenommen werden kann, dass üblicherweise ein Interesse daran besteht, dass die Aufnahmen sie nicht hergestellt, übertragen oder Dritten zugänglich gemacht werden“.[272] Unbefugte Bildaufnahmen von unbekleideten Personen sollen dann gegeben sein, wenn keine Einwilligung in die Herstellung der Aufnahme vorliegt oder eine Einwilligung sittenwidrig ist. Werden Kinder, die noch nicht wirksam einwilligen können, unbekleidet abgelichtet, so entscheidet die Einwilligung der Eltern, deren Wirksamkeit sich nach den Umständen des Einzelfalles beurteilen soll.[273] Danach sollen „Bildaufnahmen von unbekleideten Kindern in familiären Alltagssituationen, die im familiären Bereich verbleiben und allenfalls im Verwandten- oder Bekanntenkreis gezeigt werden . . . sozialadäquat und üblich“[274] sein, hingegen nicht Aufnahmen, „die auf einschlägigen Wegen neben kinder- und jugendpornographischen Schriften zu vorwiegend sexuellen Zwecken weitergegeben oder verbreitet

---

[267] Vgl. Antrag des Freistaates Bayern, BR-Drs. 127/14.

[268] Antrag des Freistaates Bayern, BR-Drs. 127/14: „*(4) Wer Bildaufnahmen, die die Nacktheit von Kindern (§ 176 Abs. 1) zur Schau stellen 1. gegen Entgelt oder im Rahmen eines Tauschsystems a) anbietet oder zugänglich macht b) sich oder einem anderen zu verschaffen unternimmt oder 2. herstellt, bezieht, liefert, vorrätig hält oder einzuführen unternimmt, um sie im Sinne der Nummer 1 Buchstabe a zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Satz 1 gilt nicht für Handlungen, die in Wahrnehmung berechtigter Interessen erfolgen, namentlich der Kunst, der Wissenschaft oder der Berichterstattung über Vorgänge des Zeitgeschehens dienen*“.

[269] Vgl. Antrag des Freistaates Bayern, BR-Drs. 127/14, 3, 7 f.

[270] Art. 1 Nr. 18 lit. a RefE (Fn. 31).

[271] RefE (Fn. 31), S. 43 f.

[272] RefE (Fn. 31), S. 44.

[273] RefE (Fn. 31), S. 44.

[274] RefE (Fn. 31), S. 44.

werden“[275]. Diese Änderung, die damit primär nicht auf die Position des Kindes bei der Aufnahme (keine Forderung eines „Posings“) abstellt, hat einen weiteren Anwendungsbereich als die §§ 184 StGB (Rn. 93 ff.).

148 Die Strafdrohung des § 201a Abs. 1 StGB-E soll gemäß dem RefE auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe erhöht werden.[276]

149 Hinsichtlich der befugt hergestellten Bildaufnahmen soll in den neu eingefügten § 201a Abs. 3, Abs. 4 StGB-E sowohl zwischen den beiden Tatbestandsalternativen des § 201a Abs. 1 StGB unterschieden werden (§ 201a Abs. 1 S. 1 StGB – § 201a Abs. 3; § 201a Abs. 1 S. 2 StGB – § 201a Abs. 4 StGB) als auch in der Strafandrohung zwischen einem bloßen Zugänglichmachen der Bildaufnahme für eine dritte Person („Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe“) und einem Zugänglichmachen der Bildaufnahme für die Öffentlichkeit oder eines Verbreitens („Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe“) unterschieden werden.[277]

7.5.8 Verbreitung, Zurschaustellung von Bildnissen (§ 33 KUG)

150 Geschützt ist durch § 33 KUG das **Recht am eigenen Bild**, das eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) darstellt. Ziel ist es, die Persönlichkeit des Betroffenen davor zu bewahren, gegen dessen Willen in der Gestalt eines Bildnisses für andere verfügbar zu werden. Eine solche Dispositionsbefugnis steht nur dem Abgebildeten selbst zu.[278]

151 Gemäß § 33 Abs. 1 KUG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer entgegen den §§ 22, 23 KUG ein Bildnis verbreitet oder öffentlich zur Schau stellt. Die Tat wird nach Absatz 2 nur auf Antrag verfolgt.

152 Unter den Begriff des Bildnisses fallen nicht nur Fotografien jeglicher Art, sondern auch Filmaufnahmen.[279] Der relativ weite Schutzbereich der Norm erfasst jede Form der **Wiedergabe der äußeren Erscheinungsweise einer Person**, soweit sie als solche auch wirklich erkennbar ist,[280] auch in Form einer Zeichnung[281], Fotomontage[282] oder Karikatur[283]. Eine nähere Konkretisierung erfolgt durch die Vorgaben der §§ 22, 23 KUG.

---

[275] RefE (Fn. 31), S. 44 f.
[276] Art. 1 Nr. 18 lit. b, bb RefE (Fn. 31).
[277] Art. 18 lit. c RefE (Fn. 31).
[278] Graf et al., Wirtschafts- und Steuerstrafrecht, § 33 KUG, Rn. 1.
[279] Fechner, Medienrecht, Kap. 4 Rn. 28; allgemein: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 206 ff.
[280] Fechner, Medienrecht, Kap. 4 Rn. 29; Beck, MMR 2008, 77 (79 „Lehrermobbing“); Näheres bei Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 202 ff.
[281] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 5.
[282] BGHZ 143 (199, 208 Verdachtsberichterstattung); Facebook-Post einer vermeintlichen Nacktaufnahme von *Silvie Meis*, abrufbar unter: http://www.bild.de/unterhaltung/leute/sylvie-meis/versteckt-hinter-dem-facebook-account-mit-dem-nackt-foto-34729330.bild.html.
[283] Vgl. Beck, MMR 2008, 77 (79 „Lehrervideo“; „Pornomontage“, „Hinrichtungsszenarien“).

153 § 22 KUG bestimmt, dass Bildnisse nur mit **Einwilligung des Abgebildeten** verbreitet oder öffentlich zur Schau gestellt werden dürfen.[284] § 23 Abs. 1 KUG schränkt das umfassende Erfordernis einer Einwilligung in einigen Bereichen ein. Ausnahmen gelten für Bildnisse aus dem Bereich der Zeitgeschichte (Nr. 1)[285] oder für Bilder, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen (Nr. 2).[286] Dies gilt allerdings nur unter der Maßgabe des Absatzes 2, dass kein berechtigtes Interesse des Abgebildeten verletzt wird. Damit hat eine Abwägung der jeweils gegenläufigen Interessen zu erfolgen.[287]

154 Ein **Verbreiten** i. S. v. § 33 KUG liegt vor, wenn einem Dritten – nicht unbedingt auf Dauer – die tatsächliche Verfügungsgewalt über das Original oder ein Vervielfältigungsstück des Bildnisses in körperlicher oder digitaler Form verschafft wird.[288] Die zweite Tathandlungsvariante, das **öffentliche Zurschaustellen**, umfasst auch die öffentliche Zugänglichmachung i. S. d. § 19a UrhG. Unter diesen Begriff fällt das **Einstellen bzw. Hochladen von Bildnissen** in das Internet.[289]

155 Im Kontext sozialer Netzwerke macht sich vor dem aufgezeigten rechtlichen Hintergrund strafbar, wer Bildnisse von anderen Menschen ins Netzwerk einstellt, ohne die betroffenen Personen vorher ausdrücklich um Erlaubnis gefragt zu haben.[290] Dass Anbieter wie Facebook, StudiVZ oder Myspace ein einfaches und schnelles Hochladen entsprechender Fotos und Videos anbieten, ändert hieran nichts.

156 Die **Ausnahmen** vom Erfordernis einer Einwilligung (§ 23 KUG) gelten nur in wenigen Fällen, etwa bei Bildnissen von einer **größeren Menschenmenge** (z. B. auf einem Konzert, einer Versammlung oder einer Demonstration; Absatz 1 Nr. 3). Von

---

[284] Im Falle einer Entlohnung wird die Erlaubnis im Zweifel angenommen (§ 22 Satz 2 KUG). Bei verstorbenen Personen ist eine Einwilligung der Angehörigen bis zum Ablauf von 10 Jahren erforderlich (§ 22 Satz 3 und 4 KUG).

[285] Abgelehnt für die gezielte Abbildung einzelner Polizeibeamter bei einem Polizeieinsatz: VG Göttingen, Die Polizei 2013, 121 = Kriminalistik 2013, 457; hierzu auch: OVG Lüneburg, DVBl. 2013, 1066 (Filmen u. Fotografieren polizeilicher Einsätze grundsätzlich zulässig; Beschlagnahme des Materials nur gerechtfertigt bei konkreten Anhaltspunkten für eine Verbreitung); siehe auch: OLG Karlsruhe, ZUM-RD 2011, 348 (Veröffentlichung eines Kinderfotos durch Großvater im Internet ohne Zustimmung des personensorgeberechtigten Jugendamtes).

[286] Eine Ausnahme besteht ferner für Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen (Nr. 3) sowie für Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient (Nr. 4).

[287] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 82.

[288] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 9; a. A. wohl Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 210 ff. (körperliche Verbreitung erforderlich).

[289] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 10; näher zu den Problemen Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 212 ff., siehe auch S. 225 ff. zu den einzelnen denkbaren Handlungsformen.

[290] Speziell zur Strafbarkeit von Polizeibeamten vgl. Willert, in: Willert/Bohrer, Soziale Netzwerke, S. 90, 97 f.

der Ausnahme ebenfalls erfasst sind Abbildungen von **Prominenten** oder ähnlichen **bekannten Personen des öffentlichen Lebens** (Absatz 1 Nr. 1).[291]

157 Keiner Einwilligung bedarf es ferner, wenn der Abgebildete nicht eindeutig erkennbar ist.[292] Eine **Erkennbarkeit** kann sich aus Gesichtszügen[293] oder aus charakteristischen Auffälligkeiten der Person auf dem entsprechenden Bildnis ergeben.[294] Auch eine schlichte Bildunterschrift kann zu einer Erkennbarkeit führen,[295] etwa im Fall einer nur von hinten fotografierten Person, die mit Markierungen auf dem jeweiligen Netzwerk versehen wird, sodass ein Rückschluss auf ihre Identität gezogen werden kann. Ähnlich wie bei einem *Verlinken*, bei dem verschiedene Seiten oder Inhalte durch einen Verweis zueinander in Beziehung gesetzt werden, führt eine solche Markierung dazu, dass das Profil der Betroffenen mit einem entsprechenden Bild oder Video verknüpft wird. Daraus folgt, dass auch fremde, nicht direkt auf einem Bildnis erkennbare Personen im Falle einer Markierung ihre Einwilligung erteilt haben müssen.

158 Sog. **Zensurbalken**, die die Augen des Betroffenen verdecken, schließen die Erkennbarkeit einer Person nicht notwendig aus. Im Einzelfall kann begründeter Anlass bestehen, dass der Abgebildete in seinem Bekanntenkreis erkannt werden kann.[296]

159 Bei sozialen Netzwerken besonders strafrechtlich relevant sind Aufnahmen von **Geburtstagsfeiern** oder **Privatpartys**. Hier ist eine Ausnahme vom Erfordernis der Einwilligung des Betroffenen (§ 23 Abs. 1 Nr. 3 KUG) nicht gegeben,[297] denn bei solchen Veranstaltungen geht es nicht um das von § 23 Abs. 1 KUG geschützte Informationsinteresse der Allgemeinheit, das seinerseits Schutz über Art. 5 Abs. 1 S. 1 GG erfährt.[298] Bei Gruppen-, Party- oder Geburtstagsfotos sind die betroffenen Personen daher vorher stets um ihre Erlaubnis zu fragen. Ein **„blindes" Hochladen** der Bilder fremder Personen ist in den meisten Fällen strafrechtlich relevant, auch wenn die einschlägigen Netzwerke ein derartiges Vorgehen einfach und legal erscheinen lassen.

160 Die von § 22 KUG geforderte **Einwilligung** der auf einem Bildnis abgebildeten Personen muss ausdrücklich erklärt werden, kann je nach den Umständen aber auch

---

[291] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 29. Zu Fragen der Einwilligung näher Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 248 ff., auch zur Frage, ob Lehrer als Personen der Zeitgeschichte eingeordnet werden können.

[292] Schertz, in: Loewenheim, Handbuch Urheberrecht, § 18 Rn. 7.

[293] BGH, GRUR 1962, 211 (Hochzeitsbild); BVerfG, ZUM 2005, 384 (technisch manipuliertes Gesicht); OLG Saarbrücken, AfP 2010, 81 (Verpixelung des Gesichts).

[294] BGH, GRUR 1979, 732 (733). Siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 202 ff.

[295] BGH, GRUR 1966, 102 (Spielgefährtin).

[296] BGH, GRUR 1962, 211.

[297] Vgl. Ulbricht, Social Media und Recht, S. 25.

[298] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 24. Für § 201a StGB: Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 309 ff.

stillschweigend erfolgen.[299] Es genügt nicht, dass die betreffende Person nur die Fotoaufnahme an sich duldet, vielmehr muss sie auch über die später erfolgende Verwendung in einem sozialen Netzwerk informiert sein.[300] Eine Erwähnung oder Anfrage um Zustimmung vor der Bildaufnahme ist bei der Absicht, sie später auf soziale Netzwerke hochzuladen, unverzichtbar.

161 Im **Hochladen eines eigenen Bildes** in einem sozialen Netzwerk kann eine Einwilligung in eine Weiterverwendung des Bildes durch andere Nutzer des Netzwerks zu sehen sein, ebenso in der anderweitigen Verwendung des Bildes durch Suchmaschinen.[301]

162 Häufig spielen die Problematik um hochgeladene Fotos und die damit verbundenen Rechtsfragen bei **Kindern** oder **Jugendlichen** eine Rolle, da diese häufig Nutzer sozialer Netzwerke sind. In Anlehnung an die §§ 104 ff. BGB wird für Geschäftsunfähige stets die Einwilligung der erziehungsberechtigten Personen gefordert. Bei beschränkt Geschäftsfähigen (§§ 107 ff. BGB) hingegen soll zur Achtung des Selbstbestimmungsrechts neben die Einwilligung der Eltern zusätzlich die Einwilligung des einsichtsfähigen Jugendlichen treten.[302] Im Hinblick auf die Strafvorschrift des § 33 KUG sollte jedoch der strafrechtliche Einwilligungsmaßstab angelegt werden, der die Einwilligung des Jugendlichen genügen lässt, wenn dieser die notwendige Einsichts- und Urteilsfähigkeit besitzt, um über Fragen des eigenen Persönlichkeitsschutzes zu entscheiden.[303]

163 Bedeutsam für die Strafbarkeit nach § 33 KUG ist, dass die Einwilligung **vor Nutzungsbeginn** vorliegen muss. Eine nachträgliche Genehmigung lässt eine Strafbarkeit nicht entfallen.

164 Da die Tat nur auf Antrag verfolgt wird (**Antragsdelikt**, § 33 Abs. 2 KUG), führt eine solche „Genehmigung" prozessual entweder zu einem Verzicht auf den erforderlichen Strafantrag oder sie ist als Rücknahme eines bereits gestellten Antrags zu deuten.[304]

165 Nach § 48 KUG **verjähren** begangene Taten nach § 33 KUG innerhalb von drei Jahren. Der Fristbeginn fällt auf den Tag, an dem die widerrechtliche Handlung zuletzt stattgefunden hat.[305]

---

[299] Dreier/Specht, in: Dreier/Schulze, UrhG, § 22 KUG Rn. 17; Wandtke et al., Praxiskommentar Urheberrecht, § 22 KUG Rn. 15.

[300] BGH, GRUR 1968, 652 (654 Ligaspieler); Siehe auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 249.

[301] OLG Köln, MMR 2011, 323. Dazu auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 253 f.

[302] Dreier/Specht, in: Dreier/Schulze, UrhG, § 22 KUG Rn. 25 f.; Wandtke et al., Praxiskommentar Urheberrecht, § 22 KUG Rn. 14; Ohly, GRUR 2012, 983 (991 f.); offengelassen bei: BGH, GRUR 1975, 561 (563); Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 252 ff.; Piltz, S. 261.

[303] Paeffgen, in: NK-StGB § 228 StGB Rn. 14 ff. vgl. auch Leffler, Der strafrechtliche Schutz des Rechts am eigenen Bild, S. 252.

[304] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 33 KUG Rn. 16.

[305] Niesler, in: Graf et al., Wirtschafts- und Steuerstrafrecht, § 33 KUG Rn. 25.

7.5.9 Straftaten gegen die persönliche Freiheit

Ähnlich wie die Beleidigungsdelikte (Rn. 7.5.4) verlagern sich auch Straftaten gegen die persönliche Freiheit (§§ 238, 240, 241 StGB) immer stärker ins Internet. Dabei ist zum einen der hohe Grad an Anonymität ausschlaggebend, den das Internet bietet. Zum anderen offerieren die Kommunikationsebenen in sozialen Netzwerken auch für diese Delikte eine geeignete Plattform. Täter von Nachstellungs-, Nötigungs- und Bedrohungsdelikten legen es nicht primär auf ihre Unbekanntheit an.[306] Über das Internet können sie ohne räumliche Nähe zum Opfer Druck aufbauen, es ausspionieren und die nächsten, meist intensiveren kriminellen Schritte vorbereiten. Dabei erreichen die Täter nicht selten, etwa durch ein Auftreten in sozialen Netzwerken, wesentlich mehr Menschen als bei einer herkömmlichen Begehungsweise. Die Folgen können gravierend, mitunter sogar tödlich sein.[307] **166**

7.5.9.1 Nachstellung/„Cyberstalking" (§ 238 StGB)

Der Schutzzweck des am 31.3.2007[308] in Kraft getretenen § 238 StGB (Nachstellung) umfasst den individuellen Lebensbereich[309] des Opfers sowie den Schutz seines seelischen Wohlbefindens.[310] Im allgemeinen Sprachgebrauch hat sich der Begriff „Stalking"[311] für die als Erfolgsdelikt[312] ausgestaltete Tathandlungsvarianten der Nachstellung durchgesetzt. Findet die Nachstellung hauptsächlich oder ausschließlich im virtuellen Raum statt, spricht man vom Phänomen des sog. „**Cyberstalking**".[313] **167**

Allgemeine Probleme des Tatbestandes sowie Fragen im Hinblick auf den Bestimmtheitsgrundsatz (Art. 103 Abs. 2 GG) werden hier nicht näher betrachtet.[314] Vielmehr wird das Augenmerk auf die speziellen Besonderheiten und Probleme im Zusammenhang mit der Nutzung sozialer Netzwerke im Internet gelegt. **168**

Häufige Auslöser für eine Nachstellung sind der erwünschte Aufbau bzw. die Abwicklung einer gescheiterten Beziehung, meist verbunden mit der verschmähten **169**

---

[306] Vor allem bei der Nachstellung sind sich Täter und Opfer häufig schon im Vorfeld persönlich bekannt: Peters, NStZ 2009, 238 (239).
[307] Siehe etwa Kirchner, Mord unter Teenagern, SZ v. 4.9.2012, S. 10.
[308] Art. 3 Gesetz zur Strafbarkeit beharrlicher Nachstellung v. 22.3.2007, BGBl. 2007 I, S. 354.
[309] BT-Drs. 16/575 v. 8.2.2006, S. 6.
[310] Gazeas, JR 2007, 497 (498).
[311] Zu diesem Begriff Lackner/Kühl, StGB, § 238 Rn. 1.
[312] Fischer, StGB, § 238 Rn. 4.
[313] Hoffmann, in: Robertz/Wickenhäuser, Orte der Wirklichkeit, S. 65.
[314] Vertiefend dazu: Mitsch, NJW 2007, 1237 (1239); Steinberg, JZ 2006, 30; zu den Erfahrungen der Praxis bei der Auslegung der Tatbestandsmerkmale: Müller/Eisenberg, DRiZ 2013, 364 ff.; vgl. auch Koalitionsvertrag zwischen CDU, CSU und SPD (Fn. 6), S. 145 („tatbestandliche Hürden" sollen gesenkt werden); hierzu auch Kaufmann, DRiZ 2014, 50; vgl. BR-Drs. 193/14 v. 6.5.2014 zum Gesetzesantrag Bayerns, § 238 StGB in ein Eignungsdelikt umzuwandeln.

Zuneigung zu einer anderen Person.[315] Durch die **persönliche Bekanntheit von Täter und Opfer** ist es in den meisten Fällen sehr wahrscheinlich, dass diese auch im virtuellen Raum Kontakt miteinander aufnehmen können. In den meisten sozialen Netzwerken ist eine große Zahl an personenbezogenen Informationen und Daten vorhanden. Auch Bilder von Personen mit direktem Einblick in das Privatleben sind – zumindest dann, wenn von etwaigen Schutzmechanismen kein Gebrauch gemacht wird – mehr oder weniger frei verfügbar. Dies ermöglicht es selbst Tätern, die nicht aus dem direkten Umfeld des Opfers stammen, sehr private Dinge über die betroffene Person in Erfahrung zu bringen und mit ihr auf verschiedene Art und Weise (z. B. in Chaträumen, mittels persönlicher Nachrichten, sog. Pinnwandposts oder Verlinkungen auf Bildern) zu kommunizieren. Hier bestehen vielfältige Möglichkeiten zum Missbrauch dieser Dienste; häufig führt dies beim Opfer zu einem regelrechten „**Psychoterror**“[316]. Einen eigenen Tatbestand für die spezifischen Phänomene des Cyberstalkings gibt es im Gesetz nicht. Aufgrund der Besonderheiten des Internet ergeben sich bei deren Subsumtion unter den Tatbestand der Nachstellung (§ 238 StGB) nicht selten Probleme.

170 Der objektive Tatbestand des § 238 StGB setzt eine unbefugte und beharrliche Nachstellung sowie eine dadurch kausal hervorgerufene und schwerwiegende Beeinträchtigung der Lebensgestaltung beim Opfer voraus. Die **Beharrlichkeit** zeichnet sich durch wiederholtes Handeln[317] des Täters aus, welches durch eine bewusste Missachtung des entgegenstehenden Opferwillens eine besondere Hartnäckigkeit zum Ausdruck bringt.[318]

171 Für die Tathandlung einer Nachstellung sind mehrere Begehungsweisen normiert. Ein Aufsuchen der räumlichen Nähe zum Opfer (§ 238 Abs. 1 **Nr. 1** StGB) kommt bei einem Handeln im Internet naturgemäß nicht in Betracht (Art. 103 Abs. 2 GG).

172 Klassisch im Bereich Social Media ist dagegen der **Versuch der Kontaktaufnahme** mithilfe von Telekommunikationsmitteln oder sonstigen Mitteln zur Kommunikation oder der Versuch der Kontaktherstellung über einen Dritten (§ 238 Abs. 1 **Nr. 2** StGB).[319] Die häufigste Begehungsart ist dabei das Versenden von SMS

---

[315] Peters, NStZ 2009, 238 (239); siehe hierzu auch die Fallkonstellation in: BGH, NJW 2013, 3383 (mit strengen Anforderungen an eine Unterbringung in einem psychiatrischen Krankenhaus aus Anlass einer Tat nach § 238 StGB).

[316] Gazeas, JR 2007, 497 (498); siehe auch: BGH, NJW 2013, 3383.

[317] Mindestens zwei Handlungen sind für die Einschlägigkeit der Beharrlichkeit erforderlich, so das OLG Zweibrücken, NJW 2010, 1827; BGHSt 54, 189 (194 f., Tz. 20) spricht jedoch gegen die Festlegung einer Mindestanzahl.

[318] Krey et al., Strafrecht BT, Rn. 444.

[319] Vgl. etwa Sonnen, in: NK-StGB, § 238 Rn. 33.

per Mobiltelefon.[320] Der Täter kann so ohne direkten Kontakt zum Opfer Beleidigungen oder sexuelle Anspielungen versenden und das Opfer damit psychisch stark belasten. Eine ebenfalls sehr verbreitete Handlungsvariante bedient sich der sozialen Netzwerke und anderer Chatrooms.[321] In diesen kann der Täter seinem Opfer u. a. Nachrichten mit verletzendem oder bedrohlichem Inhalt schreiben, beleidigende oder anstößige Einträge oder Bilder auf das Profil oder die sog. Pinnwand des Betroffenen „posten" und auf diese Weise großen psychischen Druck ausüben. Erschwerend kommt für das Opfer die große Öffentlichkeitsspanne hinzu, welche die Verunglimpfung und Nachstellung mitverfolgen kann. Je nach Art und Inhalt des veröffentlichten Artikels können **Spott und soziale Ausgrenzung** von (unbeteiligten) Dritten eine zusätzliche Folge sein; dies kann die Lebensführung des Betroffenen stark beeinträchtigen.

Durch die **dauerhafte Speicherung der Daten** speziell auf einer Internet- **173**
plattform wird eine Beseitigung der belastenden Bilder oder Einträge zusätzlich erschwert, sodass die sozialen Schwierigkeiten die eigentliche Tat oft überdauern.[322] Hierdurch entstehen beim Cyberstalking in sozialen Netzwerken gravierendere Folgen für die Opfer als bei der herkömmlichen Begehungsweise der Nachstellung. Schreibt beispielsweise ein Täter in das Profil seiner Ex-Freundin mehrfach sexuelle Anspielungen oder postet er gar anstößige Bilder, so ist die Gefahr einer schnellen Verbreitung dieser Inhalte über das Netzwerk groß. Möglicherweise ist dann ein Schul-, Arbeitsplatz- und/oder Wohnortwechsel kaum ausreichend, um für das Opfer wieder sozialen Frieden einkehren zu lassen.

Was § 238 Abs. 1 **Nr. 3** StGB (missbräuchliche Verwendung personenbezogener **174**
Daten) anbelangt, so erfährt die 1. Variante – Aufgeben von Bestellungen von Waren oder Dienstleistungen – in sozialen Netzwerken keine größere Relevanz. Die 2. Variante – die Veranlassung Dritter, mit dem Opfer in Kontakt zu treten – wirkt sich dagegen häufiger aus. Durch die Eingabe der persönlichen Daten des Opfers in Chatrooms, bei Sex-Hotlines oder Partnersuchforen bringt der Täter Dritte dazu, gegen den eigentlichen Willen des Betroffenen mit dem Opfer Kontakt aufzunehmen.[323]

§ 238 Abs. 1 **Nr. 4** StGB erfasst die **Bedrohung** von Leben, körperlicher Unver- **175**
sehrtheit, Gesundheit oder Freiheit des Opfers oder einer ihm nahestehenden Person. Das reine Drohen mit Delikten, das unterhalb der Verbrechensschwelle gem. § 241

---

[320] Peters, NStZ 2009, 238 (240; auch insgesamt zu § 238 I Nr. 2 StGB); Langer, Die Strafvorschriften der Nachstellung, S. 85. Laut der Studie der Agentur der Europäischen Union für Grundrechte (FRA), Gewalt gegen Frauen, 03/2014, S. 30, waren 4 % der 18–29 jährigen Frauen in der EU in den letzten 12 Monaten vor der Befragung Opfer von Cyber-Stalking (via E-Mail, SMS oder Internet) geworden, hingegen nur 0,3 % der 60jährigen oder älteren Frauen (abrufbar unter: http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance_de_0.pdf).

[321] Siehe Gericke, in: MüKo-StGB, § 238 Rn. 22; Wolters, in: SK-StGB, § 238 Rn. 11; Rössner/Krupna, in: HK-GS, § 238 Rn. 6. Laut der FRA-Studie (Fn. 320), S. 32, haben 11 % der befragten Frauen seit dem 15. Lebensjahr bereits beleidigende, sexuell eindeutige E-Mails und SMS bzw. unangemessene Annäherungsversuche in sozialen Netzwerken erhalten (http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance_de_0.pdf).

[322] Beuth, Facebook löscht nicht zuverlässig, Die Zeit v. 26.9.2012.

[323] Fischer, StGB, § 238 Rn. 15b; Rössner/Krupna, in: HK-GS, § 238 Rn. 7.

StGB (dazu unter 7.5.9.3) nicht strafbar ist, soll mit dieser Handlungsvariante des § 238 StGB abgedeckt werden.[324] So kann auch der Androhung einer einfachen Körperverletzung (§ 223 StGB) oder Freiheitsberaubung (§ 239 StGB) Rechnung getragen werden.

176 Der **Auffangtatbestand** des § 238 Abs. 1 **Nr. 5** StGB erfasst die den Nr. 1–4 gleichgelagerten Verhaltensweisen; in der Praxis werden allerdings die meisten Fälle von den speziell ausformulierten Tatbegehungsweisen erfasst.[325]

177 Die Nachstellung muss zudem **unbefugt**, also gegen den Willen des Opfers erfolgen. Das **Einverständnis** des Betroffenen schließt die **Tatbestandsmäßigkeit** des § 238 StGB aus.[326] Im Fall der Nachstellung in oder mit Hilfe von sozialen Netzwerken könnte ein solches Einverständnis in der **Preisgabe der eigenen Daten** gesehen werden. Der Betroffene hat sich in der Regel selbstständig bei der jeweiligen Plattform angemeldet und seine persönlichen Informationen dort eingestellt sowie meist Bilder hochgeladen. Oftmals will er gerade, dass diese Inhalte von anderen Nutzern des Netzwerks gesehen und kommentiert werden können. Allerdings würde so in sozialen Netzwerken ein auf bestimmte Delikte bezogener straffreier Raum geschaffen werden. Die **bloße Registrierung** auf einer solchen Plattform und die Teilnahme am sozialen Internetleben reichen daher nicht aus, um ein tatbestandsausschließendes Einverständnis annehmen zu können. Auch die **Bestätigung der AGB** der einzelnen Anbieter von Internetplattformen lässt darauf schließen, dass die Nutzer gerade nicht damit rechnen oder gar damit einverstanden sind, beleidigt, bloßgestellt oder psychisch verletzt zu werden; zumeist wird in den AGB darauf hingewiesen, dass eben diese Inhalte nicht geduldet werden.[327]

178 Von einer vollendeten Nachstellung ist erst dann auszugehen, wenn die Tathandlung zu einer **schwerwiegenden Beeinträchtigung der Lebensgestaltung** für das Opfer führt (**Taterfolg**). Die Tathandlung muss dabei **kausal** für die eintretenden Folgen bzw. die Reaktion des Opfers sein. Auch hier wird es regelmäßig auf die Umstände des Einzelfalls ankommen. Es gibt jedoch einige feststehende Merkmale für die Beeinträchtigung der Lebensgestaltung, die auch für das sog. Cybermobbing[328] bzw. das sog. Cyberstalking einschlägig sind. Sieht sich das Opfer durch das Handeln des Täters etwa gezwungen, den **Wohnort zu verlassen** oder nur noch in Begleitung vor die Tür zu gehen, den **Arbeitsplatz zu wechseln** (z. B. wegen Veröffentlichung von anzüglichen Fotos) oder die Telefonnummer zu ändern, so sind die Auswirkungen auf seine Lebensweise gravierend.[329] Der im Dezember 2013 beschlossene Koalitionsvertrag der Regierungsparteien CDU, CSU und SPD sieht deshalb die

---

[324] Peters, NStZ 2009, 238 (240); Fischer, StGB, § 238 Rn. 16.
[325] Peters, NStZ 2009, 238 (241); siehe aber auch Rössner/Krupna, in: HK-GS, § 238 Rn. 9.
[326] Mosbacher, NStZ 2007, 665 (667).
[327] http://de-de.facebook.com/legal/terms (Stand 15.11.2013), insb. Punkt 3 Nr. 6, 7, 8, 10 und Punkt 5 Nr. 1 („Du wirst keine Inhalte auf Facebook posten oder Handlungen auf Facebook durchführen, welche die Rechte einer anderen Person oder das Gesetz verletzen.“).
[328] Zu diesem Phänomen: Kirchhoff, Kriminalistik 2013, 491 (492, dort 2.4).
[329] OLG Hamm, NStZ-RR 2009, 175; Krey et al., Strafrecht BT1, Rn. 446.

Verbesserung der Möglichkeiten der Meldung und Anzeige von Cybermobbing und Cybergrooming (Rn. 114) in sozialen Netzwerken vor.[330]

179 Eine Änderung des Freizeitverhaltens,[331] ein erforderlicher Wechsel der E-Mail-Adresse oder eine Einschränkung sozialer Kontakte können bereits für sich genommen, je nach Einzelfall, einen gravierenden Nachteil der Lebensqualität für das Opfer bedeuten.[332] Den Austritt aus der Internetplattform oder die Löschung eines Chat-Accounts allein[333] wird man dagegen im Regelfall noch nicht als schwerwiegende Beeinträchtigung der Lebensgestaltung ansehen können. Zwar hat für viele Menschen die Pflege sozialer Kontakte zu anderen Menschen über das Internet einen hohen Stellenwert. Das Verlassen eines Forums aber führt lediglich zu einer **Verlagerung** (Telefon, E-Mail), nicht aber zu einer Einschränkung der sozialen Kontakte. Sähe man allerdings eine soziale Internetplattform als ein durch Bilder und Pinnwandfunktionen erweitertes E-Mail-Postfach an, würde die Änderung der Erreichbarkeit einer Person über diese Plattform dem Austausch der E-Mail-Adresse ähneln. Auch kann gerade bei Jugendlichen und sozial zurückgezogenen Menschen, die häufig bzw. intensiv in sozialen Netzwerken verkehren, die Notwendigkeit, sich von einer solchen Plattform zurückzuziehen, um einem Stalker zu entgehen, durchaus eine Veränderung der Freizeitgestaltung darstellen. Ob der von § 238 StGB geforderte Taterfolg durch die Löschung des Accounts eines sozialen Netzwerkes eingetreten ist, hängt daher meist von den jeweiligen Umständen des konkreten Einzelfalls ab.

180 Der subjektive Tatbestand des Grunddelikts erfordert in Bezug auf alle objektiven Tatbestandsmerkmale mindestens **Eventualvorsatz**. Hinsichtlich der Unbefugtheit können bei der herkömmlichen Nachstellung Konstellationen des Tatbestandsirrtums (§ 16 StGB) auftreten.[334] Der Täter muss – das stellt das Erfordernis, die AGB von sozialen Netzwerken anzunehmen, sicher – ausdrücklich zustimmen, niemand anderen zu beschimpfen, zu beleidigen oder zu bedrohen. Handelt er dieser Verpflichtung zuwider, kann er grundsätzlich nicht von einem Einverständnis der betroffenen Person ausgehen (vgl. bereits Rn. 177).

181 Der **Qualifikationstatbestand** des § 238 Abs. 2 StGB setzt die **Gefahr des Todes oder einer schweren Gesundheitsschädigung** für das Opfer oder einer ihm nahestehenden Person voraus. Für die Tatbegehung und den Erfolg – die **konkrete Gefährdung** – ist ebenfalls **(Eventual-)Vorsatz** erforderlich.[335] Die qualifizierenden Gefahrerfolgsmerkmale werden nicht als besondere Folge, sondern als deren

---

[330] Koalitionsvertrag zwischen CDU, CSU und SPD (Fn. 6), S. 147. Vgl. auch die FRA-Studie (Fn. 320), S. 13, wonach die Maßnahmen verbessert werden sollen, um Opfer von Cyber-Stalking proaktiv zu unterstützen.

[331] LG Lübeck, Urt. v. 14.2.2008 – 2b Qs 18/08; Peters, NStZ 2009, 238 (241).

[332] BT-Drs. 16/575 v. 8.2.2006, S. 8; Mosbacher, NStZ 2007, 665 (667).

[333] Für eine Berücksichtigung im Rahmen der Gesamtbetrachtung: Rössner/Krupna, in: HK-GS, § 238 Rn. 10.

[334] Ausf. hierzu Mosbacher, NStZ 2007, 665 (669).

[335] Vgl. Mitsch, JURA 2007, 401 (406).

Voraussetzung gesehen; daher ist § 18 StGB nicht anwendbar.[336] Folglich reicht Fährlässigkeit in Bezug auf § 238 Abs. 2 StGB nicht aus.

182 Gerade in sozialen Netzwerken wird die fahrlässige Begehung einer konkreten Gefährdung die häufigere Erscheinungsform sein. Anders als bei der herkömmlichen Nachstellung bietet das Cyberstalking nicht die Möglichkeit, die Reaktionen (Gestik, Mimik) des Opfers wahrzunehmen. Der Täter kann oft nur schwer erkennen, geschweige denn beurteilen, wie sehr seine Bemerkungen oder Bilder das Opfer tatsächlich treffen und ab welchem Zeitpunkt möglicherweise eine Gefahr für Leben oder Gesundheit der Person entstehen könnte. Deshalb mangelt es häufig an einem für § 238 Abs. 2 StGB erforderlichen Gefährdungsvorsatz.

183 Die Qualifikation des § 238 Abs. 3 StGB (**Verursachung des Todes**) ist als **erfolgsqualifiziertes Delikt** ausgestaltet, für dessen Verwirklichung nach § 18 StGB auch Fahrlässigkeit ausreichend ist.[337]

184 Wie bei den Beleidigungsdelikten muss auch bei der Nachstellung das mögliche Vorliegen eines **Verbotsirrtums** (§ 17 StGB) geprüft werden. Der „Stalker" ist sich meist bewusst, dass er mit seiner hartnäckigen Art dem Betreffenden psychisch zusetzt. Dennoch ist dadurch nicht ausgeschlossen, dass er sich nicht darüber im Klaren ist, mit seinen Handlungen eine nach § 238 StGB strafbare Nachstellung zu begehen. Allerdings gelten die obigen Ausführungen (Rn. 65) entsprechend: Ein solcher Verbotsirrtum wäre im Regelfall vermeidbar, ein Schuldausschluss insoweit zu verneinen. Ggf. kann die Einholung eines psychiatrischen Gutachtens notwendig sein, um die Frage der Schuldfähigkeit (Vorliegen einer psychischen Störung) des Täters zu klären. In diesem Fall sind weiterhin die Voraussetzungen der Unterbringung in einem psychiatrischen Krankenhaus gem. § 63 StGB zu prüfen.[338]

185 Auch die Strafverfolgung des Cyberstalkings birgt im Gegensatz zur Nachstellung im nicht virtuellen Leben einige Besonderheiten in sich. So treten **Beweisschwierigkeiten** im Bereich der tatsächlichen Identität des Handelnden auf, wenn dieser sich über ein öffentliches WLAN Netzwerk oder Internetcafé auf sozialen Internetplattformen aufhält.[339] Die Richtigkeit der bei der Registrierung in diesen Netzwerken angegebenen Personalien wird regelmäßig nicht überprüft und ist faktisch auch kaum nachprüfbar. Weitere Schwierigkeiten in Bezug auf die Probleme der Strafverfolgung in sozialen Netzwerken werden im Abschnitt zu den verdeckten Ermittlungen erläutert (siehe unter 7.6.2).

186 In Anbetracht der speziellen Ausprägungen einer Nachstellungshandlung und der spezifischen Tatsituation in sozialen Netzwerken wäre die Einführung eines Qualifikationstatbestandes, der speziell die **Phänomene des Cyberstalkings** zum Inhalt hat, zu erwägen. Ein solcher könnte der größeren Verbreitungsgefahr den Lebenskreis des Opfers betreffender Handlungen, ausgehend von der erhöhten Öffentlichkeit im

---

[336] BGH, NJW 1999, 3131 (3132); Hardtung, in: MüKo-StGB, § 18 Rn. 12; Fischer, StGB, § 18 Rn. 4.
[337] Mitsch, Jura 2007, 401 (406).
[338] Mosbacher, NStZ 2007, 665 (669).
[339] Peters, NStZ 2009, 238 (240).

Internet, gerecht werden. Die Folgen eines Cyberstalkings sind aufgrund der spezifischen Tatsituation für das Opfer häufig stärker belastend als die mit einer Begehung außerhalb des Internet verbundenen Konsequenzen. Allerdings wäre bei der konkreten Ausgestaltung eines solchen Qualifikationstatbestandes auf die **Vermeidung einer Überkriminalisierung** zu achten.

187 Wird auf Grund der tatbestandlichen Unbestimmtheit des § 238 StGB das Vorliegen eines hinreichenden Tatverdachts von der Staatsanwaltschaft abgelehnt, so folgt meist die Verweisung auf den **Privatklageweg** (§ 374 Abs. 1 Nr. 5 StPO).[340] Oftmals handelt es sich um Vorkommnisse, die nur die unmittelbaren Beteiligten betreffen und durch welche der Rechtsfriede unbeteiligter Dritter nicht gestört wird.[341]

7.5.9.2 Nötigung (§ 240 StGB)

188 Eine Nötigung setzt den rechtswidrigen Einsatz von Gewalt oder einer Drohung mit einem empfindlichen Übel voraus, mit welchem der Täter beim Opfer eine bestimmte Handlung, Duldung oder ein Unterlassen bewirkt.

189 Um die Anwendung von **Gewalt** bejahen zu können, ist eine gewisse Kraftentfaltung auf das Opfer erforderlich. Die rein psychische Wirkung einer Handlung, ohne das Hervorrufen einer konkreten, über ein gegenwärtiges, körperliches Übel hinausgehenden Gesundheitsschädigung, genügt diesen Anforderungen nicht.[342] Eine Tatbegehung mittels Gewalt wird in sozialen Netzwerken von daher regelmäßig ausscheiden.

190 In Betracht kommt allerdings die Variante der **Drohung** mit einem empfindlichen Übel. Hierbei ist der verfolgte Zweck ausschlaggebend. Soll das Opfer wirkungsvoll eingeschüchtert werden, ohne eine konkret beabsichtigte Reaktion, abgesehen von Angst und Schrecken, hervorzurufen, liegt kein angestrebter Nötigungserfolg i. S. v. § 240 StGB vor.[343] Wird dagegen auf einen bestimmten Erfolg abgezielt, beispielsweise eine Versöhnung nach einer Trennung, das Unterlassen einer Trennung oder das Aufsuchen eines bestimmten Ortes, so ist der objektive Tatbestand der Nötigung einschlägig.

191 Für das Vorliegen eines **empfindlichen Übels** muss der Täter glaubhaft machen, zu dessen Verwirklichung im Stande zu sein und dies auch zu wollen.[344] Die Empfindlichkeit des Übels bemisst sich nach der Erheblichkeit des angedrohten Nachteils. Hierbei sind grundsätzlich subjektive Empfindungen ausschlaggebend, welche stark genug sind, beim Opfer das vom Täter gewünschte Verhalten hervorzurufen.[345] In sozialen Netzwerken spielt die Drohung mit der öffentlichen Bekanntmachung von

[340] Peters, NStZ 2009, 238 (242) mit dem Hinweis auf Schätzungen, wonach rund 70 % aller Nachstellungsverdachtsfälle auf den Privatklageweg verwiesen werden.
[341] Peters, NStZ 2009, 238 (242).
[342] Träger/Altvater, in: LK-StGB, § 240 Rn. 36.
[343] Gerhold, Das System des Opferschutzes im Bereich des Cyber- und Internetstalkings, S. 144.
[344] Fischer, StGB, § 240 Rn. 32, 36.
[345] Fischer, StGB, § 240 Rn. 32a.

privaten Bildern oder persönlichen Lebensdetails eine große Rolle.[346] Ein Beispiel, welches 2012 weltweit für Aufsehen gesorgt hat, ist eine 15-Jährige aus Kanada, welche sich u. a. in Folge einer Nötigung das Leben nahm.[347]

192 Für die **Rechtswidrigkeit** eines tatbestandlich relevanten Handelns ist (neben dem Fehlen von Rechtfertigungsgründen) zusätzlich die **besondere Verwerflichkeit**, also der erhöhte Grad sittlicher Missbilligung erforderlich, welcher sich aus dem angestrebten Zweck, dem eingesetzten Mittel oder aus der Gesamtwürdigung der Zweck-Mittel-Relation ergeben kann.[348] Diesbezüglich bestehen in sozialen Netzwerken keine Besonderheiten.

193 Ein besonders schwerer Fall der Nötigung liegt in der Regel vor, wenn der Täter eine andere Person zu einer **sexuellen Handlung** nötigt (§ 240 Abs. 4 S. 2 Nr. 1 StGB). Bei Kindern als Opfer wird dann auch der Tatbestand des § 176 Abs. 4 Nr. 2, 3 StGB erfüllt sein (Rn. 114).

7.5.9.3 Bedrohung (§ 241 StGB)

194 Droht der Täter dem Opfer mit der **Begehung eines Verbrechens** gegen das Opfer selbst oder einer diesem nahestehenden Person, so verwirklicht er dadurch den Tatbestand der Bedrohung, § 241 Abs. 1 StGB.[349] Zur Verwirklichung des § 241 Abs. 2 StGB ist es erforderlich, dass der Täter wider besseres Wissen dem Opfer vortäuscht, dass ein gegen ihn oder eine ihm nahestehende Person gerichtetes Verbrechen bevorsteht. Der Unterschied zur Nötigung (§ 240 StGB) liegt in der Art der Drohung und dessen Zweckrichtung; hier soll das Opfer vor allem eingeschüchtert werden, also nicht unbedingt zu einem bestimmten Verhalten veranlasst werden.

7.5.10 Verstöße gegen das Gewaltschutzgesetz

195 Gemäß § 4 Satz 1 GewSchG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer einer bestimmten vollstreckbaren Anordnung eines Gerichts[350] nach § 1 Abs. 1 S. 1 oder 3 GewSchG, jeweils auch in Verbindung mit § 1 Abs. 2

---

[346] Vgl. nur *Süddeutsche.de* v. 26.3.2014 (http://www.sueddeutsche.de/muenchen/internet-entzug-als-strafe-richter-verhaengen-facebook-verbot-1.1920905) zum „Münchener Sex-Erpresser-Fall" mit Verurteilung zu einem „Facebook-Verbot".

[347] Ausf. hierzu Horsten, Cybermobbing: Trauer um die tote A., n-tv v. 21.10.2012.

[348] Fischer, StGB, § 240 Rn. 41 ff.

[349] Ostendorf et al., NStZ 2012, 529 (536); Bei einer widerrechtlichen Drohung mit der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit auf einer Internetplattform kann es zu einer befristeten Gewaltschutzanordnung gemäß § 1 Abs. 2 Satz 1 Nr. 1 GewSchG kommen, vgl. hierzu OLG Hamm, BeckRS 2013, 11035.

[350] Der Verstoß gegen eine vergleichsweise übernommene Verpflichtung ist nicht strafbar, vgl. Reinken, in: BeckOK-BGB, GewSchG, § 4 Rn. 2.

Satz 1 GewSchG, vorsätzlich[351] zuwiderhandelt. Nach § 4 Satz 2 GewSchG bleibt die Strafbarkeit nach anderen Vorschriften unberührt. Aus der Perspektive der Cyberkriminalität kommt eine sog. **Gewaltschutzanordnung** gemäß § 1 Abs. 1 GewSchG durch das Familiengericht[352] vor allem in Betracht, wenn eine Person einer anderen beispielsweise über soziale Netzwerke mit einer Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit widerrechtlich gedroht hat (§ 1 Abs. 2 S. 1 Nr. 1 GewSchG).[353] Der Begriff der Drohung wird dabei gleichbedeutend zu den §§ 240, 241 StGB verwendet.[354] Das Gericht kann in der Schutzanordnung insbesondere anordnen, dass es der Täter zu unterlassen hat, Verbindung zur verletzten Person, auch unter Verwendung von Fernkommunikationsmitteln, aufzunehmen (§ 1 Abs. 1 S. 3 Nr. 3 GewSchG). Ebenso ist eine Schutzanordnung denkbar, wenn eine Person in sozialen Netzwerken widerrechtlich und vorsätzlich eine andere Person dadurch unzumutbar belästigt, dass sie ihr gegen den ausdrücklich erklärten Willen wiederholt nachstellt (zum Begriff vgl. Rn. 171 ff.) oder sie unter Verwendung von Fernkommunikationsmitteln (dazu zählen auch soziale Netzwerke) verfolgt (§ 1 Abs. 2 S. 1 Nr. 2 lit. b GewSchG).[355] Der Straftatbestand des § 4 GewSchG stellt dabei eine sog. Blankettnorm dar, die erst durch eine zivilrechtliche vollstreckbare Anordnung ausgefüllt wird.[356] Das Strafgericht ist jedoch bei der Beurteilung der Frage der materiellen Rechtmäßigkeit der Schutzanordnung nicht an die Beurteilung des Familienrechts gebunden.[357]

7.5.11 Verstöße gegen das Urheberrechtsgesetz

Der Schutz von Urheberrechten durch das Strafrecht hat in den vergangenen Jahren **196**
vor allem durch die Weiterentwicklung des Internet an Bedeutung gewonnen. Dies liegt einerseits daran, dass die Zahl der Nutzer von sog. Tauschbörsen im Internet zugenommen hat. Dabei werden Dateien von Film- oder Musikwerken direkt zwischen Internet-Nutzern über sog. **Peer-to-Peer-Netzwerke** weitergegeben („getauscht"). Ein solches „Filesharing" bewegt sich nur dann im Rahmen der Legalität, wenn die Dateien in einer freien Lizenz veröffentlicht werden, die Weitergabe erwünscht ist

[351] Cirullies/Cirullies, Schutz bei Gewalt und Nachstellung, Rn. 555.
[352] Zur Zuständigkeit vgl. §§ 111 Nr. 6, 210 f. FamFG.
[353] Vgl. OLG Hamm, BeckRS 2013, 11035 = STREIT 2014, 37 (befristetes Näherungs- und Kontaktverbot nach Bedrohung auf Facebook).
[354] Cirullies/Cirullies, Schutz bei Gewalt und Nachstellung, Rn. 31; Erbarth, Das familienrechtliche Mandat, § 4 Rn. 18. Freytag, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 1 GewSchG, Rn. 17; Brudermüller, in: Palandt, BGB, § 1 Rn. 14.
[355] Cirullies/Cirullies, Schutz bei Gewalt und Nachstellung, Rn. 36.
[356] BGHSt 51, 257 (259); OLG Hamburg, BeckRS 2011, 05165.
[357] BGH, BeckRS 2014, 02525 entgegen dem Vorlagebeschluss des OLG Oldenburg, BeckRS 2013, 04750; vgl. auch OLG Hamm, NStZ 2007, 486; OLG Celle, NStZ 2007, 485; OLG Hamburg, BeckRS 2011, 05165; BT-Drs. 14/5429, S. 32.

bzw. freigegeben ist oder eine etwaige Schutzfrist für das betreffende Werk abgelaufen ist. Andernfalls kommt eine Strafbarkeit des Nutzers nach § 106 UrhG in Betracht.[358]

197 Die aktuelle Diskussion über den strafrechtlichen Schutz von Urheberrechten hängt auch damit zusammen, dass gerade soziale Netzwerke aufgrund ihrer Konzeption (Erzeugung einer möglichst großen **Transparenz** und Offenheit zwischen den Mitgliedern) und der damit einhergehenden geschaffenen Plattform Verstöße gegen Urheberrechte anderer Personen erheblich begünstigen.

198 Hinzu kommt, dass der viktimologische Grundsatz, wonach die **Hemmschwelle** zur Begehung einer Tat mit Kenntnis bzw. Wahrnehmung des potentiellen Opfers tendenziell abnimmt, bei Urheberrechtsverstößen etwa im Bereich von Musiktiteln nicht gilt. Den Konsumenten ist meist bekannt, dass nur ein Bruchteil eines für den legalen Erwerb zu zahlenden Kaufpreises an den Künstler abgeführt und der größte Teil von den (als nicht „schutzwürdig" empfundenen) Platten-/Musikfirmen einbehalten wird.

199 Das Potential möglicher Urheberrechtsverstöße wird auch dadurch verdeutlicht, dass Netzwerk-Betreiber in ihren Nutzungsbedingungen üblicherweise auf die Gefahr von Verstößen gegen das UrhG hinweisen, diese untersagen[359] und bei Zuwiderhandlung die Bilder etc. ggf. entfernen, worauf jeder Nutzer in den Nutzungsbedingungen, welche bei einer Registrierung akzeptiert werden müssen, hingewiesen wird.

---

[358] Vgl. vertiefend: Heigenhauser, Zur Strafbarkeit der Musik-, Video- und Softwarepiraterie (2007); Lang, Filesharing und Strafrecht (2009); Schäufele, Zur Strafbarkeit des Raubkopierens im Internet. Filesharing von urheberrechtlich geschützten Werken im Internet (2012); Heghmanns, MMR 2004, 14; Beck/Kreißig, NStZ 2007, 304 ff.; zum Akteneinsichtsrecht des Verletzten aus § 406e StPO: Esser, GA 157 (2010), 65 ff.; Schmidt, GRUR 2010, 673 ff. Zur parallelen zivilrechtlichen Verantwortlichkeit siehe BGH, NJW 2013, 1441 (Haftung der Eltern für Kinder); BGH, Urt. v. 8.1.2014 – I ZR 169/12 (grundsätzlich keine Haftung des Inhabers eines Internetanschlusses für das Verhalten eines volljährigen Familienangehörigen).

[359] So schreibt Facebook in seinen Nutzungsbedingungen (http://de-de.facebook.com/terms/german.php): „Dir gehören alle Inhalte und Informationen, die du auf Facebook postest." (§ 2); „Wenn du wiederholt die Rechte am geistigen Eigentum anderer verletzt, werden wir gegebenenfalls dein Konto sperren." (§ 5 Nr. 5).

Die Google Nutzungsbedingungen (http://www.google.de/policies/terms/regional.html) stellen sich wie folgt dar: „Sie behalten Ihre Rechte als Urheber und alle bestehenden gewerblichen Schutzrechte an den Inhalten, die Sie in unsere Dienste einstellen. Kurz gesagt: Was Ihnen gehört, bleibt auch Ihres. […] Achten Sie darauf, dass Sie, wenn Sie Inhalte in unsere Dienste hochladen, Ihrerseits über die hierzu eventuell notwendigen Rechte verfügen." und „Wir reagieren auf Meldungen zu mutmaßlichen Urheberrechtsverletzungen und kündigen die Konten von Personen, die wiederholt Verstöße begehen, gemäß dem im US-amerikanischen Urheberrechtsgesetz (Digital Millennium Copyright Act) vorgesehenen Verfahren."

7.5.11.1 Unerlaubte Verwertung urheberrechtlich geschützter Werke (§ 106 UrhG)

Inhalte in sozialen Netzwerken, sei es in Form von Texten, Fotos oder Videos, genießen strafrechtlichen Schutz (§ 106 UrhG), wenn es sich dabei um **Werke** oder eine Bearbeitung oder Umgestaltung eines Werkes handelt, die in den anderen als den gesetzlich zugelassenen Fällen ohne die Einwilligung des Berechtigten vervielfältigt, verbreitet oder öffentlich wiedergegeben werden. **200**

Ob es sich bei Texten, Fotos usw. um urheberrechtlich relevante Werke handelt, ist anhand einer zweistufigen Prüfung zu beurteilen:[360] Zunächst müssen die Abbildungen in den Schutzbereich des § 1 UrhG fallen, d. h. ein Werk der Literatur, Wissenschaft oder Kunst sein. § 2 Abs. 1 UrhG enthält insoweit eine (nicht abschließende) Aufzählung. Ein solches Werk muss zudem gemäß § 2 Abs. 2 UrhG eine **persönliche geistige Schöpfung** darstellen. Hierzu müssen fünf Merkmale erfüllt sein: 1) das Vorliegen einer Schöpfung, die 2) einen geistigen Gehalt aufweist, in der 3) die Individualität des Urhebers zum Ausdruck kommt, wobei 4) eine bestimmte Gestaltungshöhe erreichet werden und 5) eine Formgebung stattgefunden haben muss.[361] **201**

Mithin sind auch die **Bearbeitung** (vgl. § 3 UrhG), d. h. die Umgestaltung eines vorhandenen Werkes, durch die den individuellen Zügen desselben eine neue Individualität aufgeprägt wird,[362] und die Umgestaltung eines Werkes, bei welcher – im Gegenteil zur Bearbeitung – das benutzte Werk eben nicht nur für weitere Zwecke angepasst, sondern das Werk in abgeänderter Form genutzt wird,[363] geschützt. **202**

Auch für soziale Netzwerke sind die verbotenen Verwertungshandlungen Vervielfältigung, Verbreitung und öffentliche Wiedergabe einschlägig. **203**

Die Vervielfältigung knüpft an §§ 15 Abs. 1 Nr. 1, 16 UrhG an und meint jede körperliche Festlegung des Werkes, die geeignet ist, das Werk den menschlichen Sinnen auf irgendeine Weise mittelbar oder unmittelbar wahrnehmbar zu machen.[364] Unter einer Verbreitung versteht man das öffentliche Anbieten oder Inverkehrbringen eines Werkes (vgl. §§ 15 Abs. 1 Nr. 2, 17 UrhG). Bezüglich der öffentlichen Wiedergabe kann ebenso auf § 15 Abs. 2 UrhG verwiesen werden, nach welcher es das ausschließliche Recht des Urhebers ist, sein Werk in unkörperlicher Form wiederzugeben (vgl. dazu die nicht abschließende Aufzählung in § 15 Abs. 2 S. 2 UrhG). **204**

Darüber hinaus darf **kein gesetzlich zugelassener Fall einer Verwertungshandlung** vorliegen. Dies meint nicht etwa allgemeine Rechtfertigungsgründe, sondern vielmehr die Schranken des Urheberrechts (§§ 44a ff. UrhG). Ist eine solche Schranke **205**

---

[360] Vgl. Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 3; Ernst, in: Graf et al., Wirtschafts- und Steuerstrafrecht, § 106 UrhG, Rn. 5.
[361] Siehe: Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 9; Ernst, in: Graf et al., Wirtschafts- und Steuerstrafrecht, § 106 UrhG, Rn. 8 ff.
[362] Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 38.
[363] Vgl. Schulze, in: Dreier/Schulze, UrhG, § 23 Rn. 6 f.
[364] Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 47.

einschlägig, ist eine strafrechtlich relevante Urheberrechtsverletzung bereits tatbestandlich ausgeschlossen.[365] Eine im Übrigen tatbestandlich relevante Handlung ist nur rechtswidrig, wenn keine Einwilligung vom Berechtigten, d. h. dem Urheber oder seinem Rechtnachfolger vorliegt.[366]

7.5.11.2 Spezifika von Urheberrechtsverstößen in sozialen Netzwerken

206 Das oben beschriebene Filesharing (Rn. 196), welches regelmäßig eine große Anzahl von Urheberrechtsverstößen nach sich zieht, ist in sozialen Netzwerken nicht die häufigste Art der Urheberrechtsverletzung.[367] Vielmehr handelt es sich meist um Fotos oder Videos, die von einer anderen Person aus dem Internet stammen oder anderweitig erlangt wurden, aber nicht das Werk dieses Nutzers darstellen; diese Abbildungen werden häufig hochgeladen, „gepostet" usw., ohne dass über urheberrechtliche Konsequenzen nachgedacht wird.[368]

207 Eine weitere Möglichkeit, gegen ein Urheberrecht zu verstoßen, kann auch darin gesehen werden, dass Inhalte, die ein Nutzer eines sozialen Netzwerks auf seine Seite gestellt hat, dahingehend missbraucht werden, dass sie ohne sein Einverständnis **weiterverwendet** werden, indem etwa diese Inhalte oder Informationen von Dritten übernommen oder geteilt werden.[369] Mit der Einstellung eines Werkes durch den Berechtigten, gibt dieser als Nutzer eines sozialen Netzwerks (ebenso wenig wie außerhalb des Internet) nicht automatisch jeglichen urheberrechtlichen Schutz auf; vielmehr verbleiben ihm auch in einer solchen Situation die Rechte als Urheber. Man spricht bei etwaigen Inhalten von einem sog. User-generated Content, also urheberrechtlich relevanten Inhalten, die Nutzer in Form von Wort, Bild, Audio oder eben auch als Video ins Netz stellen.[370]

208 Eine Meldung bei Facebook unter Hinzufügung eines Links führt häufig dazu, dass dem Nutzer sog. **Vorschaubilder** der verlinkten Seite angezeigt werden, zwischen denen er beim Aufruf wählen kann. Soweit es sich bei diesen Vorschaubildern (auch) um urheberrechtlich geschützte Werke handelt, besteht für den Nutzer aufgrund von Lizenzbedingungen oder unmittelbar aus § 13 UrhG die Pflicht, am Werk auf dessen Urheber hinzuweisen. Ein solcher Fall der fehlenden Urheberrechtsbezeichnung ist

---

[365] Vgl. Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 78; Schulze, in: Dreier/Schulze, UrhG, § 106 Rn. 6.

[366] Vgl. Dreier, in: Dreier/Schulze, UrhG, § 106 UrhG, Rn. 8 f.; Heinrich, in: MüKo-StGB, § 106 UrhG, Rn. 114 f.; a. A. Dietz, in: Wandtke, Urheberrecht, S. 412, der in der Einwilligung eine Doppelfunktion sieht.

[367] Facebook bietet etwa über die Nutzung der App „*Pipe*" die Möglichkeit, Dateien im *peer-to-peer* Verfahren an andere Facebook-Nutzer zu senden (http://www.golem.de/news/dateitransfer-pipe-macht-echtzeit-filesharing-ueber-facebook-moeglich-1205-92115.html).

[368] Skurril mutet die urheber(straf)rechtlich diskutierte Konstellation an, dass zunehmend Speisen in Restaurants fotografiert und anschließend in sozialen Netzwerken im Internet „gepostet" werden; siehe hierzu: SZ Nr. 184 v. 10./11.8.2013, S. 1 („Das Netz isst mit").

[369] Vgl. Reinemann/Remmertz, ZUM 2012, 216 (221).

[370] Vgl. Reinemann/Remmertz, ZUM 2012, 216.

auch von strafrechtlicher Relevanz. Zwar fehlt es bislang an (strafrechtlicher) Rechtsprechung zur Verwendung dieser Vorschaubilder, doch wurde vereinzelt bereits über Abmahnungen an (gewerbliche) Verwender berichtet.[371]

209 Große mediale Aufmerksamkeit hat Ende 2013 die Frage erhalten, ob das **Streamen** von Videos im Internet eine (möglicherweise strafrechtsrelevante) Urheberrechtsverletzung darstellt. Auch in sozialen Netzwerken erlangt dieses Thema Relevanz, da zahlreiche Nutzer Videos von Onlineplattformen wie YouTube teilen und damit in die Online-Community einbinden. Technisch gesehen wird beim Streaming, anders als beim Herunterladen (etwa im Rahmen des Filesharings), auf dem Rechner des Nutzers keine dauerhafte Kopie des urheberrechtlich geschützten Videos erstellt. Beim Streaming erfolgt lediglich eine kurze, technisch bedingte, Zwischenspeicherung im Arbeitsspeicher, das sog. **Caching**, um eine lückenlose Wiedergabe des Videoinhalts zu gewährleisten. Diese wird regelmäßig, da ihr auch keine eigenständige wirtschaftliche Bedeutung beigemessen werden kann, als vorübergehende Vervielfältigungshandlung vom Erlaubnistatbestand des **§ 44a UrhG** gedeckt sein, so dass durch die Zwischenspeicherung auch keine Strafbarkeit ausgelöst wird.[372] Zutreffend wird darauf hingewiesen, dass bereits seit vielen Jahren eine technisch bedingte Zwischenspeicherung in nahezu sämtlichen modernen Unterhaltungsgeräten stattfindet, ohne dass hier eine Strafbarkeit angedacht wurde; für die Zwischenspeicherung auf dem PC im Rahmen des Streamings darf daher nichts anderes gelten.[373] Gewisse (technische) Widersprüche zur deutlich restriktiveren Rechtsprechung bei der Besitzverschaffung (kinder)pornographischer Darstellungen (Rn. 89 ff.) sind allerdings unverkennbar.

210 Jedenfalls durch das **Recht auf Privatkopie** (§ 53 Abs. 1 S. 1 UrhG) entfällt beim Streaming eine mögliche Strafbarkeit für vereinzelte Vervielfältigungen zum privaten Gebrauch, sofern sie nicht aus einer offensichtlich rechtswidrigen Vorlage stammen. Dabei ist der Nutzer nicht dazu verpflichtet, Nachforschungen über die Rechtmäßigkeit der Quelle anzustellen; die Rechtswidrigkeit muss sich ihm vielmehr aufdrängen.[374] Nach alledem ist die rein rezeptive Nutzung von Streamingdiensten nach überwiegender Ansicht als straffrei anzusehen.[375]

211 Urheberrechtsverstöße stehen potenziell auch dann im Raum, wenn durch die **Einstellung einer Verlinkung** zu urheberrechtlich geschütztem (meist Film-)Material andere Benutzer des sozialen Netzwerks dazu angeregt werden, das entsprechende Material herunterzuladen. Dies kann, je nach den konkreten Umständen, als Anstiftung (§ 26 StGB) zu einer strafbaren Vervielfältigung nach § 106 UrhG gewertet

---

[371] Vgl. http://www.zeit.de/digital/internet/2013-01/facebook-thumbnails.

[372] Anderes soll ausnahmsweise gelten, wenn die im Zwischenspeicher abgelegte Sequenz aufgrund ihrer Länge eigene Werkqualität besitzt.

[373] Unter Hinweis auf Fernseher und tragbare CD-Player: Hilgert/Hilgert, MMR 2014, 85 (87 f.).

[374] So etwa beim Streaming von noch nicht anderweitig (etwa auf DVD) verfügbaren Kinofilmen oder unberechtigten Konzertmitschnitten, vgl. Hilgert/Hilgert, MMR 2014, 85 (88).

[375] Vgl. Hilgert/Hilgert, MMR 2014, 85; Reinbacher, HumFoR 2012, 179; Reinbacher, NStZ 2014, 57 (61 f.); Wernert, Internet Kriminalität, S. 133; ebenso: Antwort der Bundesregierung v. 2.1.2014, BT-Drucks. 18/246, auf eine Kleine Anfrage der Fraktion Die Linke, BT-Drs. 18/195.

werden. Onlineportale, wie die zwischenzeitlich geschlossene Plattform *kino.to*, bieten zumeist die Möglichkeit, entweder durch Streaming oder Download auf das urheberrechtlich geschützte Material zuzugreifen. Während das Streaming nach überwiegender Ansicht regelmäßig aufgrund von § 44a UrhG mangels *dauerhafter* Vervielfältigungshandlung straffrei bleibt (vgl. Rn. 205), genießt der Download des Filmmaterials nicht den Schutz dieser Schrankenbestimmung. Eine Rechtfertigung des Downloads von Portalen wie *kino.to* als Privatkopie nach § 53 UrhG dürfte daran scheitern, dass die äußeren Umstände die Annahme nahelegen, dass die Quelle (etwa aufgrund ihrer unbegrenzten Kostenfreiheit und der Bereitstellung kinoaktueller Spielfilme) „offensichtlich" rechtswidrig ist.[376] Da demjenigen, der die Verlinkung aufruft, auf entsprechenden Plattformen zumeist sowohl die Möglichkeit des (straffreien) Streamings als auch des (strafbaren) Downloads zur Verfügung stehen, und dem Ersteller des Links regelmäßig nicht bekannt sein wird, ob sich der durch seinen Post auf das Video aufmerksam gewordene Nutzer für die strafbare oder die straffreie Zugangsform entscheidet, dürfte es in entsprechenden Fällen regelmäßig am Anstiftervorsatz fehlen.

7.5.11.3 Strafverfolgung durch die Staatsanwaltschaft

212 Die Staatsanwaltschaft ist gem. § 152 Abs. 2 StPO dazu verpflichtet, wegen einer verfolgbaren Straftat einzuschreiten, sofern zureichende tatsächliche Anhaltspunkte für ihre Begehung vorliegen. Sie darf das Verfahren gem. § 170 Abs. 2 StPO nur einstellen, wenn die Ermittlungen keinen genügenden Anlass zur Erhebung der öffentlichen Klage bieten (vgl. § 170 Abs. 1 StPO). Anderenfalls, d. h. wenn keine ausreichenden Gründe für die Einstellung des Strafverfahrens gegeben sind, verstieße sie gegen das **Legalitätsprinzip**.

213 Danach ist die Staatsanwaltschaft zur Verfolgung von Straftaten grundsätzlich auch dann verpflichtet, wenn diese sich in sozialen Netzwerken nur im kleineren Rahmen bewegen. Dabei ist jedoch zu beachten, dass es sich bei den Delikten des Urheberstrafrechts gemäß § 109 UrhG um **Antragsdelikte** handelt, eine Verfolgung somit grundsätzlich nur auf Antrag des verletzten Rechteinhabers möglich ist, wobei § 109 Hs. 2 UrhG der Staatsanwaltschaft eine Verfolgung von Amts wegen gestattet, soweit sie ein solches aufgrund des besonderen öffentlichen Interesses für geboten hält. Wann ein besonderes öffentliches Interesse bei Straftaten gegen das geistige Eigentum regelmäßig anzunehmen ist, konkretisieren die Nr. 261, 261a RiStBV.

214 Die einzige Ausnahme von diesem (grundsätzlichen) Antragserfordernis stellt § **108a UrhG** dar, der nicht vom Antragserfordernis des § 109 UrhG umfasst ist; die gewerbsmäßige unerlaubte Verwertung von Rechten nach § 108a UrhG stellt das einzige **Offizialdelikt** der Urheberstraftatbestände dar.

215 Es ist mittlerweile gleichwohl eher die Regel als die Ausnahme, dass Staatsanwaltschaften bei nicht gewerblichen Urheberrechtsverstößen im Internet generell und

[376] Reinbacher, NStZ 2014, 57 (61); ders., HumFoR 2012, 179.

in der Begründung pauschal von einer Strafverfolgung unter Verneinung eines für die Übernahme der Verfolgung erforderlichen öffentlichen Interesses absehen oder zwar einen Anfangsverdacht (§ 106 Abs. 1 UrhG) bejahen, das Verfahren dann jedoch „**wegen unbekannter Täterschaft**" nach § 170 Abs. 2 StPO einstellen.[377] Davon zu unterscheiden ist die Möglichkeit der Verfahrenseinstellung aus Opportunitätsgründen (§§ 153, 153a StPO), die aber die vorherige Ermittlung eines Tatverdächtigen voraussetzt.

216 Eine Beschränkung (nicht selten: ein Unterlassen) der Strafverfolgung auf der Grundlage von § 170 Abs. 2 StPO führt dazu, dass viele Urheberrechtsverstöße in sozialen Netzwerken, die naturgemäß privat und nicht gewerblich erfolgen, nicht verfolgt werden, obwohl auch diese Urheberrechtsverstöße in der Summe erheblichen Schaden bei den Berechtigten verursachen und daher grundsätzlich als strafbedürftig und strafwürdig erscheinen. Hinzu kommt, dass der Gesetzgeber bei der Schaffung des § 106 UrhG gerade keine Unterscheidung zwischen privaten und gewerblichen Urheberrechtsverstößen vorgenommen hat, obwohl eine solche im Gesetzgebungsverfahren durchaus diskutiert worden war. Eine pauschale Beschränkung der Strafverfolgungstätigkeit von Staatsanwaltschaften auf gewerbliche Urheberrechtsverstöße widerspricht daher dem Legalitätsprinzip.

217 Der Annahme einer grundsätzlichen Verfolgungspflicht der Strafverfolgungsbehörden steht auch nicht entgegen, dass es sich bei § 106 UrhG um ein **Privatklagedelikt** handelt (§ 374 Abs. 1 Nr. 8 StPO).[378] Die Staatsanwaltschaft erhebt bei diesen Delikten gemäß § 376 StPO nur dann die öffentliche Klage, wenn dies im öffentlichen Interesse liegt. Hierzu besteht für die Staatsanwaltschaft grundsätzlich ein Ermessensspielraum, der sich anhand **Nr. 86, 87 RiStBV** konkretisieren lässt. Ein solches öffentliches Interesse wird in der Regel anzunehmen sein, wenn der Rechtsfrieden über den Lebenskreis des Verletzten hinaus gestört und die Strafverfolgung ein gegenwärtiges Anliegen der Allgemeinheit ist, z. B. wegen des Ausmaßes der Rechtsverletzung, Nr. 86 Abs. 2 RiStBV.

218 Urheberrechtsverstöße in sozialen Netzwerken haben mittlerweile ein derartiges Ausmaß angenommen, dass man nicht mehr von einer geringen Bedeutung sprechen kann. So hat Twitter im Dezember 2010 rund 300 Löschungsaufforderungen wegen angeblicher Urheberrechtsverstöße vermeldet.[379] Urheberrechtsverstöße stören demnach den **Rechtsfrieden** über den Lebenskreis des Verletzten hinaus und sind zudem aufgrund dieses Ausmaßes ein gegenwärtiges Anliegen der Allgemeinheit, was eine Strafverfolgung rechtfertigt.

219 Gerade aufgrund der einfachen Verbreitungsmöglichkeiten von Bildern, Texten oder Videos (oftmals genügt es, ein Bild zu „teilen") sind solche Urheberrechtsverstöße für jeden Nutzer eines sozialen Netzwerks ohne besondere technische Fertigkeiten möglich.

---

[377] Vgl. Esser, GA 157 (2010), 65 (66 ff.).
[378] Vgl. Esser, GA 157 (2010), 65 (69 ff.).
[379] Vgl. Reinemann/Remmertz, ZUM 2012, 216.

220 Aufgrund dessen ist ein öffentliches Interesse an der Verfolgung von Urheberrechtsverstößen, auch an privaten, in sozialen Netzwerken grundsätzlich gegeben. Dass es sich bei § 106 UrhG um ein Privatklagedelikt handelt, spricht nicht per se gegen eine strafprozessuale Verfolgungspflicht.

221 Um trotz der (von den Tätern häufig ausgenutzten) Anonymität in sozialen Netzwerken den Rechteinhabern eine Geltendmachung ihrer Rechte (etwa ihres zivilrechtlichen Unterlassungs- und Schadensersatzanspruchs nach § 97 UrhG) zu ermöglichen und eine solche nicht an der unbekannten Identität des Verletzers scheitern zu lassen, gewährt § 101 UrhG ihnen einen umfassenden (zivilrechtlichen) **Auskunftsanspruch**. Nicht selten ist der mutmaßliche Verletzer dem Rechteinhaber bei Handlungen in sozialen Netzwerken nur anhand einer (zumeist dynamischen) IP-Adresse bekannt, ohne dass deren Zuordnung zu einer konkreten Person möglich wäre. § 101 Abs. 9 UrhG schafft in solchen Fällen, in denen eine Identifizierung des mutmaßlichen Rechteverletzers für den Verletzten nur anhand von Verkehrsdaten (§ 3 Nr. 30 TKG) möglich ist, die Möglichkeit, eine richterliche Anordnung zu erwirken, aufgrund derer er vom Internet Service Provider des mutmaßlichen Rechteverletzers Auskunft über die Identität des Anschlussinhabers verlangen kann. Nachdem sowohl das BVerfG[380] als auch der EuGH[381] der Vorratsdatenspeicherung solcher Verkehrsdaten strenge Grenzen gesetzt haben, erscheint die tatsächliche Erlangung der Daten für die Rechteinhaber allerdings wieder zunehmend ungewiss.[382]

7.5.11.4 Mögliche Lösungsvorschläge

222 Aufgrund der vorangegangen Ausführungen erscheint es fraglich, wie Verstößen gegen das Urheberrecht in sozialen Netzwerken entgegengewirkt werden kann. Dass sich auch die Verstöße häufen, liegt vor allem daran, dass sich die Täter einer geringen Kontrolle ausgesetzt fühlen, da nach ihrer Einschätzung das Risiko entdeckt zu werden, gering ist, auch wenn dies tatsächlich nicht der Fall ist.[383] Die Folgen eines solchen Verstoßes können neben den strafrechtlichen Konsequenzen aus § 106 UrhG auch zivilrechtliche **Abmahnungen und Schadensersatzforderungen**. Eine Möglichkeit, die Vielzahl von Urheberrechtsverstößen in sozialen Netzwerken zu vermeiden, könnte darin bestehen, dass die Betreiber sämtliche Dateien, die von Nutzern auf diesen Seiten gespeichert werden, auf etwaige Rechtverletzungen hin untersuchen bzw. filtern und Inhalte, die als unzulässig eingestuft werden, anschließend löschen.

223 Einer entsprechenden Forderung ist der EuGH jedoch in seinem Urteil vom 16.2.2012 **(SABAM/Netlog)**[384] entgegengetreten: ein solches Überwachungs- und Filtersystem durch die Betreiber eines sozialen Netzwerks verstoße sowohl gegen

---

[380] BVerfG, NJW 2010, 833.
[381] EuGH, Rs. C-293/12, C-594/12, 8.4.2014.
[382] Vgl. Dreier, in: Dreier/Schulze, UrhG, § 101 UrhG, Rn. 37.
[383] Vgl. Meier, MschrKrim 2012, 184 (196 f.).
[384] Vgl. EuGH – Rs. C-360/10 (SABAM-Netlog), 16.2.2010 (keine Pflicht für Betreiber sozialer Netzwerke zu umfassenden Überwachungs-und Filtersystemen, GRUR 2012, 382.

die Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr als auch gegen die Richtlinie 2001/28/EG zum Urheberrecht und die Durchsetzungsrichtlinie 2004/48/EG.

224 Als eine Maßnahme für einen besseren Urheberrechtsschutz wird die Einführung einer sog. **Internetsperre** erwogen, wobei zwischen einer Zugangs- und einer Inhaltssperre zu differenzieren ist.[385] Solche Sperren begegnen jedoch in Anbetracht grundrechtlicher Aspekte (u. a. Meinungsfreiheit, Berufsfreiheit) Bedenken.

225 Das Gegenteil möchte die sog. **Kulturflatrate** (auch als Internetabgabe, Flatratemodell oder Kulturwertmarke bezeichnet[386]) erreichen. Ihr Ziel ist es nicht, etwaige Seiten oder Inhalte zu sperren; sie möchte zu privaten Zwecken begangene Urheberrechtsverletzungen legalisieren und „sozialisieren", indem jeder Internetnutzer für die oben aufgezeigten Verstöße einen gewissen Betrag zahlt und diese somit kompensiert. Auch im Bundestags-Wahlkampf 2013 wurde die Möglichkeit einer Kulturabgabe, die etwa direkt vom Internet Service Provider erhoben und auf den monatlichen Anschlusspreis für den Internetzugang aufgeschlagen wird, parteiübergreifend diskutiert. Man erhofft sich von ihr, im Wege einer „second-best"-Lösung[387], anstelle der derzeit faktisch weit verbreiteten unentgeltlichen Onlinenutzung von urheberrechtlich geschützten Inhalten tatsächliche Vergütungsströme (wenn auch nicht in der Höhe einer möglichen individuellen Lizenzierung) zugunsten der Rechteinhaber zu erzeugen. Bedenken werden noch hinsichtlich der Vereinbarkeit einer solchen Kulturflatrate mit der Schrankenbestimmung des Art. 5 Abs. 2 der Informationsrichtlinie 2001/29/EG geäußert; diese dürften angesichts der neueren Rechtsprechung des EuGH und der neu formulierten Schrankenregelung in Art. 6 RL 2012/28/EU der Einführung einer Kulturflatrate im Ergebnis aber nicht entgegenstehen.[388]

226 Auch die Aufnahme eines „**fair use**"**-Rechts** (Recht auf angemessene Verwendung) nach angloamerikanischem Vorbild in das deutsche Urheberrecht wird diskutiert. Dieses würde es den Nutzern eines sozialen Netzwerks gestatten, legal eigene Bearbeitungen (etwa Remixes, Mash-Ups und Collagen) von urheberrechtlich geschützten Werken auf Plattformen zu teilen: derartige Nutzeraktivitäten werden von Künstlern und Rechteinhabern heute schon oftmals gebilligt, stärken sie doch reflexartig die Bekanntheit der Originalwerke. Ob die Einführung einer expliziten „fair use"-Regelung im deutschen Recht überhaupt erforderlich ist oder ob nicht vielmehr die bereits bestehenden Schrankenregelungen (im konkreten Fall etwa das Recht auf freie Benutzung, § 24 UrhG) genügen, ist umstritten.[389] Bisweilen wird angenommen, dass durch die Einführung eines „fair use"-Rechts nach amerikanischem

---

[385] Vgl. Paal/Hennemann, MMR 2012, 289.
[386] Vgl. Peifer, ZUM 2014, 86 (88).
[387] Peifer, ZUM 2014, 86 (89).
[388] Vgl. Peifer, ZUM 2014, 86 (89) unter Hinweis auf EuGH, NJW 2013, 2653 (VG Wort ./. Kyocera u. a.).
[389] Vgl. insgesamt zum *fair use*: Peifer, ZUM 2014, 86 (89 f.); zu einer Gegenüberstellung des amerikanischen und (angedachten) europäischen *fair use* anlässlich der Google Books Entscheidung des US-amerikanischen Supreme Court ebenfalls Peifer, GRUR-Prax 2013, 529.

Vorbild auch eine unangemessene Pönalisierung von Urheberrechtsverletzungen im Bagatellbereich (etwa durch die Verwendung von Vorschaubildern auf Facebook, hierzu Rn. 208) vermieden werden kann.[390]

7.5.12 Markenrechtliche Verstöße (§ 143 MarkenG)

227 Durch Produktverkäufe und entsprechende Ankündigungen bzw. Werbung über soziale Netzwerke drohen auch marken(straf)rechtlich relevante Rechtsverstöße. Kernmaterie des Markenstrafrechts ist § 143 MarkenG – ein **Allgemeindelikt**, bei dem die zur Vermeidung einer Überkriminalisierung gebotene Eingrenzung des tauglichen Täterkreises erst über das Erfordernis eines Handelns „im geschäftlichen Verkehr" (Rn. 233) erfolgt. Nicht als Täter kommen von vornherein der Markeninhaber, der Lizenznehmer in den Grenzen des § 30 Abs. 2 MarkenG und private Endabnehmer in Betracht.[391] Der Versuch ist strafbar (§ 143 Abs. 3 MarkenG i. V. m. §§ 12 Abs. 2, 23 Abs. 1 Alt. 2 StGB).

228 Vom strafrechtlichen Schutz des § 143 MarkenG erfasst werden nur (deutsche) **Marken** und **geschäftliche Bezeichnungen** (§ 1 Nr. 1, Nr. 2 MarkenG). § 143 MarkenG gilt auch für IR-Marken, die bei der WIPO[392] in Genf für einen Schutz (u. a.) in Deutschland eingetragen sind (vgl. §§ 107–125 MarkenG). (Europäische) Gemeinschaftsmarken[393] (§§ 125a ff. MarkenG) werden strafrechtlich dagegen nur von § 143a MarkenG geschützt.

229 Die Grundtatbestände des § 143 MarkenG verweisen auf § 14 MarkenG, der seinerseits einen wirksamen Markenschutz voraussetzt (vgl. Absatz 1; § 4 MarkenG). Die strafbare Verletzungshandlung gem. § 143 Abs. 1 Nr. 1 i. V. m. § 14 Abs. 2 Nr. 1 MarkenG liegt in der Benutzung eines mit der Marke identischen Zeichens für Waren oder Dienstleistungen **(Identitätsschutz)**. Ob eine solche Doppelidentität vorliegt, wird durch einen (restriktiven) Zeichen- und ggf. anschließenden Produktvergleich ermittelt.

230 § 143 Abs. 1 Nr. 1 i. V. m. § 14 Abs. 2 Nr. 2 MarkenG untersagt die Verwendung eines Zeichens, für das die Gefahr einer Verwechslung mit der Marke besteht **(Verwechslungsschutz)**. Geschützt wird neben der Identität auch die Ähnlichkeit der Marke.[394] Die Gefahr, dass ein Zeichen gedanklich mit einer Marke in Verbindung gebracht wird, besteht in sozialen Netzwerken vor allem bei der (meist gedankenlosen) Verwendung von Marken-Logos zu eigenen Zwecken, etwa bei Festivitäten, Einladungen oder Verkäufen.

231 Die Strafbarkeit gem. § 143 Abs. 1 Nr. 2 i. V. m. § 14 Abs. 2 Nr. 3 MarkenG knüpft an die Benutzung eines mit der Marke identischen Zeichens oder eines ähnlichen

---

[390] Kreutzer, http://www.zeit.de/digital/internet/2013-01/facebook-thumbnails/seite-2.
[391] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 143 MarkenG, Rn. 35, 40.
[392] World Intellectual Property Organization.
[393] Sog. Community Trademark (CTM).
[394] Zu den speziellen Fragen der unmittelbaren und mittelbaren Verwechslungsgefahr.

Zeichens für Waren oder Dienstleistungen, die denen nicht ähnlich sind, für die die Marke Schutz genießt. Geschützt werden soll also vor einer **Ähnlichkeit des verwendeten Zeichens ohne Verwechslungsgefahr** („Verwässerung", Nutzung für branchenfremdes Gebiet; Imagetransfer; inkompatibler Zweitgebrauch).

232 Allgemein kommt als Tathandlung nur ein (verletzender) **markenmäßiger Gebrauch** des Zeichens usw. in Betracht (vgl. § 14 Abs. 3 MarkenG); eine Verwendung einer rein beschreibenden Angabe reicht insoweit nicht.[395]

233 Ein wesentlicher Unterschied zum Urheberstrafrecht (vgl. § 106 UrhG) besteht im Markenstrafrecht darin, dass die Tathandlung zur Verwirklichung der verschiedenen Grundtatbestände des § 143 Abs. 1 MarkenG **im geschäftlichen Verkehr** erfolgen muss, was nur bei einer (selbstständigen) wirtschaftlichen Betätigung vorliegt, durch die eine Teilnahme am Erwerbsleben zum Ausdruck gebracht wird und die der Förderung des eigenen oder eines fremden Geschäftszwecks zu dienen bestimmt ist.[396] Mit dem Kriterium des geschäftlichen Verkehrs sollen vor allem rein private Handlungen vom strafrechtlichen Schutz des Markenrechts ausgeklammert werden. Die Abgrenzung erfolgt anhand einer wertenden Gesamtschau aller relevanten Umstände (Umfang/Regelmäßig-/Häufigkeit).[397]

234 Nicht zu verwechseln ist das Handeln im geschäftlichen Verkehr mit dem höheren Schweregrad eines **gewerblichen Handeln** (vgl. hierzu den Qualifikationstatbestand, § 143 Abs. 2 MarkenG). Gewinnerzielungsabsicht ist im geschäftlichen Verkehr gerade nicht erforderlich.

235 Das Tatbestandsmerkmal der **Widerrechtlichkeit** liegt nicht vor, wenn der Rechteinhaber der Benutzung (vertraglich) zustimmt, eine Schutzschranke der §§ 20–24 MarkenG einschlägig ist[398] bzw. wenn die Marke mangels Benutzung (§§ 25, 26 MarkenG) oder aus anderen Gründen (vgl. z. B. §§ 49 Abs. 2, 50 MarkenG) löschungsreif ist.[399]

236 Der jeweilige Tatbestand ist nur bei **vorsätzlichem Handeln** erfüllt (§ 15 StGB).[400] Im Rahmen des § 143 Abs. 1 Nr. 2 MarkenG muss die Benutzung zusätzlich in der Absicht erfolgen, die Unterscheidungskraft oder die Wertschätzung einer bekannten Marke auszunutzen oder zu beeinträchtigen.[401] § 143 Abs. 1 Nr. 3

---

[395] Vgl. Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 14 MarkenG Rn. 19 ff.

[396] Vgl. EuGH, GRUR 2003, 55 (57), Tz. 40 – Arsenal Football Club; BGH, GRUR, 2004, 860 (863) – Internet-Versteigerung; Hacker, in: Ströbele/Hacker, MarkenG, § 143 Rn. 19; Maske-Reiche, in: MüKo-StGB, § 143 MarkenG Rn. 73.

[397] Zum Verkauf von Waren auf einer Internetplattform siehe BGH, GRUR 2009, 871 – Ohrclips; OLG Frankfurt, GRUR 2004, 1042 (Ebay); BayObLGSt 2002, 9 (Trainingsanzüge).

[398] Siehe hierzu: LG Meiningen, NStZ 2003, 41; betreffend § 24 Abs. 2 MarkenG: BGH, GRUR 2012, 392 (Microsoft – Echtheitszertifikat). Zu beachten ist, dass markenrechtliche und urheberrechtliche Erschöpfung mitunter unterschiedlich verlaufen (vgl. § 17 Abs. 2 UrhG).

[399] Kaiser, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 143 MarkenG Rn. 17 ff.

[400] Fezer, MarkenR, § 143 Rn. 26.

[401] Je größer der Bekanntheitsgrad einer Marke, desto eher gehen die Gerichte vom Vorliegen der geforderten Absicht aus: KG, NStZ-RR 2012, 378.

lit. b MarkenG fordert, dass die entsprechende Handlung in der Absicht vorgenommen wird, die Ausnutzung oder Beeinträchtigung der Unterscheidungskraft oder der Wertschätzung einer bekannten Marke zu ermöglichen.

237 Zur Strafverfolgung ist gemäß §§ 143 Abs. 1, 4 MarkenG i. V. m. § 158 Abs. 2 StPO grundsätzlich ein Strafantrag (§§ 77 ff. StGB) erforderlich, sofern nicht ein besonderes öffentliches Interesse an der Strafverfolgung besteht (vgl. Nr. 261a RiStBV). Die Verfolgung einer Tat nach § 143 Abs. 2 MarkenG erfolgt dagegen als **Offizialdelikt** von Amts wegen.[402]

7.5.13 Ausspähen und Abfangen von Daten (§§ 202a, 202b StGB)

238 Den Tatbestand des Ausspähens von Daten (§ 202a StGB) erfüllt, wer sich oder einem anderen unter **Überwindung einer Zugangssicherung** unbefugt zu Daten Zugang verschafft, die nicht für ihn bestimmt sind und gegen unberechtigten Zugang besonders gesichert sind. Nach § 202b StGB macht sich derjenige strafbar, der sich unbefugt Daten, die nicht für ihn bestimmt sind, **aus einem nichtöffentlichen Datenübermittlungsvorgang** oder einer **elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage** verschafft.

239 Im Bereich der sozialen Netzwerke könnten die **Zugangsdaten der Benutzer** Gegenstand von Straftaten nach §§ 202a, 202b StGB sein. Ohne Weiteres sind von § 202a StGB etwa die Fälle erfasst, in denen sich der Täter unbefugt Zugang zum zentralen Datenverarbeitungssystem des sozialen Netzwerks verschafft, um dort
240 auf die Nutzerdaten zugreifen zu können. Auch „subtilere" Methoden des Zugang-Verschaffens können unter §§ 202a, 202b StGB zu subsumieren sein. Wer etwa in einem Chat im Rahmen eines sozialen Netzwerkes seinen Gesprächspartner durch Täuschung erfolgreich auffordert, ihm seine Zugangsdaten mitzuteilen, verschafft sich – ungeachtet der Frage der Sicherung der Daten und ob diese für den Täter bestimmt sind – unbefugt Zugang zu Daten, da die täuschungsbedingte Einwilligung des Berechtigten in der Regel unbeachtlich ist.[403]

241 Hingegen lassen sich unter den Tatbestand des § 202a StGB nicht die Fälle subsumieren, in denen der Täter von einem vertraglich dazu nicht berechtigten Dritten Zugangsdaten anderer Nutzer zu sozialen Netzwerken erhält, da er sich die Daten nicht unter Überwindung der Zugangssicherung verschafft. Die hier bestehende Strafbarkeitslücke will der Gesetzgeber durch den neu zu schaffenden Straftatbestand der Datenhehlerei schließen (Rn. 243 ff.).

242 In einem Gesetzentwurf des Bundesrates,[404] der aufgrund des Endes der 17. Legislaturperiode nicht mehr vom Deutschen Bundestag beschlossen werden konnte,

---

[402] Hacker, in: Ströbele/Hacker, MarkenG, § 143 Rn. 24.

[403] Bosch, in: SSW-StGB, § 202a Rn. 9; Weidemann, in: BeckOK-StGB, § 202a Rn. 18; a. A. Fischer, StGB, § 202a Rn. 12, wonach das Merkmal „unbefugt" nur erfüllt sein soll, wenn der Berechtigte annimmt, die anfragende Stelle sei zur Abfrage berechtigt.

[404] BR-Drs. 284/13 (B) v. 7.6.2013; siehe auch: BT-Drs. 17/14362 v. 10.7.2013.

sollten §§ 202a, 202b StGB jeweils zwei Qualifikationstatbestände für ein Handeln mit **Bereicherungs- oder Schädigungsabsicht** sowie für ein **gewerbs- und bandenmäßiges Handeln** angefügt werden. Die Strafandrohung sollte für ein Handeln mit Bereicherungs- oder Schädigungsabsicht auf Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren, für gewerbs- oder bandenmäßiges Handeln auf Freiheitsstrafe von sechs Monaten bis zehn Jahren lauten. Damit würden die Strafandrohungen der einfachen Datenhehlerei bzw. der gewerbs- und bandenmäßigen Datenhehlerei angeglichen. Weiterhin sollte die Strafbarkeit des Versuchs bei §§ 202a, 202b StGB angeordnet werden. Auf Antrag des Bundeslandes Hessen[405] hat der Bundesrat am 14.3.2014 beschlossen, den Gesetzesentwurf erneut beim Bundestag einzubringen.[406]

7.5.14 Vorschlag für einen Straftatbestand der Datenhehlerei

Der Ausgangpunkt um die Debatte zur Einführung eines Straftatbestandes der Datenhehlerei war der Erwerb sog. „Steuer-CDs" einzelner Bundesländer zur Verfolgung mutmaßlicher Steuersünder. Auf diesen CDs waren die Kontodaten deutscher Staatsbürger bei ausländischen Banken gespeichert. Ziel des „Ankaufs" solcher CDs war es, Steuerhinterziehung aufzudecken und zu bekämpfen. Die derzeitige Gesetzeslage, welche die strafrechtliche Beurteilung des Ankaufs von illegal erlangten Daten durch Amtsträger betrifft, ist bisher jedoch nicht eindeutig.[407] Über diese spezielle Thematik hinaus ist die Weitergabe von (illegal erworbenen) Daten bisher nur teilweise von Strafnormen des StGB erfasst. **243**

Das hessische Justizministerium hatte bereits im März 2012 die Einführung des neuen Straftatbestandes der **Datenhehlerei** (§ 259a StGB) vorgeschlagen, der sich allgemein und über die Steuer-CD-Debatte hinaus mit der strafrechtlichen Relevanz des illegalen Erwerbs und „Handelns" mit Daten bis hin zum Identitätsdiebstahl beschäftigte. Die Frühjahrskonferenz der Justizminister nahm diesen Vorstoß positiv auf.[408] Eine weitere Diskussion fand anlässlich des 69. DJT im September 2012 statt.[409] Ein anschließender Beschluss auf der Herbstkonferenz der Landesjustizminister am 15.11.2012 hatte die Chance auf Einführung des Straftatbestandes der Datenhehlerei in das StGB erhöht.[410] **244**

---

[405] BR-Drs. 70/13 v. 21.2.2014.
[406] BR-Drs. 70/13 (B) v. 14.3.3014.
[407] Näher: Klengel, ZRP 2013, 16; Kühne, GA 157 (2010), 275.
[408] 83. Konferenz der Justizministerinnen und -minister, Juni 2012, TOP II.2 (http://www.justiz.nrw.de/WebPortal/JM/justizpolitik/jumiko/beschluesse/2012/fruehjahrskonferenz12/index.php).
[409] Beschlüsse des 69. DJT, http://www.djt.de/fileadmin/downloads/69/120921_djt_69_beschluesse_web_rz.pdf.).
[410] http://www.justiz.nrw.de/JM/justizpolitik/jumiko/beschluesse/2012/herbstkonferenz12/II_9.pdf.

245 Der erste Gesetzentwurf des hessischen Justizministeriums wurde auch auf den Webseiten des IT-Portals „Netzpolitik“ veröffentlicht.[411] Im Problemdiskurs wurde betont, dass der Handel mit rechtswidrig erlangten **digitalen Identitäten** aufgrund der fortschreitenden Entwicklung des informationstechnischen Sektors kontinuierlich zunehme.[412] Solche Identitäten umfassten nicht nur Zugangsdaten zu Online-Banking-Plattformen oder Kreditkarteninformationen, sondern auch Passwörter zu sozialen Netzwerken oder E-Mail-Accounts. Mittels Schadsoftware oder ähnlichen Methoden sei es Tätern möglich, Zugang und Einsicht in derartige Bereiche zu nehmen. Dabei komme es häufig nicht nur zu unmittelbaren Vermögensverfügungen mit den Daten, sondern zunehmend auch zum Handel über Webportale und Foren. Durch den neuen Straftatbestand sollten bestehende Strafbarkeitslücken geschlossen werden im Hinblick auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

246 Nach dem **Entwurf des § 259a Abs. 1 StGB** soll mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, „wer Passwörter oder sonstige Sicherungscodes, welche den Zugang zu Daten ermöglichen und die ein anderer ausgespäht oder sonst durch eine rechtswidrige Tat erlangt hat, ankauft oder sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.“

247 Speziell im Kontext sozialer Netzwerke macht sich bei Einführung dieses Tatbestandes strafbar, wer **Zugangspasswörter**, die rechtswidrig erlangt oder ausgespäht wurden, ankauft, einem Dritten verschafft oder solche absetzt. Zu beachten ist, dass in subjektiver Hinsicht entweder eine Bereicherungs- oder Schädigungsabsicht vorliegen muss. Unklar bleibt jedoch, was unter einer Schädigung zu verstehen ist, konkret, ob darunter auch das Finden und Veröffentlichen von Sicherheitslücken fällt. Beachtlich ist, dass der Hehler mit bis zu fünf Jahren Freiheitsstrafe strenger bestraft werden soll, als derjenige, der die Daten nach § 202a StGB ausspäht (bis zu drei Jahre).

248 Nach Absatz 2 soll bestraft werden, wer Daten (§ 202a Abs. 2 StGB), die ein anderer ausgespäht oder sonst durch eine rechtswidrige Tat erlangt hat und welche von dem letzten befugten Inhaber durch Passwörter oder sonstige Sicherungscodes gesichert worden waren, ankauft oder sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Absatz 3 spricht den §§ 247, 260, 260a StGB sinngemäße Geltung zu; Absatz 4 normiert eine Versuchsstrafbarkeit.

249 Der hessische Entwurf stellt jedoch den **Erwerb von Daten, der ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dient**, nach Absatz 5 nicht unter Strafe. Damit wäre der staatliche Informationsankauf („Steuer-CD“) vom Tatbestand des § 259a StGB ausgenommen.

---

[411] https://netzpolitik.org/wp-upload/Gesetzentwurf-Datenhehlerei.pdf; kritisch Gercke, ZUM 2013, 605.

[412] Gercke, ZUM 2013, 605 (606) verweist darauf, dass die Thematik „Identitätsdiebstahl“ im Lösungsvorschlag leider völlig ausgeklammert worden ist.

Die Gesetzesbegründung verweist darauf, dass der Tatbestandsausschluss auch im Lichte der **Pressefreiheit** des Art. 5 Abs. 1 S. 2 GG auszulegen ist. So soll der Erwerb rechtswidrig erlangter Daten durch Medienmitarbeiter zum Zweck der Veröffentlichung als Erfüllung rechtmäßiger beruflicher Pflichten nicht strafbar sein, sofern er der verfassungsrechtlich geschützten Funktion der freien Presse dient.[413] Private Blogger sind damit nicht erfasst, da es sich hier nicht um eine berufliche Recherche handelt. **250**

Am 10.7.2013 hat der Bundesrat diesen Vorschlag als Entwurf eines Gesetzes zur **Strafbarkeit der Datenhehlerei** in den Deutschen Bundestag eingebracht.[414] Der Entwurf des Bundesrates enthält einige Änderungen des hessischen Entwurfs: Zum einen wird der Standort der neuen Norm ihrem systematischen Zusammenhang entsprechend nach den §§ 202a–202c StGB in § 202d StGB-neu gefunden. Zum anderen entfällt die im hessischen Entwurf vorgesehene Qualifikation für Datenhehlerei mit passwortgeschützten Daten. Stattdessen wird in § 202d Abs. 2 StGB-neu ein **eigener Datenbegriff** für die Datenhehlerei geschaffen, der nur solche Daten umfassen soll, „an deren Nichtweiterverwendung der Berechtigte ein schutzwürdiges Interesse hat und die nicht aus allgemein zugänglichen Quellen entnommen werden können." Eine solche Einschränkung ist dem Datenbegriff des § 202a Abs. 2 StGB fremd. Problematisch ist jedoch, dass § 202d StGB-neu wie auch § 259 StGB an eine rechtswidrige Vortat anknüpft, und damit Angriffe auf Daten durch sog. „Insider" mit der Berechtigung zum Datenzugriff nicht umfasst.[415] **251**

Der dem Grundsatz der Diskontinuität zum Opfer gefallende Gesetzesvorschlag ist von Hessen am 21.2.2014 erneut in den Bundesrat eingebracht worden[416] und von diesem am 14.3.2014 als Gesetzentwurf beschlossen worden.[417] **252**

7.5.15 Straftaten nach dem Versammlungsgesetz

Dass soziale Netzwerke von jüngeren Menschen auch und gerade genutzt werden, kann nicht überraschen. **253**

7.5.15.1 „Facebook-Partys"

Eine jüngere Erscheinungsform der Nutzung sozialer Netzwerke für spontane Verabredungen stellen sog. „Facebook-Partys" dar. Diese Treffen werden über Facebook oder andere soziale Plattformen im wechselseitigen Austausch organisiert und beworben. Charakteristisch sind dabei die Spontanität und die Unkontrollierbarkeit des **254**

---

[413] https://netzpolitik.org/wp-upload/Gesetzentwurf-Datenhehlerei.pdf, S. 15.
[414] BT-Drs. 17/14362 v. 10.7.2013.
[415] Gercke, ZUM 2013, 605 (608).
[416] BR-Drs. 70/14.
[417] BR-Drs. 70/14 (Beschluss).

Aufrufs, vor allem aber das nicht abschätzbare Ausmaß (Dauer, Anzahl der Beteiligten) der späteren Veranstaltung. Die Ursachen hierfür liegen in der Funktion sozialer Netzwerke; diese ermöglichen eine unkomplizierte Erstellung und Verbreitung von Terminen und Örtlichkeiten.

255 Solche „Partys" können mitunter erhebliche Kosten und Schäden verursachen, sei es durch Müllbeseitigung oder Beschädigungen an öffentlichen oder privaten Gegenständen. Den Ordnungsbehörden fällt es angesichts der beschriebenen Spezifika solcher Veranstaltungen oftmals schwer, eine verlässliche Gefahrenprognose abzugeben und entsprechende präventive Maßnahmen im Vorfeld zu ergreifen.

256 Bei Veranstaltungen mit einem von vornherein **begrenztem Personenkreis**, die ausschließlich auf einem Privatgrundstück stattfinden und keine öffentlichen Interessen berühren, scheidet ein ordnungsrechtliches Einschreiten von vornherein aus. Anders stellt sich die Situation allerdings dar, wenn die Einladung zu einem Treffen (mit Absicht oder unbedacht) an einen unbegrenzten Personenkreis gerichtet ist und sich das Geschehen in die öffentliche Sphäre erstreckt. Aufgrund der sich abzeichnenden polizeirechtlich relevanten Gefahrenlage ist ein Einschreiten der Ordnungsbehörden dann meist geboten.

257 Strafrechtlich relevant können solche „Facebook-Partys" über die Tatbestände des Versammlungsgesetzes (§§ 21 ff. VersG) werden – vorausgesetzt, dass eine solche Veranstaltung vom **Anwendungsbereich des VersG** erfasst ist. Eine Versammlung ist eine Personenmehrheit, die durch einen gemeinsamen Zweck oder Willen innerlich verbunden ist.[418] Die gemeinsame Zweckverfolgung unterscheidet eine Versammlung von einer bloßen Ansammlung. Bei einer Ansammlung aus einem äußeren Anlass heraus wird die individuelle, wenn auch u. U. gleichgerichtete Zweckverfolgung noch nicht zu einem gemeinsamen Anliegen.[419] Das BVerfG geht von einem **engen Versammlungsbegriff** aus und verlangt eine örtliche Zusammenkunft mehrerer Personen zur gemeinschaftlichen, auf die Teilhabe an der öffentlichen Meinungsbildung gerichteten Erörterung oder Kundgebung.[420]

258 Bei sog. „Facebook-Partys" steht regelmäßig der **Spaß- und Freizeitcharakter** im Vordergrund.[421] Solche Ansammlungen haben weder einen politischen noch einen gesellschaftlichen Zusammenhang. Es fehlt meist an einer zielgerichteten gemeinsamen Meinungskundgabe (ähnlich wie bei der Loveparade[422]). Eine Facebook-Party fällt damit nicht unter eine Versammlung[423], so dass die §§ 21 ff. VersG keine Anwendung finden. Im konkreten Fall können allerdings herkömmliche Straftatbestände (§§ 123, 303 StGB) verwirklicht sein. Auch eine Strafbarkeit nach § 231 Abs. 1 StGB

---

[418] Depenheuer, in: Maunz/Dürig, GG, Art. 8 Rn. 44.
[419] Vgl. Depenheuer in: Maunz/Dürig, GG, Art. 8 Rn. 46.
[420] BVerfGE 104, 92 (104); BVerfG, NVwZ 2005, 80.
[421] Dies zeigt etwa der wohl bekannteste Fall der seinerzeit 15-jährigen T. aus Hamburg. T. lud über Facebook unbemerkt öffentlich zu ihrer Geburtstagsfeier ein, worauf 1.600 Gäste erschienen. Http://www.stern.de/digital/online/facebook-fans-stuermen-geburtstagsparty-im-vorgarten-von-thessa-1692209.html.
[422] BVerfG, NJW 2001, 2459.
[423] Im Ergebnis auch Levin/Schwarz, DVBl. 2012, 10 (11).

(Beteiligung an einer Schlägerei) scheint vorstellbar, wenn eine Person einer über ein soziales Netzwerk ausgesprochenen Einladung zu einer Schlägerei folgt, sich an ihr im tatbestandlich geforderten Umfang beteiligt und es im Zuge dessen zum Tod eines Menschen oder einer schweren Körperverletzung (§ 226 StGB) kommt.

Auf solch drohende Auswüchse können und (je nach Dichte der Informationen und absehbaren Folgen) müssen Ordnungsbehörden ggf. auf der Grundlage der **polizeirechtlichen Generalklauseln** im Landesrecht (soweit keine speziellen Eingriffsermächtigungen bestehen) im Vorfeld reagieren, wenn Anhaltspunkte für eine Gefahr für die öffentliche Sicherheit und Ordnung bestehen.[424] Für etwaige Schäden können zivilrechtliche Ausgleichsansprüche entstehen. **259**

7.5.15.2 „Flashmobs“

Der Begriff Flashmob (flash = Blitz; mob von mobilis beweglich = aufgewiegelte Volksmenge, Pöbel) bezeichnet eine (im Vorfeld abgestimmte, aber im Kern spontane) Zusammenkunft (Auflauf) einer größeren Zahl von Personen, die sich im Regelfall vorher nicht untereinander kennen.[425] Aufgrund der Vielgestaltigkeit der denkbaren Erscheinungsformen lässt sich allerdings keine allgemeinverbindliche Definition finden.[426] Der Bezug zu den sozialen Netzwerken besteht darin, dass derartige Aktionen häufig über solche Netzwerke initiiert und nicht selten auch im späteren Verlauf koordiniert werden.[427] **260**

Flashmobs sind meist nur Ausdruck einer spontanen Bewegung oder eines Lebensgefühls[428] und können daher **nicht dem engen Versammlungsbegriff des Art. 8 GG** unterfallen (Rn. 257).[429] Das wäre auch bei Flashmobs erst dann der Fall, wenn die eingesetzten kommunikativen Mittel einem höheren Zeck, der Meinungskundgabe, dienen sollen oder können.[430] Zumindest aber erscheint es erwägenswert, den Flashmob von einem weiter gefassten Begriff der Versammlung zu erfassen,[431] **261**

---

[424] Hierzu, zu Maßnahmen während der Veranstaltung und zur Kostenlast ausführlich: Levin/Schwarz, DVBl. 2012, 10 (11 ff.).

[425] Zur teilweise unterschiedlichen Begriffsabgrenzung und weiteren Definitionsversuchen Neumann, NVwZ 2011, 1171 (1172); Ernst, DÖV 2011, 537 f.; Stalberg, KommJur 2013, 169.

[426] Ernst, DÖV 2011, 537 (545).

[427] Höfling/Krohne, JA 2012, 734 (736).

[428] Neumann, NVwZ 2011, 1171 (1173); Stalberg, KommJur 2013, 169 (173); differenzierter Ernst, DÖV 2011, 537 (538), der alle denkbaren Bereiche des täglichen Lebens als Anlass für einen Flashmob verstanden haben will.

[429] Vgl. Neumann, NVwZ 2011, 1171 (1173); ebenso Ernst, DÖV 2011, 537 (539); Stalberg, KommJur 2013, 169 (171); Höfling/Krohnen, JA 2012, 734 (737).

[430] BVerfG, NJW 2001, 2459 (2460 f.).

[431] So Neumann, NVwZ 2011, 1171 (1173 m. w. N.); i. E. ablehnend Ernst, DÖV 2011, 537 (539).

zumal auch bei „smart mobs“,[432] die ausdrücklich politisch motiviert sind, der Versammlungscharakter bejaht wird.[433]

262 Handelt es sich bei dem Flashmob um ein Happening oder eine Tanzchoreographie, ist zudem der Schutzbereich der **Kunstfreiheit**, Art. 5 Abs. 3 GG, eröffnet.[434]

263 Auch als **Mittel des Arbeitskampfes** findet der Flashmob zunehmend Verwendung.[435] Einschlägig sind dabei Fälle, in denen Mitarbeiter bzw. Gewerkschaftsmitglieder großer Einkaufshäuser oder Supermarktketten – neben oder zur Unterstützung eines Streiks – mit „Pfennigartikeln“ angereicherte Einkaufswagen bzw. -tüten erst befüllten und dann in den Gängen stehen ließen. Das Ergebnis waren lange Schlangen vor den Kassen und ein enormer personeller Aufwand zur Beseitigung des entstandenen Chaos.[436] Diese Mittel des Arbeitskampfes sind mit den traditionellen Methoden wie dem Streik oder der Aussperrung kaum noch vergleichbar.

264 In der gezielten Sabotage der Betriebsabläufe sieht das **BAG**[437] einen rechtfertigungsbedürftigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb des Arbeitgebers (§ 823 Abs. 1 BGB).[438] Ob ein solcher Eingriff als widerrechtlich zu bewerten ist, sei Anhand einer Interessenabwägung zu beurteilen. Die Teilnehmer des Flashmobs können sich möglicherweise auf Art. 9 Abs. 3 GG (Koalitionsfreiheit) berufen; mithin läge eine mittelbare Grundrechtskollision vor.[439] Das BAG geht davon aus, dass die den Gewerkschaften zustehenden Arbeitskampfmittel nicht nur auf die tradierten Streikmaßnahmen limitiert sind. Eine andere Wertung grenzte den Schutz durch Art. 9 Abs. 3 GG unzulässig auf die geschichtlich überlieferten Rechte i. S. e. numerus clausus ein.[440]

---

[432] Zum Begriff Neumann, NVwZ 2011, 1171 (1172); Ernst, DÖV 2011, 537 f.; Stalberg, KommJur 2013, 169; Höfling/Krohne, JA 2012, 734 (736).

[433] So Neumann, NVwZ 2011, 1171 (1173); Höfling/Krohnen, JA 2012, 734 (737); a. A. Dietel et al., VersG, 16. Aufl. (2011), § 1 Rn. 54; Ernst, DÖV 2011, 537 (539).

[434] Neumann, NVwZ 2011, 1171 (1174); a. A. Ernst, DÖV 2011, 537 (539 f.), der ihn nicht per se unter den Schutz des Art. 5 Abs. 3 GG fassen möchte; kritisch auch Stalberg, KommJur 2013, 169 (171 f.), der für den Einzelfall unterscheiden möchte, gleichzeitig aber auch dazu tendiert, den Schutzbereich der Meinungsfreiheit Art. 5 Abs. 1 GG zu eröffnen.

[435] Ernst, DÖV 2011, 537 m. w. N.

[436] Vgl. instruktiv zu diesen Fällen: Neumann, NVwZ 2011, 1171 (1177); Ernst, DÖV 2011, 537 (540).

[437] BAG, NJW 2010, 631 = NZA 2009, 1347; hierzu auch: Baeck/Winzer, NZG 2010, 100.

[438] Vgl. hierzu Neumann, NVwZ 2011, 1171 (1177).

[439] BAG, NJW 2010, 631.

[440] BVerfGE 84, 212 (229 f.); BAG, NJW 2010, 631; Neumann, NVwZ 2011, 1171 (1177) nennt es status quo.

Das **BVerfG**[441] bestätigte, dass Art. 9 Abs. 3 GG nicht ausschließlich auf Streik und Aussperrung als Formen des Arbeitskampfes beschränkt sei. Die Arbeitskampfmaßnahme müsse unter dem Gesichtspunkt der Proportionalität geprüft werden (insbesondere in Bezug auf die Teilnahme Dritter) und eindeutig als gewerkschaftlich getragene Arbeitskampfmaßnahme identifizierbar sein.[442] Flashmobs als neuartiges Mittel des Arbeitskampfes seien damit nicht von vornherein unzulässig.[443] **265**

7.5.16 Manipulierte Bewertungen auf Vergleichsportalen

Sog. Vergleichsportale im Internet bieten eine Auflistung von Produkten, die zuvor bezüglich ihrer Qualität, ihres Preises, ihres Mehrwerts oder sonstiger Bezugsgrößen bewertet und gelistet wurden. Weit verbreitet sind Plattformen für den Strompreisvergleich[444], Versicherungstarife[445], Urlaube[446], Hotels[447], Elektrogeräte[448], KFZ[449], Lebensmittel[450] aber auch für Restaurants[451] und andere Dienstleister.[452] Die Mehrzahl dieser Portale bietet den Nutzern eine Kommunikationsebene, was ihnen den Charakter sozialer Netzwerke verleiht. Gleichzeitig bietet ein solches Vergleichsportal aber auch die Möglichkeit, Bewertungen zu manipulieren oder manipulieren zu lassen. **266**

7.5.16.1 Strafbarkeit des Portalbetreibers

Erhebt das Vergleichsportal den Anspruch auf Seriosität und Fachkompetenz, kann seine Produktlistung das Käuferverhalten nachhaltig beeinflussen. Insbesondere Fachzeitschriften veröffentlichen Prüfberichte, um ihre Leser auf hochwertige Produkte aufmerksam zu machen und vor unterdurchschnittlichen Angeboten zu **267**

---

[441] BVerfG, BeckRS 2014, 49789. Der vor dem BAG unterlegene Arbeitgeberverband hatte Verfassungsbeschwerde eingelegt, weil Flashmobs in der Form der oben genannten „Pfennig-Käufe" durch etwa 50–60 Personen in Filialen und Supermärkten für etwa eine Stunde die Kassen und den Betrieb lahmgelegt hatten.

[442] BVerfG (Fn. 441), § 30.

[443] BVerfG (Fn. 441), §§ 38 ff. Wirkungsvoller Rechtsschutz sei bei fehlender gesetzlicher Grundlage anhand der anerkannten Methoden der Auslegung und der Rechtsfindung zu gewährleisten. Für eine Überschreitung dieser Grenzen bestanden im konkreten Fall keine Anhaltspunkte.

[444] Z. B. www.verivox.de.

[445] Z. B. www.financescout24.de.

[446] Z. B. www.holidaycheck.de; www.expedia.de; www.travelscout24.de.

[447] Z. B. www.trivago.de; www.swoodoo.com.

[448] Z. B. www.idealo.de; www.spargeraete.de.

[449] Z. B. www.adac.de; www.auto-vergleich-online.de; www.autobild.de/tests/vergleichstests.

[450] Z. B. www.supermarktcheck.de; www.preisvergleich-lebensmittel.de.

[451] Z. B. www.restaurant-kritik.de; www.restaurant-ranglisten.de.

[452] Z. B. www.transparo.de.

warnen.[453] Strafrechtlich relevant (Betrug, § 263 StGB) wird eine solche Vorgehensweise dann, wenn die Listung bewusst unvollständig oder sogar falsch ist.[454] Dabei sind unterschiedliche Konstellationen zu unterscheiden:

268 Werden z. B. Haushaltsgeräte getestet, kann sich ein betrugsrelevantes Handeln sowohl daraus ergeben, dass ein Merkmal des Gerätes (Stromverbrauch) bewusst nicht korrekt angegeben wird oder dass die Reihenfolge der Produkte in der Ergebnisliste bewusst verändert wird, um einen bestimmten Hersteller zu exponieren. Gibt das hinter dem Vergleichsportal stehende Unternehmen vor, die Produkte vor der Listung selbst zu prüfen bzw. prüfen zu lassen und täuscht es dann entweder über bestimmte Eigenschaften oder über die tatsächlichen Ergebnisse, ist das Tatbestandsmerkmal des **Vorspiegelns falscher Tatsachen** erfüllt. Schwieriger wird die Beurteilung, wenn es um subjektive Empfindungen des Testers geht. So ist der Geschmackstest in einem Restaurant oder der Erholungswert eines Hotels in den meisten Fällen objektiv nicht nachprüfbar. In solchen Konstellationen liegt meist schon keine Täuschung über eine Tatsache vor. Ähnlich gelagert sind die Fälle, in denen das Portal keine Testergebnisse veröffentlicht, sondern lediglich Umfragen über Beliebtheitswerte oder ein bestimmtes Kaufverhalten publiziert.

269 Die vom Portalbetreiber vorgenommene Ergebnis- oder Reihungsmanipulation (Täuschung) führt auf Seiten eines Verbrauchers kausal zu einem entsprechenden Irrtum,[455] wenn durch die Manipulation von Testergebnissen oder Umfragewerten beim Betrachter Fehlvorstellungen über die tatsächlichen Eigenschaften der Produkte entstehen.

270 Allerdings müsste dieser Irrtum kausal zu einer Vermögensfügung eines Verbrauchers geführt haben, der in einem entsprechenden Vermögensschaden resultiert. Zumindest bei einer bewusst wahrheitswidrigen Behauptung einer angeblich schlechten Eigenschaft des geprüften Produktes oder manipulierter Umfragewerte mit Bewertungsskala kann von einer direkten Beeinflussung des Kundenverhaltens ausgegangen werden. Allerdings ist auf der Ebene des Schadens nicht immer eindeutig feststellbar, bei wem dieser nun tatsächlich eingetreten ist. Zu unterscheiden sind der Käufer/Konsument und der Anbieter des möglichweise verschmähten bzw. „übergangenen" Produktes.

271 Beim **Konsumenten** ist kein Schaden anzunehmen, wenn er ein Produkt erwirbt, das tatsächlich eine gegenüber seiner „Listung" höhere Qualität aufweist. Der Betrug pönalisiert lediglich Vermögensschäden, nicht jedoch Eingriffe in die Entschließungsfreiheit (Kaufverhalten).[456] Auf ein subjektives Schädigungsgefühl des Betroffenen kommt es hierbei nicht an.[457] Erwirbt der Verbraucher dagegen

---

[453] Unter anderem ADAC, AutoBILD, ComputerBILD, etc.

[454] So z. B. besonders prominent bei Verivox, http://www.handelsblatt.com/unternehmen/handel-dienstleister/manipulationsvorwuerfe-verivox-skandal-bringt-web-portale-in-verruf/4626330.html; ebenso beim ADAC, vgl. nur statt vieler www.spiegel.de/auto/aktuell/adac-skandal-keine-weiteren-manipulationen-beim-autopreis-a-955497.html.

[455] Hefendehl in: MüKo-StGB, § 263 Rn. 228.

[456] BGH, wistra 1986, 169; BGH, NStZ 1999, 555; Lackner/Kühl, StGB, § 263 Rn. 37.

[457] BGHSt 16, 321 (325).

ein wahrheitswidrig besser bewertetes Produkt, kann sich sein Schaden aus einem objektiv nachteiligen Preis/Leistungs-Verhältnis ergeben („Fehlkauf“).[458]

Ob auch ein Schaden beim **Anbieter des Produktes** vorliegt, bedarf einer eigenständigen Prüfung. Keine Schadensrelevanz hat hier offensichtlich der Fall, in dem ein schlechteres Produkt bewusst besser bewertet wurde, da der Hersteller hier gegenüber der Konkurrenz von einer etwaig gesteigerten Konsumentennachfrage profitiert. **272**

Wurde dagegen ein Produkt absichtlich an eine niedere Platzziffer gesetzt, sind weitere Aspekte zu bedenken. Zum einen sind getäuschte Person und geschädigte Person nicht identisch, da der Konsument regelmäßig, wie ausgeführt, beim Erwerb keinen Vermögenschaden erleidet. Ein Schaden für den Hersteller kann sich daher nur über die Figur des **Dreiecksbetruges** und allenfalls daraus ergeben, dass getäuschte Kunden das Produkt aufgrund der manipulierten Listung meiden. Eine nachweisbare Kausalität wird wohl nur bei direkter Abwertung des Angebots gegeben sein (s. o.). **273**

Zudem wären auf der subjektiven Ebene – neben einem stets erforderlichen Vorsatz des Portalbetreibers – Zweifel an dessen zusätzlich erforderlicher **Bereicherungsabsicht** angebracht. Der Portalbetreiber geht bei den beschriebenen Manipulationen regelmäßig „leer“ aus. Ebenso wird eine Drittbereicherungsabsicht zugunsten eines (bevorteilten) Bewerbers selten vorhanden bzw. nachweisbar sein. Ein oben skizzierter Schaden beim „übergangenen“ Hersteller wäre jedenfalls nicht stoffgleich, denn der Vermögensabfluss bei ihm durch das negative Konsumentenverhalten führt gerade nicht als unmittelbare Kehrseite zu einem (erstrebten) Zugewinn des Portalbetreibers[459] – selbst wenn er von dem bevorteilten Bewerber eine Zuwendung erhält. In dieser Konstellation scheidet eine Strafbarkeit des Portalbetreibers wegen Betrugs aus. **274**

7.5.16.2 Strafbarkeit des Produktherstellers

Neben dem Manipulieren durch den Portalbetreiber selbst sind auch Fälle bekannt, in denen ein Anbieter bewusst Bewertungen seines eigenen Produktes fälschen lässt, um das Ergebnis zu seinen Gunsten zu beeinflussen und so Kunden auf seine Produkte aufmerksam zu machen.[460] Hierbei wird sich oftmals **spezialisierter Agenturen** bedient, die fiktive, positive Bewertungen über das Produkt oder die Dienstleistung verfassen. Diese sind in Sprache und Ausgestaltung oftmals so konzipiert, dass ein potenzieller Kunde die Fälschung nicht erkennt und die Bewertung für die eines real existenten, zufriedenen Kunden hält. Das Portal selbst dient dabei nur als „gutgläubige Plattform“. **275**

Parallel zur Problematik des manipulierenden Portalbetreibers (Rn. 267 ff.) werden durch die gefälschten Bewertungen meist falsche Tatsachen vorgespiegelt, die **276**

---

[458] Siehe hierzu Lackner/Kühl, StGB, § 263 Rn. 38 f.

[459] Vertiefend zur Stoffgleichheit: Lackner/Kühl, § 263 Rn. 59 f.

[460] Vgl. hierzu den Bericht des ZDF-Magazins Wiso (http://www.zdf.de/WISO/gefaelschte-bewertung-in-internetportalen-und-im-online-shop-30955964.html).

beim Kunden zu einem betrugsrelevanten Irrtum führen. Verfügt dieser nun, angeregt durch die anderen, vermeintlich ebenso zufriedenen Kunden, über sein Vermögen und erhält er ein Produkt, das ein nachteiliges Preis-/Leistungsverhältnis aufweist, erleidet er einen Schaden.

277 Möglichweise entsteht durch die Manipulation aber auch den anderen, ebenso das Portal nutzenden Herstellern/Diensteanbietern ein Schaden. Dazu müsste aber die bewusste Entscheidung für das manipulierte Produkt und gegen das nicht manipulierte Produkt eines anderen Herstellers/Diensteanbieters nachweisbar sein. Dies wird regelmäßig nur dann gelingen, wenn es nicht allein bei einer gefälschten Besserbewertung bleibt, sondern zusätzlich auch Konkurrenzprodukte absichtlich schlechter bewertet werden (s. o.).

278 Selbst aber, wenn man einen Schaden bei der Konkurrenz durch das Nicht-Kaufen des nicht durch positive Bewertungen geschönten Produktes annimmt, scheitert eine Strafbarkeit wegen Betruges daran, dass der **Schaden der Konkurrenzanbieter nicht die Kehrseite der erstrebten Bereicherung** durch den manipulierenden Hersteller ist: dieser erhofft seine Bereicherung aus der Akquise neuer Kunden, nicht aus dem Vermögen der Konkurrenz. Eine Strafbarkeit wegen Betruges scheidet mithin auch hier aus.

279 Gleichwohl macht sich der Hersteller möglicherweise der **strafbaren Werbung** gemäß § 16 UWG strafbar (abstraktes Gefährdungsdelikt), der eine Schädigung wirtschaftlicher Art für Dritte (im Gegensatz zum Betrug, § 263 StGB) nicht verlangt.[461] Die geforderte Tathandlung – die irreführende Werbung durch unwahre Angaben – muss in einem bestimmten Medium erfolgen, mithin in öffentlichen Bekanntmachungen oder in Mitteilungen, die für einen größeren Kreis von Personen bestimmt sind.[462] Angaben sind dabei Äußerungen, die zumindest zum Teil dem Beweis zugängliche Tatsachenbehauptungen enthalten (in Abgrenzung zu reinen Meinungsäußerungen wie etwa marktschreierischen Anpreisungen,[463] Übertreibungen ohne konkreten Tatsachenkern,[464] nichtssagenden Kaufappellen[465]). Bewertungen auf Verkaufsportalen, die von fingierten Kunden abgegebene Produkteinschätzungen darstellen, sind aber für den Betrachter erkennbar rein subjektive Einschätzungen und Anpreisungen. Dass sie professionell hergestellt wurden, ändert nichts an ihrer bewussten Formulierung als persönliche Erfahrungen eines Konsumenten. Damit verstößt ein Hersteller, der Kundenbewertungen fälschen lässt, auch nicht gegen § 16 UWG.

---

[461] Janssen/Maluga, in: MüKo-StGB, § 16 UWG Rn. 18.
[462] Janssen/Maluga, in: MüKo-StGB, § 16 UWG Rn. 18.
[463] Zur engen Auslegung: OLG Düsseldorf, WRP 1971, 277.
[464] KG, WRP 1982, 220.
[465] BGHZ 43, 140 (143 f.).

7.5.17 Verantwortlichkeit nach dem Telemediengesetz (TMG)

Soweit soziale Netzwerke dem **Anwendungsbereich** des Telemediengesetzes (TMG) unterliegen,[466] besteht für den Betreiber respektive die Nutzer des Netzwerks die Gefahr, spezielle Tatbestände des Nebenstrafrechts zu verwirklichen. Durch das TMG vom 26.2.2007 wurde die E-Commerce Richtlinie (ECRL)[467] in nationales Recht umgesetzt. **Telemedien** sind elektronische Informations- und Kommunikationsdienste, die individuell nutzbar für kombinierbare Daten (Zeichen, Bilder, Töne) bestimmt sind, denen eine Telekommunikation als Übermittlungsmedium zugrunde liegt; umfasst werden damit die Individualkommunikation (Telebanking, Datenaustausch), Informations- und Kommunikationsangebote sowie die Internetnutzung im Allgemeinen.[468] Soziale Netzwerke im Internet sind damit Telemedien i. S. d. TMG. **280**

Räumlich ist das TMG innerhalb Deutschlands anwendbar. Erfasst werden sowohl niedergelassene Diensteanbieter (**Service Provider**), § 3 Abs. 1 TMG, als auch solche Teledienste, die in Deutschland geschäftsmäßig angeboten oder erbracht werden, § 3 Abs. 2 TMG.[469] Der Diensteanbieter bildet in der Systematik des TMG den Counterpart zum Nutzer nach § 2 Satz 1 Nr. 3 TMG.[470] Betreiber sozialer Netzwerke sind als Diensteanbieter i. S. d. TMG einzustufen.[471] **281**

Als solche verarbeiten sie diverse **Daten**, die unterschiedlichen Regelungen unterliegen: **Inhaltsdaten** (d. h. Informationen eines persönlichen Profils und die Inhalte der Kommunikation, eingestellte Fotos oder Beiträge) unterfallen entweder bereichsspezifischen Gesetzen oder den allgemeinen Regeln des BDSG oder des einschlägigen LDSG; **Bestands- und Nutzungsdaten** werden hingegen vom Anwendungsbereich des TMG erfasst (vgl. § 15 TMG). Bestandsdaten sind Angaben, die für die Begründung, Durchführung und Beendigung eines Nutzungsverhältnisses notwendig sind. Die vertragliche Ausgestaltung bestimmt den Rahmen individuell. Dazu zählen in der Regel identifizierende Nutzerangaben (Name, Anschrift, E-Mail), Zugangsdaten (Nutzername, ID, Kennwort) oder andere vertragsrelevante **282**

---

[466] Zum Anwendungsbereich des TMG siehe mit zahlreichen Beispielen: Müller-Broich, in: NK-TMG, § 1 Rn. 6 ff.; Holznagel/Ricke, in: Spindler/Schuster, § 1 TMG, Rn. 10 f.

[467] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG Nr. L 178 S. 1.

[468] Ausführlich hierzu Martiny, in: MüKo-BGB, § 3 TMG Rn. 8.

[469] Martiny, in: MüKo-BGB, § 3 TMG Rn. 7.

[470] Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 TMG Rn. 7 f.

[471] Buchner, in: BeckOK-BDSG, § 29 Rn. 36; vgl. auch die beispielhafte Aufzählung bei Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG Rn. 10 f.

Informationen (Tarife, Nutzungszeiten etc.).[472] Zu den Nutzungsdaten zählen Merkmale, die der Identifikation des Nutzers dienen (IP-Adresse, Browsertyp, Cookies, Nutzerkennung).[473]

283 **Nutzungsdaten** lassen sich kategorisieren als all diese Informationen, die bei der Interaktion zwischen Nutzer und Anbieter während und durch die Dienstenutzung zwingend entstehen. **Bestands- und Nutzungsdaten** sind nicht trennscharf zu unterscheiden, teilweise unterfallen bestimmte Daten (z. B. statische IP-Adressen, Nutzername und Passwort) sowohl Bestands- als auch Nutzungsdaten.[474]

284 Eine Strafbarkeit für den Betreiber oder Moderator einer Internetseite und damit auch eines sozialen Netzwerks nach allgemeinen Straftatbeständen (z. B. §§ 184 ff. StGB) kann sich ergeben, wenn auf der in seiner Verantwortung stehenden Seite strafbare Inhalte aufzufinden sind. Allerdings normiert § 10 TMG insofern eine **Privilegierung**, die sowohl die strafrechtliche Verantwortlichkeit als auch die zivilrechtliche Schadensersatzhaftung[475] desjenigen Diensteanbieters betrifft, der nicht eigene, sondern lediglich fremde Informationen für einen Nutzer speichert. Danach ist der Betreiber einer Internetseite grundsätzlich nicht für die Inhalte Dritter etwa in einem eingerichteten Forum verantwortlich, wenn er vom konkreten Inhalt keine Kenntnis hat. Auch ist er nicht zu Stichproben und Überwachungsmaßnamen verpflichtet (§ 7 Abs. 2 S. 1 TMG).

285 Ab Kenntnis von einem rechtswidrigen, auf seinem Internetangebot gespeicherten Inhalt aber muss er „**unverzüglich**“ Maßnahmen ergreifen, gemäß § 10 Satz 1 Nr. 2 TMG also die Informationen entfernen oder den Zugang zu ihnen sperren.[476] Nur wenn er dieses versäumt, kann er straf- und zivilrechtlich für die fremden Inhalte in Haftung genommen bzw. verantwortlich gemacht werden.[477] Umstritten ist in diesem Kontext, ob sich auch ein Moderator strafbar macht, der zwar freiwillig stichprobenartig Überschreitungen des zulässigen Inhalts auf den in seiner Verantwortung liegenden Internetseiten überprüft, gleichwohl aber fahrlässig gewisse Inhalte übersieht.[478]

---

[472] Vgl. die Auflistung bei Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 14 TMG Rn. 3.

[473] Orientierungshilfe „Soziale Netzwerke“ (Stand: 14.3.2013), Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Hrsg.), S. 16 f., einsehbar auf: http://www.datenschutz.rlp.de/downloads/oh/dsb_oh_soziale_Netzwerke.pdf.

[474] Vgl. hierzu Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG Rn. 2 m. w. N.

[475] BGH, NJW 2012, 148 (150); NJW 2007, 518; OLG Stuttgart, MMR 2014, 203 (204; Bezeichnung eines Hotels als „Hühnerstall“ auf Bewertungsportal) jeweils auch zur Unanwendbarkeit auf zivilrechtliche Unterlassungsansprüche; vgl. auch BVerfG, MMR 2009, 459 (460) zur strafrechtlichen Verantwortlichkeit bei Verwendung von Hyperlinks.

[476] Vgl. Brodowski, JR 2013, 513 (520).

[477] Vgl. OLG Stuttgart, MMR 2014, 203 (Anwendbarkeit der Haftungsprivilegierung für Unterlassungsansprüche offengelassen). Zum Ganzen Brodowski, JR 2013, 513 (520).

[478] Ausführlich und mit eigenem Lösungsansatz Brodowski, JR 2013, 513 (521 ff.).

7.5.18 *Datenschutzrechtliche Sanktionstatbestände (§§ 43, 44 BDSG)*

286 Das Bundesdatenschutzgesetz (BDSG)[479] regelt zentral das Erheben (§ 3 Abs. 3 BDSG), Verarbeiten (§ 3 Abs. 4 BDSG) und die Nutzung (§ 3 Abs. 5 BDSG) von personenbezogenen Daten.[480] Als „personenbezogenes Datum" definiert § 3 Abs. 1 BDSG jede „Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Es genügt mithin, wenn die Daten auf eine Person bezogen werden können.[481] Anonymisierte Daten fallen hingegen nicht in den Anwendungsbereich des BDSG, da ihnen die Personenbeziehbarkeit fehlt.[482]

287 Dem BDSG sind **bestimmte Grundprinzipien** immanent, die auch in das speziellere TKG ausstrahlen. Zu nennen sind hier das Einwilligungskonzept, das zentrale Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG), der Zweckbindungsgrundsatz, die Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) und der Grundsatz der Erforderlichkeit.[483]

288 Genau wie auch die sonstigen Vorschriften des BDSG sind die §§ 43, 44 BDSG subsidiär, vgl. § 1 Abs. 3 BDSG. Fehlt hingegen eine Spezialregelung[484], kommen das BDSG und damit auch die §§ 43, 44 BDSG wieder zur Anwendung. Ebenso wird auf das BDSG zurückgegriffen, wenn zwar eine bereichsspezifische speziellere Norm gegeben ist, diese aber keinen Sanktionscharakter hat.[485]

289 **§ 43 Abs. 1 BDSG** enthält insgesamt 20 Bußgeldbestimmungen. Mehrheitlich beziehen sich die Tatbestände auf die (vorsätzliche oder fahrlässige) Verletzung organisatorischer oder verfahrensmäßiger Pflichten.[486] § 43 Abs. 1 Nr. 4 u. 6 BDSG ahnden dagegen materielle Verstöße (Pflichtverletzungen bei der Übermittlung und Nutzung von Daten).

290 Täter einer **Ordnungswidrigkeit** nach § 43 BDSG kann jedermann, mit Ausnahme des Betroffenen hinsichtlich seiner eigenen Daten, sein[487], wobei aber einschränkend wiederum nur natürliche Personen als taugliche Täter in Frage

---

[479] BGBl. I 2003, S. 66.
[480] Eine Darstellung der weiteren Differenzierung bei Kühling et al., Telekommunikationsrecht, S. 339, Rn. 623.
[481] Kühling et al., Telekommunikationsrecht, Rn. 622.
[482] Kühling et al., Telekommunikationsrecht, Rn. 622.
[483] Vgl. instruktiv zu allen Prinzipien: Kühling et al., Telekommunikationsrecht, Rn. 624 ff.
[484] Vertiefend zu landesrechtlichen Bußgeld- und Strafvorschriften Ehmann, in: Simitis, BDSG, § 43 Rn. 12 ff., 18 ff.
[485] Vgl. Holländer, in: BeckOK-BDSG, § 43 Rn. 4; Gola/Schomerus, BDSG, § 44 Rn. 2.
[486] Ehmann, in: Simitis, BDSG, § 43 Rn. 20.
[487] Ehmann, in: Simitis, BDSG, § 43 Rn. 22.

kommen.[488] Für Fälle etwaiger Zurechnung in Konstellationen der Verantwortungsdelegation und der Ressortverteilung ist auf §§ 30, 130 OWiG zurückzugreifen.[489] Aufgrund des im Ordnungswidrigkeitenrecht vorherrschenden Einheitstäterprinzips, § 14 OWiG, kann eine Trennung in Beteiligungsformen grundsätzlich dahinstehen.[490] Nutzer sozialer Netzwerke sind im Regelfall als *Betroffene*, § 3 Abs. 1 BDSG, d. h. nicht als für die Datenverarbeitung *Verantwortliche* anzusehen.[491]

291 Die Tatbestände des § 43 Abs. 2 BDSG pönalisieren Pflichtverstöße gegen die unrechtmäßige Erhebung und Verarbeitung personenbezogener Daten,[492] d. h. Verstöße gegen § 4 Abs. 1 BDSG.

292 Sofern die Handlung nach **§ 43 Abs. 2 BDSG** vorsätzlich und gegen Entgelt bzw. mit Schädigungs- oder Bereicherungsabsicht begangen wird, ist die Tat als **Straftat** zu verfolgen, § 44 Abs. 1 BDSG.[493] § 44 BDSG gehört zum Nebenstrafrecht.[494] Folglich sind auch die Vorschriften des Allgemeinen Teils des StGB ergänzend heranzuziehen.[495] Die Tat wird nur auf **Antrag** verfolgt, § 44 Abs. 2 BDSG. Antragsberechtigt sind abweichend von § 77 Abs. 1 StGB der Betroffene (§ 3 Abs. 1 BDSG), die verantwortliche Stelle (§ 3 Abs. 7 BDSG), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Aufsichtsbehörde (§ 38 BDSG).[496]

7.6 Prozessuale Fragestellungen

7.6.1 Zugriff auf Daten eines Benutzerkontos

7.6.1.1 Durchsuchung (§§ 102, 103 StPO)

293 Besteht der Verdacht der Begehung einer Straftat, so kann beim Beschuldigten und unter bestimmten Voraussetzungen auch bei nicht tatbeteiligten Dritten eine Durchsuchung durchgeführt werden, §§ 102 ff. StPO. Ergeben sich Anhaltspunkte für eine

---

[488] Holländer, in: BeckOK-BDSG, § 43 Rn. 6.

[489] Ausführlich hierzu Holländer, in: BeckOK-BDSG, § 43 Rn. 7 f., auch zur Frage der Geldbußen gegen das Unternehmen; siehe Ehmann, in: Simitis, BDSG, § 43 Rn. 24.

[490] Vgl. Holländer, in: BeckOK-BDSG, § 43 Rn. 6 m. w. N.

[491] Orientierungshilfe „Soziale Netzwerke“ (Fn. 473), S. 13 f. Teilweise ist diese Einordnung aber umstritten, insbesondere wegen der „Freunde finden“- Option vieler Netzwerke, LG Berlin, WRP 2012, 613 (red. Ls. und Gründe).

[492] Ehmann, in: Simitis, BDSG, § 43 Rn. 52.

[493] Ehmann, in: Simitis, BDSG, § 43 Rn. 1, § 44 Rn. 1; Gola/Schomerus, BDSG, § 44 Rn. 1; vertiefend zu der Frage, ob der Gesetzgeber in der Entscheidung der Ausgestaltung einer Sanktionsnorm als Ordnungswidrigkeit oder Strafnorm frei ist, Ehmann in: Simitis, BDSG, § 43 Rn. 4 ff.; weniger kritisch zu solchen Mischtatbeständen Gola/Schomerus, BDSG, § 43 Rn. 1.

[494] Ehmann, in: Simitis, BDSG, § 44 Rn. 3.

[495] So Holländer, in: BeckOK-BDSG, § 44 Rn. 3.

[496] Vgl. hierzu auch Ehmann, in: Simitis, BDSG, § 44 Rn. 9 ff.

Tatbegehung über oder unter Hinzuziehung sozialer Netzwerke (z. B. durch Informationsaustausch), so ist fraglich, ob die StPO eine passende Eingriffsgrundlage für die Durchsuchung eines sog. Netzwerk-„Accounts" bereitstellt.

294 Grundvoraussetzung einer Zwangsmaßnahme nach § 102 StPO, d. h. einer Durchsuchung beim **Verdächtigen** („dem, welcher als Täter oder Teilnehmer einer Straftat ... verdächtig ist") ist bereits bei Anordnung der Durchsuchung das Vorliegen eines **Anfangsverdachts** i. S. v. § 152 Abs. 2 StPO.[497] Der Verdacht darf sich also nicht erst nach bzw. aufgrund der durchgeführten Durchsuchung ergeben.[498] Im Falle einer Tatbegehung in sozialen Netzwerken muss die Staatsanwaltschaft also vorher entweder auf dienstlichem Wege oder im Wege der Strafanzeige (§ 158 StPO) von einem möglicherweise strafrechtlich relevanten Handeln einer Person Kenntnis genommen haben.

295 § 102 StPO erstreckt sich auf die Durchsuchung der Wohnung und anderer Räume sowie der Person des Verdächtigen und der ihm gehörenden Sachen. Für die Durchsuchung eines „**Accounts**" selbst kommt nur die Variante der dem Täter **gehörenden Sache** in Betracht. Gehören wird dabei nicht im zivilrechtlichen Sinne des Eigentums verstanden; stattdessen sind alle Gegenstände erfasst, „die im Besitz, Gewahrsam oder Mitgewahrsam des Verdächtigen stehen und sich in seinem Einflussbereich befinden".[499] Zieht man exemplarisch die Datenschutzrichtlinie von Facebook heran, so bleiben die Informationen, die der einzelne Nutzer Facebook zur Verfügung stellt, sein Eigentum und gehen nicht in das Eigentum von Facebook über („*Obwohl du uns gestattest, die Informationen zu verwenden, die wir über dich erhalten, bleiben diese doch stets dein Eigentum*").[500] Zudem kann der Nutzer die Daten und Inhalte auf seiner Pinnwand selbst einstellen oder löschen, sodass nur er über die jeweilige Verwendung der Daten entscheidet. Somit können die **Inhalte (elektronische Daten)** eines Accounts als dem Nutzer gehörend (Mitgewahrsam) eingestuft werden.[501]

296 Jedoch liegt auch § 102 StPO der **Sachbegriff des § 90 BGB** zugrunde, der nur körperliche Gegenstände erfasst.[502] Die Durchsuchung der **Festplatte eines heimischen Computers**, auf dem die in das Netzwerk eingestellten Inhalte als („Ausgangs")Daten ebenfalls vermutet werden, fällt damit zwar unter § 102 StPO[503]; diese Maßnahme kann sich aber in der Praxis durch die vorherige Löschung der Daten oder Vernichtung der Speichermedien als aussichtslos erweisen.[504] Der **Account** (genauer: die den Eintrag bildenden elektronischen Daten) in einem sozialen Netzwerk

[497] Michalke, StraFo 2014, 89 (89 f.).
[498] Schmitt, in: Meyer-Goßner/Schmitt, StPO, § 102 Rn. 2.
[499] Hegmann, in: BeckOK-StPO, § 102 Rn. 12.
[500] Https://www.facebook.com/about/privacy/your-info, „Wie wir uns bereitgestellte Informationen verwenden".
[501] Schmitt, in Meyer-Goßner/Schmitt, StPO, § 102 Rn. 10a; Wicker, MMR 2013, 765 (767), die für das Merkmal des „Gehörens" auf die faktischen Zugriffs- oder Verfügungsmöglichkeiten des Nutzers auf die Daten abstellt.
[502] Wicker, MMR 2013, 765 (766).
[503] Hermann/Soiné, NJW 2011, 2922 (2924).
[504] Siehe AG Reutlingen, ZD 2012, 178 (178); AG Pforzheim, Beschluss v. 21.2.2012 in: BeckOK-StPO, Überwachung und Beschlagnahme von Internet-Kommunikation in sozialen Netzwerken.

erfüllt den Sachbegriff hingegen nicht, da Daten nicht in verkörperter Form dargestellt (vgl. insoweit § 202a Abs. 2 StGB) und daher nicht als körperliche Gegenstände angesehen werden.[505]

297 Eine Sache, die sich durchsuchen ließe, wäre lediglich der vom Netzwerkbetreiber als Speichermedium genutzte **Zentralrechner des Netzwerkbetreibers** (z. B. der Fa. Facebook GmbH in Hamburg); dieser Rechner „gehört" dem „Täter" allerdings nicht (s. o.). Hier kommt insoweit nur eine Durchsuchung bei „**einer anderen Person**" (Dritter) gemäß **§ 103 Abs. 1 S. 1 StPO** in Betracht.[506] Da es sich bei der dritten Person im Rahmen des § 103 StPO um eine unverdächtige Person handelt, werden an den Erlass des Durchsuchungsbeschlusses höhere Anforderungen gestellt.[507] So ist eine **Durchsuchung** nur dann möglich, wenn sie unter anderem zur Beschlagnahme bestimmter Gegenstände dient und Tatsachen vorliegen, aus denen zu schließen ist, dass die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Hat die Staatsanwaltschaft von möglicherweise strafbarem Verhalten im Rahmen eines sozialen Netzwerkes erfahren, so ist § 103 StPO einschlägig, da der Account des Verdächtigen sich auf dem Zentralrechner in den Räumen des Netzwerkbetreibers befindet und dieser Zentralrechner eine Sache i. S. v. § 103 StPO darstellt.

298 Stets sind im Falle einer Durchsuchung die – verfassungsrechtlich determinierten – **inhaltlichen Vorgaben** des § 105 StPO für den der Maßnahme zugrundeliegenden (richterlichen) Beschluss zu beachten. Danach müssen vor allem der Zweck der Durchsuchung und ihr Umfang möglichst genau beschrieben werden.[508] Wenn die Durchsuchung der Auffindung von Beweismitteln dient, so sind auch diese möglichst genau zu konkretisieren.[509] Im Durchsuchungsbeschluss müssen daher möglichst genaue Angaben über die zu durchsuchenden Räume sowie die zu suchenden Beweismittel, zumindest eine gattungsmäßige Bestimmung[510] erfolgen.[511] Auch dem allgemeinen Grundsatz der Verhältnismäßigkeit ist bei der Anordnung einer Durchsuchung Rechnung zu tragen,[512] wobei im Falle der Durchsuchung eines Accounts

Aus diesem Grund (Gefahr des Beweismittelverlustes) wurde auch § 110 Abs. 3 StPO geschaffen, BT-Drs. 16/5846, 63.

[505] E contrario z. B. Hegmann, in: Graf, StPO, § 102 Rn. 13, wonach von § 102 StPO nur Datenträger, nicht aber die Daten selbst erfasst sind.

[506] Anders: Wicker, MMR 2013, 765 (768), wonach beim Dritten keine Durchsuchung mehr stattfinden soll, sondern nur noch eine bloße Abfrage der Daten, da die benötigten Daten schon konkret bekannt seien.

[507] Michalke, StraFO 2014, 89 (90).

[508] Hegmann, in BeckOK-StPO, § 105 Rn. 10; Schmitt, in: Meyer-Goßner/Schmitt, StPO, § 105 Rn. 5 f.; Tsambikakis, im: LR-StPo, § 105 Rn. 51.

[509] Hegmann, in: Graf, StPO, § 105 Rn. 10.

[510] Hegmann, in: Graf, StPO, § 105 Rn. 10; ders., in: BeckOK-StPO, § 105 Rn. 10.

[511] Bruns, in: KK-StPO, § 105 Rn. 4; Bär, ZIS 2011, 53 (53).

[512] Schmitt in: Meyer-Goßner/Schmitt, StPO, § 102 Rn. 15a.

Art. 2 Abs. 1 GG (Recht auf informationelle Selbstbestimmung) tangiert und in der Abwägung zu berücksichtigen ist.[513]

7.6.1.2 Durchsicht des Speichermediums (§ 110 StPO)

Befinden sich Papiere – unter diesen Begriff fallen im Rahmen des § 110 Abs. 1 StPO auch Daten[514] – „**im Gewahrsam des Betroffenen und innerhalb des Durchsuchungsobjektes**“, so können diese bereits gemäß § 110 Abs. 1 StPO durchgesehen und zur vollständigen Durchsicht vorläufig sichergestellt werden.[515] **299**

Befinden sich die Daten jedoch nicht im Durchsuchungsobjekt, so ist ihre Durchsuchung nicht von der Anordnung nach §§ 102 f. StPO gedeckt.[516] Kann auf die Daten aber vom Computer des Betroffenen aus zugegriffen werden, so kommt hierfür bei einem externen Speichermedium im Inland[517] eine sog. „**Kleine Onlinedurchsuchung**“ gemäß § 110 Abs. 3 S. 3 StPO in Betracht.[518] Sowohl § 110 Abs. 1 StPO als auch § 110 Abs. 3 StPO sind abhängig von der Durchführung einer Durchsuchung nach den §§ 102 f. StPO.[519] **300**

Durch Einfügung des § 110 Abs. 3 StPO sollte dem Umstand abgeholfen werden, dass mit der Notwendigkeit der räumlichen Begrenzung der Durchsuchung (§ 105 StPO, s. o.) ein Zugriff auf extern gespeicherte Daten ansonsten nicht möglich ist[520] und die Durchsuchung beim Inhaber des Speichermediums nur mit Mehraufwand (neuer Beschluss) und unter zeitlicher Verzögerung möglich war.[521] Nach § 110 Abs. 3 StPO darf die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen . . . auch auf hiervon **räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann**, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist.[522] **301**

---

[513] Hegmann, in: Graf, StPO, § 102 Rn. 17; Hermann/Soiné, NJW 2011, 2922 (2923) bei „Speichern von Daten auf einem Speichermedium“. Brodowski/Eisenmenger, ZD 2014, 119 (121 f.), halten Art. 10 GG als das speziellere Grundrecht für tangiert, da der Nutzer gerade keine direkte Zugriffsmöglichkeit auf seine Daten hat, sondern sich dafür eines Kommunikationsmediums bedienen muss.

[514] Bruns, in: KK-StPO, § 110 Rn. 2; Krause, Kriminalistik 2014, 213 (214).

[515] Brodowski/Eisenmenger, ZD 2014, 119 (120).

[516] Bär, ZIS 2011, 53 (53).

[517] Bär, ZIS 2011, 53 (54); Krause, Kriminalistik 2014, 213 (214 f.), der aber klarstellt, dass eine Durchsicht gemäß § 110 Abs. 3 StPO nur dann unzulässig ist, wenn *sicher feststeht*, dass sich das Speichermedium im Ausland befindet (215).

[518] Hermann/Soiné, NJW 2011, 2922 (2925).

[519] Hermann/Soiné, NJW 2011, 2922 (2925); Michalke, StraFo 2014, 89 (91 f.).

[520] Bär, ZIS 2011, 53 (53).

[521] BT-Drs. 16/5846, 63; Brodowski/Eisenmenger, ZD 2014, 119 (121); Bär, ZIS 2011, 53 (54).

[522] Brodowski/Eisenmenger, ZD 2014, 119 (122), halten diese Auslegung des Begriffs Speichermediums für zu weit und wollen soziale Netzwerke nicht darunter fassen, sondern nur „diejenigen Dienste . . . , deren alleiniger oder zumindest überwiegender Zweck es ist, eine lokale Datenspeicherung im Durchsuchungsobjekt zu ersetzen bzw. zu ergänzen“.

302 Im Rahmen der sozialen Netzwerke ist im Rahmen des § 110 StPO zwischen dem **Account-Inhaber** und dem Netzwerkbetreiber zu unterscheiden: Wird eine Durchsuchung nach § 102 StPO beim Verdächtigen angeordnet (nicht gestützt auf die Begehung einer Tat mittels seines Facebook-Accounts, s. o., da sonst kein taugliches Durchsuchungsobjekt i. S. v. **§ 102 StPO** vorliegt), so können die Ermittler nach § 110 Abs. 3 StPO auch den Account durchsuchen, da er mittels Passwort vom heimischen Rechner aus aufrufbar ist, soweit sie andernfalls einen Datenverlust befürchten. Sollte der Betroffene das **Passwort** nicht freiwillig bekanntgeben, so ist ein Zugriff dennoch möglich, wenn das Passwort bei der Durchsuchung aufgefunden wird oder es bereits vorher beim Teledienstanbieter erfragt worden ist (§ 113 TKG).[523] Die Möglichkeit der Durchsicht der Daten muss bereits im Durchsuchungsbeschluss selbst angeordnet werden[524] und das Speichermedium, auf welches sich die Durchsicht beziehen soll, muss „gegenständlich beschrieben werden".[525]

303 Der Betroffene hat bei dieser Durchsicht ein **Anwesenheitsrecht** gemäß § 106 Abs. 1 StPO, da es sich gerade nicht um eine heimliche Maßnahme handelt.[526] Zudem handelt es sich bei der Durchsicht, genauso wie bei der Durchsuchung, um eine punktuelle Maßnahme; eine mehrfache Durchsicht ist nicht von § 110 Abs. 3 StPO gedeckt.[527]

304 Gegen den **Netzwerkbetreiber** ist dagegen ein Beschluss nach **§ 103 StPO** zu erwirken, wonach die Geschäftsräume und der Zentralrechner als Sache zu durchsuchen sind. Die auf dem Rechner gespeicherten Daten fallen dann unter den Begriff der „Papiere" in § 110 Abs. 1 StPO. Papier ist sämtliches Schriftgut, das – nicht zwingend auf „Papier", sondern auch auf Bild- und Tonträgern – gespeichert ist und wegen seines Gedankeninhalts Bedeutung hat.[528] Eines Rückgriffs auf § 110 Abs. 3 StPO bedarf es hier nicht.

7.6.1.3 Beschlagnahme (§§ 94 ff. StPO)

305 Hinsichtlich der Beschlagnahme von elektronischen Nachrichten und Profilen in sozialen Netzwerken findet sich in den Beschlagnahmevorschriften der **§§ 94 ff. StPO** keine spezielle Regelung. Dennoch muss den Besonderheiten des Internet auch in strafprozessualer Hinsicht Rechnung getragen werden. Das Post- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG ist entwicklungsoffen und soll daher auch neuartige Übertragungstechniken umfassen. Dementsprechend sind auch die

---

[523] Bär, ZIS 2011, 53 (54); Krause, Kriminalistik 2014, 213 (214). Nur eine Erlangung des Passwortes unter Überwindung der Zugangssicherung ist nach § 110 Abs. 3 StPO nicht erlaubt, Brodowski/Eisenmenger, ZD 2014, 119 (123).
[524] Hermann/Soiné, NJW 2011, 2922 (2925).
[525] Hermann/Soiné, NJW 2011, 2922 (2925).
[526] Michalke, StraFO 2014, 89 (91); Hermann/Soiné, NJW 2011, 2922 (2925).
[527] Brodowski/Eisenmenger, ZD 2014, 119 (123).
[528] Bruns, in: KK-StPO, § 110 Rn. 2.

Begriffe der StPO dieser Entwicklung insoweit anzupassen, als dies der zugrunde liegenden Intention und dem Zweck der Vorschrift sowie dem durch sie gleichermaßen einzuschränkenden wie auch zu schützenden Grundrecht entspricht.[529]

Die Rechtsprechung hat bereits die Frage beschäftigt, nach welcher prozessualen Eingriffsmaßnahme eine **E-Mail** „gesichert" werden kann. **306**

§ 99 StPO schränkt das Brief-, Post- und Fernmeldegeheimnis aus Art. 10 GG ein, indem er die Beschlagnahme von Postsendungen und Telegrammen ermöglicht. Das gilt allerdings nur insoweit, als es sich um Postsendungen handelt, die *an den Beschuldigten gerichtet* sind bzw. gemäß § 99 Satz 2 StPO von ihm herrühren. Voraussetzung für die Anwendbarkeit des § 99 StPO ist also stets, dass es sich bei dem Betroffenen um einen **Beschuldigten** handelt. Als Beschlagnahmeobjekte kommen nur Postsendungen und Telegramme, also **verkörperte Nachrichten**, in Betracht – und auch diese nur dann, wenn und solange sie sich *im Gewahrsam von Post-/TK-Dienstleistern* befinden. **307**

Nach Ansicht des BVerfG kann auch eine E-Mail, obwohl es sich bei ihr nicht um einen körperlichen Gegenstand handelt, nach den §§ 94 ff. StPO sichergestellt und bei Verfahrensrelevanz beschlagnahmt werden.[530] Da kein besonderer Verdachtsgrad gefordert ist, genügt ein schlichter **Anfangsverdacht**, vgl. § 152 Abs. 2 StPO. **308**

Trotz der Feststellung, dass E-Mails grundsätzlich Gegenstand der §§ 94 ff. StPO sein können, hat bei der Prüfung der Voraussetzungen des jeweiligen Beschlagnahmerechts eine weitere Differenzierung zu erfolgen. Zur Darstellung des Meinungsstreits muss zwischen **verschiedenen Phasen der Kommunikation** mittels E-Mail unterschieden werden.[531] Phase 1 erfasst die Übertragung der auf dem Computer des Absenders erstellten E-Mail über den Internetprovider auf den Server des E-Mail-Dienstleitungsanbieters. Dort wird die entsprechende Nachricht in Phase 2 so lange zwischengespeichert, bis der mit einem Postfach registrierte Empfänger sie in Phase 3 abruft und ggfs. auf seinen Computer überträgt. Eine Phase 4 ergibt sich in den Fällen, in denen die E-Mail nach dem Abruf entweder auf dem Server des E-Mail-Dienstleistungsanbieters oder auf dem Computer des Empfängers weiterhin gespeichert bleibt. **309**

Die strafprozessualen Eingriffsgrundlagen können nun je nach Sachlage unterschiedlich ausfallen, abhängig davon, in welcher Phase sich der E-Mailverkehr befindet. Der **Übertragungsvorgang** der Phasen 1 und 3 vom Computer des Absenders auf den Server des Anbieters und von dort aus auf den Computer des Empfängers stellt unstreitig eine („dynamische") **Telekommunikation** dar und eröffnet somit zwingend den Anwendungsbereich des **§ 100a StPO**; auch hinsichtlich der vierten Phase bestehen keine Probleme, da der Schutz durch Art. 10 GG in dem **310**

---

[529] Graf, in: BeckOK-StPO, § 99 Rn. 10. Auch Daten, die in „**Clouds**" gespeichert sind, unterfallen dem Schutzbereich des Art. 10 GG, Brodowski/Eisenmenger, ZD 2014, 119 (121).

[530] BVerfG, NJW 2009, 2431 = MMR 2009, 673 m. Anm. Krüger; vgl. zum Zugriff auf Daten in der „Cloud": Wicker, MMR 2013, 765; Bär, MMR 2013, 700 (703). Zur Ablehnung von Daten als **Einziehungsobjekt** i. S. v. §§ 111b ff. StPO, 74 ff. StGB: LG Hamburg, ZD 2014, 146 ff.

[531] Bär, NStZ 2009, 397 (399); vgl. zu einem 7-Phasen-Modell: Graf, in: BeckOK-StPO, § 100a Rn. 27.

Moment endet, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang (mithin auch die Telekommunikation) beendet ist.[532]

311 Schwieriger zu beurteilen und heftig umstritten ist jedoch die rechtliche Einordnung der **zweiten Phase**, also der Zwischenspeicherung der Nachrichten auf dem Server des Diensteanbieters. Große Bedeutung erlangt hat in diesem Zusammenhang der Beschluss des 1. Strafsenats des BGH v. 31.3.2009.[533] In diesem erteilte er der Anwendung von § 100a StPO als Eingriffsgrundlage für die Beschlagnahme von bei einem E-Mail-Provider gespeicherten Nachrichten (E-Mails) eine klare Absage, da es sich bei der nur Sekunden andauernden **Zwischenspeicherung** der Mails auf dem Server des Mailanbieters nicht (mehr) um einen *Telekommunikations*vorgang handele. Es bestehe vielmehr eine mit dem herkömmlichen Postverkehr vergleichbare Lage, in der die E-Mail bis zum Zeitpunkt ihres Abrufs durch den Empfänger ähnlich wie ein Brief oder ein Telegramm bei dem Post- oder Telekommunikationsdienstleister „zwischengelagert" werde und sich in dessen Gewahrsam befinde. Die richtige Ermächtigungsgrundlage könne daher nur **§ 99 StPO** sein. Ein ausreichender Grundrechtsschutz des Art. 10 GG sei über die Voraussetzungen des § 100 StPO (hier insbesondere das Erfordernis einer richterlichen Anordnung nach § 100 Abs. 1 StPO) und der durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007 eingeführten Mitteilungspflicht des § 101 Abs. 4 Nr. 2 StPO gewährleistet.

312 Noch weiter geht der Beschluss des **BVerfG** vom 16.6.2009.[534] Ein Eingriff in das Grundrecht aus Art. 10 GG läge zwar vor. Die allgemeinen Vorschriften der **§§ 94 ff. StPO** reichten aber zum Schutz des Betroffenen aus.[535] Eine Anwendung des hinsichtlich seiner Voraussetzungen engeren § 99 StPO sei nicht notwendig; der Verhältnismäßigkeitsgrundsatz sei aber in besonderem Maße zu beachten.

313 In der **Literatur** stießen diese Ausführungen auf unterschiedliche Reaktionen.[536] Zustimmend wird argumentiert, dass in der Phase 2 keine Telekommunikation i. S. d. § 100a StPO mehr stattfinde, weil mit der Zwischenspeicherung der Nachricht im elektronischen Postfach der eigentliche Kommunikationsvorgang auf unbestimmte Zeit unterbrochen sei und die gespeicherten Daten gleichsam auf dem Mail-Server des Providers in verkörperter Form gespeichert würden.[537] Es wird außerdem auf die ausdrückliche Nennung der Anbieter von TK-Diensten und die daraus folgende bewusst weite Fassung des Anwendungsbereichs von § 99 StPO verwiesen. Ablehnend wird dagegen bereits die Möglichkeit einer analogen Anwendung der

---

[532] BVerfG, NJW 2006, 976; vgl. auch: OVG Koblenz, NJW 2013, 3671 f. Zu diesem Phasen-Modell auch: Schön, Ermittlungsmaßnahmen über das Internet, S. 89 ff., die aber sowohl die Anwendung von § 94 StPO als auch von § 99 StPO ablehnt, sondern allein § 100a StPO für maßgeblich hält.

[533] BGH, NJW 2009, 1828 = NStZ 2009, 397 m. Anm. Bär.

[534] BVerfG (Fn. 531).

[535] So auch Nack, in: KK-StPO, § 100a Rn. 22.

[536] Überwiegend jedoch in einer Linie mit BGH und BVerfG; vgl. dazu Meyer-Goßner/Schmitt, StPO, § 94 Rn. 16a m. w. N.

[537] Bär, NStZ 2009, 397 (399).

Vorschrift in Frage gestellt.[538] Von diesen generellen Bedenken abgesehen, fehle es aber bereits an einer planwidrigen Regelungslücke. Der Gesetzgeber hätte im Zuge der Neuordnung der Vorschriften der Telekommunikationsüberwachung im Rahmen der Überarbeitung des Straftatenkatalogs des § 100a StPO einen Zugriff auf serverbasiert gespeicherte Inhalte über diese Vorschrift in Betracht gezogen und den Regelungsbedarf keineswegs übersehen. Weiterhin läge auch keine vergleichbare Interessenlage vor. Bei der Beschlagnahme von digitalen Daten sei der Eingriff ungleich schwerer, da die betreffenden Daten in zeitlicher Hinsicht meist bis weit in die Vergangenheit liegende Zeitpunkte beträfen und so die Erstellung eines umfangreichen Persönlichkeitsprofils ermöglichten.

314 In Rahmen der **Kommunikation in sozialen Netzwerken** werden zwar keine E-Mails im klassischen Sinn verschickt und empfangen. Dennoch stehen auch hier durchaus vergleichbare Kommunikationsformen wie etwa private Nachrichten, über ein Chatprogramm empfangene Nachrichten sowie Pinnwandeinträge o. ä. zur Verfügung. Auch diese werden auf dem Server des Betreibers des entsprechenden sozialen Netzwerks zwischengespeichert, sodass der oben erläuterte Meinungsstand in diesen Fällen ebenfalls relevant wird.

315 Interessant ist in diesem Zusammenhang vor allem der Beschluss des AG Reutlingen vom 31.10.2011[539], in welchem erstmals von einem deutschen Gericht die Beschlagnahme der auf einem Facebook-Konto vorhandenen Nachrichteninhalte angeordnet wurde. Das Gericht stützte die Beschlagnahme auf eine **entsprechende Anwendung des § 99 StPO** und folgte in seiner Begründung der Argumentation des Beschlusses des 1. Strafsenats des BGH v. 31.3.2009. Eine direkte Anwendung der Vorschrift scheide aufgrund der fehlenden Körperlichkeit der gegenständlichen Daten aus. Eine entsprechende Anwendung auf private Nachrichten lasse sich hingegen i. S. d. Beschlusses des BGH und der befürwortenden Stimmen in der Literatur durchaus begründen. Dem ablehnenden Argument der deutlich höheren Eingriffsintensität sollte in der besonderen Konstellation der Beschlagnahme der aus Benutzerprofilen sozialer Netzwerke stammenden Daten jedoch Beachtung geschenkt werden. Diese geben üblicherweise deutlich umfangreichere Auskünfte über den Inhaber, als die Auswertung seines E-Mailverkehrs.

7.6.1.4 Überwachung der Telekommunikation (§ 100a StPO)

316 Abgesehen von der Einschlägigkeit der Vorschrift in den oben erläuterten Übermittlungsphasen 1 und 3 der Kommunikation via E-Mail bzw. in sozialen Netzwerken über private (Chat-)Nachrichten lässt sich im Hinblick auf die oben aufgeführte Argumentation lediglich feststellen, dass die Norm in den Fällen von auf Servern

[538] Neuhöfer, MMR-Aktuell 2012, 329250 (auch zum folgenden Text).
[539] AG Reutlingen, DRiZ 2012, 171.

zwischengespeicherten Daten nach Ansicht des BGH, des BVerfG und des überwiegenden Teils der Literatur nicht einschlägig ist. Es gelten hier die Ausführungen zum Zugriff auf E-Mails entsprechend.[540]

7.6.1.5 Auskunft über nach §§ 95, 111 TKG gespeicherte Daten (§ 100j StPO)

317 Im Kontext der Ermittlungen von Straftaten in sozialen Netzwerken stellt sich häufig auch die Frage nach der Erhebung einer individuellen IP-Adresse. Die IP-Adresse ist ein technischer Code, der mithilfe des Internetdienstleisters die Zuordnung zu einem Anschlussinhaber ermöglicht.[541] Strafprozessual ist die Erhebung der IP-Adresse samt Zeitstempel als Herausgabe eines Gegenstandes i. S. d. §§ 94 Abs. 1, 2; 95 Abs. 1 StPO einzustufen.[542]

318 In sozialen Netzwerken ist es durchaus üblich, dass sich Nutzer nicht mit ihrem richtigen Namen anmelden, sondern ein **Pseudonym** verwenden. In einem solchen Fall wird man vor einer Beschlagnahme der Korrespondenz (Rn. 305 ff.) zunächst die Identität des Tatverdächtigen ermitteln müssen. Hierzu bedarf es allerdings einer gesonderten fach-/bereichsspezifischen Eingriffs-/Ermächtigungsgrundlage.[543] Als Reaktion auf eine entsprechende Vorgabe des BVerfG verabschiedete der Gesetzgeber die neue Vorschrift des **§ 100j StPO**[544], der die Ermittlung von Bestandsdaten oder auch dynamischen IP-Adressen, die bei jedem Einwahlvorgang generiert werden,[545] zulässt.[546]

319 **Bestandsdaten** wie Namen und Anschrift des Nutzers können gemäß § 100j Abs. 1 S. 1 StPO abgefragt werden. Voraussetzung ist lediglich eine allgemeine Erforderlichkeitsprüfung.[547] Diese Abfrage dürfte aber im Falle eines Pseudonym-Accounts leerlaufen, da die gespeicherten Bestandsdaten nach §§ 95, 111 TKG vom Teledienstleistungsanbieter nicht unter dem Pseudonym, sondern nur unter dem richtigen Namen gespeichert werden. Eine solche Abfrage kann damit nur als zweite Stufe nach der Ermittlung des korrekten Namens des Account-Inhabers erfolgen.

320 Erforderlich ist an dieser Stelle eine Abgrenzung zu den sog. **Verbindungsdaten** (Verkehrsdaten), welche nur nach der Vorschrift des **§ 100g StPO** erhoben werden dürfen. **Verkehrsdaten** sind (in § 3 Nr. 30 TKG legaldefiniert) Daten, die bei der Erbringung eines Telekommunikationsvorganges erhoben, verarbeitet oder genutzt werden. Insbesondere fallen darunter personenbezogene Berechtigungscodes und Nutzerkennungen (PIN und PUK), die Rufnummern und Kennungen der beteiligten

---

[540] Nack, in: KK-StPO, § 100a Rn. 28.
[541] Zu den weiterhin bestehenden technischen Problemen bei der Zuordnung Brodowski, JR 2013, 513 (516 f.).
[542] BVerfGE 113, 29 (50 ff.); vertiefend hierzu: Brodowski, JR 2013, 513 (516 f.).
[543] BVerfGE 130, 151.
[544] Eingefügt durch das Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20.6.2013 (BGBl. I S. 1602) m. W. v. 1.7.2013.
[545] Graf, in: BeckOK-StPO, § 100j Rn. 19.
[546] Ausführlich Bär, MMR 2013, 700.
[547] Graf, in: BeckOK-StPO, § 100j Rn. 10 f.; Bär, MMR 2013, 700 (702).

Anschlüsse, die Standorte sowie auch Anfangs- und Endzeiten der Verbindung,[548] ebenso die Daten erfolgloser Verbindungsversuche. Standortdaten sind ebenso Verkehrsdaten, § 96 Abs. 1 Nr. 1 TKG. Sofern die Verkehrsdaten auch in Echtzeit erhoben werden dürfen, ist dies bei Standortdaten insoweit eingeschränkt, als dass die Erstellung eines Bewegungsbildes durch die Ortung eines Handys im stand-by Modus nur bei Straftaten von auch im Einzelfall erheblicher Bedeutung zulässig sein soll, § 100g Abs. 1 S. 1 Nr. 1 StPO.

321 Nach einer Ansicht sollen darunter allerdings auch die dynamischen IP-Adressen fallen.[549] Gestützt wird dies von § 96 Abs. 1 Nr. 1 TKG, der als Verkehrsdaten auch die Nummer und Kennung der beteiligten Anschlüsse umfasst. Nach anderer Auffassung sollen gerade die dynamischen IP-Adressen keine Verkehrs- sondern Bestandsdaten sein, sodass ihre Erhebung sich nach § 100j StPO richtet.[550] Der Gesetzeswortlaut ist nicht eindeutig. Für eine Zuordnung der dynamischen IP-Adressen zu den Bestandsdaten und unter die Regelung des § 100j StPO spricht, dass bei der Erfassung der dynamischen Adressen Unbeteiligte gerade von einer solchen Auskunft nicht betroffen sind und der Accountinhaber im Ergebnis genauso behandelt wird, als wenn er über eine statische Adresse verfügen würde.[551] Diese wiederum ist Bestandsdatum i. S. d. § 100j StPO. Zudem stellt § 100j Abs. 2 StPO klar, dass gerade die „zu einem bestimmten Zeitpunkt zugewiesenen Internet-Protokoll-Adresse" herausverlangt werden kann. Darunter sind **auch dynamische IP-Adressen** zu verstehen.[552]

322 Die Unsicherheit gründet letztlich wohl darin, dass der § 100j StPO erst nachträglich eingefügt wurde. Zuvor wurde die dynamische IP-Adresse weitestgehend unter die Voraussetzungen des § 100g StPO subsumiert.[553] Das BVerfG hat allerdings in seinem Urteil v. 2.3.2010 zur Vorratsdatenspeicherung[554] den § 100g Abs. 1 S. 1 StPO für mit Art. 10 Abs. 1 GG unvereinbar und damit verfassungswidrig erklärt, da den Transparenzanforderungen bei einem Eingriff in Art. 10 Abs. 1 GG beim Auskunftsersuchen über den Nutzer einer dynamischen IP-Adresse durch den § 100g Abs. 1 StPO nicht genügt werde. Die Einfügung des § 100j StPO ist als direkte Reaktion auf das Urteil des BVerfG zu werten.[555] Somit ist davon auszugehen, dass der Gesetzgeber den § 100j StPO explizit dafür geschaffen hat, um einerseits trotz Verfassungswidrigkeit des § 100g Abs. 1 S. 1 StPO weiterhin Daten verlangen und erheben zu dürfen. Zudem fallen im Ergebnis nun auch dynamische IP-Adressen, unabhängig davon, ob es sich im Einzelnen um Bestands- oder Verkehrsdaten handelt, unter die Regelung des § 100j StPO.[556]

---

548 Schmitt, in: Meyer-Goßner/Schmitt, § 100j Rn. 4.
549 LG Frankenthal, K&R 2008, 467.
550 Graf, in: BeckOK-StPO, § 100j Rn. 19.
551 Vgl. Graf, in: BeckOK-StPO, § 100j Rn. 22.
552 Schmitt, in: Meyer-Goßner/Schmitt, StPO, § 100j Rn. 4.
553 Vgl. nur Eckhardt, in: Spindler/Schuster, § 113 TKG, Rn. 9b m. w. N.
554 BVerfG, MMR 2010, 356, Tz. 278 ff.
555 Vgl. BT-Drs. 17/12879, S. 2.
556 Graf, in: BeckOK-StPO, § 100j Rn. 17 ff., 19a.

7.6.1.6 Zeugnisverweigerungsrechte und verbotene Beschlagnahme

323 Wo es um die Verwertung und Beschlagnahme von Inhalten aus Kommunikationsvorgängen geht, ist immer auch an etwaige **strafprozessuale Erhebungshindernisse** zu denken. § 53 Abs. 1 S. 1 Nr. 5 StPO schützt insbesondere Personen, die berufsmäßig an Kommunikationsdiensten mitwirken, durch die Gewährung eines Zeugnisverweigerungsrechts. Daran knüpft das Beschlagnahmeverbot gemäß § 97 Abs. 5 S. 1 StPO an, wonach die Beschlagnahme von Schriftstücken, Ton-, Bild- und Datenträgern, Abbildungen und anderen Darstellungen, die sich im Gewahrsam dieser zeugnisverweigerungsberechtigten Personen oder der Redaktion, des Verlages, der Druckerei oder der Rundfunkanstalt befinden, unzulässig ist.

324 Zu unterscheiden sind folglich **Betreiber von Foren** einerseits sowie **Blogger** und **Online-Redakteure** andererseits[557], wobei es nicht darauf ankommt, ob sie diese Tätigkeit mit Gewinnerzielungsabsicht betreiben.[558] Während erstere lediglich bei der Vermittlung fremder Kommunikation beteiligt sind,[559] sind zweite direkt vom Schutz des § 53 Abs. 1 S. 1 Nr. 5 StPO umfasst, da es sich nur bei ihrem Wirken um eine berufsmäßige Betätigung handelt.[560] Des Weiteren stellen Foren weder Druckwerke noch Sendungen dar. Eine analoge Ausweitung der Schutzgruppen auf ähnliche Berufsträger wird abgelehnt.[561]

325 Bei **Leserbriefen** ist aufgrund des Vertrauensverhältnisses zwischen Schreiber und Presse für den Journalisten ebenso ein Anwendungsfall des § 53 Abs. 1 S. 3 StPO gegeben.[562] Dies gilt auch für die anonymisierte Veröffentlichung.[563] Zu beachten ist allerdings, ob der Beitrag zum redaktionellen Teil oder eher zum Anzeigenteil des Mediums gehört. Nur Beiträge, die dem **redaktionellen Teil** zuzuordnen sind, sollen dem Anwendungsbereich des Zeugnisverweigerungsrechts unterliegen,[564] was in der Praxis allerdings zu schwierigen Abgrenzungsfragen führt und diese Art der Ab- und letztlich Begrenzung presserechtlich privilegierten Materials insgesamt in Frage stellt.

326 Inzwischen gibt es Leserbriefe nicht nur in den Printmedien, sondern vermehrt auch in den **Onlineausgaben** der jeweiligen Zeitschriften. Diesen soll nach einer Auffassung die Gleichstellung zu den gedruckten Leserbriefen versagt werden, weil

---

[557] Brodowski, JR 2013, 513 (518).
[558] BGHSt 7, 129.
[559] Brodowski, JR 2013, 513 (518).
[560] Huber, in: BeckOK-StPO, § 53 Rn. 25.
[561] BVerfG, NJW 1972, 2214; NJW 1975, 588; Senge, in: KK-StPO, § 53 Rn. 2.
[562] BVerfGE 36, 193 (204); BVerfG, NStZ 1982, 253; BGHSt 28, 240 (253); weiter allerdings Senge, in: KK-StPO, § 53 Rn. 27, der den Schutz nicht nur auf das Vertrauensverhältnis zwischen Informant und Presse sondern unter Verweis auf BVerfGE 77, 65 (75); 107, 299 (331) auch auf die Vertraulichkeit der redaktionellen Arbeit an sich stützt.
[563] BVerfGE 64, 108 (114); KG, NJW 1984, 1133; Huber, in: BeckOK-StPO, § 53 Rn. 35.
[564] BVerfG, NStZ 1983, 515; Huber, in: BeckOK-StPO, § 53 Rn. 35; a. A. Brodowski, JR 2013, 513 (518), der „Im Zweifel für die Pressearbeit“ den Schutz unabhängig von der Zuweisung zum redaktionellen oder zum Anzeigenteil gewähren will.

es an journalistischer Selektion durch eine Redaktion fehle.[565] Das Beschlagnahmeverbot gemäß § 97 Abs. 5 S. 1 i. V. m. §§ 160a Abs. 2, 53 Abs. 1 S. 3 StPO greift dann nicht ein.[566] Dieser Ansatz dürfte dem Wunsch entsprechen, den zuständigen Redakteur auch wegen Beihilfe zu einem Ehrdelikt verfolgen zu können.[567] Gleichwohl bedarf es einer solchen Konstruktion nicht zwingend, da die Pressegesetze der meisten Länder bereits die fahrlässige Veröffentlichung strafbewehrter Inhalte durch den verantwortlichen Redakteur sanktionieren.[568] Folglich muss Online-Leserbriefen nicht die Eigenschaft als Leserbrief im obigen Sinne aberkannt werden, nur um eine Strafverfolgung des Redakteurs zu ermöglichen. Die Presse soll durch dieses Verfahren unter der Androhung eventueller Strafverfolgung selbst die Verantwortung für innerhalb ihrer Zurechenbarkeit präsentierte Inhalte übernehmen.[569]

7.6.2 Verdeckte Ermittlungen

7.6.2.1 Kriminalistischer Hintergrund

Soziale Netzwerke werden im Internet von Millionen Menschen genutzt. Derzeit sind **327**
etwa 37 Mio. Deutsche in sozialen Netzwerken aktiv.[570] Durch die von den meisten Nutzern recht offenherzige und nicht durchdachte Preisgabe von persönlichen Informationen gelten solche Netzwerke als zu Ermittlungs- und Fahndungszwecken willkommene Fundgruben an Textinformationen, Bildern oder Videos.[571] Besonders effektiv wäre eine solche Ermittlung bzw. Fahndung naturgemäß vor allem dann, wenn die Polizei diese nicht offen, sondern verdeckt durchführen könnte.[572] Zudem sind die aus sozialen Netzwerken gewonnenen Erkenntnisse gerade in Kombination mit den polizeilichen Datenbanken von noch größerem Wert; mit ihnen lässt sich

[565] LG Oldenburg, NStZ 2011, 655 f.; LG Mannheim, Beschl. v. 13.5.2005 – 5 QS 23/05 m. Anm. Weber/Meckbach, NStZ 2006, 492.
[566] LG Augsburg, JR 2013, 536.
[567] So Brodowski, JR 2013, 513 (519).
[568] Z. B. Art. 11 Abs. 2 BayPrG, § 12 HPresseG, § 22 Abs. 1 Nr. 1, 8 LPresseG BW, m. w. N. und instruktiv zum Ganzen: Brodowski, JR 2013, 513 (519).
[569] Brodowski, JR 2013, 513 (519), sieht darin einen Beispielsfall für den Einsatz des Strafrechts zur Selbstregulierung bzw. Compliance.
[570] Siehe www.bitkom.org/files/documents/BITKOM_Presseinfo_Social_Media_Nutzung_29_07_2013.pdf; siehe zum Umgang mit sozialen Netzwerken auch: BITKOM, Soziale Netzwerke, Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet; siehe zum „Potential" sozialer Netzwerke auch: Irlbauer, Kriminalistik 2012, 764 (765); May/Arnd, Kriminalistik 2013, 384; Kolmey, DRiZ 2013, 242.
[571] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30 (32); zu Chancen und Risiken der Nutzung sozialer Netzwerke als Mittel zur Bekämpfung von Schwerkriminalität vgl. Dudenhausen / Kahr, Kriminalistik 2014, 275.
[572] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30 (35); Ostendorf et al., NStZ 2012, 529 (537); zu praktischen Erfahrungen im Baden-Württemberg, vgl. Weiß, Kriminalistik 2014, 335.

die Aufklärung eines Falles möglicherweise beschleunigen.[573] Darüber hinaus sind meist verdeckte technische Ermittlungen, wie zum Beispiel die Überwachung der Telekommunikation (§ 100a StPO), nicht immer erfolgsversprechend, sodass der Einsatz von verdeckten personalen Ermittlungen erforderlich ist.[574]

328 Im Rahmen von Ermittlungen innerhalb sozialer Netzwerke kann auch der Einsatz Verdeckter Ermittler relevant werden. Es muss jedoch zwischen unterschiedlichen „Graden der Öffentlichkeit" von Informationen differenziert werden.[575] Unstreitig können die Ermittlungsbehörden auf den **für die gesamte Öffentlichkeit zugänglichen** Teil der Informationen zugreifen, also etwa im Falle von Nutzerprofilen, die für jedermann freigeschaltet und deren Inhalte in vollem Umfang, etwa über Suchmaschinen, einsehbar sind.[576] Da mittlerweile die Gefahren eines solch fahrlässigen Umgangs mit den eigenen Daten (Missbrauch, Kontrolle durch potentielle Arbeitgeber etc.) der Mehrheit der Nutzer bekannt sein dürften, ist davon auszugehen, dass eine solche Situation in den allerwenigsten Fällen vorzufinden sein wird.

329 Ein höherer Begründungsaufwand besteht bereits in den Fällen, in denen die Informationen des Nutzerprofils nur **innerhalb des betreffenden sozialen Netzwerks öffentlich** gemacht wurden, dort aber dann für jeden Nutzer einsehbar sind. Soziale Netzwerke nehmen jedoch grundsätzlich jeden Interessenten auf und verlangen in aller Regel nicht die Preisgabe der wahren Identität der jeweiligen Person – daher kann es seitens der Betroffenen auch kein schutzwürdiges Vertrauen in die wahre Identität der Besucher des eigenen Nutzerprofils geben.[577] Letztlich entscheidet jeder Nutzer eines sozialen Netzwerks eigenständig, welche Inhalte er in welchem Maße öffentlich zugänglich machen will.

330 Aus diesem Grund ist in strafprozessualer Hinsicht der interessanteste Bereich von Informationen der, in dem **bestimmte Informationen nur** den „**Freundeskreis**" (etwa bei Facebook, myspace und studi.vz) bzw. den „**Followern**" (Twitter) zugänglich gemacht werden.[578]

331 Dass die Thematik von praktischer Bedeutung ist, zeigt auch die Kleine Anfrage mehrerer Abgeordneter und der Fraktion DIE LINKE an die Bundesregierung zur „**Nutzung sozialer Netzwerke zu Fahndungszwecken**".[579] Darin ging es primär um Ermittlungen in sozialen Netzwerken und den Einsatz virtueller Verdeckter

---

[573] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30 (36).
[574] Vgl. Rosengarten/Römer, NJW 2012, 1764.
[575] Graf in: BeckOK-StPO, § 100a Rn. 32g; Schulz/Hoffmann, DuD 2012, 7 (10).
[576] So auch Schulz/Hoffmann, DuD 2012, 7, (11); Ostendorf et al., NStZ 2012, 529 (537).
[577] Graf, in: BeckOK-StPO, § 100a Rn. 32h; Schulz/Hoffmann, DuD 2012, 7 (11 f.) auch zum Einsatz sog. „Functions-Accounts", die die Identität der Polizei offenlegen.
[578] Graf, in: BeckOK-StPO, § 100a Rn. 32i ff.; Henrichs, Kriminalistik 2011, 622 (626) zu den Ermächtigungsgrundlagen bei Zugriff auf öffentliche/nicht-öffentliche Daten mit und ohne Kommunikationsbezug; Ostendorf et al., NStZ 2012, 529 (537).
[579] Vgl. BT-Drs. 17/6100 v. 7.6.2011; siehe hierzu die Antwort der BReg, BT-Drs. 17/6587 v. 14.7.2011.

Ermittler. Nach Angabe der Bundesregierung können Ermittlungen in sozialen Netzwerken im Rahmen der Gefahrenabwehr[580] oder Strafverfolgung insoweit relevant werden, als auch Straftäter diese als Kommunikationsplattformen nutzen oder über sie selbst Straftaten begehen. Dabei dienen Erhebungen in sozialen Netzwerken nur als zusätzliche Erkenntnisquelle über Beschuldigte.[581]

7.6.2.2 Notwendigkeit einer Ermächtigungsgrundlage

Das BVerfG hatte im Jahr 2008 die **Online-Durchsuchung** und weitere strafprozessuale Ermittlungsmaßnahmen im Netz auf ihre Grundrechtsrelevanz[582] hin zu überprüfen. Im Fall der Online-Durchsuchung kommen dabei insbesondere Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) sowie das Telekommunikationsgrundrecht (Art. 10 GG) und die Unverletzlichkeit der Wohnung (Art. 13 GG) in Betracht.[583] Darüber hinaus hat das BVerfG das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** anerkannt, das ebenfalls auf Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gestützt wird. „Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet [. . .]; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten".[584] **332**

In seinem Urteil v. 27.2.2008 hatte das BVerfG vorrangig die Frage zu beantworten, ob es für verdeckte Ermittlungen im Netz, und damit auch speziell in sozialen Netzwerken, überhaupt einer gesetzlichen Grundlage bedarf. Es gelangte zu dem Ergebnis, dass bei der Suche nach und der Erhebung von **Inhalten** (einschließlich Kommunikationsinhalten), die **im Netz allgemein zugänglich sind**, schon gar keine **333**

[580] Vgl. hierzu ausführlich Biemann, „Streifenfahrten" im Internet, 2013; zur Aufklärungsarbeit der Polizei in den Niederlanden als Teilnehmer in einem Onlinespiel, vgl. Virtuelle Wache, SZ v. 18./19.1.2014, S. 54. Vgl. auch FRA, Gewalt gegen Frauen, 03/2014, S. 13, wonach die Polizei routinemäßig Fälle aufgreifen und untersuchen soll, in denen Cyber-Stalking relevant ist (abrufbar unter:http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance_de_0.pdf.).

[581] Siehe zum Einsatz der Social Media zur „Online-Fahndung" auch Schulz, Kap. 10 Rn. 24 ff.

[582] Vgl. hierzu: Rosengarten/Römer, NJW 2012, 1764; Brenneisen/Staack, Kriminalistik 2012, 627.

[583] Vgl. Brenneisen/Staack, Kriminalistik 2012, 627 (628); BVerfG, NJW 2008, 822 (825 ff., Tz. 181 ff.).

[584] BVerfG, NJW 2008, 822 (827, Tz. 201).

Grundrechtsrelevanz der Maßnahme vorliege. Dazu zähle die reine **Internetaufklärung** ebenso wie grundsätzlich das Herstellen einer Kommunikationsverbindung mit einem Grundrechtsträger unter einer Legende.[585]

334 Dagegen liege ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn es sich um **gezieltes Zusammentragen, Speichern und gegebenenfalls Auswerten** von allgemein zugänglichen Informationen **mit polizeilicher Zielrichtung** handelt und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Die Herstellung einer Kommunikationsverbindung mit einem Grundrechtsträger unter einer Legende, die an sich noch nicht grundrechtsrelevant sei, erreiche diesen Status dann, wenn der Vorgang unter Ausnutzung eines schutzwürdigen Vertrauens in die Identität oder Motivation des Gesprächspartners geschehe, um persönliche Daten zu erheben, die ansonsten der Behörde nicht zugänglich gemacht würden.[586]

335 Folgt man dem BVerfG, bedarf es für viele Ermittlungsmaßnahmen im Internet mangels Grundrechtsrelevanz keiner gesetzlichen Grundlage. Einer solchen Grundlage bedürfte es dementsprechend selbst beim Einsatz eines Verdeckten Ermittlers erst dann, wenn es dabei zu einem **Vertrauensmissbrauch** gegenüber dem Grundrechtsträger komme.[587]

336 Diese Grundsätze lassen sich auf verdeckte Ermittlungen in sozialen Netzwerken übertragen.[588] Sind Informationen in diesen Netzwerken **öffentlich zugänglich**, d. h. für jeden angemeldeten Nutzer[589] sichtbar,[590] und sind (außer der Anmeldung zum jeweiligen sozialen Netzwerk) keine Zugangshindernisse für die Kenntnisnahme zu überwinden, so ist ein Eingriff in Grundrechte der Betroffenen zu verneinen.[591] Die Annahme einer Vertrauensbasis schon allein dadurch, dass die Teilnahme an sozialen Netzwerken nur nach vorheriger Registrierung möglich ist, erscheint jedenfalls zweifelhaft.[592]

337 Werden Daten gezielt zusammengetragen oder gespeichert, wäre ein Eingriff in die vorgenannten grundrechtsrelevanten Positionen dagegen zu bejahen. Gleiches gilt auch dann, wenn **nicht-öffentliche Daten** erhoben werden, d. h. Daten, die nur einem **individuell überprüfbaren Personenkreis** zugänglich gemacht werden, wenn also der verdeckt ermittelnde Beamte unter Verwendung der Identität einer realen Person in Kontakt zum Betroffenen tritt. Die vom BVerfG geforderte

---

[585] Vgl. BVerfG, NJW 2008, 822 (836, Tz. 307 ff.). Siehe dazu auch Schön, Ermittlungsmaßnahmen über das Internet, S. 84 ff.

[586] Vgl. BVerfG, NJW 2008, 822 (836, Tz. 309 f.).

[587] Vgl. Rosengarten/Römer, NJW 2012, 1764 (1766).

[588] Siehe Brenneisen/Staack, Kriminalistik 2012, 627 (629); vgl. auch Wernert, Internet Kriminalität, S. 148 f.

[589] Dazu, dass etwaige Zugangsbeschränkungen wie allgemeine Anmeldeverfahren noch nicht per se die öffentliche Zugänglichkeit aufheben: Henrichs, Kriminalistik 2011, 622 (624 f.).

[590] Instruktiv zur Begriffsbestimmung; Henrichs, Kriminalistik 2011, 622 (623 f.).

[591] Ostendorf et al., NStZ 2012, 529 (537).

[592] So Sieber, Gutachten 69. DJT, C 126.

täuschungsbedingte Vertrauenseinbuße liegt immer dann vor, wenn beim Betroffenen eine durch die Polizei verursachte Fehlvorstellung darüber entsteht, wer sein Gegenüber im Netz ist.[593]

7.6.2.3 Erscheinungsformen verdeckter Ermittlungen

338 Angesicht spezifischer Eigentümlichkeiten und Besonderheiten des Internet („Nicknames") in Hinblick auf die eingeschränkte Schutzwürdigkeit von Kommunikationspartnern,[594] erscheint es immerhin erwägenswert, bezüglich der Rechtsgrundlage polizeilicher Ermittlungsmaßnahmen in sozialen Netzwerken, abgesehen von der auf das schutzwürdige Vertrauen der Betroffenen abstellenden Rechtsprechung des BVerfG, stärker auf die Art der konkreten Ermittlungsmaßnahme abzustellen.[595]

339 Hinsichtlich der Art und Weise verdeckter Ermittlungen in sozialen Netzwerken lassen sich zwei Arten feststellen. Zum einen das sog. **passiv-rezeptive Erheben von Daten**:[596] dabei kommt es zu keinerlei aktivem Tun der Ermittlungsbehörden, sondern, wie schon aus dem Wort „passiv" zu schließen ist, auf die rein passive Entgegennahme von Daten. Dies geschieht zumeist in Form einer anlassunabhängigen Recherche, die der vorbereitenden oder vorbeugenden Gefahrenabwehr oder der Erstellung eines Lagebildes dient oder die im Rahmen von Initiativermittlungen erfolgt.[597] Während das Bundeskriminalamt soziale Netzwerke dabei nur fallbezogen nutzt, verwendet etwa die Polizei des Landes Nordrhein-Westfalen selbst entwickelte Recherchetools.

340 Bei der sog. **aktiv-rezeptiven Interaktion** geht die Polizei gezielt die Interaktion mit anderen Nutzern ein, um notwendige Daten zu erheben.[598] Dieses aktive Ermitteln kann wiederum auf unterschiedliche Art und Weise geschehen. Entweder es werden gezielt konkrete Personen angesprochen, die im Fokus der Ermittlungen stehen oder die Person nimmt an einer Gruppenkonversation teil und richtet die Ansprache an die gesamte Gruppe.

341 Dieser Ansatz und die mit ihm verbundenen Unterscheidungskriterien scheinen plausibler und vor allem in der Praxis besser geeignet zu sein für die Entscheidung der Frage nach der Notwendigkeit einer Ermächtigungsgrundlage als der etwas nebulöse Gedanke des BVerfG von einem „Vertrauensmissbrauch".

---

[593] Ähnlich auch: Biemann, „Streifenfahrten" im Internet, S. 146 f.; vgl. auch Körffer, in: Willert/Bohrer, Soziale Netzwerke, S. 137, 138 ff.
[594] Vgl. Henrichs, Kriminalistik 2012, 632 (633).
[595] Vgl. nochmals Schulz, Kap. 10 Rn. 24 ff.
[596] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30 (35).
[597] Vgl. Meyer, Kriminalistik 2012, 759 (761).
[598] Vgl. Meyer, Kriminalistik 2012, 759 (762); zur Nutzung einer „Legende" oder eines „fremden" Accounts siehe Schulz/Hoffmann, DuD 2012, 7 (12 f.).

7.6.2.4 Ermächtigungsgrundlage: §§ 110a ff. StPO/§§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 1 StPO

342 Eine spezielle gesetzliche Regelung für verdeckte Ermittlungen in sozialen Netzwerken existiert derzeit nicht. Grundsätzlich kommen für solche Maßnahmen die für den Einsatz Verdeckte Ermittler geschaffenen Vorschriften der §§ 110a ff. StPO in Betracht. Darüber hinaus wären ein auf die Ermittlungsgeneralklausel (§§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 1 StPO) gestützter Einsatz eines „nicht offen ermittelnden Polizeibeamten" (NoeP) oder die Annahme einer Durchsuchung gemäß §§ 102 f. i. V. m. §§ 110, 94 ff. StPO denkbar.[599]

343 Damit Polizeibeamte als **Verdeckte Ermittler** (zur Definition: § 110a Abs. 2 StPO) tätig werden können, müssen bestimmte Voraussetzungen vorliegen. Wurde der VE-Einsatz noch bis 1992 auf die Ermittlungsgeneralklausel gestützt,[600] sind die Voraussetzungen seither in den §§ 110a ff. StPO geregelt. Nach § 110a Abs. 1 StPO darf ein VE nur eingesetzt werden, wenn es sich um eine erhebliche Straftat auf den in den § 110a Abs. 1 Nr. 1 u. 2 StPO genannten Gebieten handelt oder wenn diese Straftat gewerbs- oder gewohnheitsmäßig oder von einem Bandenmitglied oder in anderer Weise organisiert begangen worden ist (§ 110a Abs. 1 Nr. 3 u. 4 StPO). Zur Aufklärung von Verbrechen darf ein VE auch eingesetzt werden, wenn Wiederholungsgefahr besteht (§ 110a Abs. 1 S. 2 StPO). Sein Einsatz ist jedoch nur zulässig, wenn die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre (Subsidiaritätsklausel, § 110a Abs. 1 S. 3 StPO).

344 Gemäß § 110b Abs. 1 S. 1 StPO ist der Einsatz eines VE grundsätzlich nur mit (d. h. nach) Zustimmung der Staatsanwaltschaft möglich (Ausnahme: Gefahr im Verzug, § 110b Abs. 1 S. 2 StPO). Einsätze gegen einen bestimmten Beschuldigten sowie Einsätze, bei denen ein VE Wohnungen betreten muss, welche nicht allgemein zugänglich sind, bedürfen der Zustimmung des Gerichts (Ausnahme: Gefahr im Verzug, § 110b Abs. 2 S. 1, 2 StPO).

345 Die **Befugnisse** eines VE sind in § 110c StPO geregelt. Dem VE ist es gestattet, eine Wohnung unter seiner Legende mit dem Einverständnis des Berechtigten zu betreten (§ 110c S. 1 StPO). Im Übrigen richten sich die Befugnisse eines VE nach der StPO und anderen Rechtsvorschriften (Satz 3). Damit sind z. B. die §§ 102, 103, 127 Abs. 2 StPO unter den dort genannten Voraussetzungen gemeint oder Polizeigesetze (z. B. § 20g Abs. 4 BKAG) oder sonstige Gesetze (z. B. § 4 Abs. 2 BtMG).[601] Nicht gestattet ist es dem VE, Straftaten zu begehen, auch wenn es sich dabei um milieubedingte Kriminalität handelt.

346 In Bezug auf soziale Netzwerke ist zu beachten, dass die Teilnahme von Beamten unter ihrer Legende an einer Kommunikation in einer geschlossenen Benutzergruppe und unter Benutzung von Zugangsschlüsseln, die sie ohne Zustimmung eines anderen Kommunikationsteilnehmers betreten haben, nur rechtmäßig ist, wenn die

---

[599] So auch Ostendorf et al., NStZ 2012, 529 (537).
[600] Vgl. Wolter, in: SK-StPO, § 110a Rn. 1.
[601] Vgl. Meyer-Goßner/Schmitt, § 110c Rn. 3.

Voraussetzungen der §§ 110a ff. StPO bzw. §§ 20 Abs. 1, 20g Abs. 2 Nr. 5 des BKAG vorliegen.[602]

Abzugrenzen ist der VE vom „**nicht offen ermittelnden Polizeibeamten**“ **(noeP)**, der nur gelegentlich und gerade nicht unter einer Legende auftritt (hierfür sind die strengeren §§ 110a ff. StPO spezieller), wenn auch unter falschem Namen.[603] Ein typisches Beispiel sind sog. Schein(auf)käufer, etwa im Drogenmilieu. Die Rechtsfigur des noeP wird im Hinblick auf Ermittlungen im Internet durch die neue Komponente, des „virtuell nicht offen ermittelnden Polizeibeamten“, ergänzt.[604] Speziell gesetzlich geregelt ist der Einsatz eines (v)noeP nicht. Dieser wird bislang nach ständiger, wenngleich äußerst bedenklicher Rechtsprechung (ohne Rückgriff auf die §§ 110a ff. StPO) auf der Grundlage der Ermittlungsgeneralklauseln der §§ 161, 163 StPO für zulässig gehalten.[605] Für die derzeitige Praxis enthält **Anlage D der RiStBV** Richtlinien über die Inanspruchnahme von Informanten sowie über den Einsatz von Vertrauenspersonen und Verdeckten Ermittlern im Rahmen der Strafverfolgung – allerdings ohne konkrete Vorgaben für den Einsatz in sozialen Netzwerken, der angesichts der mit dieser Einsatzform verbundenen Spezifika zu erwarten wäre und daher im Rahmen einer Nachbesserung zu fordern ist. **347**

Allenfalls dann, wenn sich ein „noeP“ in einem sozialen Netzwerk zwar verdeckt, aber unter seiner wahren Identität (d. h. ohne Legende i. S. v. § 110a StPO) anmeldet (was aber ermittlungstaktisch schnell an Grenzen führt), können die von ihm gewonnenen Informationen in einem späteren Strafverfahren verwertet werden. Handelt er allerdings unter den formellen Voraussetzungen eines Verdeckten Ermittlers, müssen die Voraussetzungen des § 110a StPO vorliegen, um die erhaltenen Informationen verwerten zu können (siehe Rn. 349 ff.). **348**

7.6.2.5 Abgrenzung der Eingriffsqualität der Maßnahme: Verdeckter Ermittler (VE)/noeP

Eine Ansicht sieht in verdeckten Ermittlungen im Internet **keinen Einsatz eines VE** i. S. v. § 110a StPO.[606] Zum einen wird dieser Ansatz darauf gestützt, dass bei der Kommunikation im Internet tatsächlich nur Daten von Rechner zu Rechner übertragen werden und die Teilnehmer sich nicht körperlich begegnen, sie also selbst bei einer Identifizierung von Name, E-Mail-Adresse oder Rechnerkennung als Person „anonym bleiben“[607], was den Teilnehmern selbst bewusst sei. Aufgrund dessen, dass **349**

[602] Vgl. BT-Drs. 17/6587 v. 14.7.2011, S. 3 f; Kritisch: Weiß, Kriminalistik 2014, 335 (336).
[603] Vgl. Meyer-Goßner/Schmitt, § 110a Rn. 4; Ostendorf et al., NStZ 2012, 529 (537).
[604] Vgl. Henrichs, Kriminalistik 2012, 632 (633).
[605] Vgl. Löffelmann, in: AnwK-StPO, § 110a Rn. 7; siehe dazu BGH, NJW 1997, 1516 (1518).
[606] Vgl. Meyer-Goßner/Schmitt, § 110a Rn. 4.
[607] Nack, in: KK-StPO, § 110a Rn. 7.

die Anonymität beibehalten werde, sei auch ein Eintritt in soziale Netzwerke grundsätzlich noch kein Eingriff in Grundrechte, mit der Folge, dass auch die strengen Voraussetzungen der §§ 110a ff. StPO nicht zur Anwendung kommen müssten.[608]

350 Nach anderer Ansicht, ist die **Eingriffsqualität der Maßnahme** am Einzelfall zu bestimmen. Gewisse Indikatoren sollten dabei berücksichtigt werden: Intensität der Zugangskontrolle, die mit der Legende überwunden wird, Dauer der Ermittlungen mit Legende, Art der Beteiligung (passiv-rezeptiv oder aktiv-rezeptiv).[609] Sobald all diese Faktoren immer intensiver, länger oder aktiver werden, sind die Voraussetzungen der §§ 110a ff. StPO zu erfüllen, denn desto eher handelt der Ermittler als VE i. S. d. § 110a StPO.[610]

351 Die **Abgrenzung** des noeP vom VE ist dementsprechend danach vorzunehmen, ob es sich im konkreten Fall nur um vereinzelte Einsätze handelt, ob es nötig ist, unter einer Legende die Mitmenschen und Kollegen zu täuschen, ob hierdurch eine Gefährdung des allgemeinen Rechtsverkehrs besteht oder ob abzusehen ist, dass der ermittelnde Beamte auch künftig unter einer Legende auftreten muss.[611]

351 Der in der Praxis übliche Fall wird der sein, dass der im Internet ermittelnde Beamte als sog. „nicht offen ermittelnder Polizeibeamter" (noeP) tätig wird, sodass sich sein Ermitteln rein auf die Ermittlungsgeneralklauseln stützt. Das vom BVerfG angesprochene schutzwürdige Vertrauen und der damit einhergehende Einsatz eines VE können aber je nach Fallgestaltung durchaus tangiert sein.

7.6.2.6 Sonderfall: Onlinedurchsuchung

352 Eine in diesem Zusammenhang diskutierte verdeckte Online-Durchsuchung[612] (dabei wird dem Verdächtigen ein dafür konzipiertes Computerprogramm zugespielt, mit dessen Hilfe auf die Speichermedien seines Computers zurückgegriffen werden kann) ist auf **Grundlage der §§ 102 i. V. m. 110, 94 ff. StPO** nicht zulässig.[613] Zum einen dürfen die Sicherungsmechanismen der §§ 105 Abs. 2 und 106 Abs. 1 StPO nicht umgangen werden. Sie regeln die Art und Weise der Durchsuchung und sind – anders als bloße Ordnungsvorschriften – zwingend zu beachten. Deshalb ist es

---

[608] Vgl. Nack, in: KK-StPO, § 110a Rn. 7.
[609] Vgl. Rosengarten/Römer, NJW 2012, 1764 (1767).
[610] Sieber, Gutachten 69. DJT, C 126, sieht wegen des gesteigerten Täuschungscharakters verdeckte Ermittlungen im Netz nicht als von § 110a StPO gedeckt an, weil eine Vertrauensbeziehung ausgenutzt werde; im Ergebnis so auch Ostendorf et al., NStZ 2012, 529 (537).
[611] Vgl. Rosengarten/Römer, NJW 2012, 1764 (1765).
[612] Eingehend zur Terminologie und den Unterkategorien Onlineüberwachung und Onlinedurchsicht bzw. der Unterscheidung von Online-Durchsuchung und Quellen-TKÜ sowie den technischen Möglichkeiten: Schön, Ermittlungsmaßnahmen über das Internet, S. 108 ff. Zur Grundrechtsrelevanz: Schön, Ermittlungsmaßnahmen über das Internet, S. 130 ff.
[613] Vgl. BGH, NJW 2007, 930. Dazu auch Schön, Ermittlungsmaßnahmen über das Internet, S. 190 ff.

Ermittlungsbehörden nicht gestattet, eine grundsätzlich richterlich zu genehmigende Durchsuchungsanordnung bewusst heimlich durchzuführen.[614]

Auch systematische Erwägungen sprechen gegen die Zulässigkeit einer Online-Durchsuchung auf der Grundlage von § 102 StPO. Grundrechtsintensive Ermittlungsmaßnahmen, die auch heimlich stattfinden können, sind in §§ 100a bis 100i StPO geregelt. Gerade wegen dieser Heimlichkeit gelten besondere formelle und materielle Voraussetzungen. Für die Rechtmäßigkeit einer in § 102 StPO geregelten „offenen" Durchsuchung gelten weitaus weniger strenge Voraussetzungen. **353** **354**

Auch **§ 110 Abs. 3 StPO** ist keine taugliche Rechtgrundlage. Sie erlaubt gerade nicht den heimlichen, externen Zugriff auf gespeicherte Daten ohne Kenntnis des Adressaten der Maßnahme, sondern lediglich die – offene – Durchsicht von Daten, die sich auf externen Speichermedien befinden, auf die der Betroffene Zugriff hat. Die Regelung soll der Gefahr des Beweismittelverlusts vorbeugen. Erlaubt ist daher zunächst die Durchsicht des externen Speichers, um festzustellen, ob dort beweisrelevante Daten gespeichert sind. Entsprechende Daten dürfen nach § 110 Abs. 3 S. 2 StPO gesichert werden.[615] Aufgrund der Akzessorietät der Durchsicht zur Durchsuchung nach §§ 102 ff. StPO ist nur eine punktuelle, einmalige Durchsicht der Daten möglich und nicht das mehrmalige Einloggen zum Zwecke der Durchsicht.[616] Neben den in sozialen Netzwerken enthaltenen Daten können mittels § 110 Abs. 3 StPO auch Daten in sogenannten „Cloud"-Speichern durchgesehen werden.[617] Für eine verdeckte Onlinedurchsuchung bleibt der Anwendungsbereich des § 110 Abs. 3 StPO allerdings verschlossen.

§ 100a StPO kann mangels vorliegender Telekommunikation eine Online-Durchsuchung ebenfalls nicht rechtfertigen.[618] Die Anwendbarkeit von **§ 100c StPO** scheitert an der Tatsache, dass ein Computer durchsucht wird und nicht das in einer Wohnung nicht öffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden soll. Ebenso kann auch **§ 100f Abs. 1 StPO** nicht als Ermächtigungsgrundlage dienen. **355**

Auf die Generalklausel des **§ 161 StPO** kann die Maßnahme offensichtlich schon wegen der erheblichen Eingriffsintensität nicht gestützt werden.[619] **356**

---

[614] Vgl. BGH, NJW 2007, 930 (931 Rn. 9).
[615] Vgl. etwa bei Schön, Ermittlungsmaßnahmen über das Internet, S. 176 ff.
[616] Brodowski/Eisenmenger, ZD 2014, 119 (124).
[617] Brodowski/Eisenmenger, ZD 2014, 119 (125).
[618] Siehe auch Schön, Ermittlungsmaßnahmen über das Internet, S. 183 ff.; Körffer, in: Willert/Bohrer, Soziale Netzwerke, S. 137 (142 f.).
[619] Vgl. Schön, Ermittlungsmaßnahmen über das Internet, S. 194. Siehe auch Schön, Ermittlungsmaßnahmen über das Internet, S. 221 ff. zu landesrechtlichen Versuchen zur Regelung der Online-Durchsuchung.

7.6.3 Öffentlichkeitsfahndung (§§ 131 ff. StPO)

7.6.3.1 Notwendigkeit der Öffentlichkeitsfahndung aus kriminalistischer Perspektive

357 Eine breite Öffentlichkeit wird von den Ermittlungsbehörden zunehmend auch als Mittel der Verbrechensaufklärung interpretiert. Aus kriminalistischer Perspektive sprechen mehrere Gründe für die Notwendigkeit einer Ausweitung der in den §§ 131 ff. StPO geregelten Öffentlichkeitsfahndung auf soziale Netzwerke. Zum einen kann sich auch die Polizei in der Wahl ihrer Fahndungsmethoden nicht dem **Wandel der Zeit** entziehen. Klassische Medien, wie Zeitung und Rundfunk, aber auch die üblichen Fahndungsplakate erreichen immer weniger Menschen.[620] Das tägliche Leben spielt sich zunehmend „online" ab, was sich auch anhand der steigenden Internetnutzer und vor allem der Nutzer sozialer Netzwerke erkennen lässt, die letztendlich die Zielgruppe der meisten Fahndungsaufrufe sind.[621] Ebenso ist die im Internet im Vergleich zu den herkömmlichen Medien deutlich höhere Geschwindigkeit zu berücksichtigen, mit der die Polizei fallrelevante Informationen verbreiten kann.[622] Zudem ist die Öffentlichkeitsfahndung via sozialer Netzwerke auch flexibler und damit effizienter, da die Polizei bezüglich Zeitpunkt und Form selbst entscheiden kann, wie ein Fahndungsaufruf vonstatten gehen soll.[623]

358 Die Öffentlichkeitsfahndung in sozialen Netzwerken eröffnet den Ermittlungsbehörden jedoch nicht nur eine größere Aufmerksamkeit für ihre Arbeit auf Seiten der Benutzer, sondern ist für die Polizei auch insofern von großer Bedeutung, als sie soziale Netzwerke selbst als „**Fundgrube an Textinformationen, Bilder oder Videos**"[624] für ihre Ermittlungen nutzen kann. Die Fahndung via sozialer Netzwerke konnte bereits beachtliche Erfolge in Form der Aufklärung von Straftaten verzeichnen, sodass aus kriminalistischer Perspektive eine Notwendigkeit für sie durchaus gegeben ist.[625]

359 Allerdings sollten bei der Ausgestaltung der Öffentlichkeitsfahndung die üblichen Voraussetzungen eingehalten und **rechtsstaatliche Grundsätze** gewahrt werden. Darunter ist beispielsweise zu verstehen, dass bei der Schilderung des Sachverhalts

---

[620] Vgl. Brodowski, Verbrechersuche im sozialen Netz, in: Legal Tribune Online v. 15.11.2012 (http://www.lto.de/recht/hintergruende/h/facebook-fahndung-und-datenschutz-thema-auf-justizministerkonferenz/), vgl. Meyer, Kriminalistik 2012, 759 (761). Vgl. auch Schön, Ermittlungsmaßnahmen über das Internet, S. 212 ff.

[621] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30; vgl. Irlbauer, Kriminalistik 2012, 764 (766); Fuchs, Kriminalistik 2013, 185 (190).

[622] Vgl. Meyer, Kriminalistik 2012, 759 (761).

[623] Vgl. Irlbauer, Kriminalistik 2012, 764 (766).

[624] Henrichs/Wilhelm, Kriminalistik 2010, 30 (32). Vgl. aber zu den Gefahren, die andererseits dadurch entstehen, dass auch das polizeiliche Gegenüber diese Netzwerke nutzt und so insbesondere Mitarbeiter der Polizei identifizieren kann: Neß, Kriminalistik 2013, 516, auch zur Sorglosigkeit vieler Polizeibeamter gegenüber dem Schutz der eigenen Daten.

[625] Vgl. BfDI, Öffentlichkeitsfahndung via Facebook, ZD-Aktuell 2012, 2705; Fuchs, Kriminalistik 2013, 185 (190).

zu vermeiden ist, dass der Täter mehr über den Stand der Ermittlungen erfährt, als zwingend notwendig ist, dass Täterwissen preisgegeben wird oder auch Formalien wie Fahndungsaufrufe, die kurz und eindeutig sein sollten, gegebenenfalls mehrsprachig zu formulieren.[626]

Folglich ist daher die noch vorhandene Zurückhaltung bezüglich der Öffentlichkeitsfahndung in sozialen Netzwerken, wie sie vor allem in Deutschland vorherrscht, aufzugeben und die dadurch eröffnete Möglichkeit effektiverer Ermittlungen wahrzunehmen.[627] **360**

7.6.3.2 Wesentliche Voraussetzungen

Eine spezifische gesetzliche Regelung für die Fahndung nach Personen oder Sachen gerade via Internet fehlt in der StPO. Die Zulässigkeit einer solchen Fahndungsmethode nach Personen wird daher auf die §§ 131 ff. StPO gestützt, welche unter anderem die *Öffentlichkeits*fahndung regeln und sich nicht auf bestimmte Medien/Techniken beschränken und eben auch das Internet vorsehen.[628] § 131 StPO regelt die Ausschreibung eines Beschuldigten zur Festnahme, während § 131a StPO die Ausschreibung eines Beschuldigten oder Zeugen zur Aufenthaltsermittlung normiert.[629] § 131b StPO hat die Veröffentlichung von Abbildungen eines Beschuldigten oder Zeugen zur Identitäts- und Aufklärungsfahndung zum Gegenstand. **361**

Die von der StPO erlaubten Ermittlungsmethoden sind – soweit nicht eine spezielle Art und Weise ihrer Vornahme vorgeschrieben ist – grundsätzlich „**technikneutral**“[630]. § 131a Abs. 5 StPO nimmt daher auf alle Fahndungshilfsmittel der Strafverfolgungsbehörden Bezug. **362**

Voraussetzung für eine Öffentlichkeitsfahndung – § 131 Abs. 3 StPO (Ausschreibung zur Festnahme), § 131a Abs. 3 StPO (Ausschreibung zur Aufenthaltsermittlung), Veröffentlichung von Abbildungen (§ 131b StPO) – ist stets, dass eine **Straftat von erheblicher Bedeutung** den Gegenstand des Strafverfahrens bildet. Darunter sind Straftaten im Bereich der mittleren Kriminalität zu verstehen, was eine Einzelfallprüfung erforderlich macht.[631] **363**

Andere Formen der Aufenthaltsermittlung müssen „erheblich weniger Erfolg versprechend oder wesentlich erschwert sein“ (§§ 131 Abs. 3, 131a Abs. 3 StPO; **Subsidiaritätsklausel**). **364**

---

[626] Vgl. Clages, Grundsätze der Kriminalpraxis, S. 267.
[627] Vgl. Fuchs, Kriminalistik 2013, 185 (189).
[628] Vgl. Hilger, in: LR-StPO, § 131 Rn. 17; Walther, in: AnwK-StPO, § 131 Rn. 10, § 131a Rn. 5; Paeffgen, in: SK-StPO, § 131 Rn. 6, § 131a Rn. 7.
[629] Ebenfalls erfasst ist bei *Beschuldigten* die Ausschreibung zur Sicherstellung eines Führerscheins, zur erkennungsdienstlichen Behandlung, zur Anfertigung einer DNA-Analyse oder zur Feststellung seiner Identität (§ 131a Abs. 2 StPO).
[630] Brodowski, Verbrechersuche im sozialen Netz, in: Legal Tribune Online v. 15.11.2012.
[631] Vgl. Hilger, in: LR-StPO, § 131 Rn. 18, § 131a Rn. 6, § 131b Rn. 3; Walther, in: AnwK-StPO, § 131 Rn. 11, § 131a Rn. 5, § 131b Rn. 3.

365 Für eine Öffentlichkeitsfahndung nach einem **Beschuldigten** gemäß §§ 131 Abs. 3[632], 131a Abs. 3 StPO muss zusätzlich ein dringender Tatverdacht vorliegen.

366 Gemäß §§ 131 Abs. 4 S. 1, 131a Abs. 4 S. 1 StPO muss der Beschuldigte möglichst genau bezeichnet und soweit erforderlich beschrieben werden, um eine mögliche Verwechslung mit einer anderen Person zu verhindern.[633] Zu diesem Zweck dürfen Abbildungen beigefügt werden. Eine konkrete Beschreibung der Tatumstände ist fakultativ.

367 § 131a Abs. 4 S. 2, 3, 4 StPO verlangen zudem, dass bei der Aufenthaltsermittlung eines Zeugen erkennbar gemacht wird, dass es sich nicht um den Beschuldigten handelt (Absatz 4 Satz 2). Neben diesem formellen Erfordernis ist in Absatz 4 Satz 3 ein materiell-rechtlicher Ausschließungsgrund normiert[634], welcher besagt, dass eine Öffentlichkeitsfahndung dann unterbleiben muss, wenn überwiegende schutzwürdige Interessen entgegenstehen. Absatz 4 Satz 4 enthält darüber hinaus eine Subsidiaritätsklausel bezüglich Abbildungen von Zeugen.

368 Bezüglich der **Anordnungskompetenzen** sind die §§ 131 Abs. 3, 131c Abs. 1 S. 1, Abs. 2 StPO zu beachten. Danach dürfen im Falle der §§ 131 Abs. 1, 2 StPO sowohl Richter als auch Staatsanwaltschaft Öffentlichkeitsfahndungen veranlassen (§ 131 Abs. 3 S. 1 StPO). Besonderheiten ergeben sich in Eilfällen gemäß § 131 Abs. 3 S. 2 StPO, wenn Gefahr in Verzug ist und weder Richter noch Staatsanwaltschaft erreichbar sind, sodass dann auch Ermittlungspersonen der Staatsanwaltschaft die Befugnisse aus § 131 Abs. 3 S. 1 StPO zustehen.

369 Gemäß § 131c Abs. 1 S. 1 StPO darf grundsätzlich nur der Richter, bei Gefahr im Verzug auch die Staatsanwaltschaft Fahndungen nach § 131a Abs. 3 StPO bzw. § 131b StPO anordnen. Für länger andauernde Veröffentlichungen sind die Besonderheiten des § 131c Abs. 2 StPO zu beachten, wonach es entweder einer richterlichen Bestätigung (§ 131c Abs. 2 S. 1 StPO) oder einer solchen durch die Staatsanwaltschaft bedarf (§ 131c Abs. 2 S. 2 StPO).

7.6.3.3 Probleme der Fahndung via Internet

370 Probleme bezüglich der Fahndung in sozialen Netzwerken ergeben sich zum einen aus den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV). **Nr. 39 RiStBV** verweist auf die §§ 131 ff. StPO. Gemäß **Nr. 3.2 der Anlage B der RiStBV (Richtlinien über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren)** ist es für die Öffentlichkeitsfahndung erlaubt und zweckmäßig, Fahndungsaufrufe

---

[632] Dieser verweist auf § 131 Abs. 1, 2 StPO, die ihrerseits auf die „Voraussetzungen eines Haftbefehls [...]" (§§ 112 ff. StPO) Bezug nehmen und damit auch die Voraussetzung des dringenden Tatverdachtes erfassen.

[633] Vgl. Hilger, in: LR-StPO, § 131 Rn. 27, § 131a Rn. 8; Walther, in: AnwK-StPO, § 131 Rn. 15, § 131a Rn. 6.

[634] Vgl. Hilger, in: LR-StPO, § 131a Rn. 9; Walther, in: AnwK-StPO, § 131a Rn. 6.

auf speziellen Seiten durchzuführen. Damit sind z. B. spezielle Fahndungsseiten der Polizei gemeint, die ausschließlich den Zweck haben, Informationen über den Gesuchten an die Öffentlichkeit weiterzugeben. Jedoch sollen private Internetanbieter grundsätzlich nicht eingeschaltet werden. Die Formulierung dieses grundsätzlichen Verbotes lässt jedoch Ausnahmen zu, sodass es doch zur Einschaltung privater Internetanbieter kommt. Eine Ausnahme, von der bereits Gebrauch gemacht worden ist, ist die Nutzung von Facebook als „Fahndungs-Portal". Das wohl bekannteste Beispiel liefert die Polizeidirektion Hannover, die ein eigenes Profil bei Facebook[635] für polizeiliche Ermittlungen erstellt hat.[636]

Zum anderen entstammen die §§ 131 ff. StPO in der jetzigen Fassung dem **371**
Strafverfahrensänderungsgesetz von 1999.[637] Zu diesem Zeitpunkt konnte der Gesetzgeber ein Medium wie Facebook und dessen Reichweite nicht vorhersehen, sodass die §§ 131 ff. StPO nicht auf dem neuesten technischen Stand sind. Zwar hatte man damals ein Medium wie das Internet schon berücksichtigt, jedoch beschränkte sich die Nutzung des Internet zum damaligen Zeitpunkt darauf, dass dort auffindbare Inhalte per Abruf genutzt werden konnten, eine Interaktivität des Internetnutzers, wie sie heute stattfindet, war nicht ersichtlich geschweige denn vorhersehbar.[638] Genau diese Interaktivität der Internetnutzer, die Informationen in einer unvorhersehbaren Geschwindigkeit weiterleiten können, hatte der Gesetzgeber bei der Änderung/Schaffung der §§ 131 ff. StPO nicht im Auge.

7.6.3.4 Risiken bezüglich des Datenschutzes

Auch bei Öffentlichkeitsfahndungen in sozialen Netzwerken gelten die allgemeinen **372**
Grundsätze des Datenschutzes, also insbesondere die Achtung des **Rechts auf informationelle Selbstbestimmung**, was sich darin widerspiegelt, dass bezüglich der Verarbeitung und Nutzung personenbezogener Daten ein grundsätzliches Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG) gilt.[639]

Risiken bezüglich des Datenschutzes ergeben sich zum einen daraus, dass selbst **373**
bei der ordnungsgemäßen Löschung etwa eines Facebook-Kontos nicht alle Inhalte gelöscht werden können, da z. B. eine Verlinkung durch einen anderen Facebook-Nutzer unabhängig vom eigenen Konto existiert und somit trotz Löschung bestehen bleibt.[640] Dies ist gerade dann problematisch, wenn sich die Fahndung erledigt hat

---

[635] Vgl. http://de-de.facebook.com/PolizeiHannover.
[636] Vgl. Brodowski, Verbrechersuche im sozialen Netz, in: Legal Tribune Online v. 15.11.2012; Rammo, Polizeiliche Ermittlungen bei Facebook, in: Taeger, Die Welt im Netz – Tagungsband Herbstakademie 2011, S. 279 (280).
[637] Vgl. Paeffgen, in: SK-StPO, § 131 Rn. 1.
[638] Vgl. Henrichs/Wilhelm, Kriminalistik 2010, 30.
[639] Vgl. Holznagel et al., Telekommunikationsrecht, Rn. 651–663.
[640] Vgl. Datenverwendungsrichtlinie Facebook: http://de-de.facebook.com/full_data_use_policy #deleting.

und die Öffentlichkeitsfahndung via Facebook umgehend zu beenden ist.[641] In sozialen Netzwerken kommt es eben gerade auf größtmögliche Interaktivität an. Wenn nun Facebook-Nutzer das Fahndungsplakat der Polizei teilen, was zu dessen schneller Verbreitung und Bekanntheit führt und eben das Ziel der Fahndungsmaßnahme ist, können die Polizeidienststellen nicht mehr kontrollieren, ob diese Nutzer datenschutzrechtliche Vorkehrungen treffen, wie z. B. das Unterbinden bedenklicher Kommentare.[642] Die Kontrolle der Polizei bezüglich der Fahndungsmeldungen und Abbildungen ist damit nicht mehr in ihrer Hand, auch wenn sie ggf. das alleinige Nutzungsrecht an den betroffenen Abbildungen hat.[643]

374 Des Weiteren ließe sich argumentieren, dass eine Fahndung über Facebook aufgrund dessen, dass die Daten an einen Server in den USA übermittelt und dort seitens Facebook ausgewertet werden, nicht von § 131a Abs. 3 StPO gedeckt ist. Es besteht rechtlich gesehen ein Unterschied, ob Daten durch eine Behörde in Deutschland selbst veröffentlicht werden (was nach § 131a Abs. 3 StPO zulässig ist) und dadurch für Dritte verfügbar werden, jedoch nicht durch die Behörde aktiv weitergegeben, sondern nur zum Zwecke der Fahndung veröffentlicht werden, oder ob Daten tatsächlich an Dritte, wie z. B. Facebook, übermittelt oder ihnen zur Auftragsdatenverarbeitung überlassen werden. Diese Übermittlung und die anschließende Verarbeitung der Daten werden datenschutzrechtlich gesondert erfasst, ihre Zulässigkeit hat sich an eigenen rechtlichen Voraussetzungen zu orientieren. § 131a Abs. 3 StPO ist insoweit zu unspezifisch.[644]

375 Hinzuweisen ist auch darauf, dass einmal ins Netz gestellte Daten für immer online auffindbar sind, sodass ein über soziale Netzwerke gesuchter Tatverdächtiger trotz einer später erwiesenen Unschuld meist mit negativen Konsequenzen rechnen muss. Es bleibt die Erkenntnis, dass jede Veröffentlichung im Internet eine große Gefahr für das Recht auf informationelle Selbstbestimmung darstellt („**Das Netz vergisst nichts**“) und Beiträge im Internet kaum widerrufbar, geschweige denn vor unbefugten Dritten sicher sind.[645]

376 Die Justizministerkonferenz plant eine **Änderung der Anlage B der RiStBV**, um eine geeignete Grundlage im Hinblick auf die Öffentlichkeitsfahndung in sozialen Netzwerken zu schaffen, die sowohl datenschutzrechtlichen als auch rechtsstaatlichen Grundsätzen genügen soll.[646]

---

[641] Vgl. Irlbauer, Kriminalistik 2012, 764 (766).
[642] Vgl. Hawellek/Heinemeyer, ZD-Aktuell 2012, 2730.
[643] Vgl. Irlbauer, Kriminalistik 2012, 764 (766).
[644] Vgl. Hawellek/Heinemeyer, ZD-Aktuell 2012, 2730.
[645] Vgl. Paeffgen, in: SK-StPO, § 131 Rn. 6, § 131a Rn. 7.
[646] Beschluss der 84. Konferenz der Justizministerinnen und Justizminister 2013, TOP II.2, Nr. 2.

7.7 Sanktionsrechtliche Fragestellungen

Die Nutzung sozialer Netzwerke ist nicht nur auf Tatbestandsebene relevant, sondern kann auch auf Rechtsfolgenseite interessante Fragen aufwerfen. So ist ein 21-jähriger Student vom AG München am 24.3.2014 wegen Nötigung und Bedrohung jugendlicher Mädchen in sozialen Medien neben stationären Maßnahmen u. a. zu einem **halbjährigen Facebook-, Whatsapp- und Instagramverbot** verurteilt worden.[647] Ob eine solche Weisung (§ 10 JGG) hinreichend bestimmt ist, geschweige denn die beabsichtigte erzieherische Wirkung entfalten und auf diese Weise weiteren Übergriffen in sozialen Netzwerken vorgebeugt werden kann, ist nicht zuletzt wegen ihrer kaum durchführbaren Kontrolle äußerst fraglich. **377**

Sanktionsrechtlich interessant ist schließlich auch die Fragestellung, welche Rechtsgrundlage für eine staatliche angeordnete **Löschung strafbarer Inhalte** Anwendung findet. Eine Anwendung von §§ 74, 74d StGB sowie § 111b StPO scheitert daran, dass „Daten" nicht vom Wortlaut der Vorschriften umfasst sind.[648] Allenfalls eine Beschlagnahme des Datenträgers kommt unter den Voraussetzungen des § 74d i. V. m. § 11 Abs. 3 StGB in Betracht, da es sich bei Servern um Datenspeicher nach § 11 Abs. 3 StGB handelt.[649] **378**

7.8 Fazit und Ausblick

Am Arbeitsplatz, in der Schule und zur Überbrückung großer räumlicher Distanzen zwischen Freunden oder Familienmitgliedern wird das Internet rege genutzt. Immer mehr Menschen registrieren sich in sozialen Netzwerken. Auch die Kriminalität nimmt in diesen Netzwerken beträchtlich zu. Für den Gesetzgeber, vor allem aber für die Strafverfolgungsbehörden und Gerichte stellen sich hier tagtäglich neue Herausforderungen. Herkömmliche Straftatbestände und strafprozessuale Ermittlungsmaßnahmen stoßen angesichts der Spezifika der Kommunikation über soziale Netzwerke an ihre Auslegungs- und damit Anwendungsgrenzen. Der Gesetzgeber ist aufgerufen, die Entwicklung kritisch im Auge zu behalten und bei entstehenden Strafbarkeitslücken – immer nach Maßgabe der Kriterien der Strafwürdigkeit und Strafbedürftigkeit des jeweils in Rede stehenden normabweichenden Verhaltens – über eine Anpassung der strafrechtlichen Bestimmungen nachzudenken. **379**

---

[647] Vgl. SZ v. 26.3.2014, S. 10; SZ v. 25.3.2014, 39.
[648] LG Hamburg, ZD 2014, 146 (146 f.).
[649] LG Hamburg, ZD 2014, 146 (147).

Literatur

Ambos, K. (2014). *Internationales Strafrecht*. 4. Aufl. München: C.H. Beck.

Auer-Reinsdorff, A. (2012). Technische Lösungen sowie Informationsangebote an Eltern, Schulen und Kinder. *FPR*, 434 ff.

Baeck, U., Winzer, T. (2010). BAG: Flash-Mob-Aktion nicht generell unzulässig. *NZG*, 100.

Bär, W. (2009). Anmerkungen zum Beschluss BGH 31.03.2009, Beschlagnahme von E-mails beim Provider. *NStZ*, 397 ff.

Bär, W. (2011). Transnationaler Zugriff auf Computerdaten. *ZIS*, 53 ff.

Bär, W. (2013). Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft, Auswirkungen auf die Praxis der Strafverfolgung. *MMR*, 700 ff.

Bauer, J.-H., Günther, J. (2013). Kündigung wegen beleidigender Äußerungen auf Facebook. *NZA*, 67 ff.

Baumann, J., Weber, U. & Mitsch, W. (2003). *Strafrecht Allgemeiner Teil*. 11. Aufl. Bielefeld: Verlag Ernst und Werner Gieseking.

Beck, S. M. (2008). Lehrermobbing durch Videos im Internet ein Fall für die Staatsanwaltschaft? *MMR*, 77 ff.

Beck, S. (2009). Internetbeleidigung de lege lata und de lege ferenda – Strafrechtliche Aspekte des „spickmich"-Urteils. *MMR*, 736 ff.

Beck, S. M., Kreißig, W. (2007). Tauschbörsen-Nutzer im Fadenkreuz der Strafverfolgungsbehörden. *NStZ*, 304 ff.

Bertram, G. (2005). Der Rechtsstaat und seine Volksverhetzungs-Novelle. *NJW*, 1476 ff.

Beukelmann, S. (2012). Surfen ohne strafrechtliche Grenzen. *NJW*, 2617 ff.

Biemann, J. (2013). *„Streifenfahrten" im Internet, Die verdachtsunabhängigen Ermittlungen der Polizei im Internet*. Stuttgart: Richard Boorberg Verlag.

BITKOM (Hrsg.) (2011). *Soziale Netzwerke, Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet*. 2., erweiterte Studie. Berlin: BITKOM.

Bornemann, R. (2012). Der „Verbreitungsbegriff" bei Pornografie in audiovisuellen Mediendiensten – Straferweiternd im Internet und strafverkürzend im Rundfunk? *MMR*, 157 ff.

Braun, F., Keller, C. (2014). Kinderpornographische Inhalte im Netz. *Kriminalistik*, 208.

Brenneisen, H., Staack, D. (2012). Die virtuelle Streife in der Welt der Social Media. *Kriminalistik*, 627 ff.

Brodowski, D. (2013). Anonyme Ehrverletzungen in Internetforen. *JR*, 513 ff.

Brodowski, D., Eisenmenger, F. (2014). Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden. *ZR*, 119 ff.

Brühl, F., Gräfin von, Brandenburg, A. (2013). Cyberbedrohungen: Rechtliche Rahmenbedingungen und praktische Lösungen. *ITRB*, 260 ff.

Bündnis gegen Cybermobbing e. V. (2012). *Gefangen im Netz, Initiative zur Bekämpfung der Ursachen und Auswirkungen von Mobbing, Gewalt und Aggression im Internet*. Abbrufbar unter: http://www.bündnis-gegen-cybermobbing.de/fileadmin/pdf/berlin/broschuere_120327.pdf.

Cirullies, M., Cirullies, B. (2013). *Schutz bei Gewalt und Nachstellung*. Bielefeld: Verlag Ernst und Werner Gieseking.

Clages, H. (2012). *Der rote Faden Grundsätze der Kriminalpraxis*. 12. Aufl. Heidelberg: C.F. Müller.

Clay, S. (2010). *Cybermob, Mobbing im Internet*. Würzburg: Arena Verlag.

Cornils, K. (1999). Der Begehungsort von Äußerungsdelikten im Internet. *JZ*, 394 ff.

Däubler, W. (2014). Ungeschminktes auf Facebook. *AiB*, 26.

Derksen, R. (1997). Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt. *NJW*, 1878 ff.

Dietel, A., Gintzel, K. & Kniesel, M. (2010). *Versammlungsgesetz. Kommentar*. 16. Aufl. Köln: Carl Heymanns Verlag.

Dölling, D., Duttge, G., Rössner, D. (Hrsg.) (2013). *Handkommentar Gesamtes Strafrecht*. 3. Aufl. Baden-Baden: Nomos.

Dreier, T., Schulze, G. (2013). *Kommentar zum UrhG*. 4. Aufl. München: C.H. Beck.
Duttge, G., Hörnle, T., Renzikowski, J. (2004). Das Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung. *NJW*, 1065 ff.
Eckstein, K. (2005). Grundlagen und aktuelle Probleme der Besitzdelikte EDV, EU, Strafrechtsänderungsgesetze, Konkurrenzen. *ZStW 117*, 107 ff.
Eckstein, K. (2011). Ist das „Surfen" im Internet strafbar? – Anmerkungen zum Urteil des OLG Hamburg vom 15.2.2010. *NStZ*, 18 ff.
Eisele, J. (2012). Tatort Internet: Cyber-Grooming und der Europäische Rechtsrahmen. In: E. Hilgendorf, R. Rengier (Hrsg.), *Festschrift für Wolfgang Heinz*. Baden-Baden: Nomos.
Eisele, J. (2013). *Computer- und Medienstrafrecht*. München: C.H. Beck.
Engel-Flechsig, S., Maennel, F. A., Tettenborn, A. (1997). Das neue Informations- und Kommunikationsdienste-Gesetz. *NJW*, 2981 ff.
Erbs, G., Kohlhaas, M. (Hrsg.) (2013). *Strafrechtliche Nebengesetze, Kommentar*. München: C.H. Beck.
Erb, V. u. a. (Hrsg.) (ab 2004). *Löwe-Rosenberg, Großkommentar StPO*. 26. Aufl. Berlin: De Gruyter.
Erdemir, M. (2003). Neue Paradigmen der Pornografie? – Ein unbestimmter Rechtsbegriff auf dem Prüfstand. *MMR*, 628 ff.
Ernst, C. (2011). Die öffentlich-rechtliche Behandlung von Flashmobs und die Zurechnung von Informationsflüssen. *DÖV*, 537 ff.
Esser, R. (2010). Urheberrechtsverletzungen durch Tauschbörsen im Internet – Zum Akteneinsichtsrecht des Verletzen nach § 406e StPO. *GA*, 65 ff.
Fawzi, N. (2009). *Cyber-Mobbing. Ursachen und Auswirkungen von Mobbing im Internet*. Baden-Baden: Nomos.
Fechner, F. (2014). *Medienrecht*. 15. Aufl. Tübingen: Mohr Siebeck.
Fezer, K-H. (2009). *Markenrecht. Kommentar*. 4. Aufl. München: C.H. Beck.
Fischer, T. (2013). *Strafgesetzbuch*. 60. Aufl. München: C.H. Beck.
Fuchs, B. (2013). Schutz und Sicherheit im digitalen Raum. *Kriminalistik*, 185 ff.
Fuchs, B. (2014). Schnittstellen der Sicherheitsarchitektur. *Kriminalistik*, 174.
Gazeas, N. (2007). Der Stalking-Straftatbestand – § 238 StGB (Nachstellung). *JR*, 497 ff.
Gercke, M. (2010). Die Entwicklung des Internetstrafrechts 2009/2010. *ZUM*, 633 ff.
Gercke, M. (2013). Die Entwicklung des Internetstrafrechts 2012/2013. *ZUM*, 605 ff.
Gercke, M., Brunst, P. W. (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kolhammer Verlag.
Gerhold, S. (2010). *Das System des Opferschutzes im Bereich des Cyber- und Internetstalking*. Baden-Baden: Nomos.
Gola, P., Schomerus, R. (Hrsg.) (2010). *Bundesdatenschutzgesetz. Kommentar*. 10. Aufl. München: C.H. Beck.
Graf, J. (Hrsg.) (2012). *Kommentar Strafprozessordnung*. 2. Aufl. München: C. H. Beck.
Graf, J. P. (Hrsg.) (2013). *BeckOK-StPO* (Edition 17). München: C.H. Beck.
Graf, J. P., Jäger, M. & Wittig, P. (2011). *Wirtschafts- und Steuerstrafrecht, Kommentar*. München: C.H. Beck.
Gropp, W. (2005). *Strafrecht Allgemeiner Teil*. 3. Auflage. Berlin u. a.: Springer.
Günther, J. (2013). Unternehmensschädliche Äußerungen von Arbeitnehmern in sozialen Medien Social Media Guidelines als Mittel der Prävention. *ArbRAktuell*, 223.
Harms, S. (2003). Ist das „bloße" Anschauen von kinderpornographischen Bildern im Internet nach geltendem Recht strafbar? *NStZ*, 646.
Härting, N. (2014). Fanpages und Social Networks im Unternehmen. *ZHW*, 45 ff.
Hawellek, C., Heinemeyer, D. (2012). Polizei Hannover setzt Personen-Fahndung wegen datenschutzrechtlicher Bedenken aus. *ZD-Aktuell*, Heft 2, 02730 ff.
Heckmann, D. (2012). Persönlichkeitsschutz im Internet. *NJW*, 2631 ff.
Heghmanns, M. (2004). Musiktauschbörsen im Internet aus strafrechtlicher Sicht. *MMR*, 14 ff.

Heigenhauser, C. (2007). *Zur Strafbarkeit der Musik-, Video- und Softwarepiraterie: Eine Untersuchung einschlägiger Straftatbestände im UrhG, Markenschutzgesetz und StGB*. Wien: NWV.

Hellmann, M., Gärtner, J. (2011). Neues beim Volksverhetzungstatbestand – Europäische Vorgaben und ihre Umsetzung. *NJW*, 961 ff.

Henrichs, A. (2011). Ermittlungen im Internet, Zugriff auf öffentlich zugängliche oder nicht öffentlich zugängliche Informationen? *Kriminalistik*, 622 ff.

Henrichs, A. (2012). Verdeckte personale Ermittlungen im Internet. *Kriminalistik*, 632 ff.

Henrichs, A., Wilhelm, J. (2010). Polizeiliche Ermittlungen in sozialen Netzwerken, *Kriminalistik*, 30 ff.

Hermann, K., Soiné, M. (2011). Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz. *NJW*, 2922 ff.

Hilgendorf, E. (1997). Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internets. *NJW*, 1873 ff.

Hilgendorf, E. (2008). Beleidigung Grundlagen, interdisziplinäre Bezüge und neue Herausforderungen. *EWE* [19], 403 ff.

Hilgendorf, E. (2010). Ehrenkränkungen („flaming“) im Web 2.0 – Ein Problemaufriss de lege lata und de lege ferenda. *ZIS*, 208 ff.

Hilgendorf, E. (2012). Die strafrechtliche Regulierung des Internets als Aufgabe eines modernen Technikrechts. *JZ*, 825 ff.

Hilgendorf, E., Frank, T., Valerius, B. (2005). *Computer- und Internetstrafrecht. Ein Grundriss*. Berlin u. a.: Springer.

Hilgert, P., Hilgert, S. (2014). Nutzung von Streaming-Portalen – Urheberrechtliche Fragen am Beispiel von Redtube. *MMR*, 85 ff.

Hoffmann, J. (2010). Cyberstalking. In: F. J. Robertz, R. P. Wickenhäuser (Hrsg.), *Orte der Wirklichkeit*. Berlin u. a.: Springer.

Höfling, W., Krohne, G. (2010). Versammlungsrecht in Bewegung. *JA*, 734 ff.

Holznagel, B., Enaux, C., Nienhaus, C. (2006). *Telekommunikationsrecht*. 2. Aufl. München: C.H. Beck.

Hube, D. (2011). Die Strafbarkeit des „Cyber-Groomings“ – eine Betrachtung im Lichte gesellschaftspolitischer Forderungen. *Kriminalistik*, 71 ff.

Irlbauer, H. (2012). Gehört der Facebook-Fahndung die Zukunft? *Kriminalistik*, 764 ff.

Jandt, S., Roßnagel, A. (2011). Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz? *MMR*, 637 ff.

Jauernig, O. (2009). *Kommentar zum BGB*. 15. Aufl. München: C.H. Beck.

Kaufmann, A. (2014). Stalking – das Undsoweiter-Delikt. *DRiZ*, 50 f.

Kindhäuser, U., Neumann, U. & Paeffgen, H.-U. (2013). *NOMOS-Kommentar, Strafgesetzbuch*. 4. Aufl. Baden-Baden: Nomos.

Kirchhoff, M. (2013). IuK-Kriminalität (Cyberkriminalität) – Grundkompetenzen im Bachelorstudium der Polizei. *Kriminalistik*, 491 ff.

Klengel, G. (2013). Datenhehlerei – Über die Notwendigkeit eines neuen Straftatbestands. *ZRP*, 16 ff.

Kolmey, U. (2013). Facebook: Plattform für Fahndung der Zukunft? *DRiZ*, 242 ff.

Körffer, B. (2013). Polizeiliche Recherchen in sozialen Netzwerken zu Zwecken der Gefahrenabwehr und Strafverfolgung. In: G. Willert, J. Bohrer (Hrsg.), *Soziale Netzwerke, Umgang mit Sozialen Netzwerken und anderen Kommunikationsplattformen im Internet durch Polizeibeamtinnen und -beamte* (S. 137). Berlin u. a.: LIT Verlag.

Krause, B. (2014). Sicherung von ausländischen E-Mail-Postfächern durch heimliches Einloggen – innovativ oder unzulässig? *Kriminalistik*, 213 ff.

Krey, V., Esser, R. (2012). *Strafrecht Allgemeiner Teil*. 5. Aufl. Stuttgart: Kohlhammer.

Krey, V., Hellmann, U. & Heinrich, M. (2012). *Strafrecht Besonderer Teil*, Band 1. 15. Aufl. Stuttgart: Kohlhammer.

Krischker, S. (2013). „Gefällt mir“, „Geteilt“, „Beleidigt“? – Die Internetbeleidigung in sozialen Netzwerken. *JA*, 488 ff.
Kudlich, H. (2002). Anmerkung zu BGH, Urt. v. 27.6.2001 – 1 StR 66/01. *JZ*, 310 ff.
Kühling, J., Schall, T. & Biendl, M (2014). *Telekommunikationsrecht*. 2. Aufl. Heidelberg: C. F. Müller.
Kühne, H.-H. (2010). Strafrechtliche und moralische Fragen beim staatlichen Ankauf von illegal erlangten Bankdaten. *GA*, 275 ff.
Lackner, K., Kühl, K. (2014). *Strafgesetzbuch*. 28. Aufl. München: C.H. Beck.
Ladeur, K.-H. (2011). Was ist Pornografie heute? – Zur Notwendigkeit einer Umstellung des strafrechtlichen Pornografieverbots auf Institutionenschutz. *AfP*, 471 ff.
Lang, A. (2009). *Filesharing und Strafrecht*. Berlin: Logos Verlag GmbH.
Langer, C. (2013). *Die Strafvorschriften der Nachstellung*. Hamburg: Verlag Dr. Kovac.
Laufhütte, H. W. u. a. (2009 ff.). *Leipziger Kommentar zum Strafgesetzbuch*. Band 6 (§§ 146–210 StGB), Band 7 (§§ 211–241a StGB). 12. Aufl. Berlin: De Gruyter.
Leffler, R. (2012). *Der strafrechtliche Schutz des Rechts am eigenen Bild vor dem neuen Phänomen des Cyber-Bullying. Eine Untersuchung der Normanwendungs- und Auslegungsprobleme der strafrechtlichen Bildnisschutzvorschriften bei deren Verletzung im Rahmen von Internetdelikten*. Frankfurt am Main et al.: Peter Lang.
Leipziger Kommentar zum Strafgesetzbuch ⟶ siehe unter Laufhütte et al.
Levin, I., Schwarz, M. (2012). Zum polizeirechtlichen Umgang mit sog. Facebook-Partys – „Ab geht die Party und die Party geht ab!“ . . . oder doch nicht? *DVBl*, 10 ff.
Lindemann, M., Wachsmuth, I. (2002). Anmerkung zu BGH, Urt. v. 27.6.2001 – 1 StR 66/01. *JR*, 206 ff.
Loewenheim, U. (2010). *Handbuch Urheberrecht*. 2. Aufl. München: C.H. Beck.
Löwe-Rosenberg, Großkommentar StPO ⟶ siehe unter Erb et al.
Mahrenholz, E. G. (1998). Brauchen wir einen neuen Pornographie-Begriff? — Zur Auslegung des § 3 Abs. 1 Nr. 4 RStV. *ZUM*, 525 ff.
Marberth-Kubicki, A. (2010). *Computer- und Internetstrafrecht*. 2. Aufl. München: C.H. Beck.
Maunz, T., Dürig, G. (Hrsg.) (2013). *Kommentar GG* (Stand: 69. EL). München: C.H. Beck.
May, E., Arnd, H. (2012). Polizei und soziale Netzwerke. *Kriminalistik*, 384 ff.
Meier, B.-D. (2012). Sicherheit im Internet. *MschrKrim*, 184 ff.
Meyer, A. (2012). Das Web 2.0 – Möglichkeiten und Grenzen der strafprozessualen Ermittlung in sozialen Netzwerken. *Kriminalistik*, 759 ff.
Meyer-Goßner, L., Schmitt, B. (Hrsg.) (2014). *Strafprozessordnung*. 57. Aufl. München: C.H. Beck.
Michalke, R. (2014). Durchsuchung und Beschlagnahme – Verfassungsrecht im Alltag. *StraF$_O$*, 89 ff.
Mitsch, W. (2007). Der neue Stalking-Tatbestand im Strafgesetzbuch. *NJW*, 1237 ff.
Mitsch, W. (2007). Strafrechtsdogmatische Probleme des neuen „Stalking“-Tatbestandes. *JURA*, 401 ff.
Morozinis, I. (2011). Die Strafbarkeit der „Auschwitzlüge“ im Internet, insbesondere im Hinblick auf „Streaming-Videos“. *GA*, 475 ff.
Mosbacher, A. (2007). Nachstellung § 238 StGB. *NStZ*, 665 ff.
Müller-Broich, J. (2012). *Telemediengesetz. Kommentar*. Baden-Baden: Nomos.
Müller, I., Eisenberg, U. (2013). Der Tatbestand der Nachstellung in der strafjustiziellen Praxis. *DRiZ*, 364 ff.
Neß, M. (2013). Folgen und Gefahren der Teilnahme an Sozialen Netzwerken für Polizeibeamte. *Kriminalistik*, 516 ff.
Neuhöfer, D. (2012). Zugriff auf Facebook-Nachrichten im Strafverfahren. *MMR-Aktuell*, 329250.
Neumann, C. (2011). Flashmobs, Smartmobs, Massenpartys. *NVwZ*, 1171 ff.
Ohly, A. (2012). Zwölf Thesen zur Einwilligung im Internet – Zugleich Besprechung zu BGH, Urt. v. 19.10.2011 – I ZR 140/10 – Vorschaubilder II. *GRUR*, 983 ff.

Ostendorf, H., Frahm, L. N. & Doege, F. (2012). Internetaufrufe zur Lynchjustiz und organisiertes Mobbing. NStZ, 529 ff.
Paal, B. P., Hennemann, M. (2012). Schutz von Urheberrechten im Internet, ACTA, Warnhinweismodell und Europarecht. *MMR*, 289 ff.
Palandt (2014). *BGB. Kommentar*. 73. Aufl. München: C.H. Beck.
Peifer, K.-N. (2013). Buchausschnitte als Thumbnails – Google Books und Fair Use. *GRUR-Prax*, 529 ff.
Peifer, K.-N. (2014). Selbstbestimmung im digitalen Netz – Privatkopie, Flatrate und Fair Use. *ZUM*, 86 ff.
Peters, S. (2009). Der Tatbestand des § 238 StGB (Nachstellung) in der staatsanwaltlichen Praxis. *NStZ*, 238 ff.
Piazena, M. (2014). *Das Verabreden, Auffordern und Anleiten zur Begehung von Straftaten unter Nutzung der Kommunikationsmöglichkeiten des Internets*. Berlin: Duncker&Humblot.
Piltz, C. (2013). Soziale Netzwerke im Internet – Eine Gefahr für das Persönlichkeitsrecht. Frankfurt a.M: PL Academic Research.
Popp, A. (2013). Rechtmäßigkeit einer Durchsuchungsanordnung: Anforderungen an Anforderungen bei Äußerungen in Internet-Chat. *jurisPR-ITR 15*, Anm. 2.
Port, V. (2012). *Cyberstalking*. Berlin: Logos Verlag GmbH.
Reinbacher, T. (2012). Zur Strafbarkeit des Streamings und der Umgehung von Geo-IP-Sperren durch private Nutzer. *HumFoR*, 179 ff.
Reinbacher, T. (2014). Zur Strafbarkeit der Betreiber und Nutzer von Kino.to – zugleich eine Anmerkung zu LG Leipzig, Urt. v. 14.6.2012, Az.: 11 KLs 390 Js 191/11 = ZUM 2013, 338. *NStZ*, 57 ff.
Reinemann, S., Remmertz, F. (2012). Urheberrechte an User-generated Content. *ZUM*, 216 ff.
Robertz, J. F., Wickenhäuser, R. (Hrsg.) (2010). *Orte der Wirklichkeit – Über Gefahren in medialen Lebenswelten Jugendlicher*. Berlin: Springer.
Röder, R. (2010). Nach der letzten Änderung des § 184b StGB: Ist das Verbreiten sog. „Posing"-Fotos weiterhin straflos? *NStZ*, 113 ff.
Rosengarten, C., Römer, S. (2012). Der „virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards. *NJW*, 1764 ff.
Säcker, F., Rixecker, R. (Hrsg.) (2013/2010). *Münchner Kommentar zum BGB*, Bd. 5 (§§ 705–853), Bd. 10 (Internationales Privatrecht). München: C.H. Beck.
Safferling, C. (2011). *Internationales Strafrecht. Strafanwendungsrecht – Völkerstrafrecht – Europäisches Strafrecht*. Berlin u. a.: Springer.
Satzger, H. (1998). Die Anwendung des deutschen Strafrechts auf grenzüberschreitende Gefährdungsdelikte. *NStZ*, 112 ff.
Schäufele, M. (2012). *Zur Strafbarkeit des Raubkopierens im Internet. Filesharing von urheberrechtlich geschützten Werken im Internet*. Münster: Lit Verlag.
Scheid, A., Sigle, H. (2013). Kündigung wegen beleidigender Äußerungen des Arbeitnehmers in sozialen Netzwerken. *ArbRAktuell*, 341083.
Schertz, C., Höch, D. (2011). *Privat war gestern, Wie Medien und Internet unsere Werte zerstören*. Berlin: Ullstein.
Schliesky, U., Hoffmann, C., Luch, A., Schulz, S., Borchers, K. C. (2014). *Schutzpflichten und Drittwirkung im Internet, Das Grundgesetz im digitalen Zeitalter*. Baden-Baden: Nomos Verlag.
Schmidt, H.C. (2010). Anmerkungen zur Diskussion um die Beschränkung des Akteneinsichtsrechts in den Filesharingverfahren. *GRUR*, 673 ff.
Schön, S. (2013). *Ermittlungsmaßnahmen über das Internet*. Frankfurt: Peter Lang Verlag.
Schönke, A., Schröder, H. (Hrsg.) (2014). *Strafgesetzbuch*. 29. Aufl. München: C.H. Beck.
Schreibauer, M. (1999). Das Pornographieverbot des § 184 StGB. Regensburg: S. Roderer.
Schulz, S. E., Hoffmann, C. (2012). Staatliche Datenerhebung in sozialen Netzwerken. *DuD*, 7 ff.
Schumann, H. (1998). Zum strafrechtlichen und rundfunkrechtlichen Begriff der Pornographie. In: A. Eser (Hrsg.), *Festschrift für Theodor Lenckner zum 70. Geburtstag*. München: C.H. Beck.

Sieber, U. (1999). Internationales Strafrecht im Internet – Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace. *NJW*, 2065 ff.
Sieber, U. (2000). Mindeststandards für ein globales Pornografiestrafrecht – Eine rechtsvergleichende Analyse. *ZUM*, 89 ff.
Sieber, D. (2012). Anmerkung zu LG Aachen, Urt. v. 5.9.2012 – 94 Ns 27/12. FD-StrafR, 340802.
Sieber, U. (2012). *Straftaten und Strafverfolgung im Internet*, Verhandlungen des 69. Deutschen Juristentages, Band 1, Gutachten, C1–157. München: C.H. Beck.
Simitis, S. (Hrsg.) (2011). *Bundesdatenschutzgesetz. Kommentar*. 7. Aufl. Baden-Baden: Nomos.
Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien. Kommentar*. 2. Aufl. München: C.H. Beck.
Stalberg, J. (2013). Zu einfachgesetzlichen und grundrechtlichen Fragestellungen von Flashmobs. *KommJur*, 169.
Steinberg, G. (2006). Nachstellen – ein Nachruf? *JZ*, 30 ff.
Ströbele, P., Hacker, F. (Hrsg.) (2012). *Markengesetz Kommentar*. 10. Aufl. Köln: Carl Heymanns Verlag.
Taeger, J. (Hrsg.) (2011). *Die Welt im Netz – Tagungsband Herbstakademie*. Oldenburg: Oldenburger Verlag für Wirtschaft, Informatik und Recht.
Ulbricht, C. (2012). *Social Media und Recht*. Freiburg: Haufe.
Valerius, B. (2003). Das globale Unrechtsbewusstsein – Oder: Zum Gewissen im Internet. *NStZ*, 341 ff.
Viefhues, W. (2011). Zunahme der Nutzung von sozialen Netzwerken. *MMR-Aktuell*, 322686.
Wandtke, A.-A. (Hrsg.) (2013). *Urheberrecht*. 4. Aufl. Berlin: de Gruyter.
Wandtke, A.-A., Bullinger, W. (2009). *Praxiskommentar zum Urheberrecht*, 3. Aufl. München: C.H. Beck.
Weber C., Meckbach, A. (2006). Äußerungsdelikte in Internetforen. Zugleich Anmerkung zu LG Mannheim, Beschluss vom 13. 5. 2005 – 5 Qs 23/05. *NStZ*, 492 ff.
Weigend, T. (2011). Anmerkung zu BGH, Beschl. v. 16.3.2011 – 5 StR 581/10. *NStZ*, 570 ff.
Werle, G., Jeßberger, F. (2001). Grundfälle zum Strafanwendungsrecht. *JuS*, 35 ff.
Wessels, J., Hettinger, M. (2013). *Strafrecht Besonderer Teil 1*. 37. Aufl. Heidelberg: C.F. Müller.
Wicker, M. (2013). Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden. *MMR*, 765 ff.
Willert, G. (2013). Strafbare Handlungen im Zusammenhang mit sozialen Netzwerken. In: G. Willert, J. Bohrer (Hrsg.), *Soziale Netzwerke, Umgang mit Sozialen Netzwerken und anderen Kommunikationsplattformen im Internet durch Polizeibeamtinnen und -beamte* (S. 90 ff.). Berlin u. a.: LIT Verlag.
Wolff, H., Brink, S. (Hrsg.) (2014). *Beck-OK Datenschutzrecht* (Edition 7). München: C.H. Beck.
Wolter, J. (Hrsg.) (2010). *Systematischer Kommentar zur Strafprozessordnung*, Bd. II (§§ 94–136a). 4. Aufl. Köln: Carl Heymanns Verlag.
Wolter, J. (Hrsg.). *Systematischer Kommentar zum Strafgesetzbuch*, Bd. III (§§ 123–211), Bd. IV (§§ 212–266b). 8. Aufl. Köln: Carl Heymanns Verlag.

Kapitel 8
Arbeitsrechtliche Aspekte der Social Media

Frank Bayreuther

Inhalt

F. Bayreuther (✉)
Inhaber des Lehrstuhls für Bürgerliches Recht und Arbeitsrecht, Universität Passau, Innstr. 39, 94032 Passau, Deutschland
E-Mail: frank.bayreuther@uni-passau.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_8

8.1 Social Media und Arbeitsvertrag

8.1.1 Verpflichtung zur Teilnahme an Netzwerken

1 Eine Verpflichtung des Arbeitnehmers, sich persönlich und unter seinem Namen an sozialen Netzwerken zu beteiligen, tangiert regelmäßig dessen allgemeines Persönlichkeitsrecht und sein Recht auf informationelle Selbstbestimmung. Daher kann der Arbeitgeber vom Arbeitnehmer im Regelfall nicht verlangen, dass sich dieser in sozialen Netzwerken **im eigenen Namen anmeldet** und dort für das Unternehmen kommuniziert.[1] Vielmehr würde er mit einer dahingehenden Weisung sein Direktionsrecht nach § 106 GewO überschreiten.

Darüber hinaus sind aber auch arbeitsvertragliche Vereinbarungen, die den Arbeitnehmer verpflichten, sich persönlich an sozialen Netzwerken zu beteiligen, nur dann zulässig, wenn dies durch die Eigenart des Unternehmens und der geschuldeten Tätigkeit gerechtfertigt ist. Fehlt es dagegen an einem derart rechtfertigenden Grund, sind arbeitsvertragliche Verpflichtungen zur Teilnahme an sozialen Netzwerken in aller Regel nach **§§ 134 bzw. 307 BGB** unwirksam.

2 In der Literatur wird angenommen, dass eine Teilnahmepflicht an sozialen Netzwerken sich insbesondere für **Personalrecruiter** begründen ließe. Von diesen könne verlangt werden, dass sie sich zu berufsorientierten Netzwerken, wie etwa XING anmelden, um dort nach Personal zu suchen.[2] Das allerdings bedarf einer Einschränkung: Eine solche Pflicht ist nur dann begründbar, wenn das Netzwerk keine Anmeldung des Arbeitgeberunternehmens als solches zulässt und daher eine personalisierte Anmeldung einer natürlichen Person entweder zwingend erforderlich ist oder deren Beteiligung am Netz zumindest erheblich erleichtert. Ebenso kann in Arbeitsverträgen von Mitarbeitern im **Kommunikations- und PR-Bereich**[3] eine Teilnahmepflicht an sozialen Netzwerken vereinbart werden, dies allerdings nur dann, wenn die Art der geschuldeten Tätigkeit ein persönliches Log-in erfordert. In jedem Fall muss es zum Aufgabenbereich des Arbeitnehmers gehören, dass er in Foren Fragen zum Unternehmen oder zu dessen Produkten unter seinem Namen beantwortet.

3 Das heißt freilich nicht, dass sich der Arbeitnehmer nicht freiwillig zu einem Netzwerk anmelden und sich an diesem im Unternehmensinteresse beteiligen dürfte. Sowohl das allgemeine Persönlichkeitsrecht als auch das Recht auf informationelle Selbstbestimmung eröffnen dem Berechtigten naturgemäß auch die Entscheidung, an sozialen Netzwerken teilzunehmen und Dritten dort persönliche Daten zur Verfügung zu stellen (s. nur §§ 4a BDSG, 22 KUG). Und natürlich ist es Arbeitnehmern völlig unbenommen, sich in oder auch außerhalb von Kommunikationsplattformen positiv über ihren Arbeitgeber zu äußern.

---

[1] Schaub/Linck, ArbR-Hdb., § 53 Rn. 44b; Byers/Mößner, BB 2012, 1665 (1669); Determann, BB 2013, 181 (185); Bissels et al., BB 2010, 2433 (2434); Melot de Beauregard/Gleich, DB 2012, 2044.

[2] Byers/Mößner, BB 2012, 1665 (1669).

[3] Byers/Mößner, BB 2012, 1665 (1669).

Aus dieser selbstverständlich bestehenden Möglichkeit einer freiwilligen Netzmitgliedschaft darf indes nicht hergeleitet werden, dass der Arbeitnehmer ohne Weiteres wirksam in eine Vertragsbestimmung einwilligen könnte, die ihn zu einer solchen anhält. Denn genau an dieser Stelle stellt sich das aus dem Arbeitnehmerdatenschutz hinlänglich bekannte Problem, inwieweit der Arbeitnehmer mit Rücksicht auf seine strukturelle Unterlegenheit gegenüber dem Arbeitgeber freiwillig und damit rechtsverbindlich in eine Verwertung seiner Daten einwilligen kann.[4] Ganz gleich, wie man generell zu Zulässigkeit und Grenzen einer Einwilligung des Arbeitnehmers in eine Datenerhebung steht, sollte im vorliegenden Kontext damit außerordentlich zurückhaltend umgegangen werden und zwar nicht nur, weil der Arbeitnehmer in einem solchen Netz seine Daten gegenüber einem mehr oder weniger unüberschaubar großen Personenkreis preisgibt, sondern auch, weil er sich zumindest mittelbar dem Arbeitgeber gegenüber bindet, was die Inhalte seiner Meinungsäußerungen betrifft. Daher ist eine Vertragsklausel, die eine Pflicht zur Teilnahme des Arbeitnehmers an sozialen Netzwerken konstituiert nur wirksam, wenn Art und Weise der geschuldeten Tätigkeit einschlägige Aktivitäten des Arbeitnehmers im Netz bedingen. In allen anderen Fällen kann der Arbeitnehmer eine begonnene Mitgliedschaft jederzeit beenden, seine Aktivitäten wieder einstellen und bleibt darüber hinaus stets frei, was den Inhalt seiner Postings betrifft. Vorstellbar ist aber eine aus §§ 241 Abs. 2, 242 BGB folgende vertragliche Nebenpflicht, wonach der Arbeitnehmer, der sich auf Veranlassung des Arbeitgebers und im Unternehmensinteresse freiwillig an einem sozialen Netzwerk beteiligt hat, dem Arbeitgeber anzeigen muss, dass er sich gar nicht mehr oder jedenfalls nicht mehr im Interesse des Betriebs am Netz beteiligen will bzw. dort nicht mehr mit den vom Arbeitgeber gewünschten Inhalten auftreten möchte. **4**

8.1.2 Social Media und Arbeitszeit

Mobile technische Gerätschaften wie etwa Laptops, Smartphones u. dgl. lassen den Arbeitnehmer ständig erreichbar werden. Dieser wird so auch außerhalb seiner Anwesenheit im Unternehmen mit dienstlichen Belangen konfrontiert, etwa durch den Abruf von Mails oder die Entgegennahme von Telefonanrufen. Umgekehrt nutzen **5**

[4] Vgl. allgemein zu dem Problem der „Freiwilligkeit“: Däubler, Gläserne Belegschaften, Rn. 468 ff., 150 ff.; Gola/Schomerus, BDSG, § 4a Rn. 19 ff.; Simitis, in: Simitis, BDSG, § 4a Rn. 62 ff. Zu einer Pflicht bzw. einem freiwilligen Engagement des Arbeitnehmers zur Unterstützung des Arbeitgebers in sozialen Netzwerken siehe: Däubler, DuD 2013, 759 (761 f). Der Gesetzesentwurf zum Arbeitnehmerdatenschutz (BT-Drs. 535/10) sah einen Wegfall der Einwilligung des Arbeitnehmers nach § 4a BDSG als Rechtfertigungsgrund vor. Stattdessen sollte die Einwilligung nur in gesetzlich ausdrücklich anerkannten Fällen nach § 32 ff. BDSG-E als zusätzliches Kriterium der Erforderlichkeit Bedeutung erlangen. Der Entwurf zur europäischen Datenschutzgrundverordnung v. 25.1.2012 [KOM(2012) 11 endg.] sieht in Art. 7 Abs. 4 vor, dass die Einwilligung eine Datenerhebung nicht rechtfertigt, wenn zwischen den Beteiligten ein „erhebliches Ungleichgewicht“ besteht. Nach Erwägungsgrund 34 soll das bei Arbeitsverhältnissen generell der Fall sein.

die Vertragsparteien elektronische Kommunikationsmittel zur Flexibilisierung der Arbeitszeit und ermöglichen dem Arbeitnehmer so, dass er anfallende Arbeiten etwa von zu Hause aus erledigen kann, was viele Arbeitnehmer durchaus als vorteilhaft empfinden. Diese Kultur des „always-on" lässt die **Grenze zwischen Arbeitszeit und Ruhezeit** verschwimmen, was schwierige arbeitszeitrechtliche Fragestellungen aufwirft. Diese wiederum sind allerdings keine spezifische Besonderheit der Nutzung sozialer Medien; vielmehr resultieren diese ganz allgemein aus der Verfügbarkeit und Verbreitung von „mobile devices".

6 Wird der Arbeitnehmer außerhalb der Zeiten, in denen er im Betrieb anwesend ist, angerufen, liest er eine E-Mail, kommuniziert er dienstlich in einem sozialen Netzwerk oder erledigt er über mobile Geräte dienstliche Aufträge, so erbringt er damit seine vertraglich geschuldete Arbeitsleistung. Ist er dagegen für den Arbeitgeber nur erreichbar, hat dies regelmäßig keine arbeitsrechtliche Relevanz. Insbesondere liegt im Normalfall keine **Rufbereitschaft** vor. Rufbereitschaft erfordert nämlich, dass der Arbeitnehmer auf Zuruf unverzüglich an einen vom Arbeitgeber bestimmten Ort kommen muss, um dort seine Arbeiten zu erledigen. Darüber hinaus wird Rufbereitschaft vom Arbeitgeber zeitlich genau geplant, so dass dem Arbeitnehmer die jeweiligen Bereitschaftssequenzen genau vorgegeben werden. Dagegen weiß der Arbeitnehmer im vorliegenden Sachverhalt zwar, dass er immer einmal wieder kontaktiert werden kann, doch entscheidet er, wann er etwa E-Mails abruft und wann er sie beantwortet. Ihm bleibt es daher im Großen und Ganzen möglich, seine Freizeit noch einigermaßen hinreichend flexibel zu planen.

7 Bei der Bestimmung, ob einschlägige Aktivitäten des Arbeitnehmers im Netz als Arbeitszeit anzusehen sind, muss zunächst genau geprüft werden, ob diese überhaupt im dienstlichen Interesse erbracht wurden. Sieht der Arbeitnehmer etwa seine Mailbox immer wieder durch, ohne dass der **Arbeitgeber** ihn hierzu **veranlasst** hat, ist dies natürlich keine Arbeitszeit. Besondere Probleme bereitet es, wenn Arbeitnehmer vom Arbeitgeber zur Verfügung gestellte mobile Kommunikationsmittel oder einen dienstlichen E-Mail-Account auch privat nutzen dürfen und sie daher beispielsweise ihr E-Mail-Postfach in ihrer Freizeit immer einmal wieder auch im Hinblick auf eine etwa eingehende **Privatpost** durchsehen und bei dieser Gelegenheit auf betriebliche E-Mails stoßen und diese dann auch beantworten. Eine exakte Grenzziehung zwischen Arbeitszeit und nicht zu vergütender Ruhezeit ist in diesen Fällen nicht möglich.

8 Als Arbeitszeit können einschlägige „außerbetriebliche" Aktivitäten des Arbeitnehmers aber nur gewertet werden, wenn im **Arbeitsvertrag** festgelegt ist, dass der Arbeitnehmer auch während seiner Abwesenheit im Betrieb solche Arbeiten zu verrichten hat. Ist dies nicht der Fall, ist erforderlich, dass der Arbeitgeber angeordnet hat, dass der Arbeitnehmer auch während seiner Freizeit entsprechend aktiv wird oder aber, dass der **Arbeitgeber** – dies gegebenenfalls auch konkludent – die **Erwartung** zum Ausdruck bringt, dass der Arbeitnehmer so verfährt.[5] Fehlt es auch daran, muss der Arbeitgeber von den einschlägigen Aktivitäten des Arbeitnehmers

[5] Insoweit a. A. Bissels et al., DB 2010, 2052 (2054).

zumindest Kenntnis erlangt und diese **gebilligt oder geduldet** haben.[6] Ist eine dieser Alternativen gegeben, ist der jeweilige Zeitraum als Arbeitsleistung anzuerkennen und dem Arbeitnehmer entsprechend zu vergüten.

9 Laufen durch derartige Zusatzarbeiten des Arbeitnehmers Überstunden auf, sind diese, soweit im Arbeitsvertrag nichts Abweichendes vereinbart ist, im Umfang des durchschnittlichen Stundenarbeitslohns zu vergüten (§ 612 BGB). Insoweit ist allerdings zu beachten, dass das BAG die – sehr zweifelhafte – Ansicht vertritt, dass der Arbeitnehmer für Überstunden ohne gesonderte Überstundenabrede keinen zusätzlichen Vergütungsanspruch erwirbt, soweit unter objektiver Betrachtung für diese keine Vergütung erwartet werden kann.[7] Das soll nach Ansicht des BAG dann der Fall sein, wenn „Dienste höherer Art"[8] geschuldet werden, was insbesondere auf solche Arbeitnehmer zutreffen könnte, die typischerweise während ihrer Freizeit in dienstlichen Angelegenheiten kommunizieren. Weiter soll nach Ansicht des BAG keine Überstundenvergütung fällig werden, wenn die arbeitszeitbezogenen und arbeitszeitunabhängigen Arbeitsleistungen zeitlich verschränkt sind, insbesondere wenn sich die Vergütung in einem nicht unerheblichen Maß aus Provisionsabreden zusammensetzt.[9]

10 Bedeutung erlangt insoweit, dass im Arbeitsvertrag grundsätzlich vereinbart werden kann, dass geleistete Überstunden mit dem regelmäßigen Gehalt abgegolten sein sollen. Wird eine solche pauschale **Überstundenabgeltung** aber, wie regelmäßig, per AGB in den Vertrag eingeführt, ist diese nach der neueren Rechtsprechung des BAG nur wirksam, wenn sie das von ihr erfasste Arbeitsvolumen eindeutig beschreibt.[10] In der Vertragsklausel muss also entweder der Umfang der zusätzlichen Leistungspflicht bestimmt sein oder aber die Anordnungsbefugnis des Arbeitgebers hinsichtlich des Umfangs der zu leistenden Überstunden muss bestimmbar sein. Erforderlich ist, dass der Arbeitnehmer bereits bei Vertragsschluss erkennen kann, was gegebenenfalls auf ihn zukommt und welche maximale Leistung er für die vereinbarte Vergütung erbringen muss. Ist dies nicht der Fall, ist die Klausel nach §§ 306, 307 Abs. 1 S. 2 BGB unwirksam und fällt ersatzlos weg. Daran ändern auch die Höchstarbeitszeiten des ArbZG nichts.

11 Auch dann, wenn der Arbeitnehmer über längere Zeit außerhalb der Arbeitszeit im betrieblichen Interesse unter Zuhilfenahme neuer Medien kommuniziert hat, ergibt sich noch keine vertragliche Bindung der beiden Parteien, auch weiterhin so zu verfahren. Traditionell verfährt die Rechtsprechung mit der Annahme einer dauerhaften Festlegung neuer Leistungspflichten durch Konkretisierung des Arbeitsverhältnisses

---

[6] BAG, AP Nr. 17 zu § 1 TVG Tarifverträge: Gebäudereinigung; BAG, AP Nr. 40 zu § 611 BGB – Mehrarbeitsvergütung = NZA 2002, 1340; BAG, AP Nr. 1 zu § 1 TVG – Tarifverträge: Arbeiterwohlfahrt = NZA 1994, 1035; BAG, AP Nr. 3 zu § 14 KSchG 1969 = NZA 94, 837.

[7] BAG, NZA 2012, 861; BAG, NZA 2012, 145; BAG, NZA 2011, 1335.

[8] BAG, NZA 2011, 1335.

[9] BAG, NZA 2012, 145.

[10] BAG, NZA 2012, 2683; BAG, NZA 2012, 939; BAG, NZA 2012, 861; BAG, NZA 2011, 1335; BAG, NZA 2011, 917; BAG, NZA 2011, 575.

nämlich sehr zurückhaltend.[11] Daher ist der Arbeitnehmer nicht verpflichtet, auch weiterhin außerhalb seiner Kernarbeitszeiten entsprechende Arbeiten zu erbringen, ebenso, wie es dem Arbeitgeber freisteht, einschlägige Arbeitsleistungen nicht mehr anzuordnen oder dem Arbeitnehmer mitzuteilen, dass er diese in Zukunft nicht mehr dulden und daher auch nicht mehr vergüten wird. Entsprechend kann der Arbeitnehmer, auch wenn er in der Vergangenheit über einen längeren Zeitraum hinweg in seiner Freizeit einschlägige Überstunden geleistet hat, hieraus noch keinen Anspruch auf Anordnung, Ableistung und Vergütung weiterer Überstunden herleiten.

12 Wenn zuweilen danach gefragt wird, ob der Arbeitgeber anordnen könne, dass der Arbeitnehmer außerhalb seiner Arbeitszeit „erreichbar" ist, erweckt dies immer einmal wieder den missverständlichen Eindruck, als ginge es darum, dass der Arbeitgeber bestimmen könne, dass die einschlägigen Aktivitäten des Arbeitnehmers nicht als Arbeitsleistung gelten sollen. Das ist natürlich nicht möglich. Denn stets ist es so, dass sobald der Arbeitnehmer etwa Telefonate führt oder E-Mails beantwortet, er eine Arbeitsleistung erbringt. Vielmehr geht die Frage, richtig formuliert, dahin, ob der Arbeitgeber die **Arbeitszeit** so **flexibel verteilen** kann, dass der Arbeitnehmer nicht nur während fixer „Bürozeiten" für ihn tätig ist, sondern darüber hinaus auch bei Bedarf seine Freizeit unterbricht und per moderner Kommunikationsmittel an ihn herangetragene Anfragen oder Aufgaben erledigt. Ob das wiederum möglich ist, hängt zunächst davon ab, was im Arbeitsvertrag hierzu vereinbart ist. Ist dort eine fixe Lage der Arbeitszeit und/oder ein bestimmter Arbeitsort festgelegt, ist der Arbeitnehmer zu keiner davon abweichenden Arbeitsleistung verpflichtet.[12] Ordnet der Arbeitgeber eine solche dennoch an, braucht der Arbeitnehmer dieser Anordnung nicht nachzukommen; tut er dies aber, ist darin eine – ggf. konkludente – Vertragsänderung zu sehen, die sich indes nur auf den jeweiligen Einzelfall erstreckt, mit der also keine dauerhafte Vertragsänderung für die weitere Zukunft verbunden ist.

13 Enthält der Arbeitsvertrag dagegen keine ausdrückliche Bestimmung zur Lage der Arbeitszeit und zum Ort der Arbeitsleistung oder gibt er ausdrücklich eine flexible Arbeitszeit vor, kann der Arbeitgeber über sein **Direktionsrecht** (§ 106 GewO) die Arbeitszeit an die betrieblichen Notwendigkeiten anpassen. Letztlich Gleiches gilt für die Frage, inwieweit die Arbeitszeit im Betrieb oder von einem anderen Ort aus zu leisten ist. Stets hat der Arbeitgeber aber die Grenzen billigen Ermessens zu beachten, sodass eine Verpflichtung des Arbeitnehmers zur jederzeitigen Erreichbarkeit auf solche Arbeitsverhältnisse beschränkt sein dürfte, bei denen eine solche – mit Rücksicht auf dessen **Stellung und Funktion im Betrieb**, sowie auf die Art der geschuldeten Leistung – im betrieblichen Interesse auch tatsächlich geboten ist.

14 Arbeitszeit sind derart geleistete Arbeiten aber in jedem Fall. Was die Parteien aber tun können, ist zu bestimmen, dass derartige Leistungszeiträume keiner gesonderten Vergütungspflicht unterliegen. Bei Licht betrachtet, handelt es sich bei einer solchen

---

[11] BAG, AP Nr. 51 zu § 611 BGB – Mehrarbeitsvergütung = NZA 2010, 120; BAG, AP Nr. 121 zu § 615 BGB = NZA 2007, 801; BAG v. 9.3.2005 – 5 AZR 231/04, nicht amtl. veröff.; BAG, NZA 2004, 1184; grundlegend: BAG, PersR 1997, 179 (II 2e aa der Gründe); BAG v. 30.10.1991 – 5 AZR 6/91, nicht amtl. veröff. (II 2 der Gründe).

[12] Bissels et al., DB 2010, 2052 (2054).

Abrede also um nichts anderes als um eine Pauschalisierungsabrede, die bereits eingangs dieses Abschnitts dargestellt wurde.

15 Schließlich ist darauf hinzuweisen, dass die Vorgaben des **öffentlichen Arbeitszeitrechts** bzw. des zwingenden Urlaubsrechts auch für die Nutzung moderner Kommunikationsmittel außerhalb des Arbeitsplatzes uneingeschränkte Geltung beanspruchen, mag es auch so sein, dass diese in der betrieblichen Realität häufig keine hinreichende Beachtung finden. So wäre dem Arbeitnehmer, soweit nicht die besonderen Ausnahmen nach § 10 ArbZG greifen, eine Arbeit an Sonn- und Feiertagen eigentlich vollständig verboten. Auch ist dem Arbeitnehmer eine tägliche Ruhezeit von mindestens elf Stunden zu gewähren (§ 5 Abs. 1 ArbZG). Selbst wenn man davon ausgeht, dass das Versenden einer kurzen E-Mail oder die Annahme eines Telefonats noch keine Arbeitsaufnahme i. S. d. ArbZG darstellt,[13] würde dies der in manchen Dienstleistungsunternehmen geübten Praxis der mehr oder weniger 24-stündigen Erreichbarkeit der Beschäftigten klar entgegenstehen. Ebenso darf der Arbeitgeber den Arbeitnehmer während des Urlaubs nicht zu einschlägigen Aktivitäten veranlassen: §§ 8, 13 BUrlG.

8.2 Private Nutzung von sozialen Netzwerken während der Arbeitszeit

8.2.1 Vom Arbeitgeber nicht gestattete soziale Kommunikation während der Arbeitszeit

16 Hat der Arbeitgeber die **Privatnutzung** betrieblicher Kommunikationsmittel **ausgeschlossen** bzw. nicht zugelassen (s. dazu 8.1.), finden auf eine dennoch stattfindende unberechtigte Nutzung betrieblicher Ressourcen die Grundsätze Anwendung, die die Rechtsprechung zur **unerlaubten Internetnutzung** während der Arbeitszeit herausgearbeitet hat.[14] Insoweit geht es nicht um etwaige Inhalte der Kommunikation, also nicht darum, was der Arbeitnehmer postet, vielmehr ist hier zunächst maßgebend, dass der Arbeitnehmer während des Kommunikationsvorgangs nicht die arbeitsvertraglich geschuldete Leistung erbracht hat, dies aber vorgibt, wenn er für den fraglichen Zeitraum Arbeitsentgelt beansprucht.[15] Kündigungsrechtlich wird dies allgemein mit dem Begriff „Arbeitszeitbetrug“ umschrieben.[16] Dies gilt

[13] Bissels et al., DB 2010, 2052 (2054).
[14] BAG, NZA 2007, 922; BAG, NZA 2006, 980; BAG, NZA 2006, 98; s. dazu auch: Lützeler/Bissels, ArbRAktuell 2011, 499; Bissels et al., BB 2010, 2433; Byers/Mößner, BB 2012, 1665; Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a a.E., 18 ff.; Frings/Wahlers, BB 2011, 3126 (3130). S. zur Parallelproblematik bei Mitarbeitern der Verwaltung Schulz, Kap. 10 Rn. 113 ff.
[15] Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a a.E., 18 ff.; Frings/Wahlers, BB 2011, 3126 (3131); Kramer/Rasche, FA 2013, 330 (331).
[16] Allg. Preis, in: Staudinger, BGB, § 626 Rn. 145.

zunächst völlig unabhängig davon, ob der Arbeitnehmer für den jeweiligen Kommunikationsvorgang auf betriebliche Ressourcen zurückgegriffen hat oder nicht. Da die Nutzung von sozialen Netzwerken in der Praxis aber häufig Hand in Hand mit der verbotenen Privatnutzung betrieblicher Ressourcen geht, werden beide Aspekte in der rechtlichen Bewertung meist zusammengezogen,[17] obwohl sie rechtlich eigentlich voneinander zu unterscheiden wären. Freilich ist es so, dass der mit der Vorenthaltung von Arbeit verbundene Vertrauensverlust des Arbeitgebers in die Redlichkeit noch weiter vertieft wird, wenn der Arbeitnehmer für seine Kommunikation betriebliche Ressourcen ohne Erlaubnis nutzt oder derart gegen eine entgegenstehende vertragliche Abrede bzw. gegen eine einschlägige Weisung des Arbeitgebers verstößt.[18] Je nach den Umständen des Einzelfalls kann dieser Aspekt dann sogar den mit dem Abrechnungsbetrug verbundenen Vertrauensschaden übersteigen.[19]

17 Ob das Verhalten des Arbeitnehmers allerdings tatsächlich eine Kündigung des Arbeitsverhältnisses, gar eine außerordentliche Kündigung, rechtfertigt oder ob es nicht einer vorherigen Abmahnung bedarf, ist im Rahmen der im Anwendungsbereich der §§ 1 KSchG bzw. 626 BGB erforderlichen Verhältnismäßigkeitsprüfung anhand folgender Gesichtspunkte zu entscheiden:

18
- Hat der Arbeitnehmer für die fragliche Kommunikation auf betriebliche Ressourcen zurückgegriffen (Dienstrechner, Internetzugang am Arbeitsplatz, Smartphones des Unternehmens, etc.)?
- Welchen zeitlichen Umfang hat die fragliche Kommunikation erreicht? Während ein lediglich marginales Abschweifen von der Arbeit oder eine Nutzung betrieblicher IT-Ressourcen in minimalem Umfang häufig folgenlos bleiben oder allenfalls eine Abmahnung eröffnen wird, kann eine exzessive Netzkommunikation während der Arbeitszeit sogar eine außerordentliche Kündigung ohne vorherige Abmahnung rechtfertigen.[20] Dabei lassen sich für die Feststellung, wann eine exzessive Nutzung vorliegt, keine festen Maßstäbe herausbilden.[21] So kommt es etwa auf die Art des Arbeitsplatzes an oder darauf, welche Gefahren und Risiken für den Betrieb oder Dritte damit verbunden sind, dass sich dieser nicht auf seine Arbeit konzentriert.[22] Das BAG hat etwa eine Privatnutzung von über einer Stunde an zwei Werktagen als ausreichend angesehen.[23] Verschiedene LAG waren dagegen der Ansicht, dass eine Nutzungsdauer von 1 bis 5 Stunden innerhalb eines Monats bzw. innerhalb eines Jahres nicht ausreiche.[24]

---

[17] Vgl. BAG, NZA 2006, 98.
[18] Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 100; Schaub/Linck, ArbR-Hdb., § 53 Rn. 18; Frings/Wahlers, BB 2011, 3126 (3131); Göpfert/Wilke, ArbRAktuell 2011, 159.
[19] Göpfert/Wilke, ArbRAktuell 2011, 159; Waltermann, NZA 2007, 529 (531).
[20] Schaub/Linck, ArbR-Hdb., § 53 Rn. 18; § 127 Rn. 96; § 132 Rn. 28.
[21] BAG, NZA 2007, 922, Rn. 30; Bissels et al., BB 2010, 2433 (2434).
[22] Bissels et al., BB 2010, 2433 (2434).
[23] BAG, NZA 2007, 922.
[24] LAG Niedersachsen, NZA-RR 2010, 406; LAG Rheinland Pfalz v. 13.12.2007 – 10 Sa 505/07; LAG Rheinland-Pfalz, MDR 2006, 1355.

- Hat die Kommunikation zum Up- oder Download erheblicher Datenmengen geführt und/oder wurden dadurch die betrieblichen Kommunikationssysteme verlangsamt oder gar beeinträchtigt?
- Hat die Kommunikation beim Arbeitgeber zusätzliche Kosten verursacht?
- Welche Inhalte hat der Arbeitnehmer kommuniziert? Naturgemäß ist eine Kündigung dann besonders gerechtfertigt, wenn rufschädigende, strafbare oder pornografische Inhalte kommuniziert wurden.[25]
- Hat der Arbeitnehmer eigenmächtig Programme in den betrieblichen Systemen installiert, um die Kommunikation erst zu ermöglichen, diese zu verschleiern oder sonstige Schutzvorrichtungen des Arbeitgebers umgangen? In solchen Fällen ist eine Kündigung des Arbeitsverhältnisses regelmäßig auch ohne zuvorige Abmahnung gerechtfertigt.[26]

8.2.2 Erlaubte Privatnutzung

8.2.2.1 Rechtsquelle der Gestattung, insbesondere: keine betriebliche Übung

Eine Erlaubnis zur privaten Kommunikation in sozialen Netzwerken kann sich aus dem **Arbeitsvertrag**, aus einer einschlägigen Betriebsvereinbarung oder ggf. auch aus Tarifvertrag ergeben.[27] Allerdings erwirbt der Arbeitnehmer noch keinen Anspruch auf Zugang zu den fraglichen Ressourcen, nur weil der Arbeitgeber die Nutzung über einen längeren Zeitraum schlicht toleriert.[28] Daraus ergibt sich weder eine **betriebliche Übung** noch eine konkludente Abänderung des Arbeitsvertrags auf individualrechtlicher Ebene.[29] Das gilt jedenfalls dann, wenn ein ausdrückliches Nutzungsverbot des Arbeitgebers besteht; dieses steht der Annahme einer auf Nutzungsgestattung gerichteten Willenserklärung des Arbeitgebers entgegen. In großen Betrieben kommt noch dazu, dass meist nicht der Personalverantwortliche die Nutzung duldet, der zur rechtsgeschäftlichen Abänderung des Arbeitsvertrags berechtigt wäre, sondern vielmehr ein Dienstvorgesetzter ohne Personalkompetenz. Schließlich hat das BAG darauf hingewiesen, dass „kleine Annehmlichkeiten" nicht zur betrieblichen Übung erstarken und noch weniger ein Verhalten des Arbeitnehmers, mit dem dieser seine vertragliche Hauptleistungspflicht verletzt.[30] **19**

[25] Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a.
[26] BAG, NZA 2006, 980; Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 100.
[27] Schaub/Linck, ArbR-Hdb., § 53 Rn. 18.
[28] Schaub/Linck, ArbR-Hdb., § 53 Rn. 18; s. zum Ganzen auch Waltermann, NZA 2007, 529.
[29] Zu dieser Rechtsfigur s. BAG, DB 2013, 2568; Bissels et al., BB 2010, 2433; Frings/Wahlers, BB 2011, 3126 (3130); Koch, NZA 2008, 911 (912 f.); a. A. Schaub/Linck, ArbR-Hdb., § 53 Rn. 18.
[30] BAG, NZA 2006, 977.

8.2.2.2 Umfang der Nutzung

20 Häufig wird in Rechtsprechung und Literatur im Vorliegenden von der „erlaubten Privatnutzung" gesprochen,[31] was erneut ungenau ist, weil rechtlich gesehen eigentlich zwischen der Nutzung betrieblicher Ressourcen zum Zweck der Kommunikation in sozialen Netzwerken und der Erlaubnis, während der Arbeitszeit privat zu kommunizieren, unterschieden werden müsste. Denkbar sind folgende Varianten: 1) Der Arbeitgeber gestattet dem Arbeitnehmer betriebliche, insbesondere mobile Kommunikationsmittel privat zu nutzen (wie etwa: Smartphones, Tablets, usw.), dies aber nur während seiner Freizeit (also vergleichbar der Möglichkeit, ein Dienstfahrzeug außerhalb der Arbeitszeit privat nutzen zu dürfen). 2) Der Arbeitgeber gestattet dem Arbeitnehmer, während der Arbeitszeit soziale Netzwerke zu nutzen, dies indes nur mit dessen Privatgeräten. 3) Der Arbeitgeber lässt beides zu, also die Nutzung betrieblicher Gerätschaften zum Zwecke der privaten Kommunikation und zwar auch während der Arbeitszeit.

21 Allerdings ist es auch an dieser Stelle so, dass die verschiedenen Sachkonstellationen in der betrieblichen Praxis häufig ineinander übergehen. So wird es häufig so sein, dass wenn der Arbeitgeber die Privatnutzung von „ortsfester" Informationstechnologie im Betrieb erlaubt, er dem Arbeitnehmer damit meist konkludent gestattet, zumindest in einem nicht erheblichen Umfang, diese auch während der Arbeitszeit zu nutzen. Dennoch ist zu beachten, dass wenn der Arbeitgeber die außerdienstliche Nutzbarkeit eines Geräts auf die Freizeit des Arbeitnehmers beschränkt, der Arbeitnehmer gegen seine vertraglichen Pflichten verstößt, wenn er mit diesem während der Arbeitszeit in sozialen Netzwerken kommuniziert.[32] Abhängig von den weiteren Umständen des Einzelfalls, insbesondere des zeitlichen Umfangs der Nutzung, kann ein derartiges Verhalten eine Abmahnung bzw. Kündigung rechtfertigen,[33] obwohl der Arbeitgeber dem Arbeitnehmer, umgangssprachlich gesprochen, die „Privatnutzung" der einschlägigen betrieblichen Ressourcen erlaubt hat. Die Dinge liegen dann kaum anders, als wenn ein Arbeitnehmer, dem die private Nutzung eines Dienstwagens erlaubt ist, während der Arbeitszeit mit diesem eine Privatfahrt unternimmt.

22 Soweit dem Arbeitnehmer auch gestattet ist, die jeweiligen Ressourcen während der Arbeitszeit zu nutzen, stellt sich in der Praxis häufig das Problem einer **exzessiven Nutzung**. Eine solche kann sich daraus ergeben, dass der Arbeitnehmer den zeitlichen Umfang des zulässigen Gebrauchs überschreitet.[34] Ist dieser allerdings in der maßgeblichen Gestattungsgrundlage (Arbeitsvertrag, Arbeitsordnung, Betriebsvereinbarung) gar nicht oder nur durch auslegungsbedürftige Generalklauseln beschrieben (wie etwa: „geringfügig", „in vertretbarem Umfang" o. dgl.) bedarf

---

[31] Kramer, NZA 2006, 194; ders., NZA 2004, 457 (459); Waltermann, NZA 2007, 529 (531 ff.); Frings/Wahlers, BB 2011, 3126 (3130); Moll/Dendorfer, § 35 Rn. 203 ff.

[32] Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a a.E., 18 ff.; Frings/Wahlers, BB 2011, 3126 (3131); Kramer/Rasche, FA 2013, 330 (331).

[33] Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 100.

[34] Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 100; Schaub/Linck, ArbR-Hdb., § 53 Rn. 18, § 127 Rn. 96, § 132 Rn. 28, jeweils m.w.N.

es vor Ausspruch einer Kündigung meist einer Abmahnung.[35] Anderes gilt wiederum, wenn sich der Arbeitnehmer mit der Nutzung völlig „in der Oktave vergreift", was etwa dann der Fall ist, wenn die Nutzung in einem auffälligen Missverhältnis zur Arbeitsleistung steht oder es sonst offensichtlich ist, dass die an den Tag gelegte Nutzung nicht rechtens sein kann.[36] Entsprechendes gilt, wenn der Arbeitnehmer im Netz inakzeptable Verhaltensweisen zeigt.[37]

8.3 Außerdienstliche Nutzung – Kündigung des Arbeitsverhältnisses wegen Äußerungen des Arbeitnehmers in sozialen Netzwerken

8.3.1 Allgemeines zur außerdienstlichen Meinungsäußerung des Arbeitnehmers

8.3.1.1 Bedeutung der Problematik

Kündigungen des Arbeitsverhältnisses wegen Äußerungen des Arbeitnehmers in sozialen Netzwerken waren zuletzt Gegenstand zahlreicher instanzgerichtlicher Entscheidungen.[38] Insoweit muss man sich zunächst eines vor Augen führen: Die Problematik, inwieweit Meinungsäußerungen (i. w. S.) des Arbeitnehmers in seiner Freizeit den Arbeitgeber zur Auflösung des Arbeitsverhältnisses berechtigen können, ist alles andere als neu. Schon immer mussten sich die Arbeitsgerichte mit Kündigungen auseinandersetzen, die der Arbeitgeber ausgesprochen hatte, weil er sich etwa durch eine herablassende Äußerung des Arbeitnehmers beleidigt fühlte, die dieser gegenüber seinen Kollegen gemacht hat.[39] Verändert hat sich lediglich die **Qualität der Kommunikation** und alleine deshalb haben einschlägige Fälle zuletzt immer mehr Aufmerksamkeit auf sich gezogen (wobei freilich hinzukommt, dass diese Thematik in der Literatur derzeit gewissermaßen in Mode ist). Fiel früher eine einschlägige Äußerung vielleicht am abendlichen Stammtisch und wurde diese dort von fünf Personen wahrgenommen, ist sie jetzt einem großen, wenn nicht gar unbeschränkten Nutzerkreis zugänglich.[40] Fast noch wichtiger erscheint die beweisrechtliche Situation. Während die am Stammtisch am Arbeitgeber geäußerte Kritik der menschlichen Vergesslichkeit und damit der Vergänglichkeit anheim gegeben

23

[35] BAG, NZA 2007, 922; Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 100; Schaub/Linck, ArbR-Hdb., § 127 Rn. 96; Kramer, NZA 2004, 457 (459).
[36] BAG, NZA 2006, 98; Schaub/Linck, ArbR-Hdb., § 127 Rn. 96.
[37] BAG, NZA 2013, 27.
[38] LAG Frankfurt, AuA 2014, 123; LAG Hamm, BB 2012, 2688; LAG Berlin-Brandenburg, BB 2009, 661; ArbG Hagen, ArbRB 2012, 365; ArbG Dessau-Roßlau, ArbRB 2013, 108; ArbG Duisburg, NZA-RR 2013, 18; ArbG Bochum v. 9.2.2012 – 3 Ca 1203/11; BayVGH, NZA-RR 2012, 302; VG Ansbach v. 16.1.2012 – AN 14 K 11.02132.
[39] Hierzu statt vieler Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 86 m.w.N.
[40] Göpfert/Wilke, ArbRAktuell 2011, 159.

war, ist die im Netz gefallene Äußerung dort mehr oder weniger dauerhaft auffindbar.[41] Darüber hinaus ist der Arbeitgeber beweisrechtlich eben nicht auf unsichere Zeugen angewiesen, die vor Gericht ihren Kollegen belasten müssten. Vielmehr kann er sie ganz einfach festhalten und einen Ausdruck o. dgl. in Augenschein nehmen lassen. Damit steigert sich seine Chance, die Kündigung am Ende auch durchsetzen zu können und entsprechend eher ist der Arbeitgeber geneigt, eine solche auch auszusprechen.

8.3.1.2 Schutz der Meinungsäußerung des Arbeitnehmers durch Art. 5 GG

24 Meinungsäußerungen des Arbeitnehmers im Internet und in Social Media genießen grundsätzlich den Schutz durch das **Grundrecht auf freie Meinungsäußerung des Art. 5 GG**. Wie im allgemeinen Verfassungsrecht ist auch im Arbeitsrecht der Schutzbereich des Art. 5 Abs. 1 S. 1 GG weit zu verstehen. Meinungen sind durch das Element der Stellungnahme, des Dafürhaltens, der Beurteilung geprägt. Gleichgültig ist dabei, auf welchen Gegenstand sie sich beziehen und welchen Inhalt sie haben; sie können politische oder unpolitische, öffentliche oder private Angelegenheiten betreffen. Auch ist unerheblich, ob diese vernünftig oder unvernünftig, wertvoll oder wertlos sind.[42] Überdies besteht Meinungsfreiheitsschutz auch für **Tatsachenäußerungen** zumindest dann, wenn sie meinungsbezogen sind und damit zur Meinungsbildung beitragen. Jedoch nehmen **bewusst unwahre Tatsachenbehauptungen**[43] nicht am Grundrechtsschutz teil. Das gleiche gilt für **Formalbeleidigungen**.[44] Dagegen fällt die Äußerung einer „Schmähkritik" im Ansatz durchaus in den Schutzbereich des Art. 5 Abs. 1 S. 1 GG.[45] Genau an dieser – für das Arbeitsrecht entscheidenden – Stelle bedarf es dann aber einer sorgfältigen Abwägung mit kollidierenden Rechtspositionen des Arbeitgebers. In deren Folge tritt das Grundrecht der Meinungsfreiheit regelmäßig dann zurück, wenn die Äußerung nur noch auf Verunglimpfung des Arbeitgebers, eines Vorgesetzten oder eines Kollegen abzielt, für die also Meinungsbildung – und sei es in noch so polemischer und zugespitzter Form – keine Rolle mehr spielt.[46]

25 Das Recht auf freie Meinungsäußerung besteht nicht schrankenlos. Im Arbeitsverhältnis muss es sich einer **Konkordanzabwägung** mit kollidierenden Rechtspositionen des Arbeitgebers bzw. der vom Arbeitnehmer angegriffenen Kollegen stellen. Das sind namentlich das allgemeine Persönlichkeitsrecht sowie die Berufsfreiheit des Arbeitgebers aus Art. 12 GG, die dessen wirtschaftliche Betätigungsfreiheit vor Störungen schützt. Darüber hinaus ist aber zu beachten, dass sich die Beteiligten hier

---

[41] Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a; Notzon, öAT 2013, 180.
[42] BVerfGE 124, 300 (320); 90, 241 (247); 61, 1 (8); BAG, NZA 2006, 917; BAG, NZA 2006, 650.
[43] BVerfGE 114, 339 (352); 99, 185 (187); 85, 1 (15); 61, 1 (8).
[44] BVerfGE 82, 43 (51); 60, 234 (242); BAG, NZA 2006, 917; BAG, NZA 2006, 650.
[45] BVerfGE 85, 1 (16); 82, 272 (280 ff., insb. 285); 82, 43 (51).
[46] BVerfGE 85, 1 (16); 82, 272 (283 f.); BAG, NZA 2006, 917; BAG, NZA 2006, 650; BAG v. 17.2.2000 – 2 AZR 927/98.

durch ein gemeinsames Vertragsverhältnis gebunden haben, das **gegenseitige Treue- und Rücksichtnahmepflichten** nach den §§ 241 Abs. 2 und 242 BGB begründet.[47] Zwar ist es natürlich mitnichten so, dass der Arbeitnehmer sich nicht mehr auf seine Meinungsfreiheit berufen dürfte und an Unternehmensinteressen gebunden wäre, nur weil er mit dem Arbeitgeber ein Arbeitsverhältnis eingegangen ist. Vielmehr ist er im außerdienstlichen Bereich zunächst einmal in seiner Meinungsäußerung frei. Umgekehrt kann aber eben auch nicht unberücksichtigt bleiben, dass er sich mit dem Vertragsschluss verpflichtet hat, auf Rechtsgüter und berechtigte Interessen des Arbeitgebers in angemessene Weise Rücksicht zu nehmen und dass sich aus dem Arbeitsvertrag gegenseitige Loyalitäts- und Rücksichtnahmepflichten ergeben. Daher dürfen die zu Art. 5 GG entwickelten Grundsätze, die das Verhältnis des Bürgers zum Staat abbilden, aber auch diejenigen, die Rechtsverhältnisse zwischen Privatrechtssubjekten betreffen, zwischen denen keine vertragliche Bindung besteht, nicht unbesehen im Verhältnis 1:1 auf das Arbeitsverhältnis übertragen werden.[48]

26 Plakativ lässt sich das am Beispiel der öffentlichen Kritik an der Produktpalette eines Unternehmens verdeutlichen. Während etwa ein Mitglied einer Naturschutzorganisation völlig frei darin ist, in der Öffentlichkeit dafür einzutreten, dass ein bestimmtes Produkt eines Unternehmens aus ökologischen Gründen nicht hergestellt oder vertrieben werden sollte, dürfte eine derartige Stellungnahme des Verkaufsleiters des Unternehmens dieses zur Kündigung des Arbeitsvertrags berechtigen. Hier bedarf es einer entsprechend sorgfältigen und eingehenden Einzelfallabwägung. S. zu dieser Problematik auch unter dem Abschn. 8.4.1.

8.3.2 Kommunikation im vertraulichen Bereich

27 Nimmt der Arbeitnehmer in sozialen Netzwerken zum Arbeitgeber, zum Unternehmen, zu innerbetrieblichen Vorgängen oder Kollegen Stellung, spielt es bei der rechtlichen Beurteilung eine Rolle, ob die fragliche Kommunikation im vertraulichen Bereich des Netzwerkes erfolgt ist oder ob sich der Arbeitnehmer öffentlich entäußert hat. Traditionell erkennt die Rechtsprechung[49] nämlich einen **geschützten Bereich vertraulich gemachter Äußerungen** an. Darf der Arbeitnehmer darauf bauen, dass eine in einem vertraulichen Kreis gemachte Äußerung nicht nach außen getragen wird, kann er sich über den Arbeitgeber, das Beschäftigungsunternehmen oder auch über Kollegen so äußern, wie er dies möchte. Denn niemand kann den Arbeitnehmer verpflichten, über seinen Arbeitgeber positiv zu denken und vor allem muss er bei **Äußerungen im Privatbereich** nicht damit rechnen, dass diese zu einer

---

[47] BAG, NZA 2006, 917; BAG, NZA 2006, 650; BAG v. 17.2. 2000 – 2 AZR 927/98; ausführlich Bauer/Günther, NZA 2013, 67; Hinrichs/Hörtzk, NJW 2013, 648; Wiese, NZA 2012, 1 (4).

[48] Schaub/Linck, ArbR-Hdb., § 53 Rn. 29 ff.

[49] BAG, NZA 2010, 698; BAG v. 17.2.2000 – 2 AZR 927/98; BAG, AP Nr. 66 zu § 626 BGB. Grundsätzlich zum Schutz der Vertraulichkeit des gesprochenen Wortes vgl. BVerfG, BeckRS 2009, 38648 [zu III 1a]; BVerfG, NJW 2007, 1194 [zu II 1] m.w.N.

Störung des Betriebsfriedens oder einer Belastung des Vertrauensverhältnisses zum Arbeitgeber führen. Darüber hinaus ist die Rechtsprechung der Ansicht, dass wenn alleine der Gesprächspartner gegen den Willen des Arbeitnehmers die Vertraulichkeit aufhebt, dies grundsätzlich nicht zulasten des Arbeitnehmers geht.

28 Allerdings muss der Kreis der Vertrauenspersonen eng gezogen werden. Eine negative Äußerung verliert ja nicht an Qualität, nur weil sie gegenüber wenigen Personen getätigt wird. Beleidigt der Arbeitnehmer den Arbeitgeber in einer abendlichen Stammtischrunde vor einem halben Dutzend Kollegen, ändert das weder etwas an deren Charakter, noch kann der Arbeitnehmer ernsthaft damit rechnen, dass diese vertraulich bleibt. Gerade die unter dem Deckmantel der Verschwiegenheit gemachte Beleidigung macht häufig besonders schnell die Runde und manche Intrige nimmt so ihren Anfang.[50]

29 Vertraulichkeit kann daher nur bei Anwesenheit weniger Personen erwartet werden und regelmäßig wird es darauf ankommen, dass ein gewisses Näheverhältnis zwischen dem Arbeitnehmer und seinen Gesprächspartnern besteht. Überdies besteht eine **Wechselbeziehung** zwischen Zahl und Person der Zuhörer und der gefallenen Äußerung. So leuchtet natürlich völlig ein, dass der Arbeitnehmer im engsten Familienkreis, beispielsweise gegenüber seinem Ehegatten, entäußern kann, was er will und insoweit nur durch elementare vertragliche Treuepflichten beschränkt wird (etwa: Wahrung von Betriebs- oder Geschäftsgeheimnissen). Umgekehrt schwindet der Grad der Vertraulichkeit desto mehr, je weiter der Gesprächspartner dem Arbeitnehmer entfernt ist.

30 Inwieweit sich diese Grundsätze auf die Kommunikation in sozialen Netzwerken übertragen lassen und dort Vertraulichkeit erwartet werden darf, ist sowohl in der Rechtsprechung, als auch im Schrifttum umstritten.

31 Eine enge Auffassung vertritt, dass in sozialen Netzwerken grundsätzlich keine Vertraulichkeit erwartet werden kann. Eine solche gibt es nach dieser Meinung auch nicht in Räumen mit Zugangsbeschränkungen, wie etwa im Chat- oder Freundesbereich von Netzwerken.[51]

32 Die Gegenansicht will danach differenzieren, wie viele und ggf. welche Nutzer die fragliche Kommunikation einsehen können. Vertraulich sind danach sog. „private" bzw. Chat-Mitteilungen, weil diese in der Regel an einen Empfänger, jedenfalls[52] aber an einen stark begrenzten Empfängerkreis gerichtet sind.[53] Diese Nachrichten

---

[50] Bauer/Günther, NZA 2013, 67 (68).

[51] ArbG Hagen, ArbRB 2012, 365 (Rn. 63); ArbG Dessau-Roßlau, ArbRB 2013, 108 (Rn. 34); VG Ansbach v. 16.1.2012 – AN 14 K 11.02132, Rn. 35; Schaub/Linck, ArbR-Hdb., § 53 Rn. 44a; Müller-Glöge, in: ErfKomm, § 626 BGB, Rn. 88; Notzon, öAT 2013, 180 (181); Braun, jurisPR-ITR 20/2012 Anm. 5; ähnlich Geuer/Seidl, jurisPR-ITR 5/2012 Anm. 4; in der Tendenz auch Bauer/Günther, NZA 2013, 67.

[52] Facebook bietet beispielsweise die Möglichkeit, private Nachrichten auch an mehr als einen Adressaten zu senden. Genauso kann auch ein Gruppenchat geführt werden.

[53] ArbG Duisburg, NZA-RR 2013, 18; ArbG Hagen, ArbRB 2012, 365 (Rn. 63); ArbG Bochum v. 9.2.2012 – 3 Ca 1203/11, Rn. 29 (aus anderen Gründen aufgehoben durch das LAG Hamm, BB 2012, 2688, welches indes die Frage der Vertraulichkeit dahinstehen lässt); BayVGH, NZA-RR 2012, 302; Kock/Dittrich, DB 2013, 934 (937); a. A. Bauer/Günther, NZA 2013, 67 (70), wonach dies allenfalls

sind grundsätzlich mit dem üblichen E-Mail-Verkehr gleichzusetzen. Umgekehrt scheidet für öffentliche Postings jede Erwartung der Vertraulichkeit aus.[54] Insoweit ist unerheblich, ob die fragliche Äußerung an der eigenen oder einer fremden „Pinnwand" kundgetan wird, weil sie aufgrund ihres unbegrenzten Empfängerkreises so oder so nicht mehr vertraulich ist.[55]

33 Innerhalb dieser Ansicht umstritten ist, wie Äußerungen zu qualifizieren sind, die lediglich an einen eingeschränkten Personenkreis adressiert sind, namentlich als Postings in „Gruppen" oder der „Freundesliste". Denkbar ist insoweit, danach zu unterscheiden, ob der fragliche Bereich zwar zugangsbeschränkt ist, das entscheidende Zugangskriterium aber alleine die Anmeldung zum Netzwerk ist, sodass dort gemachte Äußerungen im Ergebnis öffentlich sind.[56] Ist die Gruppe dagegen nur für vernetzte Personen („Freunde") einsehbar, mag die Annahme eines geschützten Vertrauensbereichs schon näher liegen. Weiter ließe sich danach differenzieren, wie groß der potentielle Personenkreis ist, den die Nachricht erreichen kann.[57]

34 Gegen eine derartige Differenzierung spricht freilich, dass Postings, welche lediglich durch entsprechende Privatsphäre-Einstellungen beschränkt sind, ohne Weiteres hunderte, wenn nicht tausende potentielle Empfänger ansprechen können, sodass der Nutzer im Grunde eben doch keinerlei Kontrolle über den Empfängerkreis hat.[58] Darüber hinaus mündet eine Beurteilung nach dem Kreis der potenziellen Empfänger in eine schwierige Einzelfallabwägung, deren Ausgang für den Rechtsanwender nicht sicher absehbar ist. Daher spricht viel dafür, an dieser Stelle restriktiv zu verfahren und eher nur zielgerichtete Nachrichten, denen von ihrer Funktion her gesehen die Qualität eines „Vier-Augen-Gesprächs" zukommt (Mails, Chats), als vertraulich zu behandeln.

35 „Like" oder „Gefällt-mir"-Buttons, also Schaltflächen, mit denen Mitglieder sozialer Netzwerke Beiträge anderer Mitglieder bewerten, sind Kommentare auf einer fremden Pinwand und als solche öffentlich. Einmal getätigt, kann der Kreis der potentiellen Empfänger nämlich nicht mehr begrenzt werden.[59] Ihnen kommt jedoch regelmäßig kein arbeitsrechtlich relevanter Aussagegehalt zu: s. 8.3.3.

---

dann gelten kann, soweit der Nutzer von der Verschwiegenheit seines Gesprächspartners ausgehen durfte.

[54] LAG Frankfurt, AuA 2014, 123; LAG Berlin-Brandenburg, BB 2009, 661.

[55] Kort, NZA 2012, 1321 (1322 f.); Wahlers, jurisPR-ITR 8/2012, Anm. 2; Rosenbaum/Tölle, MMR 2013, 209 (210); ArbG Hagen, ArbRB 2012, 365 (Rn. 63), das einen derartigen Pinnwand-Eintrag mit einem Aushang am Schwarzen Brett des Betriebes vergleicht.

[56] ArbG Duisburg, NZA-RR 2013, 18 (Rn. 32); Bauer/Günther, NZA 2013, 67 (70); Wahlers, jurisPR-ITR 8/2012, Anm. 2; Pawlak/Smeyers, öAT 2013, 26 (28 f.); Kort, NZA 2012, 1321 (1323 f.).

[57] Zintl/Naumann, NJW-Spezial 2013, 306; wohl auch Bissels, jurisPR-ArbR 37/2012, Anm. 1; Stoffels, in: BeckOK-ArbR, § 626 BGB, Rn. 106a.5; Howald, ArbRAktuell 2013, 195.

[58] ArbG Duisburg, NZA-RR 2013, 18 (Rn. 32); Kock/Dittrich, DB 2013, 934 (937).

[59] ArbG Dessau-Roßlau, ArbRB 2013, 108 (Rn. 34); Bauer/Günther, NZA 2013, 67 (70 f.).

8.3.3 Inhaltliche Abwägung

36 Das BAG unterzieht die in Zusammenhang mit Meinungsäußerungen des Arbeitnehmers kollidierenden Positionen beider Vertragsparteien einer **umfassenden Abwägung**. Einerseits betont das Gericht, dass der Arbeitgeber das außerdienstliche Verhalten seiner Beschäftigten nur sehr eingeschränkt beeinflussen kann und darf. Auch weist es in ständiger Rechtsprechung darauf hin, dass Arbeitnehmer grundsätzlich berechtigt sind, unternehmensöffentliche Kritik am Arbeitgeber und den betrieblichen Verhältnissen zu äußern. Eine sachliche Kritik am Arbeitgeber ist in aller Regel vom Recht des Arbeitnehmers auf freie Meinungsäußerung gedeckt, wobei die Kritik gegebenenfalls auch überspitzt und polemisch ausfallen kann. Umgekehrt muss der Arbeitnehmer aber keine in grobem Maße **unsachlichen Angriffe** hinnehmen (s. auch oben, Rn. 24 ff.). Erst recht können **Beleidigungen** des Arbeitgebers, seiner Vertreter und Repräsentanten oder auch von Arbeitskollegen, die nach Form und Inhalt eine erhebliche Ehrverletzung für den Betroffenen bedeuten, einen gewichtigen Vertragsverstoß darstellen und eine Kündigung auch ohne vorherige Abmahnung rechtfertigen. Entsprechendes gilt für **bewusst wahrheitswidrig aufgestellte Tatsachenbehauptungen**, etwa wenn sie den Tatbestand der üblen Nachrede erfüllen.[60]

37 Was im Rahmen dieser Abwägung zu beachten ist, ist, dass die Äußerung stets in den **Kontext** gestellt werden muss, in dem sie steht.[61] Einer Äußerung darf kein Sinn beigelegt werden, den sie nicht besitzt. Umgekehrt kann es so sein, dass eine auf den ersten Blick „harmlose“ Bemerkung beleidigenden Charakter annehmen kann, wenn für einen hinreichend großen Kreis von Empfängern klar ist, dass die vermeintlich neutral erscheinende Äußerung eindeutig dazu gedacht ist, die betreffende Person herabzuwürdigen. So kann es etwa sein, dass kritische Äußerungen eines Arbeitnehmers im betrieblichen Wahlkampf letztlich nur darauf zielen, der Belegschaftzu verdeutlichen, dass der Arbeitnehmer die Bildung eines Betriebsrats als sinnvoll ansieht, was der Arbeitgeber selbstverständlich hinzunehmenhat.

Die Rechtsprechung zur kündigungsrechtlichen Gewichtung von Äußerungen des Arbeitnehmers in seinem sozialen Umfeld und zunehmend auch in sozialen Netzwerken ist reichhaltig und soll hier deshalb wenigstens skizzenhaft nachgezeichnet werden, weil sie der Praxis eine Handreichung für die Beurteilung einschlägiger Fälle bietet.

38 Die Gleichsetzung noch so umstrittener betrieblicher Vorgänge und der Vergleich des Arbeitgebers oder der für ihn handelnden Personen mit dem nationalsozialistischen Terrorsystem, den Menschen, die diese Verbrechen begingen oder gar mit den Konzentrationslagern des Nationalsozialismus, stellt in jedem Fall eine grobe Beleidigung des Arbeitgebers und zugleich eine Verharmlosung des begangenen Unrechts und eine Verhöhnung seiner Opfer dar, ist daher völlig inakzeptabel und begründet

---

[60] BAG, NZA 2010, 698; BAG, NZA 2006, 980; BAG, NZA 2006, 650; BAG v. 17.2.2000 – 2 AZR 927/98; BAG, NZA 1987, 808.

[61] BAG, 31.7.2014, 2 AZR 505/13; NZA 2006, 980.

in der Regel eine (auch fristlose) Kündigung des Arbeitsverhältnisses.[62] Auch die „scherzhafte" Äußerung, dass sich ein Vorgesetzter trotz eines dreimaligen Bandscheibenvorfalls „noch sehr gut an Fußballspielen beteiligen und bewegen" könne, sowie, dass er zuletzt in Wirklichkeit gar nicht operiert worden sei, sondern lediglich ein „Pause gebraucht hat, da er in mehrere Machenschaften verwickelt sei", hat das BAG wegen des darin enthaltenen Vorwurfs des Arbeitszeitbetrugs und der Untreue als kündigungsgeeignet eingestuft.[63] Dagegen sah das BAG die Aussage „wenn der Chef so weiter macht, macht er die Firma irgendwann einmal kaputt" als eine zwar zugespitzte, aber noch zulässige Kritik an der Unternehmenspolitik des Arbeitgebers an. Nicht mehr toleriert hat es hingegen die Aussage „da werden Millionen verschoben" und „da werden Zahlen schon hingedreht oder manipuliert", weil dem Arbeitgeber derart kriminelle Machenschaften (Untreue, Unterschlagungen, Bilanzfälschung) unterstellt werden.[64]

39 Der VGH München stufte einige kritische und auch polemische Äußerungen einer (schwangeren) Arbeitnehmerin über einen Kunden ihres Arbeitgebers auf ihrem privaten Facebook-Account als nicht kündigungsgeeignet ein.[65] Selbst die schärfste der in diesem Zusammenhang gefallenen Äußerungen („kotzt mich an") bewegte sich nach Ansicht des Gerichts noch im Rahmen des Möglichen. Hingegen soll nach dem LAG Hamm eine für eine außerordentliche Kündigung geeignete Beleidigung gegeben sein, wenn ein Azubi auf seinem privaten Facebook-Profil unter der Rubrik Arbeitgeber „Menschen-Schinder & Ausbeuter, Leibeigener, dämliche Scheiße für Mindestlohn − 20 % erledigen" angibt.[66]

Nach der Rechtsprechung wiegt eine unzulässige Äußerung umso schwerer und ist entsprechend umso kündigungsrelevanter, je überlegter sie erfolgte.[67] **Spontane Meinungskundgaben**, die im Rahmen einer verbalen Auseinandersetzung in beiderseits aufgeheizter Stimmung und daher gewissermaßen „im Eifer des Gefechts fallen", sind weitaus weniger gravierend zu bewerten als bewusste und zielgerichtete Stellungnahmen.

40 Bedeutung erlangt das in sozialen Netzwerken insbesondere mit Blick auf die Betätigung von **„Like-it" oder „Gefällt-mir"-Buttons**. Insoweit muss schon beachtet werden, dass einem derartigen Klick kaum ein bedeutender Erklärungswert zukommt und es keineswegs so ist, dass sich der Arbeitnehmer dadurch in jedem Fall die fragliche Meinungskundgabe vollumfänglich zu eigen machen würde. Nicht selten erweist sich die vermeintliche Zustimmung bei Licht betrachtet als kaum mehr als eine ggf. leichtfertige Kundgabe der Kenntnisnahme der Mitteilung.[68] Vor allem ist ein solcher Klick meist schnell gemacht und erweist sich deshalb häufig als kaum

---

[62] BAG, NZA 2006, 650.
[63] BAG, NZA 2010, 698.
[64] BAG, NZA 2006, 980; vgl. BVerfGE 93, 266; BAG, NZA 2006, 650.
[65] BayVGH, NZA-RR 2012, 302.
[66] LAG Hamm, BB 2012, 2688.
[67] BAG, NZA 2010, 698; LAG Hamm, BB 2012, 2688; ArbG Duisburg, NZA-RR 2013, 18.
[68] Kaumanns, K&R 2012, 445; a. A. Bauer/Günther, NZA 2013, 67 (70 f.): „virtuelle Sympathiebekundung".

mehr als eine spontane Reaktion ohne eingehendere Überlegung. Zur fehlenden Vertraulichkeit von Zustimmungserklärungen s. Abschn. 8.3.2.

41 Geradezu gegenteilig verhalten sich die Dinge, wenn **umfassende Äußerungen** gemacht werden und dies insbesondere, wenn deren Niederschreiben einige Zeit in Anspruch nimmt. Erst recht nicht mehr auf eine Spontanäußerung kann sich der Arbeitnehmer berufen, wenn er die fragliche Stellung über mehrere Monate auf der maßgeblichen Seite lässt, obwohl er die Möglichkeit gehabt hätte, diese dort zu entfernen. Die Erklärung genießt dann unter keinen Umständen mehr den Charakter einer augenblicklichen, wenn auch heftig überzogenen Unmutsäußerung. Vielmehr will derjenige, der eine Äußerung über längere Zeit aufrecht erhält, gerade, dass sie zur Kenntnis genommen und der Arbeitgeber in der dargestellten Eigenschaft gesehen wird.[69]

8.3.4 Verrat von Betriebs- und Geschäftsgeheimnissen

42 Dass der Arbeitnehmer auch in sozialen Netzwerken zur Wahrung von Betriebs- und Geschäftsgeheimnissen verpflichtet ist, versteht sich und bedarf keiner näheren Erörterung. Insoweit gilt in sozialen Netzwerken nichts anderes als sonst im Arbeitsverhältnis auch. Der Arbeitnehmer ist im Rahmen seiner arbeitsvertraglichen Rücksichtnahmepflicht grundsätzlich verpflichtet, **Betriebs- und Geschäftsgeheimnisse** nicht gegenüber Dritten zu offenbaren. In sensiblen Bereichen wird überdies häufig eine Geheimhaltungspflicht im Arbeitsvertrag vereinbart, mit der die grundständige, bereits aus § 242 BGB folgende Verschwiegenheitspflicht erweitert werden kann. Darüber hinaus bedroht § 17 UWG Arbeitnehmer, denen im Rahmen ihres Dienstverhältnisses Geschäfts- oder Betriebsgeheimnisse anvertraut oder zugänglich gemacht geworden sind, mit strafrechtlichen Konsequenzen, wenn sie diese während des Dienstverhältnisses unbefugt an Dritte zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilen.

43 Geschäfts- und Betriebsgeheimnisse sind dabei alle Tatsachen, die in einem Zusammenhang mit dem Geschäftsbetrieb stehen, nur einem eng begrenzten Personenkreis bekannt und nicht offenkundig sind und nach dem Willen des Arbeitgebers und im Rahmen eines berechtigten wirtschaftlichen Interesses geheim gehalten werden sollen. Dazu gehören etwa der Gegenstand von Patenten, Gebrauchsmustern und Lizenzen, technisches Know-how und technische Verfahren (und zwar auch dann, wenn diese nicht dem gewerblichen Rechtsschutz unterliegen) Warenbezugsquellen, Absatzgebiete, Kunden- und Preislisten, Bilanzen, Inventuren oder auch die Kreditwürdigkeit des Unternehmens. Entscheidend ist stets, dass die fraglichen Tatsachen nur einem bestimmten Personenkreis zugänglich sind und darüber hinaus der betreffende Vorgang nach dem ausdrücklich oder konkludent erklärten Willen des

[69] LAG Hamm, BB 2012, 2688; a. A. aber: ArbG Duisburg, NZA-RR 2013, 18.

Arbeitgebers geheim zu halten ist.[70] Allgemein bekannte und übliche Verfahren oder Tatsachen sind dagegen auch dann keine Geschäfts- und Betriebsgeheimnisse, wenn der Arbeitgeber sie als solche bezeichnet.

Die Verletzung der arbeitsvertraglichen **Geheimhaltungspflicht** ist, dies freilich abhängig von der Schwere des Verstoßes, häufig ein **Grund für die Kündigung** des Arbeitsverhältnisses. Dabei ist im Rahmen der kündigungsrechtlichen Verhältnismäßigkeitsprüfung zu beachten, dass die Verletzung einer Verschwiegenheitspflicht im Internet in aller Regel als besonders schwerwiegend einzustufen ist, weil dort das Risiko, dass die Information den Unternehmensbereich endgültig verlässt und das Geheimnis daher für den Arbeitgeber dauerhaft verloren ist, als besonders hoch einzuschätzen ist. Dazu kommt, dass es sich bei Geschäfts- und Betriebsgeheimnissen regelmäßig um Tatsachen handelt, die nicht vom Schutzbereich des Art. 5 Abs. 1 GG gedeckt sind, sodass sich der Arbeitnehmer, wenn er diese in einem sozialen Netzwerk preisgibt, insoweit auch nicht auf sein Grundrecht der Meinungsfreiheit berufen kann. **44**

8.3.5 Offenbarung von Gesetzesverstößen und anderen Missständen im Unternehmen, Whistleblowing

Was die Möglichkeit bzw. Grenzen für die Veröffentlichung von Gesetzesverstößen durch Arbeitnehmer betrifft, ergeben sich im Zusammenhang mit sozialen Netzwerken keine grundsätzlichen Besonderheiten. Vielmehr beanspruchen die allgemeinen Grundsätze Geltung. Nach der Rechtsprechung des BAG[71], die durch die *Heinisch*-Entscheidung des EGMR[72] allerdings eine gewisse Modifikation erfahren hat,[73] kommt es an dieser Stelle erneut auf eine einzelfallbezogene Abwägung der widerstreitenden Rechtspositionen an. Aufseiten des Arbeitnehmers streitet dabei dessen in Art. 5 GG (bzw. aus Sicht des EGMR in Art. 10 EMRK) garantiertes **Grundrecht auf Meinungsfreiheit**, wobei das BAG lange Zeit allerdings mehr die Befugnis des Arbeitnehmers in den Vordergrund gerückt hat, seine staatsbürgerlichen Rechte wahrzunehmen. Der Arbeitgeber kann sich seinerseits auf seine Grundrechte aus Art. 12 und 14 GG berufen. Aus der Perspektive des Arbeitsrechtlers sollten freilich nicht alleine grundrechtliche Positionen gegeneinander abgewogen werden, sondern es sollte auch in die Betrachtung mit eingestellt werden, dass der Arbeitnehmer sich mit dem Arbeitsvertrag dem Arbeitgeber gegenüber durch **besondere Rücksichtnahmepflichten** gebunden hat. Während es einer Umweltschutzorganisation völlig **45**

---

[70] Schaub/Linck, ArbR-Hdb., § 53 Rn. 29 ff.
[71] BAG, NZA 2007, 502; BAG, NZA 2004, 427.
[72] EGMR, NZA 2011, 1269 – Heinisch.
[73] Die Anforderungen des EGMR setzen etwa um: LAG Köln, NZA-RR 2012, 298; LAG Schleswig-Holstein, BB 2012, 1862, wenngleich beide Gerichte im Ergebnis zu Entscheidungen gelangen, die weitgehend auf der Linie des BAG liegen.

unbenommen ist, einen entdeckten Verstoß eines Unternehmens gegen Umweltrecht in der Öffentlichkeit zu brandmarken, können die sich aus dem Arbeitsvertrag ergebenden Loyalitätspflichten dem Arbeitnehmer auferlegen, sich erst einmal innerbetrieblich darum zu bemühen, dass Missstände abgestellt werden. Insgesamt rechtfertigt eine überschießende Anzeige, abhängig von ihrer Schwere, regelmäßig die Kündigung des Arbeitsverhältnisses.

46 In die danach erforderliche Abwägung ist insbesondere das Interesse der Allgemeinheit einzustellen, über den einschlägigen Sachverhalt informiert zu sein bzw. deren Interesse daran, dass dieser staatlichen Behörden gegenüber gemeldet wird.

47 Im Regelfall ist allerdings vor der Offenbarung des fraglichen Sachverhalts ein **innerbetrieblicher Klärungsversuch** erforderlich. Eines solchen bedarf es nur dann nicht, wenn es um Straftaten von einigem Gewicht oder um schwerwiegende Verfehlungen geht, die gewichtige Interessen der Allgemeinheit berühren. Weiterhin braucht es dann keiner innerbetrieblichen Abklärung, wenn sich der Arbeitnehmer mit einer Nichtanzeige der Gefahr einer eigenen Strafverfolgung aussetzen würde oder aber, wenn er die fraglichen Handlungen selbst begeht, sodass ein vorheriger innerbetrieblicher Klärungsversuch keinen Erfolg verspricht.

48 Nicht zwingend erforderlich ist, dass sich der vom Arbeitnehmer gemeldete **Sachverhalt** dann tatsächlich als **zutreffend** erweist. Auch ist unerheblich, ob es in einem späteren Strafverfahren zu einer Verurteilung des Arbeitgebers bzw. der handelnden Personen kommt. Doch darf der Arbeitnehmer weder eine **wissentlich falsche**, noch leichtfertig eine unrichtige Anzeige erheben. An dieser Stelle kann auch die Motivation des Arbeitnehmers eine gewichtige Rolle spielen.

49 Weiter kommt es darauf an, welchen **denkbaren Schaden** der Arbeitnehmer mit seiner Anzeige anrichten kann und schließlich, ob die gewählte Reaktion verhältnismäßig ist. Letzteres erlangt in Zusammenhang mit einschlägigen Stellungnahmen des Arbeitnehmers in sozialen Netzwerken große Bedeutung. Insoweit ist nämlich zu beachten, dass ein soziales Netzwerk häufig nicht geeignet ist, um Missstände abzustellen, sondern allenfalls die Öffentlichkeit hierüber informieren kann. Meist wird der Arbeitgeber auf diese Art und Weise jedoch nur angeprangert. So macht es beispielsweise wenig Sinn, wenn ein Spediteur in einem Blog beschuldigt wird, Höchstlenkzeiten nicht einzuhalten, ohne dass die zuständige Straßenverkehrsbehörde hiervon Kenntnis erhält. Weiter kann die Kundgabe im Netz einen unbegrenzt weiten Personenkreis erreichen und ist daher potenziell dazu geeignet, dem Arbeitgeber erheblichen Schaden zuzufügen, zumal sich einmal in die Welt gesetzte negative Schlagzeilen meist nicht mehr rückgängig machen lassen und das Unternehmen daher nur eine eingeschränkte Möglichkeit hat, sich bei unrichtigen oder überzogenen Verdächtigungen zu rehabilitieren. Postings in Netzwerken können daher rasch die Qualität einer Mitteilung an die Presse erlangen und diese ggf. sogar übertreffen. Daher muss danach gefragt werden, ob im jeweiligen Einzelfall nicht eine Mitteilung etwa an eine Aufsichtsbehörde oder auch eine Strafanzeige der richtigere Weg gewesen wäre.

8.4 Arbeitnehmerdatenschutz in sozialen Netzwerken, Recherchen und Überwachungstätigkeiten des Arbeitgebers in sozialen Netzwerken

8.4.1 Allgemeines

Der Arbeitnehmer kann sich über die mittelbare Drittwirkung der Grundrechte auch im Arbeitsverhältnis sowohl auf sein allgemeines Persönlichkeitsrecht[74] als auch auf sein Recht auf informationelle Selbstbestimmung[75] berufen. Beide Rechte müssen sich freilich einer Konkordanzabwägung mit grundrechtlich geschützten Belangen des Arbeitgebers stellen. Zu fragen ist also, ob ein etwaiger Eingriff in das Persönlichkeitsrecht des Arbeitnehmers durch die Wahrnehmung überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt ist. Als einschlägige Rechtspositionen aufseiten des Arbeitgebers kommen dabei insbesondere der Schutz seines Eigentums (Art. 14 GG) vor unbefugten Zugriffen Dritter und seine Berufsfreiheit (Art. 12 GG) in Betracht. Auf einfachrechtlicher Ebene fordert § 32 Abs. 1 S. 1 und 2 BDSG eine im Ergebnis weitgehend ähnliche Abwägung, sodass die Grundsätze, die die Rechtsprechung zum allgemeinen Persönlichkeitsrecht herausgearbeitet hat, auf § 32 BDSG übertragen werden können und umgekehrt. **50**

Insoweit sollte allerdings beachtet werden, dass die Einschränkungen, die das Verfassungs-, Datenschutz- und Strafprozessrecht staatlichen Behörden bei einschlägigen Aktivitäten bzw. Ermittlungen vorgibt, nicht unbesehen, gleichsam im Verhältnis 1:1 auf das **Arbeitsrecht übertragen** werden können. Zwischen dem Zugriff des Staats auf die Daten seiner Bürger und einem privaten Austauschverhältnis bestehen signifikante Unterschiede, was die Informationsbeschaffung angeht, die nicht einfach eingeebnet werden dürfen. Es ist etwas völlig anderes, ob der Staat dem Bürger als ein „Überwachungsorgan" entgegentritt und damit dessen natürliche Freiheit und Selbstentfaltungsinteresse einschränkt, oder ob sich in einem Dauerschuldverhältnis eine Vertragspartei einen Eindruck über seinen Vertragspartner bilden, den Status quo der gegenseitigen Rechtsbeziehung prüfen oder sich einen Überblick über den Stand der Vertragsdurchführung verschaffen möchte. Während es keine wertungsfreie Datenverarbeitung durch den Staat gibt und der Staat daher ohne triftigen Grund von seinen Bürgern nichts zu wissen braucht, liegen die Dinge völlig anders, wenn ein Gläubiger in einer Vertragsbeziehung sich darüber informieren will, ob und ggf. auch in welcher Qualität er die Arbeitsleistung erhalten hat und erst recht, wenn der Arbeitgeber gar nur den jeweiligen Produktionsfortschritt abklären will. Schließlich darf auch nicht übersehen werden, dass der Arbeitgeber bei einschlägigen „Recherchen" meist auf seine eigenen IT-Systeme und Gerätschaften **51**

[74] BVerfGE 117, 202 (229) = NJW 2008, 822 (Rn. 199); BVerfG, JZ 2007, 576 = MMR 2007, 93; BAG (st. Rspr.), vgl. NJW 1985, 702 (Rn. 48) [GrS]; BAG, NZA 2005, 839; BAG, NZA 2012, 1025 (Rn. 29 f.).

[75] BVerfGE 65, 1 = NJW 1984, 419; BVerfGE 120, 378 = NJW 2008, 1505 (Rn. 63).

zugreift und eben nicht in fremde Rechnersysteme eindringt. Selbst was etwa eine E-Mail „des“ Arbeitnehmers betrifft, ist es nicht zwangsläufig so, dass diese in persönlichkeitsrechtlicher Sicht ausschließlich dem Arbeitnehmer zuzuordnen wäre, weil die Postadresse möglicherweise der Sphäre des Arbeitgebers näher steht (etwa: Müller@einkauf-firmaXY.de). Was schließlich soziale Netzwerke betrifft, wird in der Diskussion häufig übersehen, dass es nach den Art. 5, 2 und 1 Abs. 2 GG natürlich auch dem Arbeitgeber freisteht, sich an einem solchen zu beteiligen und dort zu kommunizieren. Daher dürfen nicht immer dann, wenn der Arbeitgeber im Netz „surft“ und dabei auf eine abfällige Äußerung des Arbeitnehmers über ihn stößt, sogleich die Grundsätze der Arbeitnehmerüberwachung herangezogen werden.

52 Am Rande kann für die Bewertung der Rechtmäßigkeit von „Recherchen“ des Arbeitgebers in sozialen Netzwerken schließlich noch eine Frage Bedeutung erlangen, die im Arbeitnehmerdatenschutzrecht intensiv umstritten ist und bislang nicht abschließend geklärt werden konnte. Es geht darum, ob der Arbeitgeber „**Diensteanbieter**“ i. S. v. § 3 Nr. 6 TKG ist. Wäre das der Fall, wären dem Arbeitgeber bei „Ermittlungen“ im Netz ganz erhebliche Restriktionen auferlegt. Grob gesprochen würde das (einfachrechtliche) Arbeitnehmerdatenschutzrecht keine Anwendung mehr finden, vielmehr würde der Arbeitgeber nach § 88 TKG zum Adressaten eines grundrechtsähnlichen, der Regelung des Art. 10 GG nachgebildeten „Fernmeldegeheimnisses“. Dieses lässt einen Zugriff ausschließlich auf sog. Verkehrsdaten (§ 3 Nr. 30 TKG) und auch dies nur in einem sehr begrenzten Umfang zu (s. §§ 96 ff. TKG).[76] Die Verletzung des Fernmeldegeheimnisses stellt dabei einen gewichtigen Verstoß gegen die Rechtsordnung dar, der nach den §§ 201 und 206 StGB strafbewehrt ist.

53 Die Frage, ob der Arbeitgeber **Telekommunikationsanbieter** ist, wird in Rechtsprechung und Literatur uneinheitlich beantwortet. Höchstrichterliche Rechtsprechung fehlt. In den Instanzen geht das OLG Karlsruhe, das den Arbeitgeber einschränkungslos als Anbieter ansieht,[77] am weitesten, wobei sich der Sachverhalt allerdings durch einige Besonderheiten auszeichnet und die Entscheidung insoweit nicht komplett verallgemeinerungsfähig ist.[78] Die wohl überwiegende Ansicht in der Literatur hält den Arbeitgeber dagegen nur, umgekehrt aber auch immer dann für einen Diensteanbieter, wenn er den Arbeitnehmern die private Nutzung betrieblicher

[76] Zu den Einzelheiten: Elschner, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 22.1, Rn. 87 ff.

[77] OLG Karlsruhe, K&R 2005, 181 (zu § 206 StGB, besonderer Sachverhalt); in der Tendenz wohl LAG Hamm, DuD 2013, 50, welches die Frage letztlich aber dahinstehen lässt.

[78] S. die Analyse von Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 224 ff. (225).

„Telekommunikationsdienste“ (§ 3 Nr. 24 TKG) gestattet hat.[79] Hat er diese dagegen untersagt, soll er nicht als Anbieter zu qualifizieren sein.[80] Nicht immer ganz klar wird dabei allerdings, ob der Arbeitgeber in dieser Konstellation insgesamt zum Telekommunikationsanbieter werden soll – so dass auch ein Zugriff des Arbeitgebers auf dienstlich ausgetauschte Daten nur in den engen Grenzen des TKG zulässig wäre – oder ob die Einschränkungen des TKG sich nur auf den privaten Bereich der Kommunikation beziehen sollen.

54 Die Rechtsprechung der Landesarbeitsgerichte tendiert dagegen dazu, den Arbeitgeber generell nicht den Regeln des TKG zu unterwerfen.[81] Hierfür sprechen die besseren Gründe. Der Arbeitgeber gestattet dem Arbeitnehmer die Nutzung von Betriebsmitteln, erbringt aber weder ganz noch teilweise geschäftsmäßig („nachhaltig“) Telekommunikationsdienste, so dass schon der Grundtatbestand des § 3 Nr. 6, 10 u. 24 TKG nicht erfüllt ist. Ebenso wenig sind die Arbeitnehmer Dritte i. S. d. § 3 Nr. 10 TKG, weil der Arbeitgeber dem Arbeitnehmer nicht wie ein externer Anbieter gegenübertritt. Vor allem aber wäre es höchst unbefriedigend, wenn der Arbeitgeber eigene Daten (etwa: Aufträge, Reklamationen, usw.) für den Fall nicht mehr einsehen kann, dass sich die Privatkommunikation des Arbeitnehmers nicht von dessen dienstlicher Korrespondenz trennen lässt, zumal er so gesetzlich zwingenden Dokumentationspflichten wie §§ 257 Abs. 1 Nr. 2 und 3 HGB oder § 147 Abs. 1 Nr. 2 und 3 AO nicht genügen könnte.

55 Das bedeutet freilich nicht, dass der Arbeitgeber deshalb frei in der Erforschung von Kommunikationsinhalten wäre. Vielmehr folgt daraus lediglich, dass er dabei den Schranken unterliegt, wie sie sich aus dem allgemeinen Persönlichkeitsrecht des Arbeitnehmers, dessen Recht auf informationelle Selbstbestimmung und dem Arbeitnehmerdatenschutz ergeben. Letztlich erlangt diese Frage für „Recherchen“ des Arbeitgebers in sozialen Netzwerken allerdings keine übermäßige Bedeutung, weshalb ihr an dieser Stelle auch nicht noch weiter nachgegangen werden soll. Gewicht erlangt sie nämlich nur dann, wenn der Arbeitgeber, um im Netz Nachforschungen anzustellen, Gerätschaften oder Accounts überwacht, die er den Arbeitnehmern zur Verfügung gestellt hat. Häufig liegen die Dinge aber so, dass der Arbeitgeber sich

---

[79] Franzen, in: ErfKomm, § 32 BDSG, Rn. 26; Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 144 ff.; Schaub/Linck, Arbeitsrechts-Handbuch, § 53 Rn. 20 f.; Mengel, Compliance und Arbeitsrecht, Kap. 7 Rn. 18 ff.; Schröder, Datenschutzrecht, Kap. 3, 5.a.aa.; Kilian et al., Computerrechts-Hdb., Individueller Arbeitnehmerdatenschutz Rn. 28; Seifert, in: Simitis, BDSG, § 32 Rn. 87; Hegewald, in: Münchener Anwaltshandbuch IT-Recht, Teil 8 Rn. 82 ff.; Sassenberg/Mantz, BB 2013, 889; Fischer, ZD 2012, 265; Kiesche/Wilke, AiB 2012, 92; Panzer-Heemeier, DuD 2012, 48; Störing, CR 2011, 614; de Wolf, NZA 2010, 1206; Vietmeyer/Byers, MMR 2010, 807; Hilber/Frik, RdA 2002, 89; Lindemann/Simon, BB 2001, 1950; Gola, MMR 1999, 322.

[80] OVG Lüneburg, PersR 2012, 40; VG Karlsruhe, NVwZ-RR 2013, 797.

[81] LAG Berlin-Brandenburg, DB 2011, 1281; LAG Niedersachsen, NZA-RR 2010, 406; VGH Hessen, NJW 2009, 2470; Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 200 ff. (246); Diercks, K&R 2014, 1; Schuster, CR 2014, 21; Fülbier/Splittgerber, NJW 2012, 1995; Schimmelpfennig/Wenning, DB 2006, 2290; Haußmann/Krets, NZA 2005, 259; in der Tendenz wohl auch Kort, DB 2011, 2092.

schlicht von einem eigenen Gerät aus in ein Netz einwählt. Darauf, ob er Telekommunikationsanbieter ist, käme es dagegen nur dann an, wenn der Arbeitnehmer von dienstlichen „Devices" aus kommuniziert und der Arbeitgeber auf diese zugreift, etwa weil er nach dort gespeicherten Kommunikationsprotokollen bzw. Daten sucht oder aber etwa, wenn der Arbeitgeber in die Mailkommunikation des Arbeitnehmers eindringt.

8.4.2 Recherchen des Arbeitgebers in sozialen Netzwerken über Stellenbewerber

56 Für den Arbeitgeber kann es bei der **Bewerberauswahl**, aber auch bei Beförderungsentscheidungen interessant sein, sich im Internet oder in sozialen Netzwerken **Informationen** über den Bewerber bzw. den Arbeitnehmer (die beide im Weiteren zusammenfassend als „Bewerber" bezeichnet werden) zu verschaffen. Derartige Recherchen sind nach §§ 3 Abs. 3, 4 und 11 Nrn. 1 und 7 BDSG an den Vorgaben des BDSG zu messen.[82] Eine Einwilligung des Bewerbers in die Recherche ist zwar theoretisch denkbar, in der Praxis meist jedoch nicht zu bewerkstelligen.[83] Der Arbeitgeber müsste den Bewerber darüber informieren, dass und in welchem Umfang er Informationen über ihn im Internet erheben will, ihm die nach § 4a Abs. 1 S. 2 BDSG erforderlichen Hinweise erteilen und der Bewerber müsste – im Regelfall[84] – schriftlich in die Datenerhebung einwilligen.[85]

57 In der Quintessenz ist eine derartige Bewerberrecherche daher nur möglich, wenn sie durch eine **Rechtsvorschrift zugelassen** ist.[86] Einschlägig ist § 32 Abs. 1 BDSG. Danach dürfen personenbezogene Daten eines Beschäftigten und damit auch eines Stellenbewerbers (§ 3 Abs. 11 Nr. 7 BDSG) erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Darüber hinaus muss die Datenerhebung geeignet und

---

[82] Schmidt, in: ErfKommt Art. 2 GG, Rn. 91.

[83] Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 88 f.; Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 42; Oberwetter, BB 2008, 1562 (1563); Bissels et al., BB 2010, 2433 (2436).

[84] Lembke, in: Henssler et al., Arbeitsrecht, Vorb. BDSG, Rn. 64; Simitis, in: Simitis, BDSG, § 4a Rn. 43; Plath, in: Plath, BDSG, § 4a Rn. 15.

[85] Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 81, 88 mit dem zutr. Hinweis, dass jedenfalls dann von einer konkludenten Einwilligung gesprochen werden kann, wenn in der Bewerbung auf die Internetpräsenz des Bewerbers hingewiesen wird; Seifert, in: Simitis, BDSG, § 32 Rn. 49; Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 43; Bissels et al., BB 2013, 2869 (2870); einschränkend Forst, NZA 2010, 427 (429), die Anmeldung zu einem beruflichen Netzwerk könne u. U. bereits eine Einwilligung darstellen.

[86] Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 82 f.; Oberwetter, BB 2008, 1562 (1563).

angemessen sein.[87] Daneben kommt möglicherweise auch eine Rechtfertigung nach § 28 Abs. 1 S. 1 Nr. 3 BDSG in Betracht. Danach ist eine Datenerhebung zulässig, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Bewerbers an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse des Arbeitgebers offensichtlich überwiegt. Allerdings ist umstritten, inwieweit neben § 32 BDSG die allgemeine „schuldrechtliche" Erlaubnisnorm des § 28 Abs. 1 S. 1 BDSG überhaupt anwendbar ist.[88] Die überzeugenderen Argumente sprechen dabei wohl für eine Konkurrenz beider Normen. Eine Darstellung dieses Streitstands lohnt im vorliegenden Kontext jedoch nicht, weil sich die Anforderungen beider Erlaubnistatbestände im Ergebnis letztlich decken.[89] Denn zwangsläufig wäre im Rahmen der nach § 32 BDSG erforderlichen Abwägung zu berücksichtigen, ob bzw. in welchem Umfang der Arbeitnehmer die betreffenden Informationen im Internet allgemein zugänglich gemacht hat[90], und umgekehrt greift das Gebot der Direkterhebung (§ 4 Abs. 1 BDSG) nicht, wenn die Arbeitgeberrecherche durch den Erlaubnistatbestand des § 32 BDSG gedeckt ist (§ 4 Abs. 2 S. 2 Nr. 1 BDSG).[91]

Eine für die **Praxis hilfreiche Handreichung** bei der erforderlichen Abwägung **58**
der gegenseitigen Interessen bietet dabei § 32 Abs. 6 S. 2 des 2010 vorgelegten, dann aber nicht verabschiedeten Entwurfs für ein Arbeitnehmerdatenschutzgesetz.[92] Dort war vorgesehen, dass der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben darf, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Was Daten aus sozialen Netzwerken betrifft, wurde angenommen, dass das schutzwürdige Interesse des Beschäftigten überwiegt, außer wenn

---

[87] Franzen, in: ErfKomm, § 32 BDSG, Rn.8; Lembke, in: Henssler et al., Arbeitsrecht, § 32 BDSG, Rn. 4; Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 44; Stamer/Kuhnke, in: Plath, BDSG, § 32 Rn. 16 ff.; Forst, NZA 2010, 427 (429).

[88] Ein Konkurrenzverhältnis nehmen an: eingehend Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 57 ff.; ders., NZA 2009, 867; Joussen, JbArbR 47 (2010), 69 (85); Stamer/Kuhnke, in: Plath, BDSG, § 32 Rn. 8 f.; Gola/Schomerus, BDSG, § 32 Rn. 2, 30b; Lembke, in: Henssler et al., Arbeitsrecht, § 32 BDSG, Rn. 4; Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 44; Küttner/Kania, Personalbuch, Nr. 384 Rn. 2; Frings/Wahlers, BB 2011, 3126 (3127); Bissels et al., BB 2010, 2433 (2436); Forst, NZA 2010, 427 (429 f.); Für ein Spezialitätsverhältnis: Franzen, in: ErfKomm, § 28 BDSG, Rn. 1, unter Hinweis auf entsprechenden gesetzgeberischen Willen, der sich indes auch BT-Drs. 16/13657, S. 20 nicht eindeutig entnehmen lässt; Seifert, in: Simitis, BDSG, § 32 Rn. 17; Däubler, in: Däubler et al., BDSG, § 32 Rn. 8; Däubler, Gläserne Belegschaften, Rn. 184 ff.; wohl auch Ernst, NJOZ 2011, 953 (954).

[89] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 78; wohl auch Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 88.

[90] Seifert, in: Simitis, BDSG, § 32 Rn. 50; Gola/Schomerus, BDSG, § 32 Rn. 30b.

[91] Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 80; Gola/Schomerus, BDSG, § 32 Rn. 35a; a. A. aber Däubler, in: Däubler et al., BDSG, § 32 Rn. 56 f.; Däubler, Gläserne Belegschaften, Rn. 248 f.; Stamer/Kuhnke, in: Plath, BDSG, § 32 Rn. 19, 27.

[92] Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes v. 15.12.2010, BT-Drs. 17/4230 (im Folgenden: „BDSG-E").

es sich um soziale Netzwerke handelt, die der Darstellung der beruflichen Qualifikation dienen (§ 32 Abs. 6 S. 3 BDSG-E). Daran anknüpfend lassen sich folgende Grundsätze festmachen:

59 1. Der Arbeitgeber kann Daten, die ganz allgemein über **Suchmaschinen ohne Netzmitgliedschaft** frei zugänglich sind, jederzeit erheben. Er kann also etwa den Bewerber „googlen" und die auf öffentlichen Webseiten zugänglichen Informationen einsehen.[93] Dabei ist jedoch zu beachten, wie alt die Veröffentlichung ist, in welchem Kontext sie erfolgte und ob der Beschäftigte nach den erkennbaren Umständen noch die Herrschaft über die Veröffentlichung hat.[94]
Allerdings hatte § 32 Abs. 6 S. 2 BDSG-E auch vorgesehen, dass der Arbeitgeber den Beschäftigten vor der Erhebung (etwa in einer Stellenanzeige) darauf hinweisen muss, dass er eine entsprechende Recherche vornehmen wird. Das indes erscheint als eine unnütze Förmelei, die in der Praxis überdies nur schwer leistbar ist und dem Bewerber letztlich kaum einen Zugewinn an Schutz bringt. Ein solcher Hinweis ist daher nicht erforderlich.[95]

60 2. Dagegen ist es dem Arbeitgeber verwehrt, sich ohne ausdrückliche Einwilligung des Bewerbers oder des Arbeitnehmers in „**freizeitorientierten**" **Netzwerken** anzumelden oder eine bestehende Mitgliedschaft zu nutzen, um dort Informationen über diesen zu sammeln.[96] Erst recht darf der Arbeitgeber nicht unter einer **falschen Identität**, anonym oder mit einem Pseudonym am Netzwerk teilnehmen, um sich so Zutritt zum zugangsbeschränkten Bereich eines Netzwerks zu verschaffen (beispielsweise um sich als vermeintlicher „Freund" des Arbeitnehmers anzudienen).[97]

61 3. In sozialen **Netzwerken**, die der Darstellung der **beruflichen Qualifikation** des Bewerbers dienen, darf der Arbeitgeber zumindest dann recherchieren, wenn die

---

[93] Küttner/Kania, Personalbuch, Nr. 384 Rn. 2; Schaub/Linck, Arbeitsrechts-Handbuch, § 26 Rn. 11b; Franzen, in: ErfKomm, § 32 BDSG, Rn. 14; Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 88; Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 45; Determann, BB 2013, 181 (188); Ernst, NJOZ 2011, 953 (954); Bissels et al., BB 2010, 2433 (2436); Forst, NZA 2010, 427 (429); Kania/Sansone, NZA 2012, 360 (363 f.); a. A. wohl Wedde, in: Däubler et al., BDSG, § 28 Rn. 58.

[94] Gola/Schomerus, BDSG, § 32 Rn. 35; Determann, BB 2013, 181 (188); vgl. auch Seifert, in: Simitis, BDSG, § 32 Rn. 50; Oberwetter, BB 2008, 1562 (1564).

[95] Ebenso Beckschulze/Natzel, BB 2010, 2368 (2370).

[96] Küttner/Kania, Personalbuch, Nr. 384 Rn. 2; Schaub/Linck, Arbeitsrechts-Handbuch, § 26 Rn. 11; Schmidt, in: ErfKomm, Art. 2 GG, Rn. 90; Stamer/Kuhnke, in: Plath, BDSG, § 32 Rn. 27; Determann, BB 2013, 181 (188); Bissels et al., BB 2013, 2869 (2871 f.); Zilkens/Cavin, ZD 2013, 603 (604); Bissels et al., BB 2010, 2433 (2436); Kania/Sansone, NZA 2012, 360 (363 f.).

[97] Frings/Wahlers, BB 2011, 3126 (3127); Determann, BB 2013, 181 (188); s. auch Küttner/Kania, Personalbuch, Nr. 384 Rn. 2; Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 89 mit dem zutr. Hinweis, dass die Betreiber freizeitorientierter Netzwerke i. d. R in den AGB eine reine Privatnutzung vorsehen, sodass dem Arbeitgeber lediglich eine Erstellung eines Nutzerprofils unter Verschleierung der Nutzung möglich wäre; ebenso Forst, NZA 2010, 427 (429); wohl a. A. Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 45.

jeweilige Darstellung zur eigenen Präsentation auch gegenüber (potenziellen) Arbeitgebern genutzt wird.[98]

4. Umstritten ist, ob die unter (2.) dargestellten Grundsätze auch für die per Suchmaschine erreichbaren Informationen aus freizeitorientierten Netzwerken gelten bzw. für solche Informationen, die im nicht geschützten, öffentlich zugänglichen Bereich eines Netzwerkes niedergelegt sind. Der erwähnte Gesetzesentwurf zum Arbeitnehmerdatenschutz hatte einen Zugriff auf derartige Daten ausgeschlossen.[99] Doch spricht in der Tat einiges dafür, dass der Arbeitgeber jedenfalls solche **Netzwerkinformationen** zur Kenntnis nehmen darf, die er bereits über eine **Suchmaschinenrecherche** erreicht. Lässt man nämlich eine „öffentliche Suche" im Grundsatz zu und erlaubt man dem Arbeitgeber damit, in eine Suchmaschine erst einmal „hineinzusehen", wäre es realitätsfern, ihn gleichzeitig zu verpflichten, vor bestimmten Suchergebnissen die Augen verschließen zu müssen.[100] Darüber hinaus wird der Arbeitgeber wohl auch den „**Jedermannsbereich**" von sozialen Netzwerken einsehen dürfen. Netzwerkteilnehmern ist es zumutbar, Informationen, die sie nicht allgemein zugänglich machen wollen, im geschützten Privat-/Freundesbereich festzuhalten und in vielen Fällen ist es ihnen darüber hinaus auch möglich, Informationen gezielt gegen eine Wiedergabe in Suchmaschinen zu sperren.[101] **62**

8.4.3 Arbeitnehmerüberwachung und Beschaffung von Beweismitteln in sozialen Netzwerken

8.4.3.1 Beweiserhebung

Vor allem dann, wenn der Arbeitgeber eine Kündigung des Arbeitsverhältnisses auf Äußerungen des Arbeitnehmers in sozialen Netzwerken stützen will, stellt sich die **63**

[98] Küttner/Kania, Personalbuch, Nr. 384 Rn. 2, mit der Einschränkung, dass eine Datenerhebung auch hier über ein dem Arbeitgeber zurechenbares Profil erfolgen muss; Schaub/Linck, Arbeitsrechts-Handbuch, § 26 Rn. 11; Schmidt, in: ErfKomm, Art. 2 GG, Rn. 90; Stamer/Kuhnke, in: Plath, BDSG, § 32 BDSG, Rn. 27; Zilkens/Cavin, ZD 2013, 603 (604); Forst, NZA 2010, 427 (429); Kania/Sansone, NZA 2012, 360 (363 f.); kritisch Frings/Wahlers, BB 2011, 3126 (3127) mit dem Hinweis, auch bei Karriereplattformen würden private Kontakte geknüpft; ebenso Bissels et al., BB 2013, 2869 (2869 f.); Ernst, NJOZ 2011, 953 (955); Bissels et al., BB 2010, 2433 (2436).

[99] Zustimmend Riesenhuber, in: BeckOK-BDSG, § 32 BDSG, Rn. 89.2; kritisch insb. Ernst, NJOZ 2011, 953 (956) mit dem Hinweis, die Unterscheidung zwischen rein privaten und beruflichen Netzwerken sei praktisch nicht möglich.

[100] Frings/Wahlers, BB 2011, 3126 (3127), der Gesetzesentwurf sei „nicht praktikabel"; Determann, BB 2013, 181 (188); a. A. offenbar Riesenhuber, in: BeckOK-BDSG, § 32 Rn. 88, Erhebung überschießender Daten sei „unvermeidlich" und daher erforderlich, nicht jedoch deren Verarbeitung und Nutzung.

[101] Frings/Wahlers, BB 2011, 3126 (3127); Bissels et al., BB 2013, 2869 (2871); Oberwetter, BB 2008, 1562 (1564); Bissels et al., BB 2010, 2433 (2436); Kania/Sansone, NZA 2012, 360 (363 f.); a. A. wohl Wedde, in: Däubler et al., BDSG, § 28 Rn. 58.

Frage nach der Verwertbarkeit von Beweisen, die der Arbeitgeber dort durch eigene Recherchen gewonnen hat. Insoweit sind zwei Fragen zu unterscheiden. Zunächst geht es darum, ob die **Beweiserhebung** des Arbeitgebers rechtmäßig war. Ist dies nicht der Fall, ist auf der zweiten Stufe zu prüfen, ob aus der rechtswidrigen Beweiserhebung ein **Beweisverwertungsverbot** folgt. Was Beweisermittlungen des Arbeitgebers in sozialen Netzwerken betrifft, liegen keine höchstrichterlichen Entscheidungen vor. Allerdings hatte das BAG in den vergangenen Jahren zahlreiche Gelegenheiten, um sich mit datenschutzrechtlich relevanten Informationserhebungen seitens des Arbeitgebers zu befassen. Faustformelhaltig lässt sich die Rechtsprechung dahingehend zusammenfassen, dass präventive Maßnahmen höheren Rechtfertigungslasten unterliegen als repressive und ebenso heimliche Ermittlungen durch gewichtigere Sachgründe gedeckt sein müssen, als offen vorgenommene Ermittlungen. Insgesamt hat das BAG, was Überwachungsmaßnahmen angeht, jeweils eine vermittelnde Position eingenommen. Es betont, dass einschlägige Aktivitäten des Arbeitgebers durch hinreichend gewichtige Sachgründe gerechtfertigt sein müssen. Nicht ausreichend ist daher das schlichte Beweisführungsinteresse des Arbeitgebers.[102] Vielmehr müssen zu dem allgemeinen Beweisführungsinteresse weitere Gesichtspunkte hinzutreten, die das Interesse an der Beweiserhebung trotz der Verletzung des Persönlichkeitsrechts als gerechtfertigt erscheinen lassen.

64 Daraus hat das BAG in mehreren Entscheidungen zu Zulässigkeit und Grenzen der Videoüberwachung im Betrieb gefolgert, dass von Bedeutung ist, wie viele Personen der Überwachungsmaßnahme ausgesetzt sind, ob diese anonym oder bekannt ist, ob die überwachten Arbeitnehmer einen Anlass für den Eingriff gegeben haben, insbesondere ob diese einer bereits begangenen oder drohenden Straftat oder Rechtsgutsverletzung verdächtig sind, wo die Überwachungsmaßnahmen stattfinden, wie lange und intensiv diese sind und welche Technik dabei eingesetzt wird und ob durch diese auf die Belegschaft ein (unzulässiger) lang andauernder oder ständiger Überwachungsdruck ausgeübt wird.[103] Besteht ein **hinreichend dichter Kontrollanlass**, lässt das BAG auch eine heimliche Überwachung der betroffenen Arbeitnehmer zu. Einen solchen hält das BAG namentlich dann für gegeben, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die Überwachungsmaßnahme praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.[104]

65 Ganz ähnlich hat das BAG mehrfach entschieden, dass Detektive dann zur (heimlichen) Observation von Arbeitnehmern eingesetzt werden können, wenn gegen

---

[102] Ebenso: BVerfGE 106, 28 [unter C II 4 a bb]; BAG, NZA 2012, 1025 (Rn. 29 f.); BAG, NJW-Spezial 2014, 147 (Rn. 27); BGH, NJW-RR 2010, 1289; BGHZ 27, 284.

[103] BAG, NJW 2014, 810; BAG, NZA 2013, 1433; BAG, NZA 2012, 1025 (Rn. 30); BAG, NZA 2008, 1187; BAG, NZA 2004, 1278; BAG, AP Nr. 42 § 87 BetrVG 1972 – Überwachung.

[104] BAG, NJW 2014, 810 (Rn. 50); BAG, NZA 2012, 1025; BAG, NZA 2003, 119; Ebenso: EGMR, EuGRZ 2011, 471 (Köpke); LAG Hamm v. 15.7.2011 – 10 Sa 1781/10; unentschieden dagegen: BAG, NZA 2011, 571.

diese ein konkreter Verdacht besteht, die detektivische Tätigkeit zur Klärung der Beweisfrage erforderlich ist und nicht andere, mildere Maßnahmen als genügend erscheinen.[105] Gleiche Grundsätze bestehen für Tor- und Taschenkontrollen.[106] In diese Reihe fügt sich auch eine Entscheidung des BGH in einer Strafsache, wonach die heimliche Überwachung einer „Zielperson" mittels eines GPS-Empfängers zwar grundsätzlich strafbar ist, aber bei Vorliegen eines starken berechtigten Interesses an der Datenerhebung sich im Zuge der Abwägung ausnahmsweise ergeben kann, dass das Merkmal des unbefugten Handelns bei derartigen Einsätzen von GPS-Technik zu verneinen ist. Präventiv darf der Arbeitgeber in Verkaufseinrichtungen Testkäufer einsetzen, die die Ehrlichkeit der Mitarbeiter überprüfen (sog. „Wechselgeldfalle"), wenn er ansonsten keine anderweitige reelle Chance hat, um die Zuverlässigkeit seiner Mitarbeiter zu überprüfen.[107]

Bei der Bewertung von Überwachungsmaßnahmen in sozialen Netzwerken müssen diese Abwägungsgesichtspunkte dann allerdings noch um die tatsächlichen und rechtlichen Besonderheiten derartiger Kommunikationsplattformen erweitert werden. **66**

Auf der einen Seite darf – worauf schon eingangs dieses Abschnitts hingewiesen wurde – eben nicht übersehen werden, dass es dem Arbeitgeber völlig frei steht, sich selbst an einem sozialen Netzwerk zu beteiligen und dort zu kommunizieren. So macht es einen gewaltigen Unterschied, ob der Arbeitgeber heimlich in der Fabrikationshalle eine Videokamera anbringt oder ob er im Netz surft. Insoweit unterliegt er selbst dann keinen Einschränkungen, wenn er das tut, um sich darüber zu informieren, welches Ansehen das Unternehmen oder seine Produkte genießen. Der Arbeitgeber kann wie jeder andere auch an öffentlichen Kommunikationsprozessen teilnehmen, sodass einschlägige Aktivitäten nicht unbesehen als Überwachungsmaßnahmen qualifiziert werden dürfen. Persönlichkeits- und datenschutzrechtlich relevant werden einschlägige Vorgänge erst dann, wenn der Arbeitgeber die so gewonnenen Daten über den Arbeitnehmer verwendet, wenn er im Netz **gezielt** über Arbeitnehmer **recherchiert**[108] und das insbesondere dann, wenn er sich mit **falscher Identität** an sozialen Netzwerken beteiligt. Die Grenzziehung zwischen beiden Tatbeständen fällt freilich schwer und wird die Gerichtspraxis in den nächsten Jahren sicherlich noch intensiv beschäftigen. Ausnahmslos datenschutzrechtlich relevant wird der Vorgang freilich dann, wenn der Arbeitgeber sich durch Täuschung Zugang zum „Freundesbereich" eines Netzwerkes verschafft, um so Informationen über den Arbeitnehmer zu bekommen, die offensichtlich nicht für ihn bestimmt sind.[109] **67**

---

[105] BAG, NZA-RR 2011, 231; BAG, NZA 2009, 1300; BAG, NZA 1998, 1334; ähnlich auch: BGH, NJW-RR 2009, 1189.
[106] BAG, NZA 2008, 1008; BAG, NZA 2000, 421; BAG, NZA 1988, 811.
[107] BAG, NZA 2000, 148.
[108] Ernst, NJOZ 2011, 953 (957); Wybitul, Hdb. Datenschutz in Unternehmen, S. 107.
[109] Kort, NZA 2012, 1321 (1325).

68 Auf der anderen Seite kommt „Ermittlungsaktivitäten“ in sozialen Netzwerken eine gewisse Tendenz zu, die Vertraulichkeit des gesprochenen Wortes zu tangieren. Wie bereits unter 8.3.1. aufgezeigt wurde, räumt die Rechtsprechung der Vertraulichkeit des Wortes einen hohen Stellenwert ein. Sie erkennt einen geschützten Raum an, in dem jedermann unbeobachtet sich selbst überlassen ist oder mit Personen seines besonderen Vertrauens ohne Rücksicht auf gesellschaftliche Verhaltenserwartungen verkehren kann.[110] Wie dargestellt darf der Arbeitnehmer darauf vertrauen, dass eine in der Privatsphäre gefallene Äußerung nicht nach außen getragen wird.[111] Damit stellt sich auch an dieser Stelle die oben (Rn. 23 ff.) bereits ausführlich erörterte Problematik, ob ein und ggf. welcher Bereich eines sozialen Netzwerkes in der beschriebenen Weise vertraulich ist. Eben deshalb gilt, dass wenn sich der Arbeitgeber den Zugang zum beschränkten Personenkreis eines Forums (Freundesliste etc.) erschleicht oder er den Zugangsschutz einer geschlossenen (geheimen) Gruppe oder eines passwortgeschützten Forums überwindet, indem er den Arbeitnehmer über seine Identität täuscht, die Beweiserhebung ohne Weiteres rechtswidrig ist.[112]

8.4.3.2 Beweisverwertung

69 Grundsätzlich kennt das deutsche Zivilprozessrecht zwar kein ausdrückliches prozessuales **Verwendungs- bzw. Verwertungsverbot** für rechtswidrig erlangte Informationen oder Beweismittel. Nach der ständigen Rechtsprechung des BVerfG[113], des BGH[114] und des BAG[115] ergibt sich vielmehr aus Art. 103 GG bzw. aus § 286 ZPO die grundsätzliche Pflicht des Richters, den von den Parteien vorgetragenen Sachverhalt und die von ihnen angebotenen Beweise zu berücksichtigen.[116] Die Aufrechterhaltung einer funktionstüchtigen Rechtspflege und das Streben nach einer materiell richtigen Entscheidung sind wichtige Belange des Gemeinwohls, weshalb die Gerichte grundsätzlich gehalten sind, die Wahrheit zu ermitteln. Dagegen würde ein uneingeschränktes Verwertungsverbot unzulässig erlangter Beweismittel den Anspruch der Parteien auf rechtliches Gehör unverhältnismäßig einschränken.

---

[110] BVerfG v. 27.7.2009 – 2 BvR 2186/07; BVerfG, NJW 2007, 1194; BVerfGE 106, 28; BVerfGE 90, 255 (Rn. 21).

[111] BAG, NZA 2010, 698; BAG v. 17.2.2000 – 2 AZR 927/98; BAG, AP Nr. 66 zu § 626 BGB.

[112] Bauer/Günther, NZA 2013, 67 (70); Pawlak/Smeyers, öAT 2013, 26 (28 f.); Kort, NZA 2012, 1321 (1323 f.).

[113] BVerfGE 11, 218 (220); 60, 247 (249); 70, 288 (293) – Bierlieferungsquote; BVerfG v. 31.3.2006 – 1 BvR 2444/04 (Rn. 18); BVerfG v. 4.4.2007 – 1 BvR 2941/06; BVerfG, FamRZ 2008, 673 (Rn. 10); BVerfG, NJW 2011, 49; BVerfG, NJW 2014, 206 (Rn. 19).

[114] BGH, WM 2011, 1533 (Rn. 6 f.); BGH, NJW 2007, 372 (374); BGH, NJW 2003, 1123 (Rn. 17); BGH, NJW 2000, 1420 (1421); BGH, NJW 1995, 1210; BGH, NJW 1992, 1817 (1819).

[115] BAG, NZA 2014, 243; BAG, NZA 2012, 1025; BAG, NZA 2011, 571; BAG, NZA 2009, 974; BAG, NZA 2008, 1008; BAG, NZA 2003, 1193.

[116] Schmidt-Aßmann, in: Maunz/Dürig, GG, Art. 103 Rn. 94 ff.; Reichold, in: Thomas/Putzo, ZPO, § 286 Rn. 2a; Greger, in: Zöller, ZPO, § 286 Rn. 2; Baumbach et al., ZPO, § 286 Rn. 13, 22; Prütting, in: MüKo-ZPO, § 286 Rn. 12; Helle, JZ 2004, 340; Kort,NZA 2012, 1321 (1325); Lunk, NZA 2009, 457; Schlewing, NZA 2004, 1071; Röckl/Fahl, NZA 1998, 1035.

Allerdings zieht das BAG eine Grenze dort, wo eine Überwachung unter keinem Gesichtspunkt zulässig war, insbesondere weil kein Anfangsverdacht erkennbar war oder ihre Unverhältnismäßigkeit einigermaßen offen zu Tage lag. Hier greift nach der neuen Rechtsprechung ein **Beweisverwertungsverbot**. Zudem ist zu beachten, dass es bislang in fast allen Fällen so war. dass die Beweiserhebung selbst zulässig war, sodass den Ausführungen des Gerichts zur Verwertbarkeit von in unzulässiger Weise gewonnenen Beweismitteln letztlich eher nur die Qualität eines obiter dictum zukommt. Dass das BAG bei eindeutig rechtswidrigen Erhebungen ein Verwertungsverbot annimmt, überzeugt dabei auch deshalb, weil es schon einer gehörigen Portion an Scharfsinn bedarf, um das eigentlich Verbotene nachträglich doch noch zum Erlaubten zu machen. Das wiederum gilt umso mehr, als auf beiden Ebenen dieselben grundrechtlich geschützten Positionen miteinander konkurrieren, denn das Interesse des Arbeitgebers, die gegen ihn verübte Straftat aufzuklären und den Schuldigen herauszufinden, unterscheidet sich in nichts von seinem Interesse, eine gegen diesen ausgesprochene Kündigung vor Gericht dann auch tatsächlich durchzusetzen. **70**

Für diese Sichtweise spricht auch, dass wenn die Verwertung rechtswidrig erlangter Beweismittel ohne Weiteres zulässig wäre, der Arbeitgeber es relativ zwanglos erst einmal mit einer verdeckten Überwachung versuchen könnte. Zwar weiß er, dass das verboten ist. Doch weiß er dann eben auch, dass ihm das im Erfolgsfall nicht schaden wird (jedenfalls theoretisch nicht, denn in der Betriebspraxis können unzulässige Überwachungsmaßnahmen, zumindest dann, wenn sie erfolglos sind, sowohl das Arbeitsklima als auch das Verhältnis mit dem Betriebsrat belasten). **71**

Erforderlich ist daher in jedem Fall eine sehr sorgfältige bis eher strenge Abwägung dahingehend, ob der mit der Beweisverwertung verbundene neuerliche Eingriff in das Persönlichkeitsrecht des betroffenen Arbeitnehmers wirklich durch das Interesse des Arbeitgebers an einem materiell richtigen Urteil aufgewogen wird. Insoweit richtet das BAG zunehmend strengere Anforderungen an den Sachvortrag des Arbeitgebers. Er muss hinreichend genau darlegen, woraus er den Verdacht herleitet, warum sich dieser gegen den überwachten Personenkreis richtet, was er ansonsten unternommen hat und warum tatsächlich keine weniger einschneidenden Mittel zur Aufklärung des Verdachts zur Verfügung standen. So genügen etwa bloße pauschale Hinweise auf nur diffus dargestellte Vermögensdelikte im Betrieb, Waren- oder Kassendifferenzen nicht. Weiter darf mit Verwertung des rechtswidrig erlangten Beweismittels keine erhebliche Verletzung des Persönlichkeitsrechts verbunden sein.[117] Das ist nach Ansicht des BAG insbesondere dann der Fall, wenn mit der Informationsbeschaffung die Vertraulichkeit des gesprochenen Wortes verletzt wurde.[118] **72**

Genau das deutet daraufhin, dass ein unzulässiger Zugriff des Arbeitgebers auf soziale Netzwerke häufig ein Beweisverwertungsverbot nach sich ziehen wird. Das gilt zumindest dann, wenn der Arbeitgeber oder ein von ihm beauftragter Dritter einschlägige Zugangshürden, namentlich durch Täuschung über seine Identität, überwindet und er so an Informationen gelangt, die ersichtlich nicht für die Öffentlichkeit oder **73**

[117] BAG, NZA 2014, 243 NZA 2011, 571; BAG, NZA 2009, 974; BAG, NZA 2008, 1008.
[118] BAG, NZA 2009, 974s. BAG, NZA 2014, 243 Rn. 56 ff.

jedenfalls nicht für ihn bestimmt waren.[119] Dagegen ergibt sich alleine aus dem Umstand, dass einschlägige Aktivitäten des Arbeitgebers mitbestimmungswidrig waren, kein Beweisverwertungsverbot.[120]

8.5 Kollektivrechtliche Regelungen, Mitbestimmung und betriebliche Guidelines

74 Anordnungen, Weisungen und Maßnahmen des Arbeitgebers im Zusammenhang mit der Nutzung sozialer Netzwerke können fallabhängig ein Mitbestimmungsrecht des Betriebsrats auslösen. Mit Rücksicht auf den Gesetzesvorbehalt des § 87 Abs. 1 BetrVG kein Mitbestimmungsrecht des Betriebsrats ist allerdings eröffnet, soweit der Arbeitgeber in Anordnungen oder so genannten „**Social Media Guidelines**" nur die bestehende Rechtslage wiederholt. Das ist beispielsweise der Fall, wenn er die Belegschaft auffordert, keine strafbaren Inhalte im Internet einzusehen oder aus diesem zu laden. Ebenfalls kein Mitbestimmungsrecht besteht, soweit einzelne Passagen von Guidelines nur appellativen Charakter haben, etwa wenn sie nicht mehr als das „ethisch-moralische Erscheinungsbild" des Unternehmens beschreiben sollen.[121]

75 Darüber hinaus ist im Zusammenhang mit Vorgaben des Arbeitgebers im Bereich der Nutzung von Social Media zu beachten, dass diese häufig nur das **Arbeitsverhalten** betreffen und Anweisungen des Arbeitgebers hierzu nicht mitbestimmungspflichtig sind.[122] Das Arbeitsverhalten ist immer dann betroffen, wenn der Arbeitgeber die Arbeitspflicht des Arbeitnehmers unmittelbar konkretisiert, also Anordnungen trifft, die vom Arbeitnehmer bei der Erbringung seiner geschuldeten Arbeitsleistung zu beachten sind. Verbietet der Arbeitgeber der Belegschaft, technische Kommunikationsmittel zu privaten Zwecken zu nutzen, ist das also grundsätzlich ebenso mitbestimmungsfrei, wie wenn ein Spediteur es unterbindet, dass die bei ihm beschäftigen Fahrer die Firmen-LKW zu Privatfahrten nutzen. Nichts anderes gilt, wenn der Arbeitgeber einen Arbeitnehmer anweist, nicht während seiner Arbeitszeit über eigene Gerätschaften privat mit Dritten zu kommunizieren.[123] Im Ansatz mitbestimmungsfrei ist es daher auch, wenn der Arbeitgeber die Privatnutzung zulässt, sie indes nach Art und Umfang einschränkt.

76 Anders, als es vielleicht auf den ersten Blick den Anschein hat, spricht keine dieser Fallgestaltungen das Ordnungsverhalten des Arbeitnehmers an (§ 87 Abs. 1 Nr. 1 BetrVG). Normen, Maßnahmen oder Weisungen des Arbeitgebers betreffen

---

[119] Kort, NZA 2012, 1321 (1325).
[120] BAG, NZA 2008, 1008; BAG, NZA 2003, 1193.
[121] BAG, NZA 2008 1248.
[122] BAG, NZA 2013, 467 (Rn. 14); BAG, NZA 2008, 1248 (Rn. 58); Fitting et al., BetrVG, § 87 Rn. 64 ff.; Kania, in: ErfKomm, § 87 BetrVG, Rn. 18; Clemenz, in: Henssler et al., Arbeitsrecht, § 87 BetrVG, Rn. 62, 64; kritisch Richardi, in: Richardi, BetrVG, § 87 Rn. 501.
[123] LAG Hamm, NZA-RR 2007, 20; Forst, ZD 2012, 251 (254); Frings/Wahlers, BB 2011, 3126 (3130).

dann das Ordnungsverhalten, wenn sie Verhaltensregeln vorgeben, die das Zusammenleben und Zusammenwirken der Arbeitnehmer außerhalb deren Arbeitsverhalten gestalten, gewährleisten oder aufrechterhalten sollen.[124] Verbietet der Arbeitgeber aber nur die Privatnutzung von betrieblichen Kommunikationsmitteln, lässt er diese zu oder beschränkt er den Umfang der zugelassenen Privatnutzung, übt er lediglich sein Direktionsrecht nach § 106 GewO aus, indem er erklärt, dass er (nicht) auf einen (beschränkten) Teil der vertraglich geschuldeten Arbeitsleistung verzichten will und/oder den Arbeitnehmern (nicht) gestattet, sein Eigentum für unternehmensfremde Zwecke zu nutzen.

77 Mittelbar eingreifen kann hingegen das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG. Danach steht dem Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von **technischen Einrichtungen** zu, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Als technische Einrichtung gilt dabei nicht nur die Hardware moderner Kommunikationstechnik, vielmehr fällt auch jegliche Form von Software unter den Tatbestand. Dabei ist nach der ständigen Rechtsprechung des BAG nicht erforderlich, dass die technische Einrichtung ausschließlich oder überwiegend die Überwachung des Arbeitnehmers zum Ziel hat. Vielmehr genügt, wenn die Einrichtung auf Grund ihrer technischen Gegebenheiten objektiv zur Überwachung von Arbeitnehmern geeignet ist.[125]

78 Was daraus dann aber genau für die Einführung und Verwendung moderner Informationstechnologien im Betrieb folgt, ist letztlich offen. Dass dies bislang nicht eindeutig geklärt werden konnte, liegt wiederum daran, dass der Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG nicht auf die **Informationsgesellschaft** zugeschnitten ist, sondern noch aus einer Zeit stammt, als der Arbeitgeber nur ganz vereinzelt eine technische Einrichtung in Betrieb genommen hatte (wie etwa ein neues Stechuhrensystem), das zur Überwachung der Arbeitnehmer geeignet war. Daher eignet sich die Norm in ihrer gegenwärtigen Fassung nur sehr bedingt zur Anwendung auf das Informationszeitalter, das Unternehmen in kürzesten Abständen eine Anpassung der im Betrieb verwendeten Software abverlangt. Theoretisch lässt sich nämlich mit jedem Gerät, das Daten aufzeichnen oder speichern kann, die Arbeitsleistung oder das Verhalten seines jeweiligen Nutzers ermitteln. Entsprechend wäre das Aufspielen einer jeden neuen Software auf einen vorhandenen Rechner, jedes Upgrade eines Programms oder etwa der Erwerb eines PC, eines Laptops oder eines Mobiltelefons bzw. dessen Weitergabe an einen Arbeitnehmer mitbestimmungspflichtig.[126] Das wiederum erscheint aber insoweit nicht zielführend, als die meisten Geräte zunächst einmal nur reinen Betriebszwecken dienen, indem sie Produktionsvorgänge steuern, Aufträge verwalten, Buchungen vornehmen oder Kommunikationsmöglichkeiten mit Dritten eröffnen sollen. Der Arbeitnehmer erhält sie in allererster Linie deshalb, damit er mit diesen seine Arbeitsleistung erbringen kann.

---

[124] Grundlegend: BAG, NZA 2000, 1176. BAG, NZA 1990, 320.
[125] BAG, NZA 2005, 839; BAG, NZA 2004, 1278; BAG, NZA 1985, 671; BAG, NZA 1985, 669.
[126] So in der Tat: Klebe et al., BetrVG, § 87 Rn. 37; Däubler et al., BetrVG, § 87 Rn. 201; Fitting et al., BetrVG, § 87 Rn. 246; Worzalla, in: Henssler, Arbeitsrecht, BetrVG, § 87 Rn. 366.

79 Daher sprechen sich viele Stimmen in der Literatur dafür aus, den **Begriff der „technischen Einrichtung“** so einzuschränken, dass er erst dann greift, wenn auf Grund der jeweiligen Programmierung auch tatsächlich einschlägige Daten erfasst werden können.[127] Aber auch das erweist sich bei Licht betrachtet kaum als eine nennenswerte Begrenzung des Tatbestands, weil mehr oder weniger jede Software bei Eingabe entsprechender Befehle Rückschlüsse auf das Verhalten des jeweiligen Nutzers zulässt (etwa: Nutzungsdauer, abgerufene Seiten, Chatprotokolle u. dgl.). Und dennoch bleibt mangels greifbarer Alternativen kaum eine andere Wahl, als an diese Definition anzuknüpfen und sie dadurch praxistauglich zu machen, indem man sie mit Augenmaß anwendet und Erwerbs- und Installationstatbestände, die erkennbar neutral sind, aus dem Mitbestimmungstatbestand ausnimmt, so dass etwa der bloße Ankauf eines Mobiltelefons und dessen Weitergabe an den Arbeitnehmer kein Mitbestimmungsrecht des Betriebsrats auslösen würde. Umgekehrt gilt dann aber auch, dass das Verbot oder die Erlaubnis der Privatnutzung von betrieblichen Kommunikationsmitteln immer dann mitbestimmungspflichtig wird, wenn diese mit der Ankündigung einschlägiger Kontrollmaßnahmen verbunden werden oder aber die Arbeitnehmer im Gegenzug zur Nutzungsmöglichkeit sich mit Überwachungsmaßnahmen des Arbeitgebers einverstanden erklären sollen.[128] Zuzugeben ist, dass diese Grenzziehung nicht scharf und für die Betriebspraxis mit Rechtsunsicherheiten verbunden ist. Diesen lässt sich nur über den Abschluss klarstellender **Betriebsvereinbarungen** begegnen.

80 Davon unabhängig wird Arbeitgebern in der Literatur häufig empfohlen, Guidelines zur Nutzung von Social Media im Betrieb festzulegen, zumindest dann, wenn Arbeitnehmern internettaugliche Geräte zur Nutzung überlassen werden.[129] Mögliche Regelungsgegenstände sind dabei:

- Allgemeine Grundsätze zum Gebrauch betrieblicher Kommunikationsmittel: Art und Weise der Nutzung von Hard- und Software, Einrichtung und Gebrauch von Passwörtern, Speicherort von Daten
- Datensicherung, Archivierung und Löschen von Daten
- Verbot der eigenmächtigen Installation von Software, Laden von Apps, Verbot des Abschaltens bzw. der Umgehung von Sicherheitsprogrammen und -sperren, Einwahl in fremde Netzwerke (z. B. an Bahnhöfen, am Flughafen oder in Hotels u. dgl.), Nutzung der Geräte im Ausland, Weitergabe der Geräte an Dritte, Verhalten im Verlustfall
- Hinweis und Aufklärung über Risiken und Folgen der möglicherweise unbewussten Preisgabe betrieblicher und persönlicher Daten in sozialen Netzwerken

---

[127] Richardi, in: Richardi, BetrVG, § 87 Rn. 505; Fitting et al., BetrVG, § 87 Rn. 232; a. A. Däubler, Gläserne Belegschaften, Rn. 761 f., der allein die Programmierbarkeit für ausreichend erachtet; ebenso Däubler et al., BetrVG, § 87 Rn. 191.

[128] Für eine generelle Mitbestimmungspflicht der Erlaubnis/des Verbots der Privatnutzung: Däubler, Gläserne Belegschaften, Rn. 828.

[129] Frings/Wahlers, BB 2011, 3126 (3132); Lützeler/Bissels, ArbRAktuell 2011, 499; Lelley/Fuchs, CCZ 2010, 147.

- Verhalten zur Nutzung sozialer Netzwerke im Auftrag des Arbeitgebers[130], wie etwa: Auftreten im Namen der Firma, Gebrauch von Unternehmenskennzeichen, geschäftlichen Bezeichnungen, Nutzung von Firmenlogos, Bewerberrecherchen
- Verbot der Nutzung betrieblicher Kommunikationsmittel zu Privatzwecken, Umfang einer erlaubten Privatnutzung betrieblicher Kommunikationsmittel
- Verbot einer inhaltlich unangemessenen Privatnutzung (Laden strafbarer, gewaltverherrlichender oder pornografischer Inhalte)
- Nutzung sozialer Netzwerke während der Arbeitszeit, ggf. beschränkt nach Dauer, Anlass und Umfang der Nutzung (etwa: lediglich geringfügige Nutzung, keine Nutzung während der Arbeitszeit, sondern nur während der Pausen).

Literatur

Bauer, J.-H., Günther, J. (2013). Kündigung wegen beleidigender Äußerungen auf Facebook – Vertrauliche Kommunikation unter Freunden? *NZA*, 67 ff.

Baumbach, A., Lauterbach, W., Albers, J. & Hartmann, P. (2014). *Zivilprozessordnung. Kommentar*. 72. Aufl. München: C.H. Beck.

Beckschulze, M., Natzel, I. (2010). Das neue Beschäftigtendatenschutzgesetz – Eine Darstellung des aktuellen Gesetzentwurfs vom 25.8.2010. *BB*, 2368 ff.

Bissels, A. (2012). Kündigung eines Ausbildungsverhältnisses wegen beleidigender Äußerungen bei Facebook. *JurisPR-ArbR* 37/2012, Anm. 1.

Bissels, A., Domke, C. & Wisskirchen, G. (2010a). BlackBerry & Co.: Was ist heute Arbeitszeit? *DB*, 2052 ff.

Bissels, A., Lützeler, M. & Wisskirchen, G. (2010b). Facebook, Twitter & Co.: Das Web 2.0 als arbeitsrechtliches Problem. *BB*, 2433 ff.

Bissels, A., Ziegelmayer, D. & Kiehn, B. (2013). Gesucht, gefunden, angesprochen: Rechtliche Tücken des „Active Sourcing". *BB*, 2869 ff.

Braun, F. (2012). Erlaubte Beleidigung des Ex-Arbeitgebers auf Facebook. *JurisPR-ITR* 20/2012 Anm. 5.

Byers, P., Mößner, S. (2012). Die Nutzung des Web 2.0 am Arbeitsplatz: Fluch und Segen für den Arbeitgeber. BB, 1665 ff.

Däubler, W. (2010). Gläserne Belegschaften? 5. Aufl. Frankfurt a. M.: Bund-Verlag.

Däubler, W. (2013). Persönlichkeitsschutz des Arbeitnehmers im Internet? *DuD*, 759 ff.

Däubler, W., Klebe, T., Wedde, P. & Weichert, T. (2010). *Bundesdatenschutzgesetz. Kommentar*. 3. Aufl. Frankfurt a. M.: Bund-Verlag, Frankfurt a. M.

Determann, L. (2013). Soziale Netzwerke in der Arbeitswelt – Ein Leitfaden für die Praxis. *BB*, 181 ff.

Diercks, N. (2014). Social Media im Unternehmen – Zur Zweckmäßigkeit des Verbots der (privaten) Nutzung unter besonderer Berücksichtigung von § 88 TKG. *K & R*, 1 ff.

Ernst, S. (2011). Social Networks und Arbeitnehmer-Datenschutz. *NJOZ*, 953 ff.

Fischer, J. (2012). Arbeitnehmerschutz beim E-Mail-Verkehr – Von der funktionalen Bestimmung bis zum Fernmeldegeheimnis. *ZD*, 265 ff.

Fitting, K., Engels, G., Schmidt, I., Trebinger, Y. & Linsenmaier, W. (2014). *Betriebsverfassungsgesetz. Kommentar*. 27. Aufl. München: Verlag Franz Vahlen.

Forst, G. (2010). Bewerberauswahl über soziale Netzwerke im Internet? *NZA*, 427 ff.

Frings, A., Wahlers, U. (2011). Social Media, iPad & Co. im Arbeitsverhältnis. *BB*, 3126 ff.

[130] S. oben, Rn. 1 ff.

Fülbier, U., Splittgerber, A. (2012). Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber? *NJW*, 1995 ff.
Geuer, E., Seidl, A. (2012). Ersatz von Anwaltskosten nach ehrverletzenden Aussagen auf Pinnwand bei Facebook. *JurisPR-ITR 5/2012*, Anm. 4.
Gola, P. (1999). Neuer Tele-Datenschutz für Arbeitnehmer? – Die Anwendung von TKG und TDDSG im Arbeitsverhältnis. *MMR*, 322 ff.
Gola, P., Schomerus, R. (2012). *Bundesdatenschutzgesetz, Kommentar*. 11. Aufl. München: C.H. Beck.
Göpfert, B., Wilke, E. (2011). Facebook-Aktivitäten als Kündigungsgrund. *ArbRAktuell*, 159 ff.
Haußmann, K., Krets, J. (2005). EDV-Betriebsvereinbarungen im Praxistest. *NZA*, 259 ff.
Helle, J. (2004). Die heimliche Videoüberwachung – zivilrechtlich betrachtet. *JZ*, 340 ff.
Henssler, M., Willemsen, H. J. & Kalb, H.-J. (Hrsg.) (2012). *Arbeitsrecht. Kommentar*. 5. Aufl. Köln: Verlag Dr. Otto Schmidt.
Hess, H., Worzalla, M., Glock, D., Nicolai, A., Rose, F.-J. & Huke, K. (2014). *Betriebsverfassungsgesetz. Kommentar*. 9. Aufl. Köln: Luchterhand.
Hilber, M., Frik, R. (2002). Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat. *RdA*, 89 ff.
Hinrichs, L., Hörtz, M. (2013). Web 2.0: Bild' Dir Deine Meinung – auf Kosten des Arbeitgebers? *NJW*, 648 ff.
Hoeren, T., Sieber, U. & Holznagel, B. (2013). *Handbuch Multimedia-Recht* (Loseblatt, Stand: 36. Ergänzungslieferung 2013). München: C.H. Beck, München.
Howald, B. (2013). Meinungsfreiheit im Arbeitsverhältnis. *ArbRAktuell*, 195 ff.
Joussen, J. (2010). Die Neufassung des § 32 BDSG – Neues zum Arbeitnehmerdatenschutz? *JbArbR* 47, 69 ff.
Kania, T., Sansone, P. (2012). Möglichkeiten und Grenzen des Pre-Employment-Screenings. *NZA*, 360 ff.
Kaumanns, P. (2012). Anmerkung zum Urteil des ArbG Dessau-Roßlau vom 21.03.2012 (AZ: 1 Ca 148/11; Fundstelle: K & R 2012, 442) – Zur Frage der Kündigung wegen Betätigung des „Gefällt-mir"-Buttons zu abwertender Äußerung über Arbeitgeber. *K & R*, 445 ff.
Kiesche, E., Wilke, M. (2012). Fernmeldegeheimnis im Arbeitsverhältnis – Ungeklärte Fragen und eine nicht überzeugende Gerichtsentscheidung. *AiB*, 92 ff.
Kilian, W., Heussen, B. (2013). *Computerrechts-Handbuch* (Stand: August 2013). München: C.H. Beck.
Klebe, T., Ratayzak, J., Heilmann, M. & Spoo, S. (2010). *Betriebsverfassungsgesetz. Kommentar*. 16. Aufl. Frankfurt a. M.: Bund-Verlag.
Koch, F. (2008). Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel. *NZA*, 911 ff.
Kock, M., Dittrich, A. (2013). Unmutsäußerungen und Beleidigungen auf Facebook & Co. als Kündigungsgrund. *DB*, 934 ff.
Kort, M. (2011). Einsatz von IT-Sicherheitsmaßnahmen durch den Arbeitgeber: Konsequenzen einer Anwendung des Telekommunikationsgesetzes (TKG). *DB*, 2092 ff.
Kort, M. (2012). Kündigungsrechtliche Fragen bei Äußerungen des Arbeitnehmers im Internet. *NZA*, 1321 ff.
Kramer, S. (2004). Internetnutzung als Kündigungsgrund. *NZA*, 457 ff.
Kramer, S. (2006). Kündigung wegen privater Internetnutzung. *NZA*, 194 ff.
Kramer, S., Rasche, J. (2013). Facebook-Posting als Kündigungsgrund. *FA*, 330 ff.
Lelley, J. T., Fuchs, O. (2010). My Space is not Your Space – Einige arbeitsrechtliche Überlegungen zu Social Media Guidelines. *CCZ*, 147 ff.
Leupold, A., Glossner, S. (2013). *Münchener Anwaltshandbuch IT-Recht*. 3. Aufl. München: C.H. Beck.
Lindemann, A., Simon, O. (2001). Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung. *BB*, 1950 ff.
Lunk, S. (2009). Prozessuale Verwertungsverbote im Arbeitsrecht. *NZA*, 457 ff.

Lützeler, M., Bissels, A. (2011). Social Media-Leitfaden für Arbeitgeber: Rechte und Pflichten im Arbeitsverhältnis. *ArbRAktuell*, 499 ff.
Maunz, T., Dürig, G. (Begr.) (2013). *Grundgesetz. Kommentar* (Loseblatt, Stand: 69. Ergänzungslieferung). München: C.H. Beck.
Melot de Beauregard, P., Gleich, C. (2012). Social Media am Arbeitsplatz – Chancen und Risiken. *DB*, 2044 ff.
Mengel, A. (2009). *Compliance und Arbeitsrecht*. München: C.H. Beck.
Moll, W. (2012). *Münchener Anwaltshandbuch Arbeitsrecht*. 3. Aufl. München: C.H. Beck.
Müller-Glöge, R., Preis, U. & Schmidt, I. (Hrsg.) (2014). *Erfurter Kommentar zum Arbeitsrecht*. 14. Aufl. München: C.H. Beck.
Notzon, M. (2013). Arbeitsrecht meets Facebook. *öAT*, 180 ff.
Oberwetter, C. (2008). Bewerberprofilerstellung durch das Internet – Verstoß gegen das Datenschutzrecht? *BB*, 1562 ff.
Panzer-Heemeier, A. (2012). Der Zugriff auf dienstliche E-Mails. *DuD*, 48 ff.
Pawlak, K., Smeyers, L. (2013). Außerdienstliche Aktivitäten in sozialen Netzwerken – Gefahr für den Arbeitsplatz? *öAT*, 26 ff.
Plath, K.-U. (Hrsg.) (2013). *Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG*. Köln: Verlag Dr. Otto Schmidt.
Rauscher, T., Wax, P. & Wenzel, J. (Hrsg.) (2013). *Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen*. 4. Aufl. München: C.H. Beck.
Richardi, R. (Hrsg.) (2014). *Betriebsverfassungsgesetz. Kommentar*. 14. Aufl. München: C.H. Beck.
Röckl, J., Fahl, C. (1998). Kündigung nach heimlicher Videoüberwachung. *NZA*, 1035 ff.
Rolfs, C., Giesen, R., Kreikebohm, R. & Udsching (Hrsg.), P. (2014). *Beck'scher Online-Kommentar Arbeitsrecht*. München: C.H. Beck.
Röller, Jürgen (Hrsg.) (2013). *Küttner, Personalbuch*. 20. Aufl. München: C.H. Beck, München.
Rosenbaum, B., Tölle, D. (2013). Aktuelle rechtliche Probleme im Bereich Social Media. *MMR*, 209 ff.
Sassenberg, T., Mantz, R. (2013). Die (private) E-Mail-Nutzung im Unternehmen. *BB*, 889 ff.
Schaub, G. (Begr.) (2013). *Arbeitsrechts-Handbuch*. 15. Aufl. München: C.H. Beck.
Schimmelpfennig, H.-C., Wenning, H. (2006). Arbeitgeber als Telekommunikationsdienste-Anbieter? *DB*, 2290 ff.
Schlewing, A. (2004). Prozessuales Verwertungsverbot für mitbestimmungswidrig erlangte Erkenntnisse aus einer heimlichen Videoüberwachung? *NZA*, 1071 ff.
Schröder, Georg (2012). *Datenschutzrecht*. München: Deutscher Taschenbuch Verlag.
Schuster, F. (2014). Der Arbeitgeber und das Telekommunikationsgesetz. *CR*, 21 ff.
Simitis, S. (Hrsg.) (2011). *Bundesdatenschutzgesetz. Kommentar*. 7. Aufl. Baden-Baden: Nomos.
von Staudinger, J. (Begr.) (2011). *Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, §§ 620–630 (Dienstvertragsrecht 3)*. Berlin: Sellier/de Gruyter.
Störing, M. (2011). Anmerkung zu einer Entscheidung des LAG Berlin-Brandenburg vom 16.02.2011 (4 Sa 2132/10; CR 2011, 611) – Zur Frage der Gebundenheit des Arbeitgebers an das Fernmeldegeheimnis bei nachhaltiger Ermöglichung der privaten Nutzung der E-Mail-Funktion. *CR*, 614 ff.
Thomas, H., Putzo, H. (Begr.) (2013). *Zivilprozessordnung. Kommentar*. 34. Aufl. München: C.H. Beck.
Thüsing, G. (2009). Datenschutz im Arbeitsverhältnis. *NZA*, 865 ff.
Thüsing, G. (2010). *Arbeitnehmerdatenschutz und Compliance*. München: C.H. Beck.
Vietmeyer, K., Byers, P. (2010). Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis. *MMR*, 807 ff.
Wahlers, U. (2012). Außerordentliche Kündigung wegen Kundenbeleidigung auf privater Facebook-Pinnwand. *JurisPR-ITR* 8/2012, Anm. 2.
Waltermann, R. (2007). Anspruch auf private Internetnutzung durch betriebliche Übung? *NZA*, 529 ff.

Wiese, G. (2012). Internet und Meinungsfreiheit des Arbeitgebers, Arbeitnehmers und Betriebsrats. *NZA*, 1 ff.

de Wolf, A. (2010). Kollidierende Pflichten: zwischen Schutz von E-Mails und „Compliance“ im Unternehmen. *NZA*, 1206 ff.

Wolff, H. A., Brink, S. (Hrsg.) (2014). *Beck'scher Online-Kommentar Datenschutzrecht*. München: C.H. Beck.

Wybitul, T. (2011). *Handbuch Datenschutz im Unternehmen*. Frankfurt a. M.: Verlag Recht und Wirtschaft.

Zilkens, M., Cavin, A. (2013). Soziale Netzwerke im Umfeld kommunaler Aufgabenerfüllung. *ZD*, 603 ff.

Zintl, D., Naumann, D. (2013). Verhalten von Arbeitnehmern im Bereich Social Media. *NJW-Spezial*, 306 f.

Zöller, R. (Begr.) (2014). *Zivilprozessordnung. Kommentar*. 30. Aufl. Köln: Verlag Dr. Otto Schmidt.

Kapitel 9
Medien- und internetrechtliche Anforderungen an Social Media

Hannes Beyerbach

Inhalt

9.1 Einleitung

Mit dem Begriff der Social Media liegt ein Terminus vor, der als solcher keine rechtliche Relevanz aufweist. Vielmehr beschreibt der Begriff ein tatsächliches Phänomen der Kommunikation in Zeiten des „Web 2.0“, das Berührungspunkte zu einer Vielzahl von Rechtsgebieten und Teilrechtsgebieten aufweist. Ursprung des mit den Social Media verbundenen Füllhorns an unterschiedlichen technisch und inhaltlich motivierten Rechtsfragen ist vor allem die Tatsache, dass das **Internet** zwischen den Sender und den Empfänger geschaltet wird. Dieses wiederum ist selbst gerade **1**

H. Beyerbach (✉)
Akademischer Rat, Lehrstuhl für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien, Universität Mannheim, Schloss Westflügel, 68131 Mannheim, Deutschland
E-Mail: beyerbach@uni-mannheim.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_9

nicht als Medium rechtlich relevant,[1] sondern als Plattform und **Übertragungsweg** für grundrechtliche Entfaltung verschiedensten Zuschnitts, als „inhaltsneutraler Verbund miteinander kompatibler Computernetze“,[2] als „immaterieller Kommunikationsraum“.[3] Social Media stellen dabei eine spezielle Erscheinungsform des Internets dar und werfen nach dem eben Gesagten in zwei Richtungen Rechtsfragen auf:

2 Zum einen ist zu fragen, welche rechtlichen **Vorgaben für Social Media als solche** gelten, d. h. für Plattformen wie Facebook oder sonstige unter den Begriff subsumierbare Anwendungen wie Foren, Chats oder Kommentarfunktionen. Insoweit können sie ein eigenständiges, möglicherweise reguliertes Medium ebenso darstellen wie einen reinen Übertragungsweg für die Ausübung eines Kommunikationsgrundrechts durch eine andere Anwendung[4]. Sie sind deshalb als Anwendung selbst rechtlich zu kategorisieren, können demgegenüber aber auch bloßes Mittel zur Vornahme grundrechtlich geschützter Tätigkeiten sein. Insbesondere in der Abgrenzung zum Rundfunk, dessen ursprüngliche, klassische Definition eine Unterscheidung von sonstigen elektronischen Angeboten schwierig macht, ist erforderlich. Letztere bildet gleichzeitig eine entscheidende Weichenstellung in der rechtlichen Bewertung: So ist nicht nur relevant, ob Social Media als **Rundfunk** zu qualifizieren sind und demnach dessen Regelungsregime unterfallen, sondern auch, ob die Betätigung der Rundfunkanstalten in sozialen Netzwerken rundfunkrechtliche Relevanz aufweist.

9.2 Die Vorgaben für Social Media als solche

3 Rechtliche Vorgaben können sich einfachgesetzlich in beide Richtungen insbesondere aus dem Rundfunkstaatsvertrag (RStV) und dem Telemediengesetz (TMG) ergeben. Ausgangspunkt für eine sichere rechtliche Einordnung ist dabei die **Terminologie** der beiden Regelwerke. Die Rechtsanwendung wird insoweit dadurch erschwert, dass die Begrifflichkeiten im Laufe der Zeit geändert wurden und zudem uneinheitlich sind. Auch verwendet das Unionsrecht andere Begriffe als das nationale Recht. In Letzterem decken sich die verfassungsrechtlichen Begriffe wiederum nicht mit den einfachrechtlichen und diese sind zudem nicht identisch mit den außerhalb des juristischen Sprachgebrauchs verwendeten Termini. Begriffliche Abgrenzungen sind deshalb in mehrere Richtungen erforderlich.

---

[1] Degenhart, CR 2011, 231 (234); a. A. Weigl, Meinungsfreiheit, S. 24. Terminologisch etwas unklar Klaes, ZUM 2009, 135 (138 ff.), der das Internet „als Primärmedium“ untersucht, dann aber auf einzelne Dienste abstellt, die über das Internet angeboten werden. Wie hier Mecklenburg, ZUM 1997, 525 (527), der das Internet als „Medium erster Ordnung“ bezeichnet im Gegensatz zu den Medien zweiter Ordnung (Presse, Rundfunk), die Inhalte auswählen, strukturieren und präsentieren.

[2] Kube, in: Isensee/Kirchhof, HStR IV, § 91 Rn. 4.

[3] Rossen-Stadtfeld, Bewegtbildangebote, S. 73.

[4] Kube (in: Isensee/Kirchhof, HStR IV, § 91 Rn. 6) qualifiziert das Internet deshalb zutreffend als zunehmend bedeutsamen Freiheitsraum.

Der Zugang wird erschwert durch das Phänomen der **Konvergenz**, d. h. die Tatsache, dass die verschiedenen Mediengattungen durch die Digitalisierung immer mehr zusammenwachsen, ineinander übergehen und miteinander kombiniert werden.[5] Die ursprünglich – d. h. vor dem Einsatz digitaler Übertragungstechniken – mögliche präzise Definition und Abgrenzung nach dem Herstellungs- und Verbreitungsweg ist dadurch entfallen, zumindest aber infrage gestellt. Auch stellt sich in den Randbereichen zusehends die Frage, ob nicht verschiedene Medienarten zu Unrecht ungleich behandelt werden, wenn für die eine Gattung eine wesentlich andere (insbesondere: strengere) Regulierung statuiert wird als für eine andere, obwohl es sich um ähnliche Inhalte handelt. **4**

9.2.1 Begriffliches und Abgrenzungen

9.2.1.1 Social Media als Rundfunk im Sinne der Verfassung

Bereits bei der Frage, wann es sich bei Internet-Anwendungen um **Rundfunk** handelt, ist eine differenzierte Betrachtung erforderlich, deren Ergebnis bisher keinesfalls eindeutig ausfällt. Die Antwort weist dabei nicht nur eine akademische Bedeutung auf: Rundfunk im Sinne des RStV ist zulassungspflichtig und besonderen Vorschriften unterworfen, die für die anderen Mediengattungen nicht gelten und für die Veranstalter eine strenge Bindung bedeuten. Diese Vorschriften sind zurückzuführen auf grundgesetzliche Vorgaben, bei welchen die Unterscheidung deshalb zu beginnen hat. **5**

Das **Grundgesetz** kennt als Medien allein den Rundfunk, die Presse und den Film (Art. 5 Abs. 1 S. 2 GG). Mediale Ausdrucksformen, die sich nicht diesen drei kommunikativen Ausdrucksformen zurechnen lassen, stellen sich verfassungsrechtlich im Regelfall als Meinungsäußerung dar (Art. 5 Abs. 1 S. 1 Hs. 1 GG).[6] Zwar gelten für alle vier Freiheiten dieselben Schranken – nämlich insbesondere die allgemeinen Gesetze im Sinne des Art. 5 Abs. 2 GG. Auch auf verfassungsrechtlicher Ebene ist die Unterscheidung der Freiheiten aber dennoch nicht entbehrlich. Denn namentlich mit der Zuordnung einer Verhaltensweise zur Rundfunkfreiheit ist eine besondere, auf die Rechtsprechung des Bundesverfassungsgerichts zurückgehende Dogmatik verbunden. **6**

Das **Bundesverfassungsgericht** (BVerfG) versteht die Rundfunkfreiheit nicht als natürliche, sondern als normgeprägte, „dienende“ Freiheit, die auf gesetzliche **7**

[5] Ausführlicher zum Phänomen der konvergenten Medien u. a. Kempermann, Content-Regulierung, S. 8 ff.; Lent, Rundfunk-, Medien-, Teledienste, S. 36 ff.; Paal, Medienvielfalt, S. 55 ff.; Gounalakis, Konvergenz, Teil C, insb. C 12 ff.; Jungheim, Medienordnung, S. 5 ff.; Schmidtmann, Einordnung, S. 137 ff.

[6] Siehe allgemein zur Konkurrenz der Kommunikationsfreiheiten im Bereich von Internetanwendungen Weigl, Meinungsfreiheit, S. 103 ff. S. auch Luch/Schulz, MMR 2013, 88 (89), die aber die Kommunikationsfreiheiten mit Blick auf das Internet etwas formalistisch auslegen.

Ausgestaltung angewiesen ist, um in Anspruch genommen zu werden.[7] Diese **Sonderdogmatik** begründet es mit der Aktualität, Suggestivkraft und Breitenwirkung von Informationen, die mittels Rundfunk übertragen werden[8], und stellt insoweit ein besonderes Bedürfnis danach fest, vorherrschende Meinungsmacht in diesem Bereich zu verhindern.[9] Die dafür geschaffenen einfachgesetzlichen Sonderregeln sind aber nur dann einschlägig, wenn es sich bei der jeweiligen Anwendung zumindest um Rundfunk im verfassungsrechtlichen Sinne handelt.

8 Bereits dieser kann nicht in einer ein für alle Mal gültigen Weise definiert werden.[10] Auch liefert die einfachgesetzliche Definition des **§ 2 RStV** allenfalls Anhaltspunkte, jedoch keine Definition von Verfassungsrang. Gleichwohl deckt der verfassungsrechtliche Rundfunkbegriff sich ungefähr mit der inzwischen abgelösten Definition des § 2 Abs. 1 RStV a. F., nach welcher Rundfunk definiert wurde als „für die Allgemeinheit bestimmte Veranstaltung und Verbreitung von Darbietungen aller Art in Wort, Ton und in Bild unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters. Der Begriff schließt Darbietungen ein, die verschlüsselt werden oder gegen besonderes Entgelt empfangbar sind, sowie Fernsehtext".[11] Entscheidend ist demnach, dass mit rundfunkspezifischen Mitteln Informationsinhalte verbreitet werden[12], bei denen es sich nicht um reine Individualkommunikation handelt. Rundfunk ist also „elektronische Massenkommunikation".[13] Dabei ist das technische Element der Definition – wie auch das inhaltliche – entwicklungsoffen, so dass beispielsweise nicht nur die terrestrische Verbreitung von Hörfunk und Fernsehen unter Art. 5 Abs. 1 S. 2 GG fällt, sondern auch die modernen Verbreitungsformen.

9 Fehlt indes entweder das technische oder das inhaltliche Moment, liegt kein Rundfunk im Sinne des Grundgesetzes vor. Keinesfalls also ist das Internet als solches dem Rundfunk zuzuordnen.[14] Denn nicht alle Internetanwendungen sind

---

[7] Vgl. BVerfGE 57, 295 (320); 73, 118 (152 f.); 83, 238 (295 f.); 95, 220 (236 f.).

[8] BVerfGE 90, 60 (87). Zunächst wurde das Erfordernis einer positiven Ordnung freilich mit der damals noch herrschenden Frequenzknappheit begründet, vgl. BVerfGE 12, 205 (261). Das BVerfG hat inzwischen indes betont, dass seiner Auffassung nach die Sondersituation des Rundfunks auch dann fortbestehe, wenn die mit der Frequenzknappheit und dem hohen Finanzbedarf für die Veranstaltung von Programmen verbundenen Schwierigkeiten durch die technischen Entwicklung wegfielen, vgl. BVerfGE 119, 181 (214 f.).

[9] BVerfGE 57, 295 (323 f.); 73, 118 (159 f.); 95, 163 (172).

[10] BVerfGE 74, 297 (350 f.); Bethge, in: Sachs, GG, Art. 5 Rn. 90.

[11] Wie hier die ganz h. M., vgl. Degenhart, in: BK-GG, Art. 5 Abs. 1 und 2 Rn. 667; Starck, in: v. Mangoldt/Klein/Starck, GG, Art. 5 Rn. 95; Schulze-Fielitz, in: Dreier, GG, Art. 5 Rn. 99; Brand, Rundfunk, S. 41 ff. (insb. S. 152 f.).

[12] Degenhart, in: BK-GG, Art. 5 Abs. 1 und 2 Rn. 670. Dafür wird von Degenhart zu Recht auch der Wortlaut des GG bemüht, der von Berichterstattung „durch den Rundfunk" spricht (vgl. dens., a. a. O., Rn. 673).

[13] Degenhart, in: BK-GG, Art. 5 Abs. 1 und 2 Rn. 682. Ebenso: Gersdorf, Rundfunkbegriff, S. 142 f. und 177.

[14] In diese Richtung aber Bethge, in: Sachs, GG, Art. 5 Rn. 90b, der allerdings in derselben Randnummer feststellt, dass Internetdienste aufgrund ihrer begrifflichen Unschärfe nicht pauschal kategorisiert werden könnten.

auch als „**Darbietungen**“ im Sinne der obigen Definition zu qualifizieren. Reine Individualkommunikation ohne Relevanz für die individuelle oder öffentliche Meinungsbildung wie etwa E-Mail-Dienste oder solche Abruf-Dienste, bei denen der Anwender einen einzelnen Inhalt gezielt auswählt und sich sodann herunterlädt, ohne dabei ein „Programm“ zu verfolgen – wie etwa internetbasierte Spiele –, stellen deshalb keinen Rundfunk dar. Sobald aber der Anbieter eine Darbietung verbreitet, liegt **Rundfunk im Sinne des Art. 5 Abs. 1 S. 2 GG** vor.[15]

Social-Media-Angebote wie Weblogs, YouTube oder Wikipedia, welche gleichsam ein digitales „Programm“ in Form einer Auswahl an präsentierten Inhalten darstellen, das der Nutzer durch Klicken „einschalten“ kann, sind demnach unter den verfassungsrechtlichen Rundfunkbegriff zu subsumieren.[16] Auch für Twitter wird man das noch annehmen können, weil die „Follower“ eines Nachrichten platzierenden Users von diesem ebenfalls ein Programm erstellt bekommen, wenn es auch in der Regel[17] aus wenigen, sehr kurzen Botschaften ohne die weiteren Elemente besteht, welche dem Fernsehen nach Auffassung des BVerfG seine besondere **Suggestivkraft** verleihen; die unter die Rundfunkfreiheit zu fassenden an die Allgemeinheit gerichteten Beiträge können auch scheinbar trivial sein.[18] **10**

Netzwerkplattformen wie insbesondere Facebook liefern dem Nutzer gleichfalls eine Darbietung, wie sie für den verfassungsrechtlichen Rundfunkbegriff erforderlich ist. Denn wenn der Nutzer sich registriert hat, sieht er nach dem Login auf seiner persönlichen Seite eine durch Algorithmen entwickelte Liste von Freunden, Statusmeldungen und Werbeelementen. Dass die Seite teilweise auf seinem eigenen Nutzerverhalten beruht und der Nutzer zudem über Facebook auch Nachrichten versenden kann, ändert an der Qualifizierung der Gesamtseite als „Darbietung“ nichts:[19] Die Beiträge der Nutzer erschöpfen sich darin, Teile der Inhalte erstellen und anderen Usern mitteilen zu können; die Gesamtdarstellung aber gleicht visuell einem Fernsehprogramm mit unbewegten Bildern und ist deshalb als Rundfunk im Sinne des Grundgesetzes einzustufen. Dass der Nutzer dabei eine größere zeitliche Wahlfreiheit hat als beim klassischen Fernsehen, schadet nicht.[20] **11**

Damit fällt – wenn man die denkbaren Ausdrucksformen sozialer Medien betrachtet[21] – auch das Angebot eines einzelnen **Podcasts** nicht aus dem Rundfunkbegriff **12**

---

[15] So auch Starck, in: v. Mangoldt et al., GG, Art. 5 Rn. 163.

[16] Für Individualkommunikation – und damit gegen die Einordnung als Rundfunk – aber Schmidtmann, Einordnung, S. 342 ff. Unter die Pressefreiheit werden Angebote wie YouTube gefasst von Kühling, in: Gersdorf/Paal, Informations- und Medienrecht, Art. 5 GG, Rn. 76.

[17] Mittlerweile können – im Gegensatz zur ursprünglichen Form – über Twitter auch Bilder hochgeladen und verbreitet werden, vgl. zum Ganzen auch Krieg, K&R 2010, 73 (73 f.).

[18] Zutreffend insoweit Rossen-Stadtfeld, Bewegtbildangebote, S. 45. I. Erg. auch Schmidtmann, Einordnung, S. 338.

[19] Wie hier Rossen-Stadtfeld, Bewegtbildangebote, S. 47; a. A. offenbar Kunisch, Rundfunk, S. 76 f. und Degenhart, in: Merten/Papier, HGR IV, § 105 Rn. 30, der Abrufdienste – im Gegensatz zu Zugriffsdiensten – vom Rundfunkbegriff ausnimmt (a. a. O., Rn. 31).

[20] Vgl. Schulz, in: Hahn/Vesting, § 2 RStV, Rn. 20 m. w. N.

[21] Vgl. hierzu umfassend Hohlfeld/Godulla, Kap. 2.

heraus.[22] Daran könnte man allein dann zweifeln, wenn man die einzelne zum Download bereitgestellte Datei als solche betrachtet und nicht die Webseite, auf welcher verschiedene Podcasts (auch als „Video on demand" bezeichnet) präsentiert werden. Wenn man indes das Abrufen einer solchen Datei als rein passiven Vorgang des „Konsumierens" betrachtet und beachtet, dass auch die Auswahl der hochgeladenen Podcasts eine Programmentscheidung darstellt, wird man auch diese Erscheinungsform der Social Media als Rundfunk im verfassungsrechtlichen Sinne qualifizieren müssen.[23] Denn Art. 5 Abs. 1 S. 2 GG verlangt gerade nicht, dass es sich um Darbietungen handelt, die in einem anspruchsvollen Sinne Faktor der Meinungsbildung sind;[24] solcherlei publizistische Relevanz ist nicht erforderlich, um von einer Darbietung im Sinne der obigen Definition auszugehen.[25] Im Ergebnis stellen sich somit sämtliche Social-Media-Angebote als Rundfunk im verfassungsrechtlichen Sinne dar.[26] Damit stellt sich im vorliegenden Zusammenhang die Frage nicht, ob die Entwicklung einer „**Internetdienstefreiheit**" nötig ist, die alle Kommunikationsinhalte erfasst, die an einen unbestimmten Personenkreis gerichtet sind.[27] Richtigerweise wird man auf diese Innovation aufgrund der Öffnung der Rechtsprechung des BVerfG für sog. rundfunkähnliche Kommunikationsdienste[28] und aufgrund des klaren Wortlauts des Art. 5 Abs. 1 S. 2 GG verzichten können und müssen.[29]

---

[22] So Ricker/Schiwy, Rundfunkverfassungsrecht, Abschnitt B, Rn. 71 f. (interaktive Kommunikationsdienste als Individualkommunikation).

[23] Vgl. Gersdorf, Rundfunkbegriff, S. 158 f.

[24] So aber Trute, VVDStRL 57 (1998), 216 (241 Fn. 99); Lent, Rundfunk-, Medien-, Teledienste, S. 88. Wie hier im Ergebnis Held, Online-Angebote, S. 85 f., der freilich auf das Merkmal der Darbietung im Rahmen des verfassungsrechtlichen Rundfunkbegriffes komplett verzichtet.

[25] Zutreffend Brand, Rundfunk, S. 118 ff. und S. 189 (zur Einordnung von Near Video on Demand als Rundfunk) und Hartstein et al., RStV, § 2 Rn. 15 m. w. N., die darauf verweisen, dass nur solche Angebote aus dem Rundfunkbegriff herausfielen, „denen meinungsbildende Wirkung in jeder Hinsicht fehlt".

[26] Vgl. auch Weigl, Meinungsfreiheit, S. 101; Schwartmann, in: Schwartmann, Praxishandbuch, Kap. 3 Rn. 17; unentschieden Beater, Medienrecht, § 5 Rn. 279 f., der für Telemedien einen „funktional über die Meinungsfreiheit hinausreichenden Schutz" verlangt, „der dem von Presse und Rundfunk gleichsteht".

[27] So zuletzt vertreten von Holznagel und Schumacher, vgl. Holznagel, AfP 2011, 532 (534 f.); Holznagel/Schumacher, in: Kloepfer, Netzneutralität, S. 47 (58); dies., ZRP 2011, 74 (77). Für eine „Freiheit sui generis" Wellenreuther, Presseähnliche Telemedien, S. 69 ff. S. auch bereits Mecklenburg, ZUM 1997, 525 (insb. 535 ff.).

[28] Vgl. BVerfGE 83, 238 (302 f.).

[29] So auch Degenhart, in: Merten/Papier, HGR IV, § 105 Rn. 31; ders., in: FS Stern, S. 1299 (1311 f.); Kunisch, Rundfunk, S. 29 f.; Neuhoff, ZUM 2012, 371 (376); Schmidtmann, Einordnung, S. 240 ff. Ebenso Hain, K&R 2012, 98 (103), der für die Aufgabe der Sonderdogmatik zur Rundfunkfreiheit plädiert. Für eine Neuregelung de constitutione ferenda („Die Freiheit der Medien wird gewährleistet") Sporn, K&R 2013, Beihefter 2/2013 zu Heft 5, S. 1 (5).

9.2.1.2 Social Media als Rundfunk im einfachrechtlichen Sinne?

Mit diesem grundrechtlichen Befund ist allerdings noch keine endgültige Aussage über die einfachrechtliche Behandlung der sozialen Medien, insbesondere im Vergleich mit dem „klassischen" Fernsehen und Hörfunk, gewonnen. Da die Rundfunkfreiheit ein **normgeprägtes Grundrecht** darstellt, zeigt sich der wirkliche Gehalt der grundrechtlichen Gewährleistung erst nach einem Blick in die einfachgesetzliche Rechtslage – zumal dem Gesetzgeber bei der Ausgestaltung der Rundfunkordnung ein weiter Gestaltungsspielraum zugestanden wird.[30] **13**

Seit dem zum 01.06.2009 in Kraft getretenen 12. RÄStV[31] wird Rundfunk dabei einfachrechtlich durch § 2 Abs. 1 S. 1 RStV definiert als „**linearer Informations- und Kommunikationsdienst**; er ist die für die Allgemeinheit und zum zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen". Der Gesetzgeber hat durch Schaffung dieser Definition das für den verfassungsrechtlichen Rundfunkbegriff immer noch anerkannte Merkmal der „Darbietung" gestrichen und seine Definition an die unionsrechtlichen Vorgaben der Richtlinie über audiovisuelle Mediendienste (**AVMD-RL**)[32] angepasst, welcher das Element der Linearität entnommen wurde. Negativ abgegrenzt wird der Begriff des Rundfunks sodann von Telekommunikationsdiensten und Telemedien (§ 2 Abs. 1 S. 3 RStV) und von einzelnen Angeboten, die nach § 2 Abs. 3 RStV im Wege eines Negativkatalogs aus dem Rundfunkbegriff herausgenommen werden, insbesondere Angeboten für weniger als 500 Nutzer (§ 2 Abs. 3 Nr. 1 RStV); Angeboten, die zur unmittelbaren Wiedergabe aus Speichern von Empfangsgeräten bestimmt sind (§ 2 Abs. 3 Nr. 2 RStV); nicht journalistisch-redaktionell gestalteten Angeboten (§ 2 Abs. 3 Nr. 4 RStV) und solchen Sendungen, die jeweils gegen Einzelentgelt freigeschaltet werden (§ 2 Abs. 3 Nr. 5 RStV). **14**

Wenn man davon ausgeht, dass die hier interessierenden **Social-Media-Angebote** wie insbesondere soziale Netzwerke, Kommentarfunktionen, Foren, Blogs und Wissensplattformen sich zumeist an mehr als 500 potenzielle Nutzer richten, sind es – außerhalb der einzelnen entgeltpflichtigen Sendungen i. S. d. § 2 Abs. 3 Nr. 5 RStV, wie sie z. B. mit kostenpflichtigen Podcasts vorlägen, und denjenigen Seiten, die weder Bewegtbild noch Ton verbreiten – insbesondere vier Merkmale, an denen die (auch) einfachrechtliche Rundfunkeigenschaft dieser Angebote scheitern könnte: Nämlich das Merkmal der **Linearität** nach Abs. 1 S. 1, das des Sendeplans sowie **15**

---

[30] Vgl. nur BVerfGE 97, 228 (267).

[31] 12. Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (12. RÄStV), abrufbar unter: http://www.urheberrecht.org/law/normen/rstv/RStV-12/materialien/.S. zur Entwicklung des Begriffs Schulz, in: Hahn/Vesting, § 2 RStV, Rn. 5 ff.

[32] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10.03.2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste), Abl. EU 2010 L 95 S. 1. Ausführlicher zu den europarechtlichen Hintergründen Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 RStV, Rn. 3 ff.

die Bestimmung zur unmittelbaren Wiedergabe aus Speichern von Empfangsgeräten und die fehlende journalistisch-redaktionelle Gestaltung als Negativmerkmale.

16 Der RStV definiert dabei bedauerlicherweise nicht, was unter **Linearität** zu verstehen ist; vielmehr übernimmt der Gesetzgeber hier lediglich die Begrifflichkeit der AVMD-RL. Vor diesem Hintergrund ist von Linearität dann auszugehen, wenn eine Punkt-zu-Mehrpunkt-Verbindung vorliegt[33], d. h. im Einklang mit Art. 1 lit. e) AVMD-RL ein Programm gleichzeitig an eine Vielzahl von Empfängern gerichtet wird.[34] Das Gegenstück zu solchen Diensten bilden die sogenannten Abrufdienste („Push"-Dienste), bei denen der Nutzer den Zeitpunkt und die konkreten Inhalte bestimmt, die er sieht und die somit von den Inhalten abweichen (können), die zum selben Zeitpunkt von anderen Nutzern desselben Dienstes ausgewählt werden. Begrifflich unterscheidet das europäische Recht dabei zwischen Fernsehprogrammen, audiovisuellen Mediendiensten auf Abruf und Diensten der Informationsgesellschaft[35], während der RStV unter dem Oberbegriff der „Informations- und Kommunikationsdienste" zwischen Rundfunk, rundfunkähnlichen Telemedien, Telemedien und Telekommunikationsdiensten unterscheidet.

17 Rundfunk ist dabei ein **Verteildienst** und insoweit „linear", während sich die Telemedien häufig dadurch auszeichnen, dass dem Nutzer die zentrale Rolle zukommt, indem er auf die Inhalte zugreift und sie abruft, ohne an eine bestimmte Zeit oder inhaltliche Zusammenstellung gebunden zu sein. Gerade die für das Web 2.0 und die aus ihm hervorgegangenen Social Media entscheidende **soziale Interaktion** und das so entstehende Zusammenspiel zwischen Anbieter, Nutzer und weiteren Nutzern ist es, die sie von den linearen Verteildiensten unterscheidet.

18 Darüber hinaus ist für den seit 2009 geltenden Rundfunkbegriff umstritten, welchen inhaltlichen Anforderungen ein elektronisch verbreitetes Angebot genügen muss, um Rundfunk im Sinne des RStV zu sein. Hatte der Gesetzgeber unter dem alten RStV noch das Merkmal der „**Darbietung**" aus dem verfassungsrechtlichen Rundfunkbegriff in den einfachrechtlichen übernommen, fehlt ein solches Tatbestandsmerkmal – außerhalb des negativen Merkmals der fehlenden journalistisch-redaktionellen Gestaltung – nunmehr. Der neue Rundfunkbegriff ist mithin auf dem Papier inhaltsneutral ausgestaltet. Daraus ergibt sich ein Widerspruch zum Willen des Gesetzgebers, der ausweislich der Begründung zum 12. RÄStV erklärte, der neue Begriff stelle dieselben inhaltlichen Anforderungen wie der zuvor Kodifizierte auf, da er Angebote „für die Allgemeinheit und damit die bereits

---

[33] Hartstein et al., RStV, § 2 Rn. 21.

[34] Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 RStV, Rn. 41e. Kritisch zur Einführung dieses Merkmals in Zeiten zunehmender Angebote von Online-Zugriffs- und Abrufdiensten mit Rundfunkinhalten und hybriden Formen Kunisch, Rundfunk, S. 111 („Entwicklung [. . .] außer Betracht gelassen").

[35] Vgl. Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 RStV, Rn. 41h.

bisher herangezogenen Kriterien der Breitenwirkung, Aktualität und Suggestivkraft" umfasse.[36]

Ob diese Beschränkung des einfachgesetzlichen Rundfunkbegriffs auf Angebote, die in ihrer Meinungsrelevanz dem Fernsehen ähneln, sich tatsächlich widerspruchsfrei unter das **Merkmal der „Allgemeinheit"** subsumieren lässt, erscheint jedoch zweifelhaft.[37] Überzeugender ist es, die inhaltlichen Anforderungen aus der AVMD-RL abzuleiten, welche in Art. 1 lit. a) und in ihrem Erwägungsgrund 18 unter die audiovisuellen Mediendienste nur solche Dienstleistungen fasst, „für die ein Anbieter die redaktionelle Verantwortung trägt und deren Hauptzweck die Bereitstellung von Sendungen[38] zur Information, Unterhaltung oder Bildung der allgemeinen Öffentlichkeit ist". Diese Merkmale könnten über eine **richtlinienkonforme Auslegung** in § 2 Abs. 1 RStV hineingelesen werden.[39] Eine andere Lösung besteht darin, die Meinungsrelevanz – und damit im Ergebnis das eigentlich gestrichene Erfordernis einer „Darbietung" – als ungeschriebenes Tatbestandsmerkmal in § 2 Abs. 1 RStV anzuerkennen[40] oder diese Anforderungen unter das Merkmal der journalistisch-redaktionellen Gestaltung zu subsumieren. **19**

Auf welchem methodischen Weg auch immer, wird man den einfachgesetzlichen Rundfunkbegriff in jedem Falle nach der herrschenden Ansicht so auslegen müssen, dass er nur Angebote umfasst, die in ihrer Meinungsrelevanz Fernsehsendungen entsprechen. Die **Orientierung an der Fernsehähnlichkeit** wird noch dadurch verstärkt, dass Rundfunk nach der gesetzlichen Definition nur vorliegen kann, wenn Bewegtbilder oder Ton entlang eines Sendeplans veranstaltet und verbreitet werden – eine Formulierung, die ersichtlich Fernsehen und Hörfunk klassischer Prägung als Idealtypus im Auge hat. **20**

Social-Media-Anwendungen sind deshalb nur dann **Rundfunk im Sinne des RStV**, wenn: **21**

- mit ihnen Bewegtbild oder Ton verbreitet wird und dabei ein Sendeplan verfolgt wird *und*
- das Angebot ein linearer Informations- und Kommunikationsdienst ist *und*
- sie für mehr als 500 potenzielle Nutzer angeboten werden *und*
- das Angebot journalistisch-redaktionell gestaltet ist *und*
- sie nicht zur unmittelbaren Wiedergabe aus Speichern von Empfangsgeräten bestimmt sind.

---

[36] Vgl. die Nachweise bei Hartstein et al., RStV, § 2 Rn. 19 und die vor der Kommentierung abgedruckte Begründung.

[37] Kritisch auch Schulz, in: Hahn/Vesting, Rundfunkrecht, § 2 RStV, Rn. 20 m. w. N.

[38] Worunter die AVMD-RL eine Abfolge von Bildern mit oder ohne Ton versteht, die Einzelbestandteil eines von einem Mediendiensteanbieters erstellten Sendeplans oder Katalogs ist und deren Form und Inhalt mit der Form und dem Inhalt von Fernsehsendungen vergleichbar ist (Art. 1 lit. b AVMD-RL).

[39] So der Vorschlag von Hartstein et al., RStV, § 2 Rn. 19 und Kunisch, Rundfunk, S. 115.

[40] Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 RStV, Rn. 411 f. und Holznagel/Nolden, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 5 Rn. 65.

22 Im Einzelnen bedeutet dies für die verschiedenen Erscheinungsformen von Social Media Folgendes: **Netzwerkplattformen** wie insbesondere Facebook erfüllen das Merkmal der Linearität nicht, weil hier der Inhalt teilweise von den Nutzern generiert wird und von ihm individuell Inhalte zu einem beliebigen Zeitpunkt abgerufen werden, die nicht vom Seitenbetreiber im Rahmen eines „Sendeplans“[41] für eine Vielzahl von Nutzern zum zeitgleichen Empfang vorgesehen sind.[42]

23 Auch **kollaborative Wissensplattformen** wie namentlich Wikipedia sind dadurch geprägt, dass Nutzer Inhalte generieren können und somit den vermeintlichen „Sendeplan“ beeinflussen können. Sodann werden die Änderungen des Nutzers in den Artikel übernommen, der danach für alle anderen in der identischen Form sichtbar ist. Die Ansammlung der Artikel und der einzelne Artikel als solcher mögen dabei den Anschein eines journalistisch-redaktionell erstellten Beitrages hervorrufen. Allerdings weiß der Konsument solcher Plattformen, dass der Inhalt durch die Web 2.0-Gemeinschaft generiert wird und somit gerade nicht in der Hand einer „Redaktion“ liegt. Das verhindert eine **journalistisch-redaktionelle Gestaltung**.[43] Zudem kommt es zu einem Abrufen der Seite zu verschiedenen, individuell gewählten Zeitpunkten, so dass auch dieses Angebot nicht linear ist. Im Übrigen werden bei den gängigen Plattformen dieser Art keine Bewegtbilder übertragen.

24 Zu einer entsprechenden Wertung gelangt man bei den **Multimedia-Plattformen** wie Vimeo und YouTube. Zwar werden hier Bewegtbilder und Ton übertragen. Auch hier scheitert die einfachgesetzliche Rundfunkeigenschaft aber an der fehlenden Linearität des Angebots: Denn nicht alle Nutzer sehen zum selben Zeitpunkt dieselben Inhalte. Es liegt also – im Gegensatz zu einzelnen Near-Video-on-Demand-Diensten im Rahmen des sogenannten Hybrid-TV, denen nach (allerdings umstrittener)

---

[41] Unter einem Sendeplan wird ein inhaltlich zusammenhängender, geschlossener, zeitlich begrenzter Teil eines Rundfunkprogramms (§ 2 Abs. 2 Nr. 2 RStV) bzw. eine Abfolge von bewegten Bildern mit oder ohne Ton, die Einzelbestandteil eines von einem Mediendiensteanbieter erstellen Sendeplans oder Katalogs ist (Art. 1 lit. b) AVMD-RL), verstanden. Ein Sendeplan setzt voraus, „dass der Rundfunkanbieter die einzelnen inhaltlichen Elemente (Sendungen) seines Programms in einer gewissen Reihenfolge zusammenstellt. Er nimmt eine redaktionelle Gestaltung seines Angebots vor, die von den Nutzern nicht beeinflusst werden kann, sondern nur so verfügbar ist, wie vom Anbieter vorgegeben.“ (Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 Rn. 43 f.).

[42] So auch Kunisch, Rundfunk, S. 136.

[43] S. dazu ausführlicher unten Rn. 49 ff.

Auffassung die Rundfunkeigenschaft zukommt[44] – ein klassischer **Abruf- und kein Verteildienst** vor, wie er für Rundfunk erforderlich wäre.[45]

Schwieriger zu kategorisieren sind schließlich jedoch die **Blogging- und Micro blogging-Dienste**, sofern sie auch Bewegtbilder und Ton als sogenannter Push-Dienst (d. h. zeitgleich an alle Nutzer, die den Dienst abonniert haben[46]) übertragen. Denn hier werden häufig in journalistisch-redaktioneller Gestaltung Inhalte vermittelt, die vom Anbieter zusammengestellt und präsentiert werden, so dass zudem auch ein „Sendeplan" vorläge und die Linearität bejaht werden kann.[47] Was Push-Dienste wie Twitter betrifft, hat der Gesetzgeber diese jedoch mit dem Ausschlussgrund des § 2 Abs. 3 Nr. 2 RStV wieder vom Rundfunkbegriff ausgenommen. Video on Demand und vergleichbare Dienste (Pod- und Vodcasts) werden demnach generell nicht als Rundfunk im einfachgesetzlichen Sinne behandelt.[48] **25**

Durch dieses Konvolut an positiven und negativen Definitionsmerkmalen hat der Gesetzgeber also sichergestellt, dass im Ergebnis alle Abruf- („Pull"-)Dienste nicht als Rundfunk im Sinne des Rundfunkstaatsvertrags gelten. Eine über das „Anschalten" hinausgehende Einwirkungsmöglichkeit des Nutzers lässt den Dienst entweder zu einem nicht linearen werden oder verhindert, dass das Angebot zum zeitgleichen Empfang bestimmt ist. Ist es gerade das Wesen von sozialen Medien, dass eine Interaktion der Nutzer untereinander und eine Mitgestaltung des „Programms" des Anbieters durch den Nutzer ermöglicht wird, so verhindert diese für das **Web 2.0** typische **Kommunikationsmöglichkeit**, dass das Medium nicht nur im verfassungsrechtlichen, sondern auch im einfachrechtlichen Sinne als Rundfunk angesehen wird.[49] **26**

---

[44] S. dazu Müller-Terpitz/Rauchhaus, in: Medien und Wandel, S. 309 (324); Kunisch, Rundfunk, S. 136 f.
Falsch ist es jedoch in jedem Falle, Near-Video-on-Demand-Diensten zwar die einfachrechtliche, nicht aber die verfassungsrechtliche Rundfunkeigenschaft zuzusprechen (so aber wohl Kuper, IPTV, S. 48 f., der zunächst auf die Begründung zum 12. RÄStV verweist, welche diese Dienste als Rundfunk im Sinne des RStV ansieht, und sodann feststellt, dass „aber umstritten" sei, ob diese als Rundfunk im verfassungsrechtlichen Sinne anzusehen seien; richtiger, aber etwas missverständlich, ders., a. a. O., S. 53). Denn die mit der Einordnung als Rundfunk i. S. d. RStV verbundene strenge Regulierung ist nur dann gerechtfertigt, wenn die Dienste dem Regime der Rundfunkfreiheit mit ihrer speziellen Dogmatik unterfallen. Der verfassungsrechtliche Rundfunkbegriff ist also weiter als der einfachrechtliche.

[45] Vgl. Kunisch, Rundfunk, S. 134 f.; DLM, Überarbeitung des Dritten Strukturpapiers/Internet-Radio und IP-TV, S. 5 [abrufbar unter: www.alm.de/fileadmin/forschungsprojekte/GSPWM/Beschluss_IP-TV.pdf].

[46] So insbesondere beim Microblogging-Dienst Twitter: Hier werden Textnachrichten an diejenigen Teilnehmer gleichzeitig versandt, die die Beiträge des Versenders abonniert haben (sog. Follower).

[47] Vgl. Kunisch, Rundfunk, S. 132 und – vorsichtiger – Hartstein et al., RStV, § 2 Rn. 23.

[48] Hartstein et al., RStV, § 2 Rn. 23 und 25; Kunisch, Rundfunk, S. 133.

[49] Vgl. Paschke, Medienrecht, Rn. 115 f. und 118; Vesting, in: Hahn/Vesting, Rundfunkrecht, § 1 RStV, Rn. 33b.

9.2.1.3 Social Media als Telemedien

27 Rechtlich folgt daraus, dass die Social-Media-Angebote als **Telemedien i. S. d. §§ 1 Abs. 4 TMG, 2 Abs. 1 S. 3 RStV** einzustufen sind. Dieser Begriff – der erstmalig im Jugendmedienstaatsvertrag (JMStV) verwendet wurde und mit dem Erlass des Telemediengesetzes (TMG) zu einem zentralen Begriff des Medienrechts wurde[50] – ist nicht nur außerhalb des juristischen Sprachgebrauchs wenig gebräuchlich[51], sondern gesetzlich in § 2 Abs. 1 S. 3 RStV und § 1 Abs. 1 S. 1 TMG auch nur negativ definiert[52] als „alle elektronischen informations- und Kommunikationsdienste[53], soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes sind, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach Satz 1 und 2 sind".

28 Nach § 3 Nr. 24 TKG liegt ein **Telekommunikationsdienst** vor, wenn der Dienst „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze" besteht, „einschließlich Übertragungsdienste in Rundfunknetzten". § 3 Nr. 25 TKG wiederum erfasst „Dienste, die keinen räumlich und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird".[54] Das TKG ist somit für elektronische Informations- und Kommunikationsdienste nur einschlägig, soweit der Dienst allein ein technischer ist, also soweit die Übertragung als solche angesprochen ist. Sobald mit dem Dienst auch ein Inhalt übertragen wird – seien es Bewegtbilder, E-Mail-Texte oder sonstige gesendete oder abrufbare Inhalte – handelt es sich entweder um Rundfunk oder Telemedien. Treffend abgrenzen lassen sich die Rechtsbereiche daher mit der Feststellung, dass das Telekommunikationsrecht die Dienste *der* Telekommunikation[55] regelt, während das (Tele-)Medienrecht die Dienste *durch* Telekommunikation zum Gegenstand hat.[56] Telekommunikation kann auch

---

[50] Bis zum 9. RÄStV wurde insoweit der Begriff der Multimediadienste verwandt.

[51] Paschke, Medienrecht, Rn. 72. Passender und besser mit dem Unionsrecht in Einklang zu bringen wäre der Begriff der „Telemediendienste" (Paschke, a. a. O., Rn. 74; Roßnagel, NVwZ 2007, 743 [744]. So im Übrigen auch die amtliche Begründung zum TMG) oder schlicht der „Mediendienste".

[52] Das Merkmal der „Nicht-Linearität" ist damit keine Voraussetzung des Telemedienbegriffs, vgl. Kunisch, Rundfunk, S. 117 f. m. w. N.

[53] Auch dieser Terminus, der den Oberbegriff für alle Multimedia-Angebote darstellt, ist nicht positiv definiert. Gleiches gilt für den Begriff des noch zu erörternden dem Rundfunk vergleichbaren Telemediums i. S. d. § 20 Abs. 2 RStV. Kritisch insoweit Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 RStV, Rn. 63b.

[54] Das betrifft z. B. Telefonmehrwertdienste wie die 0900-Rufnummern.

[55] Nach § 3 Nr. 22 TKG ist Telekommunikation „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen". Letztere werden nach § 3 Nr. 23 TKG verstanden als „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können."

[56] Oster, in: Fechner, Konvergenz, S. 8 (15).

als **technische Seite** des Internets und anderer Kommunikationsmedien bezeichnet werden.[57]

Da im vorliegenden Kontext insbesondere die **inhaltlichen Anforderungen** an Social Media und ihre medienrechtliche Regulierung – die wiederum mit der Meinungsrelevanz bzw. den Kriterien „Aktualität, Suggestivkraft, Breitenwirkung" ebenfalls auf inhaltliche Kriterien abstellt – angesprochen sind, handelt es sich bei den sozialen Medien auch nicht um Telekommunikationsdienste. Die telekommunikationsrechtlichen Fragen spielen deshalb hier keine Rolle. Einschlägig sind die Social Media damit als Telemedien i. S. d. §§ 1 Abs. 1 S. 1 TMG, 2 Abs. 1 S. 3 RStV. **29**

9.2.1.4 „Mit dem Rundfunk vergleichbare Telemedien" (§ 50 RStV)

Die rechtlichen Anforderungen hinsichtlich des Inhalts und des Zugangs zu sozialen Medien ergeben sich folglich aus allen Normen, die auf „Telemedien" abstellen. Soweit auf „Telekommunikation" oder „Rundfunk" Bezug genommen wird, ist der jeweilige Tatbestand nicht erfüllt. Das gilt – wie an späterer Stelle noch relevant werden wird – insbesondere für die Zulassungspflicht des Rundfunks (§ 20 Abs. 1 RStV) und die speziellen Regeln gegen Medienkonzentration (§§ 25 ff. RStV), aber zum Beispiel auch für die speziellen, wesentlich strengeren Werberegeln des Rundfunks. Ob diese **Ungleichbehandlung** gerechtfertigt ist, wird noch zu untersuchen sein. **30**

Freilich hält der Gesetzgeber die trennscharfe Unterscheidung von Rundfunk und Telemedien nicht konsequent durch. Neben den im Folgenden dargestellten Regelungen für Telemedien als solche ordnet er die Geltung einiger Vorschriften, die auf den Rundfunk abzielen, auch für Telemedien an. Hierbei wird die Kategorie der „mit dem Rundfunk vergleichbaren", d. h. an die Allgemeinheit gerichteten[58] Telemedien bzw. diejenige der „**fernsehähnlichen Telemedien**" eingeführt: Für Letztere wird eine entsprechende Geltung von Werbevorschriften des Rundfunks angeordnet (§ 58 Abs. 3 RStV), während Erstere nach § 50 RStV nach denselben Regeln wie der Rundfunk Übertragungskapazitäten zur Verbreitung ihres Programms zugewiesen bekommen. Nach den §§ 1 Hs. 2, 20 Abs. 2 RStV benötigen zudem Anbieter elektronischer Informations- und Kommunikationsdienste einer Zulassung zur Veranstaltung des Dienstes, soweit dieser „dem Rundfunk zuzuordnen ist" – womit rundfunkähnliche Dienste gemeint sind.[59] Es ist dem Gesetzgeber mithin bewusst, dass Telemedien dieselbe Wirkung wie Rundfunk (im einfachgesetzlichen Sinne) entfalten können und dass das Phänomen der **Konvergenz** der Medien dazu führt, dass eine rein formale Betrachtung mit einer strengen Fernsehregulierung und einer wesentlich liberaleren Aufsicht über die Telemedien der tatsächlichen Austauschbarkeit der Mediengattungen nicht hinreichend Rechnung trägt.[60] **31**

---

[57] Haug, Internetrecht, Rn. 43.
[58] Die Legaldefinition findet sich in § 50 RStV.
[59] Holznagel/Kibele, in: Spindler/Schuster, Recht der elektronischen Medien, § 20 RStV, Rn. 8.
[60] S. zu den zulassungspflichtigen Telemedien sogleich, Rn. 39 ff.

32 Von § 50 RStV werden dabei Telemedien erfasst, die zwar nicht im einfachrechtlichen, jedenfalls aber im verfassungsrechtlichen Sinne Rundfunk darstellen und denen dieselbe Wirkung wie dem Rundfunk im einfachrechtlichen Sinne zukommt, nach der Terminologie des RStV die **an die Allgemeinheit gerichteten Telemedien**.[61] Wie dieser Typus auszulegen ist, ist höchst umstritten. Hier können im Ergebnis ähnliche Erwägungen angestellt werden wie im Rahmen des § 20 Abs. 2 RStV[62], zu welchem die Landesmedienanstalten ein Strukturpapier entwickelt haben, das an späterer Stelle diskutiert werden soll[63] und für § 50 RStV ebenfalls relevant sein könnte. Im Ergebnis wird es auch hier die Möglichkeit der Interaktion sein, welche Social Media auszeichnet, ihnen aber gleichzeitig die Eigenschaft als „mit dem (einfachrechtlichen) Rundfunk vergleichbare Telemedien" nimmt. Das unten zu § 20 Abs. 2 RStV Gesagte gilt insoweit entsprechend.

9.2.1.5 Social Media als Plattformen i. S. d. RStV?

33 Vor dem Blick auf den Rechtsrahmen für Telemedien bleibt noch ein letzte terminologische Klarstellung: Das Rundfunkrecht kennt die **Regulierung sogenannter Plattformen** (§§ 52 ff. RStV). Eine unbefangene Wahrnehmung dieses Begriffs könnte den Eindruck entstehen lassen, mit diesen Regelungen seien Vorschriften zu einer speziellen Regulierung bestimmter Erscheinungsformen sozialer Medien geschaffen worden, welche oft als „Plattformen" bezeichnet werden, wie etwa im Falle der Wissensplattformen oder der Netzwerkplattformen.[64]

34 Diese Vorschriften haben indes andere Adressaten vor Augen: Unter einem von den §§ 52 ff. RStV erfassten Plattformbetreiber wird gem. § 2 Abs. 2 Nr. 12 RStV derjenige verstanden, der auf digitalen Übertragungskapazitäten oder digitalen Datenströmen Rundfunk und vergleichbare Telemedien – auch hier taucht also diese spezielle Art der Telemedien erneut auf – auch von Dritten mit dem Ziel zusammenfasst, diese Angebote als Gesamtangebot zugänglich zu machen, oder wer über die Auswahl für die Zusammenfassung entscheidet.[65] Die Plattformbetreiber werden abgegrenzt von den Telekommunikationsdiensteanbietern, die lediglich die Übertragung des Signals übernehmen, und den inhaltlich verantwortlichen Rundfunkveranstaltern, die ausschließlich ihr Rundfunkangebot vermarkten (§ 2 Abs. 2 Nr. 12 Hs. 2 RStV). Zweck der §§ 52 ff. RStV ist es nämlich, diejenigen zu regulieren, die gleichsam als „Flaschenhals"[66] bzw. „**Gate-Keeper**"[67] den Zugang zu Rundfunk

---

[61] Hartstein et al., RStV, § 50 Rn. 12.
[62] So auch Holznagel/Hahne, in: Spindler/Schuster, § 50 RStV, Rn. 6.
[63] S. unten, Rn. 39 ff.
[64] Ausführlicher zu den Gattungen der Social Media Hohlfeld/Godulla, Kap. 2.
[65] Nicht erfasst werden also Plattformen, auf denen lediglich Telemedien angeboten werden, die nicht mit dem Rundfunk vergleichbar sind, sich also nicht an die Allgemeinheit richten bzw. denen keine Meinungsrelevanz zukommt, vgl. Broemel, ZUM 2012, 866 (873).
[66] Holznagel et al., Elektronische Medien, S. 190.
[67] Paschke, Medienrecht, Rn. 747.

und rundfunkähnlichen Diensten vermitteln, indem sie bestimmen, was der Zuschauer überhaupt empfangen kann.[68] Der Zusatz „auch von Dritten" der obigen Definition macht deutlich, dass es gerade um die Auswahl der verschiedenen Angebote geht, nicht um einen möglichen begrenzten Zuschnitt des eigenen Programms.[69] Die dazu etablierten **Diskriminierungsverbote** (§§ 52c f. RStV), Belegungspflichten und die Entgeltregulierung (§ 52d RStV) dienen der Sicherung der Meinungsvielfalt. So bestimmt § 52b Abs. 1 S. 1 Nr. 1 RStV einen sogenannten „must-carry"-Bereich von Programminhalten, die über die Plattform angeboten werden müssen, sowie in § 52 Abs. 1 S. 1 Nr. 2 RStV einen „can carry"-Bereich von Inhalten, aus denen ein vielfältiges Programmangebot bereitgestellt werden muss.

35 Von diesen Verpflichtungen werden diejenigen nicht erfasst, die ausschließlich eigenes Programm vermarkten oder zusammenfassen. Soweit demnach ein Anbieter sozialer Medien selbst in seiner inhaltlichen Verantwortung angesprochen ist, ist er kein Plattformanbieter. Denn er dient nicht als „Flaschenhals" zur Auswahl, Vermittlung – und folglich auch Ausgrenzung – fremder Inhalte. Eine weitere Ausnahme vom Anwendungsbereich der Plattformregulierung statuiert § 52 Abs. 1 S. 2 Nr. 1 RStV für **reine Internetplattformen** ohne marktbeherrschende Stellung. Denn in einem offenen Netzwerk ist die Stellung des „Plattform"-Betreibers nur dann mit derjenigen eines Betreibers in einem geschlossenen Netzwerk vergleichbar, wenn die marktbeherrschende Stellung den Effekt bewirkt, dass der Netzwerkbetreiber über die Frage, ob ein Inhalt zugänglich ist, entscheidet.[70]

36 Die vermeintliche Ausgrenzung bestimmter (potenzieller) Angebote durch Präsentation einer eigenen Auswahl durch Social-Media-Anbieter ohne marktbeherrschende Stellung ist demnach keine Frage der Plattformregulierung i. S. d. §§ 52 ff. RStV. Gleichwohl wirft ein solcher Ausschluss **Fragen nach Vielfaltssicherung** ebenso auf wie solche nach der Rolle des Wettbewerbsrechts. Auf die denkbare Marktmacht und den inhaltlichen Einfluss von Social-Media-„Plattformen" antworten die §§ 52 ff. RStV nicht; sie haben nur den „Mittler" zwischen den eigentlichen Anbietern und dem Nutzer im Blick und Internetplattformen auch nur dann, wenn sie eine marktbeherrschende Stellung innehaben. Ob sich aus anderen Vorschriften angemessene Reaktionen auf die Vielfalts- und Wettbewerbsbeschränkungen marktmächtiger sozialer Medien ergeben oder ob es geboten wäre, den Anwendungsbereich mancher Regulierungsansätze auf jene zu erweitern, wird vor diesem Hintergrund noch zu untersuchen sein.

---

[68] Holznagel/Jahn, in: Spindler/Schuster, Recht der elektronischen Medien, § 52 RStV, Rn. 2.

[69] Wie hier auch Hartstein et al., RStV, § 52 Rn. 9 und Wagner, in: Hahn/Vesting, Rundfunkrecht, § 52 RStV, Rn. 13. Anders wohl Paschke, Medienrecht, Rn. 750. Erfasst werden in der Praxis z. B. die Angebote Kabel Deutschland, Kabel BW, Sky und T-Home, vgl. KEK, Dritter Konzentrationsbericht, S. 306 ff. und Hartstein et al., a. a. O. S. auch die detaillierte Liste bei Wagner, a. a. O., Rn. 15.

[70] Vgl. Broemel, ZUM 2012, 866 (874) mit Verweis auf die Begründung zum 10. RÄStV.

9.2.2 Die Vorgaben des Rundfunkrechts für Social Media

37 Wie aber reagiert das einfache Recht nun auf Social Media? Nach dem Vorstehenden sind diese vor allem dadurch charakterisiert, was sie nicht sind: Sie sind insbesondere kein Rundfunk im einfachrechtlichen Sinne und sie stellen keine Plattformen im Sinne des RStV dar. Als Telemedien werden sie aber dennoch nicht nur vom **Telemediengesetz** erfasst: Auch der **Rundfunkstaatsvertrag** hält Regelungen bereit, die explizit an Telemedien adressiert sind. Das ist auch konsequent, stellen doch zahlreiche Telemedien Rundfunk im verfassungsrechtlichen Sinne dar, so dass Rechtsregeln dort angebracht sind, jedenfalls aber erwartet werden, wo die normgeprägte Rundfunkfreiheit ausgestaltet wird.

9.2.2.1 Ausgangspunkt: Zulassungsfreiheit

38 Als Ausgangspunkt zum Abschnitt über die Telemedien (§§ **54 ff. RStV**) stellt das Rundfunkrecht zugleich deklaratorisch den wichtigsten Unterschied der Telemedien im Verhältnis zum Rundfunk fest: ihre Zulassungsfreiheit nach § 54 Abs. 1 S. 1 RStV – eine Rechtsfolge, die sich bereits aus § 4 TMG ergeben hätte. Das Rundfunk- und Telemedienrecht kennt folglich keine Zulassungs- oder Anmeldepflichten, die spezifisch an der Eigenschaft als Telemedium anknüpfen.[71] Damit weitet der ausgestaltende Gesetzgeber die für den klassischen Rundfunk vom BVerfG für erforderlich erachtete präventive Kontrolle[72] nicht auch auf die ebenfalls dem Schutzbereich der Rundfunkfreiheit unterfallenden Telemedien aus. Diese Differenzierung wird im Ergebnis durch das Zusammenspiel von verfassungsrechtlichen Vorgaben – in ihrer dogmatischen Lesart durch das BVerfG – und unionsrechtlichen Regelungen erzwungen. Denn das europäische Recht fordert einen **zulassungsfreien Zugang** zu „Diensten der Informationsgesellschaft“ mit Ausnahme von Fernsehen und Hörfunk.[73]

9.2.2.2 Ausnahme: Zulassungspflichtige Telemedien

39 Wie bereits oben angedeutet, hält der Gesetzgeber diese trennscharfe Differenzierung zwischen dem klassischen Hörfunk und Fernsehen auf der einen und den Telemedien auf der anderen Seite nicht durch. Für die bereits erwähnte Kategorie der dem Rundfunk zuzuordnenden (d. h. „**rundfunkähnlichen**“) **Telemedien** wird in § 20 Abs. 2 S. 1 RStV die Zulassungspflicht wie für den klassischen Rundfunk angeordnet. Wann von rundfunkähnlichen Telemedien in diesem Sinne auszugehen ist, lässt

---

[71] S. Heckmann, jurisPK-Internetrecht, Kap. 1 Rn. 224 ff. m. w. N. auch zur Zulassungspflicht nach anderen Gesetzen.
[72] BVerfGE 57, 295 (326).
[73] Art. 4 Abs. 1 der RL 2000/31/EG, Abl. EG Nr. L 178 vom 17.07.2000, S. 1 ff. – E-Commerce-Richtlinie; vgl. auch Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 17.

sich nur schwer bestimmen und nicht pauschal beurteilen; folglich verzichtet der RStV auch auf einen Katalog bestimmter Angebote oder eine zusätzliche Konkretisierung dieses folgenschweren Attributs. Dogmatisch hat sich die Auslegung dieses Begriffes an den Eigenschaften zu orientieren, welche vom BVerfG dem Rundfunk zugeschrieben werden und die seine grund- und einfachrechtliche Sondersituation rechtfertigen, nämlich den Topoi Breitenwirkung, Aktualität und Suggestivkraft.[74]

Um die gebotene **verfassungskonforme Auslegung** und Anwendung des § 20 Abs. 2 RStV zu vereinfachen, haben sich die – verfahrensrechtlich für die Beurteilung zuständigen[75] – Landesmedienanstalten auf ein Strukturpapier geeinigt, das in der Praxis zur Definition herangezogen wird. Danach ist ein Dienst umso rundfunkähnlicher, je höher die Wirkintensität der verbreiteten Inhalte als solche ist, je stärker die redaktionelle Gestaltung der Inhalte ist, je realitätsnaher sie präsentiert werden, je größer die Reichweite und die gleichzeitige Rezeptionsmöglichkeit ist und je weniger Interaktivität des Nutzers den Rezeptionsvorgang bestimmt.[76] Diese ebenfalls noch relativ abstrakten Kriterien werden sodann weiter erläutert. Danach ist relevant, wie aktuell die Inhalte sind, in welchem Maße die strukturelle Abfolge und die redaktionelle Gestaltung den Nutzer vom „Umschalten" abhält, ob Bild und Ton als „dem Rundfunk wesensimmanent[e]" Elemente kombiniert werden („Kraft der bewegten Bilder"), und wie einfach die Bedienung für den Nutzer ist. Lakonisch stellt das Strukturpapier am Ende dieser Präzisierungen fest: „Je mehr und je stärker die genannten Merkmale erfüllt sind, desto rundfunktypischer ist ein Dienst. Bei Überschreiten einer bestimmten Schwelle erfolgt die Einordnung als Rundfunk".[77] **40**

Wendet man diese Kriterien auf die gängigen Social-Media-Anwendungen an, so stellen sich diese im Zweifel nicht als rundfunkähnlich dar: **Netzwerkplattformen** wie insbesondere Facebook kombinieren nicht Bild und Ton (wenn von den Nutzern auch Videos verlinkt werden können) und sind durch eine hohe Interaktivität der Nutzer geprägt. Diese sind keine passiven Konsumenten, sondern teilen ihre Gedanken – etwa als sogenannte Statusmeldung – mit und kommentieren die Inhalte anderer. Zwar mögen diese Seiten über eine redaktionelle Gestaltung verfügen; die jeweilige Gestaltung liefert indes eher den Rahmen für die Aktivitäten und Interaktionen der Nutzer. Die wichtige Rolle des Nutzers bewirkt daher, dass trotz der hohen Breitenwirkung und Aktualität der gängigen Plattformen das Gesamtbild nicht für ein dem Rundfunk ähnliches Telemedium spricht. **41**

Auch **kollaborativen Wissensplattformen** wie insbesondere Wikipedia kommt diese Eigenschaft nicht zu. Sie stellen sich nicht als „Programmabfolge" dar, sondern halten lediglich einen Fundus von Wissensartikeln bereit, deren Abruf zudem davon abhängt, dass der Nutzer nach dem konkreten Stichwort sucht. „Vorgestellt" wird ihm bei solchen Plattformen allein eine geringe Anzahl an Artikeln auf der Startseite, die **42**

---

[74] Schulz, in: Hahn/Vesting, Rundfunkrecht, § 20 RStV, Rn. 63.

[75] Nach der aktuellen Rechtslage muss die Feststellung nicht mehr einvernehmlich von allen Landesmedienanstalten getroffen werden, wie dies vor dem 10. RÄStV der Fall war.

[76] DLM, Drittes Strukturpapier zur Unterscheidung von Rundfunk und Mediendiensten, Ziffer 2.4.1, abrufbar unter: http://www.alm.de/fileadmin/user_upload/3Strukturpapier.pdf.

[77] DLM, a. a. O., Ziffer 2.4.2. a. E.

er mehrheitlich aber ignorieren und zugunsten des von ihm sodann gesuchten Inhalts verlassen wird. Hinzu kommt, dass die Artikel durch die Nutzer weitergeschrieben und korrigiert werden können und dass in ihnen dem Bewegtbild eine höchstens marginale Bedeutung zukommt. Im Ganzen sind sie deshalb mit dem Fernsehen nicht vergleichbar. Entsprechendes gilt für **Blogs**: Diese werden zumeist nicht von einer solchen Vielzahl an Nutzern besucht, dass ihnen die erforderliche Breitenwirkung zukommt. Zudem wird bei diesen Erscheinungsformen sozialer Medien häufig keine solch große Zahl an ständig aktualisierten Inhalten vorliegen, dass ihre Wirkmacht auch nur annähernd mit dem Fernsehen verglichen werden kann. Erst recht gilt dies für Microblogging-Dienste (wie namentlich Twitter), deren Inhalten nur ein geringer Grad an Suggestivkraft zukommt.

43 Auch **Multimediaplattformen** wie insbesondere YouTube und Vimeo erfüllen die Kriterien des erwähnten Strukturpapiers nicht. Zwar werden hier Bewegtbilder zum Abruf bereitgehalten. Allerdings hängen die Inhalte, die von den Nutzern gesehen werden, stark von den Suchbegriffen ab, die sie eingeben. Es ist eher das konkrete Nutzerverhalten – das also nicht als passiv bezeichnet werden kann –, das zu einem „wirkmächtigen" Inhalt führt, als die redaktionelle Gestaltung der Seite. Insoweit gilt hier das Gleiche wie für die Wissensplattformen. Es ist der aktive Nutzer, der von einem Inhalt zum nächsten springt und sich selbst vom „Umschalten" abhält. Die redaktionelle Gestaltung der Seite tritt daher im Verhältnis zum individuellen, aktiven Suchverhalten des Nutzers zurück, der zudem durch seine Kommentare unter den Videoclips die Gesamtwirkung der Seite erheblich mitgestaltet. Das bewirkt, dass – wie im Übrigen auch bei den Wissensplattformen – die aktuell konsumierten und kommentierten Inhalte sehr stark zwischen den Nutzern differieren. Das verleiht den bewegten Bildern der Multimediaplattformen eine erheblich geringere Wirkmacht als denjenigen eines Fernsehprogramms, das vom Nutzer als solches „hingenommen" werden muss. Alle gängigen Social-Media-Anwendungen erfüllen vor diesem Hintergrund die Anforderungen an rundfunkähnliche Telemedien nicht. Für sie bleibt es daher bei der **Zulassungsfreiheit**, wie sie für Telemedien die Regel ist. Im Ergebnis zeigt die Subsumtion der Social Media unter § 20 Abs. 2 RStV, dass diese Norm wohl kaum einen Anwendungsbereich aufweist. Die strenge Herausnahme nichtlinearer Dienste aus dem Rundfunkbegriff lässt § 20 Abs. 2 RStV zumeist ins Leere laufen.[78]

9.2.2.3 Vorgaben für Telemedien

44 Diese Zulassungsfreiheit besteht nach § 54 Abs. 1 S. 1 RStV „**im Rahmen der Gesetze**". Für das Rundfunkrecht ist damit der spezielle Abschnitt der §§ 54 ff. RStV angesprochen, der sich an „Telemedien", d. h. alle Kategorien von Telemedien

[78] Kempermann, Content-Regulierung, S. 213 f.

und damit auch alle Social Media richtet;[79] auf deren Geltung weist auch das Telemediengesetz in § 1 Abs. 4 ausdrücklich hin.[80] Die Vorschriften gehen zurück auf Vorgängernormen des Mediendienstestaatsvertrags (§§ 4, 11 MDStV)[81], dessen Kategorisierung der Multimediadienste in Tele- und Mediendienste damit im Ergebnis – entgegen der Begründung zu den §§ 54 ff. RStV[82] – nicht entfallen ist.[83]

9.2.2.4 Inhaltliche Vorgaben für alle Telemedien

Für sämtliche Telemedien ordnet in diesem Rahmen zunächst § 54 Abs. 1 S. 2 RStV die Geltung der „**verfassungsmäßigen Ordnung**“ an, wie sie parallel für den privaten Rundfunk nach § 41 Abs. 1 S. 1 RStV auch gilt. Satz 3 erweitert die Grenzen der Zulassungsfreiheit sodann auf die **allgemeinen Gesetze** und die gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre. Damit wird der Schrankenbereich des Art. 5 Abs. 1 GG, dessen Schutzbereich die Social-Media-Anwendungen sowohl als Rundfunk, aber auch – soweit man sie anders bewerten wollte – als Presse oder Meinungsäußerung zuzuordnen sind, deklaratorisch für die einfachgesetzliche Bewertung wiederholt. Die dabei aus dem Kanon des Art. 5 Abs. 2 GG noch fehlenden Vorschriften zum Schutze der Jugend befinden sich im noch zu behandelnden Jugendmedienschutz-Staatsvertrag (JMStV).[84] § 54 Abs. 1 RStV sichert über die Bezugnahme auf die Schranken der Kommunikationsfreiheiten einen meinungsneutralen, nicht spezifisch gegen Telemedien gerichteten inhaltlichen Mindeststandard auch für Social Media ab. Diese Mindestanforderungen sind wesentlich weniger streng als die Vorgaben für den Rundfunk im einfachgesetzlichen Sinne.[85] **45**

Anders als Hörfunk und Fernsehen sind Telemedien insbesondere nicht zu **Vielfalt** verpflichtet. Denn die besonderen Gefahren für die Meinungsvielfalt bestehen nach der „klassischen“ Sichtweise außerhalb des Rundfunks im Sinne des RStV nicht – jedenfalls nicht in der gleichen Weise wie namentlich beim Fernsehen, dessen bewegten Bildern die besondere, auch eine rechtliche Sonderkonstruktion rechtfertigende Suggestivkraft zugeschrieben wird. Mit der verfassungsmäßigen Ordnung sollen – wie im Rahmen des Art. 2 Abs. 1 GG – sämtliche formell und materiell **46**

[79] Etwas unpräzise daher Schmittmann, in: Schwartmann, Praxishandbuch, 10. Kapitel, Rn. 18, der den VI. Abschnitt des RStV nur auf Telemedien mit journalistisch-redaktionellem Inhalt bezieht.
[80] Dort heißt es: „Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich aus dem Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag).“
[81] Vgl. hierzu Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 6 ff.
[82] Abgedruckt bei Held, a. a. O., Rn. 5.
[83] Vgl. nochmals Dörr/Schwartmann, Medienrecht, Rn. 272 m. w. N.
[84] S. unten, Rn. 78 ff.
[85] Hartstein et al., RStV, § 54 Rn. 2.

verfassungsmäßigen Gesetze angesprochen sein[86], während der Begriff der „allgemeinen Gesetze" in gleicher Weise auszulegen ist wie im Rahmen des Art. 5 Abs. 2 GG. Damit sind es die allgemeinen Strafvorschriften und Rechtsvorschriften des bürgerlichen Rechts, die grundsätzlich zu Beschränkungen des „Programms" von Telemedien herangezogen werden dürfen; die Schwelle zu einem Verbot ist dabei allerdings entsprechend hoch. Man wird, was diese Schwelle betrifft, die hohen Hürden übertragen können, die für das Verbot einer Meinungsäußerung gelten. Außerhalb des Jugend- und Ehrschutzes sowie von Strafnormen ist die Betätigung der Social Media deshalb grundsätzlich wenigen inhaltlichen Beschränkungen unterworfen. Lediglich ein „**Mindestmaß an gegenseitiger Achtung**" wird gewährleistet.[87]

47 Im Gegensatz zu § 41 Abs. 1 S. 2 RStV bezieht § 54 Abs. 1 RStV die **Menschenwürde** und die „sittlichen, religiösen und weltanschaulichen Überzeugungen anderer" nicht in diesen Mindeststandard ein. Auch diese fehlende Bezugnahme ist der geringeren Meinungsrelevanz geschuldet, die den Telemedien im Verhältnis zum Fernsehen attestiert wird. Die Menschenwürde wiederum wird zumeist ohnehin von den allgemeinen Gesetzen und Strafvorschriften erfasst; im Übrigen findet über § 4 Abs. 1 S. 1 Nr. 8 JMStV eine Bindung an die oben genannten Topoi unter dem Blickwinkel des Jugendschutzes statt.[88]

48 Ebenfalls für alle Telemedien gilt die Vorgabe des § 54 Abs. 3 RStV.[89] Hiernach muss bei der Wiedergabe von **Meinungsumfragen**, die der Anbieter des jeweiligen Telemediums selbst durchgeführt hat, angegeben werden, ob die Umfrage repräsentativ ist. Auch wenn grundsätzlich also keine inhaltliche Regulierung stattfinden soll, müssen Telemedien dort, wo sie in besonderer Weise Sachlichkeit in Anspruch nehmen und (scheinbar) reine Tatsachen präsentieren, kenntlich machen, inwieweit die Daten wissenschaftlichen Maßstäben genügen, d. h. inwieweit der Nutzer sich auf sie „verlassen" kann. Diese den journalistischen Sorgfaltsregeln entnommene Verpflichtung[90] ist ein Fremdkörper in dem Pflichtenprogramm der Telemedien, die ja eigentlich allein durch die allgemeinen Gesetze und den Ehr- und Jugendschutz beschränkt werden.

---

[86] So Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 54 RStV, Rn. 4. Ebenso: Hahn/Witte, in: Hahn/Vesting, Rundfunkrecht, § 41 RStV, Rn. 8 und Hartstein et al., RStV, § 41 Rn. 3 zur Parallelverbürgung für den privaten Rundfunk. Enger: Holznagel/Krone, in: Spindler/Schuster, Recht der elektronischen Medien, § 41 RStV, Rn. 5.

[87] Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 63 mit Verweis auf BVerfGE 57, 295 (325 f.).

[88] S. zum Ganzen auch Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 63.

[89] Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 54 RStV, Rn. 15; Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 68.

[90] Die Vorschrift des § 54 Abs. 3 RStV entspricht § 10 Abs. 2 RStV, so dass auf die Kommentierungen zu dieser Vorschrift zurückgegriffen werden kann. Im Pressekodex ist diese Frage in Ziffer 2 Richtlinie 2.1 geregelt (abgedruckt bei: Hartstein et al., RStV, § 10 Rn. 3). Ausführlicher zu den Sorgfaltspflichten Ricker/Weberling, Handbuch des Presserechts, 39. Kap., Rn. 6 ff.

9.2.2.5 Inhaltliche Vorgaben für journalistisch-redaktionell gestaltete Angebote

Denn die inhaltlichen Maßstäbe für Telemedien werden zwar in der Folge in dieselbe Richtung von § 54 Abs. 2 RStV erweitert.[91] Dieser richtet sich aber an eine weitere Kategorie von Telemedien, nämlich die „Telemedien mit journalistisch-redaktionell gestalteten Angeboten". Sie müssen, wenn in ihnen „insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, den **anerkannten journalistischen Grundsätzen**" entsprechen. Mit diesem Erfordernis wird der Tatsache Rechnung getragen, dass aufgrund der Konvergenz der Medien ein Telemedium inhaltlich zum einen dem entsprechen kann, was in gedruckter Form als „Presse" einzuordnen ist, zum anderen aber – bezogen auf einzelne Beiträge – ähnlich wirken kann wie eine Informationssendung oder Berichterstattung im Rundfunk. Für Letztere folgt die Bindung an die anerkannten journalistischen Grundsätze aus § 10 Abs. 1 RStV, für Erstere aus den Landespressegesetzen und dem selbstregulativen Pressekodex des Deutschen Presserats.[92] **49**

Wenn also das Teilangebot eines Telemediums in seiner Gestaltung entweder einem Presse- oder einem Rundfunkbericht entspricht, muss es auch den Sorgfältigkeitsmaßstäben dieser beiden Mediengattungen genügen. Durch diese als solche überzeugende Differenzierung wird es nicht dem technischen Zufall überlassen, welchen inhaltlichen Maßstäben die Berichterstattung genügen muss. Schwierig ist es dann aber zu bestimmen, wann ein solches hier angesprochenes „**publizistisches Telemedium**"[93] vorliegt, d. h. wann von einem journalistisch-redaktionell gestalteten Angebot i. S. d. § 54 Abs. 2 RStV auszugehen ist. Der Rundfunkstaatsvertrag schweigt zu dieser Frage, die an verschiedenen Stellen rechtlich relevant wird, so z. B. auch bei der Impressumspflicht und dem Gegendarstellungsrecht. Die Rechtsprechungspraxis ist daneben auch eher mit der Frage der Verantwortlichkeit der Telemedienanbieter nach den §§ 7 ff. TMG und den Grundsätzen der Störerhaftung befasst.[94] Diese Aspekte sind zwar von den im vorliegenden Kontext angesprochenen Grundsätzen zu trennen. Die für das hier interessierende Merkmal geltenden Grundsätze wirken allerdings mittelbar auf die einzelnen Voraussetzungen der denkbaren Ansprüche ein[95], etwa dadurch, dass ein Verstoß gegen die **Sorgfaltspflichten** zum Verschulden i. S. d. § 276 BGB führt. Man wird bei der Bestimmung dieser Kategorie von Telemedien vom Sinn und Zweck der Regelung ausgehen müssen: Verhindert **50** **51**

[91] A.A. aber Breutz/Weyhe, in: Paschke et al., Hamburger Kommentar, 39. Abschnitt, Rn. 191. Aus der dort in Bezug genommenen Entscheidung BGH, NJW-RR 2009, 1413 ff. ergibt sich diese Schlussfolgerung jedenfalls nicht.

[92] Ausführlicher: Hartstein et al., RStV, § 10 Rn. 3 ff.

[93] Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 54 RStV, Rn. 6.

[94] S. hierzu den gesonderten Beitrag von Spindler, Kap. 5.

[95] Etwas missverständlich daher Breutz/Weyhe, in: Paschke et al., Hamburger Kommentar, 39. Abschnitt, Rn. 186 ff., die beide Fragen nicht hinreichend unterscheiden. Wie hier aber Lent, in: Gersdorf/Paal, Informations- und Medienrecht, § 54 RStV, Rn. 3 ff.

werden sollen willkürlich erscheinende Effekte der Konvergenz. Dort, wo im virtuellen Raum eine Entsprechung zu dem entstanden ist, was klassischerweise als Presse oder Rundfunk geschützt wird, soll eine starre Orientierung an der Technik und dem Verbreitungsweg bei der rechtlichen Regulierung vermieden werden. Man dachte insbesondere an die „**elektronische Presse**“, die gleich sorgfältig berichten sollte wie das klassische Printmedium.[96] Schwierig zu qualifizieren sind demgegenüber diejenigen Online-Angebote, die nicht die Zeitung oder das Fernsehen in das Internet transportieren, sondern möglicherweise sogar von journalistischen Laien gestaltet sind oder eine internetspezifische Erscheinungsform darstellen, für die es keine Entsprechung in gedruckter oder gesendeter Form gibt.

52 Eindeutige Stellungnahmen zu gerade diesen Grenzfällen sind selten. Um Orientierung zu erlangen, wird vereinzelt auf Rechtsprechung und Literatur zu § 41 des Bundesdatenschutzgesetzes (BDSG)[97] zurückgegriffen[98], der ebenfalls den Terminus der journalistisch-redaktionellen Gestaltung kennt. Im Kontext dieser Norm verlangt der BGH mit Blick auf die Einbeziehung in den Schutzbereich der Presse- und Rundfunkfreiheit, dass dem Angebot eine **meinungsbildende Wirkung** für die Allgemeinheit zukommen und diese prägender Bestandteil sein müsse.[99] Damit ist freilich auch nur ein weiteres abstraktes Kriterium gewonnen, das recht vage bleibt. Die Definitionsmerkmale des (einfachgesetzlichen) Pressebegriffs, insbesondere dasjenige der Periodizität, zu übertragen, ist insoweit keine Lösung, weil sich die gedruckte, zumeist laufend erscheinende Publikation wesentlich von einem Telemedium unterscheidet. Für dieses muss also eigenständig formuliert werden, was unter journalistisch-redaktioneller Gestaltung im Bereich der Online-Medien gemeint ist.[100] Insbesondere ist zu beachten, dass sich prinzipiell jedes Telemedium an die Allgemeinheit richtet, aber – sonst wäre die gesetzgeberische Differenzierung gegenstandslos – nicht jedes Telemedium auch die entsprechende Meinungsrelevanz aufweist, die mit der journalistisch-redaktionellen Gestaltung verbunden ist.

53 Es ist vor diesem Hintergrund am überzeugendsten, den **Sinn und Zweck** der von § 54 Abs. 2 RStV angesprochenen Kategorie aus dem systematischen Zusammenhang der Vorschriften für Telemedien zu entwickeln. Den besten Ansatz hat deshalb *Held* aufgezeigt: Zu Recht weist er darauf hin, dass die Definition des journalistisch-redaktionell gestalteten Angebots mit Blick auf die damit verbundenen Pflichten vorzunehmen ist.[101] Dort, wo die journalistischen Sorgfaltspflichten

---

[96] So die Begründung zur aktuellen Fassung des RStV, abgedruckt bei Hartstein et al., RStV, § 54.

[97] Dieser lautet: „Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.“

[98] S. dazu die Nachweise bei Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 42. S. zuletzt in diesem Sinne auch Lauber-Rönsberg, ZD 2014, 177 (181).

[99] BGH, NJW 2009, 2888 (2890) – spickmich.de.

[100] Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 48. Vgl. auch Weiner/Schmelz, K&R 2006, 453 (457).

[101] Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 48.

(§ 54 Abs. 2 RStV), die Benennung eines „presserechtlich" Verantwortlichen zusätzlich zu den sonstigen Impressumsangaben (§ 55 Abs. 2 S. 1 RStV) oder ein Gegendarstellungsrecht (§ 56 RStV) keinen Sinn ergeben oder offensichtlich nicht zur Art und Funktionsweise des Angebots passen, kann es sich nach dem Willen des Gesetzgebers nicht um ein journalistisch-redaktionell gestaltetes Telemedium handeln.

Wenn der Betreiber einer Website z. B. offensichtlich, d. h. für den Nutzer mühelos erkennbar, für einen Beitrag nicht selbst verantwortlich ist und sich diesen auch nicht zurechnen lassen muss, hilft die Nennung eines Verantwortlichen dem Betroffenen nicht weiter. Zudem ist zu beachten, dass die Geltung der journalistischen Sorgfaltsanforderungen auch für Beiträge, die einzelne Laien auf einer Internetseite platziert haben, bzw. generell für **journalistische Laien** eine wesentliche und ihnen aufgrund ihrer fehlenden Ausbildung kaum zumutbare Rechtsfolge ist – zumal dann, wenn man bedenkt, dass die Verletzung dieser Sorgfalt zu verschulden ist (§ 276 BGB) und zivilrechtliche Ansprüche nach sich ziehen kann.[102] **54**

Es muss sich daher um ein Telemedium handeln, das aus Sicht des Betroffenen wie ein Presseerzeugnis oder eine Fernsehsendung wirkt, d. h. diesen Eindruck vermittelt. Nach dem „**Benutzerhorizont**" muss von dem Telemedium der Eindruck vermittelt werden, dass das Angebot bewusst aus verschiedenen Quellen ausgewählt und von dem Anbieter zusammengestellt wurde und dass dabei auf eine gewisse verfestigte Organisationsstruktur zurückgegriffen wurde, die gerade nicht in einem eher zufälligen und vom Anbieter inhaltlich nicht kontrollierten Beitrag der Nutzer besteht. Vielmehr muss über die Rolle der anderen („dritter") Nutzer hinaus ein „Programm" präsentiert werden, das aus Benutzersicht vom Anbieter systematisch und organisiert zur Information ausgewählt wurde und das ihm auch suggeriert, der Anbieter wolle ihn qualifiziert, professionell und glaubwürdig informieren.[103] Erst dann sind Anordnungen wie die zur journalistischen Sorgfalt oder zu einem direkt gegen den Anbieter des Telemediums gerichteten Gegendarstellungsanspruch sinnvoll und zumutbar.[104] **55**

Was bedeutet dies nun für Social Media? **Netzwerkplattformen** wie insbesondere Facebook treten für den Nutzer nicht als Informationskanal und Instrument der Meinungsbildung auf. Auch werden die Inhalte – objektiv und aus Sicht des Nutzers – nicht ausgewählt und aufbereitet; vielmehr bestehen solche Dienste im Wesentlichen aus den Interaktionen der Nutzer und den von ihnen ausgetauschten und „geposteten" Inhalten, die gerade nicht dem Betreiber der Seite zuzuordnen sind. **56**

---

[102] Ricker/Weberling, Handbuch des Presserechts, 39. Kap., Rn. 10.

[103] Wie hier Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 49 ff. und Rn. 54. Zu weitgehend deshalb Zoebisch, ZUM 2011, 390 (393), der es ausreichen lässt, wenn „die Internetseite an Dritte gerichtete Informationen vorsieht, die über die reine selbstdarstellende Information des Anbieters hinausgehen".

[104] Einen anderen Ansatz wählt Kempermann. Er sieht das entscheidende Merkmal in der massenkommunikativen Wirkweise, d. h. in der Meinungsrelevanz (vgl. dens., Content-Regulierung, S. 242 f.). In der Regel wird dieser Ansatz allerdings zur selben Einordnung führen wie der hier vertretene Ansatz. Ähnlich auch Weiner/Schmelz, K&R 2006, 453 (457).

Dies ist gewollt und vom Nutzer auch unmittelbar erkennbar. Ihm ist bei der Benutzung klar, dass die meisten Inhalte von ihm selbst generiert wurden oder von den mit ihm vernetzten Personen stammen. Die Interaktionsmöglichkeiten der Nutzer und die fehlende planmäßig-organisierte und professionelle Präsentation von Inhalten durch den Seitenbetreiber bewirken deshalb, dass Netzwerkplattformen nicht journalistisch-redaktionell gestaltet sind.

57 **Kollaborative Wissensplattformen** (wie insbesondere Wikipedia) sind ebenfalls nicht als journalistisch-redaktionell gestaltet einzustufen:[105] Zwar liegt hier mit den – teilweise sehr umfassenden und viele Quellen auswertenden – Artikeln eine Sammlung meinungsbildungsrelevanter Informationen vor, die auf der Seite präsentiert werden und als Zusammenstellung empfunden werden können. Allerdings ist es gerade die Natur solcher kollaborativen Seiten, dass die Artikel von den Nutzern hochgeladen und fortgeschrieben werden und dass der abrufende Nutzer diese deshalb nicht dem Seitenbetreiber zuschreibt. Eine „**Endredaktion**", die noch einmal den gesamten Artikel vor dem Hochladen überprüfte und ihn von Anbieterseite „absegnet", existiert hier gerade nicht. Eine solche Prüfung und Sichtung der Artikel wäre aber Voraussetzung für eine journalistisch-redaktionelle Gestaltung.[106]

58 Entsprechendes gilt für **Multimediaplattformen** wie YouTube oder Vimeo. Hier sind es die Nutzer, die Videos hochladen und kommentieren. Der einzelne Videobeitrag wird sogar mit dem Namen desjenigen, der ihn hochgeladen hat, angezeigt. Der Nutzer weiß deshalb, dass es keine organisierte, verfestigte Redaktion gibt, welche die Verantwortung für die Inhalte übernimmt. Darauf, welchen Inhalt die einzelnen Video-Beiträge haben, kommt es deshalb nicht an. Der einzelne Nutzer, der eine Serie von Videos hochlädt, wird demgegenüber zumeist nicht einen solchen Spezialisierungs- und Organisationsgrad erreichen, dass er selbst als Anbieter eines journalistisch-redaktionell gestalteten Angebots anzusehen ist.

59 **Microblogging-Dienste** (insbesondere Twitter) erfüllen diese Voraussetzungen in der Regel ebenfalls nicht. Namentlich Twitter zeichnet sich aus Sicht des Nutzers nicht dadurch aus, dass der Anbieter oder ein einzelner Dritter, dessen „Follower" der Nutzer ist, Informationen gezielt auswählen, aufbereiten und so präsentieren, dass sie Meinungsbildungsrelevanz entfalten. Vielmehr erscheinen die einzelnen Nachrichten (sog. Tweets) nicht als Teil eines Ganzen, das als publizistisch-professionelles Angebot empfunden würde. Hiergegen spricht bei Microblogging-Diensten auch die begrenzte Zeichenzahl. Bei **Blogs** mag das im Einzelfall anders sein. Wenn der Anbieter eines solchen Blogs gezielt Quellen auswertet und hieraus Informationen selbst zusammenträgt und dem Nutzer Nachrichten mit Meinungsbildungsrelevanz präsentiert, dürfte bei einer gewissen organisatorischen Verfestigung bzw. Kontinuität ein journalistisch-redaktionell gestaltetes Angebot vorliegen.[107] In diesem Falle jedoch kommt der Interaktion mit dem Nutzer praktisch keine Bedeutung mehr zu;

---

[105] Wie hier Lent, in: Gersdorf/Paal, Informations- und Medienrecht, § 54 RStV, Rn. 5.1.

[106] Vgl. Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 41 unter Verweis auf VG Stuttgart, AfP 2010, 308 ff.

[107] Vgl. Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 58a; a. A. Kitz, ZUM 2007, 368 (371). der sogar verlangt, dass es „zumindest vorstellbar" sein müsse, dass das Angebot ernsthaft

er konsumiert den Blog dann wie eine Zeitung, so dass das Medium im Zweifel nicht mehr zu den Social Media zu zählen ist.

Insgesamt ist es deshalb auch hier – ähnlich wie bei der Definition des Rundfunks im einfachgesetzlichen Sinne – die **Interaktion der Nutzer** mit dem Anbieter der Seite und der Nutzer unter einander, die das Angebot auf der einen Seite zu einem sozialen Medium macht und die ihm gerade deshalb die Eigenschaft der journalistisch-redaktionellen Gestaltung verwehrt. Man könnte allein daran denken, dass moderierte Foren und Bewertungsplattformen, bei denen die Beiträge alle von einer „**Redaktion**" gelesen und sodann sortiert auf der Seite zur Verfügung gestellt werden[108], die eben beschriebenen Anforderungen erfüllen. Allerdings ist hierfür erforderlich, dass das Angebot für den Nutzer erkennbar durch eine bestimmte Person bzw. den Seitenbetreiber zusammengestellt und dargeboten wird und dass den Inhalten eine gewisse Meinungsrelevanz zukommt. Diese Eigenschaft dürfte jedoch nur wenigen Bewertungsplattformen zukommen, nicht zuletzt weil in der Regel der einzelne Beitrag des Nutzers als solcher erkennbar ist und im Vordergrund der Seite steht.[109] **60**

Das schließt es jedoch nicht aus, dass **einzelnen Beiträgen** (etwa einer einzelnen Internetseite eines sozialen Netzwerks) aufgrund ihrer Bearbeitung, Präsentation und Meinungsrelevanz diese journalistisch-redaktionelle Gestaltung zukommt. Sofern diese „trennbar" sind von dem übrigen, durch Nutzerinteraktion geprägten Angebot, gilt § 54 Abs. 2 RStV für diesen Teil – sofern aus Sicht des Nutzers die organisierte, systematische Gestaltung durch den Anbieter (i. d. R. Betreiber der Internetseite) erkennbar ist. Denn hierfür ist nicht Voraussetzung, dass das Gesamtangebot journalistisch-redaktionell gestaltet ist.[110] In einem solchen Fall besteht die Pflicht zur journalistischen Sorgfalt bezogen auf diesen einzelnen, abtrennbaren Teil mit der gebotenen Ausgestaltung. Darüber hinaus sind Social Media aber grundsätzlich gerade nicht zur journalistischen Sorgfalt verpflichtet. Ihre Sorgfaltspflichten werden vielmehr durch die §§ 7–10 TMG und die Grundsätze **Störerhaftung** sowie das sonstige allgemeine Zivilrecht bestimmt.[111] **61**

Zu beachten ist bei der Bewertung einzelner Beiträge bzw. Angebote, dass der Gesetzgeber in § 54 Abs. 2 RStV ein **Regelbeispiel** aufgenommen hat, indem er „insbesondere" die Telemedien unter den Begriff fassen will, die „vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild" wiedergeben. Wenn demgegenüber ein Blog oder ein Forum eher durch eigene Stellungnahmen des **62**

als periodisches Druckerzeugnis in Betracht käme. Diese Auslegung wird den Telemedien als besonderer Verbreitungsform von Informationen und als aliud zu Presse jedoch nicht gerecht.

[108] Prominente Beispiele sind z. B. spickmich.de und meinprof.de. Vgl. zu dieser Erscheinungsform Weigl, Meinungsfreiheit, S. 180 ff.

[109] Wie hier Lent, in: Gersdorf/Paal, Informations- und Medienrecht, § 54 RStV, Rn. 5.1.

[110] Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 56, der wiederum auf Jäger, jurisPK-ITR 4/2007, Anm. 4, Abschnitt II. verweist.

[111] Insoweit sei nochmals auf den Beitrag von Spindler, Kap. 5 verwiesen.

Betreibers oder der Nutzer geprägt ist und fast keine Bewegtbild- oder Pressequellen ausgewertet und zitiert werden, müssen besondere Anhaltspunkte vorgebracht werden, mit welchen die journalistisch-redaktionelle Gestaltung begründet wird.

63 Wenn soziale Medien nach diesen Wertungen zur journalistischen Sorgfalt verpflichtet sind – und dies ist nach dem vorstehend Gesagten namentlich im Falle von **moderierten Foren und Plattformen** sowie bei informierenden und systematisch aktualisierten Blogs denkbar –, dann ist damit zunächst die Pflicht zur sorgfältigen Recherche verbunden, d. h. eine stärkere Verpflichtung dazu, den Wahrheitsgehalt einer Aussage, die veröffentlicht werden soll, zu prüfen und diesen bei der Veröffentlichung auch nicht zu verfälschen bzw. sogar entsprechend kenntlich zu machen. Dabei sind für jede Art von Information (Bilder, grafische Darstellungen, Interviews, Vorausberichte, Leserbriefe) spezielle Regelungen anerkannt, die eine Irreführung des Nutzers vermeiden sollen.[112] Diesen Pflichten zur Sachlichkeit, Seriosität und Wahrheit in einer Weise nachzukommen, dass die Veröffentlichung irreführender oder sogar falscher Informationen als unverschuldet (d. h. nicht sorgfaltswidrig) anzusehen ist, wird für einen journalistischen Laien – und um solche wird es sich bei den betroffenen Social Media in der Regel handeln – oft eine sehr hohe Hürde darstellen. Auch die detaillierten **Regeln des Pressekodexes** zum Persönlichkeitsschutz – die u. a. die Berichterstattung über Straftäter, Kranke und in ihren Heimatländern verfolgte Oppositionelle erfasst[113] – bergen für den Laien ein nicht unerhebliches Haftungsrisiko. Dieses Risiko wird noch dadurch erhöht, dass die Sorgfaltspflicht nicht nur bezüglich der vom Anbieter selbst recherchierten Informationen besteht, sondern auch für die Inhalte von Dritten, die der Anbieter journalistisch-redaktionell gestaltet zur Verfügung stellt.[114]

9.2.2.6 Rundfunkrechtliche (allgemeine) Impressumspflicht

64 Neben den in § 54 Abs. 1 RStV in Bezug genommenen allgemeinen Vorschriften zur inhaltlichen Bindung statuiert § 55 RStV eine **Informationspflicht für Telemedien**. Die dort enthaltene allgemeine Impressumspflicht verpflichtet in ihrem Absatz 1 Anbieter aller Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, den Namen und die Anschrift sowie bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten“. Diese Verpflichtung dient dem Verbraucherschutz und sichert die Rechtsverfolgung im Falle von Rechtsverletzungen durch

---

[112] Vgl. Ziffer 2 des Pressekodexes, abgedruckt bei Hartstein et al., RStV, § 10 Rn. 3.
[113] Ziffer 8, insb. Richtlinien 8.1, 8.3, 8.4 und 8.6.
[114] Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 54 RStV, Rn. 10.

den Anbieter der Seite ab.[115] Gleichzeitig trägt sie zur Offenheit des Kommunikationsprozesses in der Weise bei, dass sie Transparenz auch bei Telemedien schafft, wo diese bei Presse und Fernsehen bereits gegeben ist.[116]

Damit wird eine **anonyme Meinungsäußerung im Internet** jedenfalls durch den Anbieter des Telemediums selbst nicht gewährleistet.[117] Diese (vermeintliche) Beschränkung der Rundfunkfreiheit – welche, wie oben gesehen, sämtliche Social-Media-Angeboten in ihrem Schutzbereich erfasst – ist verfassungskonform.[118] Zum einen stellt die Rundfunkfreiheit nach (noch) herrschender Ansicht eine normgeprägte Freiheit dar, so dass sich solcherlei Beschränkungen zumeist als Ausgestaltung und nicht als Eingriff darstellen. Zum anderen kommt vielen Telemedien, erst recht sozialen Medien, Meinungsrelevanz zu, so dass Vorkehrungen zum Missbrauch und zum Schutz der Meinungspluralität nötig werden können. Gleichzeitig muss gerade in diesem für die Kommunikationsfreiheiten wichtigen Bereich effektiver Rechtsschutz ermöglicht werden. Das rechtfertigt es, die Anbieter zur Transparenz zu verpflichten – zumal, wenn diese Transparenz nur wenige Angaben erfasst, die über eine bloße personale Zuordnung hinaus wenig preiszugeben verpflichten. Ob den Kommunikationsfreiheiten überhaupt das Recht entnommen werden kann, anonym seine Meinung zu äußern[119], spielt deshalb für die Impressumspflicht keine Rolle. **65**

Was die Erfüllung der Anforderungen betrifft, so hat sich die Rechtsprechung mittlerweile auf einige **Leitlinien** darüber geeinigt, wann die Angaben „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" sind: So müssen die Daten zwar nicht zwingend unter dem Begriff „Impressum" abgespeichert werden.[120] Allerdings muss die Rubrik so unmissverständlich bezeichnet sein, dass der Benutzer diese Angaben dahinter vermutet. Das wird z. B. für Titel wie „Mich"[121] oder „Kontakt"[122] angenommen; verneint wurde es im Einzelfall z. B. für die Betitelung mit „Info"[123]. Unmittelbare Erreichbarkeit wird allgemein angenommen, wenn zu den **66**

---

[115] So die Begründung zur Vorgängernorm im Mediendienstestaatsvertrag (abgedruckt bei Held, in: Hahn/Vesting, Rundfunkrecht, § 54 RStV, Rn. 1).

[116] Vgl. zu diesem Ziel Hoffmann-Riem et al., Konvergenz, S. 42. Für Presseerzeugnisse statuieren die Pressegesetze eine § 55 Abs. 1 und 2 RStV entsprechende Impressumspflicht; für den Bereich des privaten Rundfunks können die Angaben über die Landesmedienanstalt in Erfahrung gebracht werden (vgl. dazu Paschke, Medienrecht, Rn. 1332). Publizitätspflichten ergeben sich zudem auch aus § 23 RStV.

[117] Wohl aber eine – nach außen – anonyme Äußerung in einem Forum, das seinerseits der Impressumspflicht unterliegt, vgl. hierzu die Begründung zum 9. RÄStV, mit welchem § 55 RStV geschaffen wurde (abgedruckt bei Hartstein et al., RStV, vor § 55 Rn. 1).

[118] Ebenso Held, in: Hahn/Vesting, Rundfunkrecht, § 55 RStV, Rn. 11.

[119] S. zur Diskussion um anonyme Meinungsäußerungen zuletzt – aus Sicht des Datenschutzrechts – etwa Härting, NJW 2013, 2065 ff. und Heckmann, NJW 2012, 2631 ff. sowie – monographisch – Brunst, Anonymität im Internet, 2009.

[120] BGH, NJW 2006, 3633 (3635).

[121] KG, MMR 2007, 791.

[122] BGH, NJW 2006, 3633 (3635); LG Traunstein, MMR 2005, 781.

[123] LG Aschaffenburg, MMR 2012, 38 (39). Kritisch dazu Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 3; Lange, ZJS 2013, 141 (146 f.).

Angaben nicht mehr als **zwei Klicks** nötig sind[124] und – zur leichten Erkennbarkeit – eine entsprechend große Schriftgröße gewählt wurde.[125]

67 Kritisiert wurde zuletzt jedoch beispielsweise, dass in der offiziellen **Facebook-App** das Impressum nicht angezeigt wird.[126] Sofern es sich um eine dem Verpflichteten zurechenbare Anwendungsform handelt, muss er im Rahmen des § 55 RStV auch dafür sorgen, dass das Impressum nicht nur auf der allgemeinen Webseite bzw. am PC-Bildschirm zu lesen ist, sondern auch in den „offiziellen" Anwendungen für Smartphones.[127] Darüber hinaus stellen sich jedoch für Social Media als solche keine speziellen Anforderungen an die Art der Zugänglichmachung des Impressums. Zu beachten ist jedoch, dass die Gegebenheiten des einzelnen Telemediums möglicherweise aus technischen Gründen nur bestimmte Lösungen zulassen. So muss beispielsweise auch bei Verlinkungslösungen im Rahmen von Twitter-Accounts die dortige 160-Zeichen-Begrenzung beachtet werden.[128]

68 Umstrittener ist jedoch der **Adressatenkreis**. Jedenfalls der Betreiber der Seite, dem auch die veröffentlichten Informationen zuzurechnen sind, wird von der Impressumspflicht erfasst. Anbieter eines Telemediums kann allerdings nicht nur der Seitenbetreiber sein. Voraussetzung für ein Telemedium nach § 2 RStV ist nämlich allein ein „Dienst"[129], d. h. ein elektronisch verbreitetes Angebot. Ein solcher Dienst kann auch innerhalb eines anderen, übergeordneten Dienstes angeboten werden. Insbesondere bei sogenannten **Portalen** aller Art – seien sie zur Kommunikation, Information oder zum Verkauf gedacht – kann neben den Betreiber der Seite auch der einzelne Anbieter treten.[130] Was Social Media betrifft, kann dies namentlich dann der Fall sein, wenn Betroffene innerhalb einer größeren Seite über eine eigene Unterseite und einen Account verfügen, so z. B. bei Facebook, YouTube oder Twitter.

69 Mit auf einer Website zusammengefassten Informationen wird der Einzelne Plattformnutzer damit zum Anbieter im Sinne des § 55 Abs. 1 RStV. Wer also ein **eigenes Profil** auf Facebook erstellt hat und dieses mit Fotos, Kommentaren, Statusmeldungen, einer „Chronik" und Verlinkungen bestückt, kann damit grundsätzlich impressumspflichtig werden. Von dieser Kennzeichnungspflicht ist der jeweilige Profil- bzw. Seiteninhaber nur dann befreit, wenn die Ausschlussgründe gegeben sind. So sind Telemedien, die ausschließlich persönlichen oder familiären Zwecken dienen, nach § 55 Abs. 1 RStV nicht zu diesen Angaben verpflichtet.

---

[124] BGH, NJW 2006, 3633 (3635).

[125] Ausführlicher zur Rechtsprechung Held, in: Paschke et al., Hamburger Kommentar, 71. Abschnitt, Rn. 33 ff. und Haug, Internetrecht, Rn. 425 ff.

[126] Schwenke, Social Media, S. 61.

[127] Vgl. auch Rockstroh, in: Splittgerber, Praxishandbuch Rechtsfragen Social Media, Kap. 2 Rn. 153 unter Verweis auf OLG Hamm, CR 2010, 609 (611) zur iPhone-App.

[128] Diese und weitere Einzelfragen finden sich bei Schwenke, Social Media, S. 59 ff. sowie Rockstroh, in: Splittgerber, Praxishandbuch Rechtsfragen Social Media, Kap. 2 Rn. 155 ff.

[129] Held, in: Hahn/Vesting, § 55 Rn. 21.

[130] OLG Düsseldorf, MMR 2008, 682; Held, in: Paschke et al., Hamburger Kommentar, Abschnitt 71 Rn. 27.

Wann hiervon auszugehen ist, ist im jeweiligen Einzelfall zu bestimmen. Dabei kann der **begrenzte Zugang** zur Seite – z. B. des Facebook-Profils nur für selbst „hinzugefügte" Freunde – den persönlichen Zweck ergeben. Genauso kann sich dieser Zweck aber auch aus dem **Inhalt** ergeben, wenn die Seite nicht zugangsbeschränkt ist, wie dies etwa bei einer nicht auf den Zugriff durch Freunde beschränkten Facebook-Seite oder einer privaten Webseite („Familienhomepage") der Fall wäre.[131] Hier ist aus den dargestellten Inhalten heraus ersichtlich, dass das Angebot allein der Darstellung der eigenen Person für andere, insbesondere für nahestehende Personen dienen soll. Dahinter tritt das Interesse „unbekannter" Dritter an der Identität des Seitenbetreibers, das hinter der Impressumspflicht steht, zurück.[132] Das ist aber nur dann der Fall, wenn die Seite *ausschließlich* persönlichen und familiären Zwecken dient. Der Wortlaut der Norm ist mithin ernst zu nehmen. **70**

Ausweislich der Gesetzesbegründung soll die **gelegentliche private wirtschaftliche Tätigkeit** dennoch keine Impressumspflicht auslösen.[133] Der Gesetzgeber hatte dabei kleinere Geschäfte wie unter Zuhilfenahme eines privaten eBay-Accounts vor Augen, bei denen er kein Bedürfnis für einen entsprechenden informationellen Verbraucherschutz sah, zumal die Akteure selbst Verbraucher i. S. d. BGB sind. In diesem Sinne ist der Begriff „persönlich" auszulegen. Freilich wäre insoweit eine Klarstellung im Gesetzeswortlaut wünschenswert gewesen, gehen doch die Impressumsvorschriften bei geschäftlicher Tätigkeit dem Grundsatz nach von einer Verpflichtung aus, die nur bei *ausschließlich* privaten Zwecken dienender Nutzung ausgeschlossen sein soll. **71**

Für die hier interessierenden sozialen Medien ist davon auszugehen, dass eine **Facebook-Profilseite** oder ein YouTube-Profil nur dann nicht der Impressumspflicht unterliegt, wenn sich entweder aus dem Zugangskreis oder aus den Inhalten für einen objektiven Nutzer ergibt, dass mit der Seite allein persönliche Zwecke des Inhabers verfolgt werden. Die Facebook-Seite eines Unternehmens ist deshalb nicht von der Impressumspflicht befreit[134], ebenso wenig die eines Freiberuflers wie z. B. eines Architekten oder Rechtsanwalts. Gleiches gilt für eine **Twitter-Profilseite**, auch wenn diese nicht in der gleichen Weise mit einer Fülle von Informationen gefüllt ist wie bei anderen Social-Media-Anwendungen.[135] Auch reine „Fan-Seiten" von **72**

[131] Vgl. Held, in: Hahn/Vesting, Rundfunkrecht, § 55 RStV, Rn. 27 f.; Stadler, ZD 2011, 57 (58 f.).
[132] Zutreffende Erwägung bei Ott, MMR 2007, 354 (356); Held, in: Hahn/Vesting, Rundfunkrecht, § 55 RStV, Rn. 27.
[133] S. dazu die Begründung zum 9. RÄStV: „(. . .) Veräußerung von Waren, unmittelbar durch den privaten Anbieter oder aber über dritte Plattformen. In diesen Fällen ist entweder durch die persönliche Bekanntschaft zwischen Anbieter und Nutzer oder aber über den Plattformanbieter sichergestellt, dass die schutzwürdigen Belange der Beteiligten gewahrt werden können. Eine Kennzeichnungspflicht würde ansonsten dazu führen, dass entweder die Privatsphäre in diesen Fällen nicht mehr geschützt wäre oder aber die Kommunikation unterbliebe." (abgedruckt bei Held, a. a. O., Rn. 6, sowie bei Hartstein et al., RStV, vor § 55 Rn. 1).
[134] Vgl. Held, in: Hahn/Vesting, Rundfunkrecht, § 55 RStV, Rn. 27a.
[135] So auch Krieg, K&R 2010, 73 (74 f.).

Unternehmen oder bestimmter Marken, von denen aus Produkte beworben werden oder die offizielle Unternehmensseite verlinkt wird, sind impressumspflichtig.[136]

73 Von ausschließlich persönlichen Zwecken kann im Übrigen – gleichsam als Gegenausnahme – nicht mehr ausgegangen werden, wenn das betroffene Telemedium journalistisch-redaktionell gestaltet ist. Man mag darüber streiten, ob dann bereits begrifflich keine persönlichen Zwecke mehr vorliegen.[137] Jedenfalls aber ist das scheinbar rein persönliche Angebot dann überlagert durch Zwecke der Informationsvermittlung und -auswertung mit meinungsbildender Relevanz. In diesen Fällen aber müssen Vorkehrungen zum Schutz der Meinungsvielfalt getroffen werden, schon um das meinungsrelevante Telemedium in dieser Hinsicht nicht zu Unrecht gegenüber der Presse und dem Fernsehen zu privilegieren. § 55 Abs. 2 RStV ist deshalb nicht nur als Qualifikationstatbestand zu Absatz 1 zu sehen, sondern auch als lex specialis, die eine Berufung auf die Ausschlusstatbestände im Interesse der Meinungspluralität nicht mehr zulässt.

74 Eine andere Frage ist, wie die Impressumspflicht erfüllt werden kann, wenn – wie bei Twitter – nur ein begrenzter Raum zur Verfügung steht. Man wird hier zwar keine „**abgeschwächte**“ **Impressumspflicht** annehmen können, weil sich die Plattform nach dem Recht und nicht das Recht nach der Plattform richtet. Allerdings wird nach den jeweiligen Gegebenheiten und Funktionsweisen u. U. eine Verlinkung, die über höchstens 2 Klicks zu erreichen ist, dem Sinn und Zweck wie auch dem Wortlaut der Impressumsvorschriften genügen;[138] auch dürfte es bei **Smartphone- und Tablet-Anwendungen** genügen, wenn zum Impressum weit nach unten gescrollt werden muss, weil solche Anwendungen inzwischen allgemein üblich sind und das Recht diese Abrufform nicht verbieten möchte.[139] Keinesfalls aber darf die plattformspezifische Lösung dazu führen, dass die Information nicht mehr leicht zugänglich und erkennbar ist.[140] Weil die angeführten Fragen die Gerichte zumeist über die Regelungen des TMG beschäftigen, soll auf die Impressumspflicht unten noch einmal eingegangen werden. Denn neben die allgemeine Impressumspflicht des RStV treten die Kennzeichnungspflichten des TMG. Diese werfen andere Rechtsfragen auf und werden in anderen Kontexten relevant werden als die Normen des RStV und sollen deshalb getrennt von § 55 Abs. 1 RStV thematisiert werden.[141]

---

[136] S. aus der Rspr.: LG Regensburg, MMR 2013, 246 (247); LG Aschaffenburg, MMR 2012, 38; OLG Düsseldorf, MMR 2008, 682. Ein entsprechender Praxisratgeber rät Profilinhabern deshalb dazu, „im Zweifel“ von der Impressumspflicht auszugehen, vgl. Schwenke, Social Media Marketing und Recht, S. 51.

[137] In diese Richtung offenbar Held, in: Hahn/Vesting, Rundfunkrecht, § 55 RStV, Rn. 29; Weiner/Schmelz, K&R 2006, 453 (458).

[138] So auch Krieg, K&R 2010, 73 (75) für Twitter.

[139] Vgl. auch Pießkalla, ZUM 2014, 368 (373).

[140] Etwas zu kritisch aber OLG Hamburg MMR 2003, 105 ff., das von leichter Verfügbarkeit schon dann nicht mehr ausgeht, wenn bei normaler Bildschirmauflösung zum Impressum nach rechts „gescrollt“ werden muss.

[141] S. sogleich, Rn. 90 ff.

9.2.2.7 Gegendarstellungsanspruch

Der Gegendarstellungsanspruch stellt eine weitere Pflicht dar, die das Rundfunkrecht nur gegenüber eine bestimmten Art von Telemedien anordnet. § 56 RStV verpflichtet allein die bereits erwähnten journalistisch-redaktionell gestalteten Angebote zu einer solchen Gegendarstellung. Mit der Erstreckung dieses typischen Instituts des Medien-, insbesondere Presserechts dachte der Gesetzgeber – wie aus dem Bezug auf Angebote, „in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden" – namentlich an die **elektronische Presse**.[142] Wie bereits erwähnt, sind indes nur die wenigsten Social-Media-Angebote journalistisch-redaktionell gestaltet in diesem Sinne. Neben bestimmten Blogs und moderierten Bewertungsplattformen sind hier allein vereinzelte redaktionell gestaltete Unterseiten von Netzwerkplattformen denkbar, die von diesen trennbar und selbstständig sind.[143] Die sonstigen Social Media werden von § 56 RStV – ebenso wie von § 54 Abs. 2 RStV – nicht erfasst.[144] In den wenigen Fällen, in denen soziale Medien nach § 56 RStV zu einer Gegendarstellung verpflichtet sind, stellt dieser Anspruch ein klassisches Instrument zum Persönlichkeitsschutz dar, das sich weitgehend mit dem allgemeinen Gegendarstellungsanspruch des Presse- und Rundfunkrechts deckt und neben die sonstigen allgemeinen zivilrechtlichen[145] Ansprüche tritt. Insoweit sei auf das gesonderte Kapitel zur Haftung verwiesen.[146] Dass sich auch die Verpflichtung zur Gegendarstellung nur auf die journalistisch-redaktionell gestalteten Telemedien bezieht, ist – wie bei der Geltung der publizistischen Grundsätze – als sachgerecht anzusehen. Hierdurch wird wiederum dem Phänomen der **Konvergenz** Rechnung getragen. Dort, wo im Internet presseähnlich berichtet wird oder Angebote präsentiert werden, die dem Fernsehen entsprechen, sollte der Anbieter auch denselben Bindungen unterliegen wie die klassische Presse bzw. der klassische Rundfunk. Wenn die Schwelle zur journalistisch-redaktionellen Gestaltung aber nicht überschritten ist, kann ein solcher Gegendarstellungsanspruch nicht geltend gemacht werden; analoge Anwendungen des Presserechts oder des § 56 RStV scheiden in diesen Fällen

75

---

[142] Vgl. Mann, in: Spindler/Schuster, Recht der elektronischen Medien, § 56 RStV, Rn. 7; Schulz, in: Hahn/Vesting, Rundfunkrecht, § 56 RStV, Rn. 1 und 5 („massenkommunikative Telemedien"); Seitz, in: Hoeren et al., Multimedia-Recht, Teil 8 Rn. 84.

[143] S. hierzu Rn. 49 ff.

[144] Anders aber Zoebisch, ZUM 2011, 390 (393), der jede informierende und über Selbstdarstellung hinausgehende Internetseite erfassen möchte. Damit wären letztlich alle sozialen Medien der Gegendarstellungspflicht unterworfen. Wie hier Fiedler, in: Gersdorf/Paal, Informations- und Medienrecht, § 56 RStV, Rn. 4 ff., der von „presseäquivalente[n] journalistisch-redaktionelle[n] Telemedien" spricht.

[145] Der Anspruch aus § 56 RStV wird vom Gesetz selbst, das nach § 56 Abs. 3 S. 1 RStV den Rechtsweg zu den ordentlichen Gerichten eröffnet, auch als zivilrechtlicher Anspruch angesehen. Kritisch dazu und zur zugehörigen Rechtsprechung des BGH, die er als widersprüchlich ansieht: Schulz, in: Hahn/Vesting, Rundfunkrecht, § 56 RStV, Rn. 9.

[146] S. dazu den Beitrag von Spindler, Kap. 5.

aus.[147] **Anspruchsverpflichtet** ist hier der Anbieter des journalistisch-redaktionell gestalteten Mediums. Hierunter versteht die herrschende Meinung nur denjenigen, der eigene Inhalte anbietet (sogenannter Content-Provider), nicht aber Zugangsvermittler (Host-Provider) und solche Anbieter, die nur fremde Angebote zur Verfügung stellen.[148]

76 Spezifische Probleme zum Gegendarstellungsanspruch des § 56 RStV sind denn auch selten. Die Voraussetzungen des Anspruchs, ebenso wie seine Ausschlussgründe (§ 56 Abs. 2 und 4 RStV), decken sich mit denen des sonstigen Medienrechts. Die Art und Weise der Gegendarstellung wird allerdings hier durch die Art des Mediums beeinflusst. So ist die Gegendarstellung so lange wie die Tatsachenbehauptung, auf welche sie sich bezieht, in unmittelbarer Verknüpfung mit ihr anzubieten, § 56 Abs. 1 S. 3 RStV. Diese Möglichkeit zur unmittelbaren Verknüpfung besteht bei Telemedien im Gegensatz zum Fernsehen, Hörfunk oder zur Presse und macht die Gegendarstellung hier möglicherweise effektiver als bei den anderen Medien. Die Regelung zur Dauer der Verfügbarkeit ist nötig, weil die von der Gegendarstellung betroffenen Behauptungen ebenfalls dauerhaft abrufbar sein können; nur auf diese Weise kann die nötige **Waffengleichheit** hergestellt werden. Anders als im Presserecht hat im Rahmen des § 56 RStV die Gegendarstellung jedoch in gleicher Aufmachung wie die Tatsachenbehauptung zu erfolgen, § 56 Abs. 1 S. 2 RStV, und es werden Erwiderungen auf die Gegendarstellung hinsichtlich tatsächlicher Angaben[149] erlaubt, solange sie nicht unmittelbar mit ihr verknüpft sind, § 56 Abs. 1 S. 5 RStV.[150]

9.2.2.8 Datenschutzregeln

77 Siehe zum Datenschutz insgesamt den Abschnitt zu den **§§ 11 ff. TMG** (Rn. 99 ff.).

9.2.2.9 Unzulässige Werbung

78 Mit **§ 58 RStV** hält das Rundfunkrecht auch eine spezielle Werbevorschrift bereit, die sich nur an Telemedien richtet. Sie ersetzt für diese die umfangreichen Regelungen des Rundfunks, welche in den §§ 7–8a sowie 15–18 RStV für Werbung und wirtschaftliche Betätigungen normiert sind. Das Werberecht der Telemedien fußt auf **drei Säulen**: dem **Wettbewerbsrecht**, das auch das sonstige Werberecht prägt; den

---

[147] Überzeugend insoweit Mann, in: Spindler/Schuster, Recht der elektronischen Medien, § 56 RStV, Rn. 11 f.

[148] Vgl. zum Meinungsstand Schulz, in: Hahn/Vesting, Rundfunkrecht, § 56 RStV, Rn. 16 f.

[149] Einschließlich des üblichen „Redaktionsschwanzes" als bloßer Hinweis auf die Rechtslage, vgl. Mann, in: Spindler/Schuster, Recht der elektronischen Medien, § 56 RStV, Rn. 28. A.A. Hartstein et al., RStV, § 56 Rn. 12.

[150] Kritisch zu diesen beiden Charakteristika des Anspruches aus § 56 RStV mit Blick auf die Pressefreiheit Mann, in: Spindler/Schuster, Recht der elektronischen Medien, § 56 RStV, Rn. 21 und 26 f.

werberelevanten **Vorschriften des Jugendschutzes** sowie **§ 58 RStV**. Das Wettbewerbsrecht stellt dabei übergreifende Verhaltensregeln auf, die sich als solche nicht speziell auf Werbung beziehen, sondern sämtliche unlauteren Geschäftspraktiken erfassen. Die wettbewerbsrechtliche Generalklausel des § 3 UWG macht insoweit viele Verstöße gegen Werberegeln zu Wettbewerbsverstößen und fungiert in Verbindung mit einigen Spezialtatbeständen, insbesondere den §§ 4 Nr. 3 und 11; 5, 6, 7 UWG, als Abwehranspruch für Wettbewerber des rechtswidrig werbenden Anbieters. Während die jugendschützenden Vorschriften seit 2003 einheitlich für Rundfunk und Telemedien im Jugendmedienschutzstaatsvertrag (JMStV) geregelt sind (§ 6 i. V. m. §§ 2 Abs. 1; 3 Abs. 2 Nr. 1 JMStV)[151], gilt § 58 RStV nur für Telemedien.

79 Dass für Telemedien **andere Werberegeln** erforderlich sind als für das Fernsehen und den Hörfunk, folgt bereits aus den technischen Gegebenheiten. Viele Werbepraktiken des Fernsehens sind für Telemedien, insbesondere Social Media, nicht tauglich oder dort nicht gebräuchlich. Telemedien sind beispielsweise weniger durch Produktplatzierungen („product placement“) oder klassische Werbespots geprägt als vielmehr durch neue und internetspezifische Werbevarianten. So ist für sie die sogenannte Bannerwerbung typisch, d. h. die Einblendung einer Werbegrafik in eine aufgerufene Internetseite, oder auch völlig neue Varianten des personalisierten Marketings, die gerade bei den Netzwerkplattformen beliebt sind. So werden beispielsweise die „Likes“ von Facebook-Nutzern dazu genutzt, ihnen auf sie zugeschnittene Werbebanner zu präsentieren oder es werden Werbepostings auf die sogenannte Pinnwand bzw. die Chronik gesetzt, in denen Freunde dazu genutzt werden, ein Produkt zu „bewerben“, das sie in der Vergangenheit mit einem „gefällt mir“-Klick versehen haben. Auch bietet das Internet mit dem Gebot anonymer Nutzung (§ 13 Abs. 6 TMG) die Möglichkeit, mittels anonymer Profile bzw. Kennungen Rezensionen, Kommentare o. ä. zum eigenen Produkt abzugeben und auf diese Weise den Eindruck zu erwecken, es handele sich um die Stellungnahme eines neutralen Dritten. Solcherlei „**kaschierte**“ **Werbung** wird durch die Interaktionsmöglichkeiten, welche Social Media auszeichnen, in besonderer Weise befördert. Klassische Medien, namentlich der Rundfunk, kennen diese Werbeformen nicht.[152]

80 Die Vorgaben, die das Rundfunkrecht den meisten sozialen Medien macht, sind freilich nicht zahlreich. Sofern es sich nicht um Fernsehtext handelt und das Medium nicht „fernsehähnlich“ und gleichzeitig auch kein audiovisueller Mediendienst auf Abruf ist, greift allein **§ 58 Abs. 1 S. 1 RStV**. Die Vorschrift zu Gewinnspielen (§ 58 Abs. 4 RStV) hat für Social Media aus tatsächlichen Gründen kaum Anwendungsfelder.

---

[151] S. dazu ausführlicher Kreile, in: Dörr et al., Handbuch Medienrecht, Abschnitt J, Rn. 77 ff. Insbesondere ist eine Werbung für alkoholische Getränke in Plattformen, die sich an Kinder und Jugendliche richten oder sie besonders ansprechen, verboten (§ 6 Abs. 5 JMStV). Zum Jugendmedienschutz sogleich, Rn. 84 ff.

[152] Ausführlicher zu den Werbevarianten im Bereich der Social Media – aus eher praktischer Sicht – Lichtnecker, GRUR 2013, 135 ff. sowie – aus datenschutzrechtlicher Sicht – Venzke, ZD 2011, 387 ff.

81 § 58 Abs. 1 S. 1 RStV normiert sodann für Telemedien einen der wichtigsten Grundsätze des Werberechts, nämlich das Gebot der **Trennung von Werbung und Programm**. Dieser Grundsatz ist im Kern im gesamten Medienrecht anerkannt[153] und verpflichtet den Anbieter dazu, das Programm für den Nutzer erkennbar von der Werbung zu trennen. Spezielle Vorschriften zur Handhabung des Trennungsgebots existieren dabei für die Telemedien nicht. Es hängt vielmehr vom Einzelfall ab, ob dieser Grundsatz hinreichend gewahrt wurde oder nicht. Das Trennungsgebot kann als Transparenzgebot verstanden werden; es tritt neben die Verpflichtung aus § 6 TMG, nach welcher geschäftliche Kommunikation als solche zu kennzeichnen ist.[154] Verhindert wird so insbesondere die sogenannte Schleichwerbung. Schwierigkeiten in der konkreten Ausgestaltung ergeben sich insoweit weniger für die Fälle der Bannerwerbung, die üblicherweise sofort als solche erkennbar ist. Es sind eher die **Hyperlinks**, bei welchen es im Einzelfall schwierig sein kann, das Trennungsgebot zu wahren. Es muss für den Nutzer jedenfalls erkennbar sein, dass er über den Link zu einem werbenden Angebot gelangt.[155] Die Einzelheiten sind jedoch umstritten. So ist eine „Zwischenseite" mit einem Hinweis auf den werbenden Charakter, ein Hinweis unter dem Hyperlink oder das Aufführen unter einer bestimmten Rubrik der betroffenen Internetseite genauso wie zahlreiche andere Lösungen denkbar. Entsprechendes gilt auch für die Methode des sogenannten viralen Marketings, bei der auf Videoplattformen Imagevideos zu einem Unternehmen oder Produkt zur Verfügung gestellt werden, die nicht als „offizieller Werbespot" erkennbar sind. Auch hier muss für den Nutzer deutlich werden, dass es sich um einen gesponserten bzw. einen werbenden Beitrag handelt; anderenfalls wird gegen § 58 RStV, u. U. auch gleichzeitig gegen § 6 TMG, verstoßen.[156]

82 Sobald aber für den Nutzer des Telemediums der werbende Teil der Inhalte als solcher erkennbar ist, sind grundsätzlich alle gängigen Werbemethoden sozialer Medien rundfunkrechtlich zulässig. Auch die Integration von Werbung in das „Programm" ist hier weniger problematisch als beim Fernsehen, wo das Trennungsgebot des § 7 Abs. 3 S. 1 und 2 RStV strenger gehandhabt wird und entweder eine dauerhafte **Kennzeichnung** als „Werbesendung" verlangt oder die deutlich sichtbare Abtrennung vom Programm. Bei den Telemedien besteht insoweit die Gefahr des zufälligen Hinzuschaltens ohne Kenntnisnahme von den werbenden Teilen des Programmes nicht, so dass ein Hinweis zu Beginn eines Programmteils als ausreichend erachtet werden kann;[157] auch hier ist die Ausgestaltung aber stark vom konkreten Einzelfall abhängig. Die Kennzeichnung muss jedenfalls nicht ausdrücklich den Begriff „Werbung" verwenden; auch Bezeichnungen wie „gesponsert" im Falle der von Facebook in

---

[153] Kreile, in: Dörr et al., Handbuch Medienrecht, Abschnitt J, Rn. 16.

[154] Hartstein et al., RStV, § 58 Rn. 3.

[155] So die h. M., vgl. Stenner, Werbung, S. 167; Hartstein et al., RStV, § 58 Rn. 3; Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 58 RStV, Rn. 14; Petersen, Medienrecht, § 15 Rn. 27.

[156] Vgl. Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 36; Schulz, in: Hahn/Vesting, Rundfunkrecht, § 58 RStV, Rn. 4.

[157] Überzeugend insoweit Stenner, Werbung, S. 168 f.

die individuelle Startseite integrierten, personalisierten Werbeinhalte erfüllen den Zweck des § 58 Abs. 1 S. 1 RStV und sind daher zulässig. Nicht gekennzeichnete Werbung – sei es aufgrund nicht erkennbarer Integration ins sonstige Angebot, aufgrund von nicht hinreichend erkennbarer Verlinkung oder im Falle von als Kunden- bzw. Nutzerreaktion getarnter Schleichwerbung – ist aber stets unzulässig und über § 4 Nr. 3 UWG i. V. m. § 3 Abs. 3 UWG auch **wettbewerbswidrig**; auch Verstöße gegen die §§ 4 Nr. 11 (etwa bei „gekauften Nutzermeinungen“[158]); 5 UWG kommen in Betracht, so dass Wettbewerber bei Vorliegen einer Wettbewerbshandlung mit entsprechenden Konkurrentenklagen reagieren können.[159]

83 Neben das Kennzeichnungsgebot des § 58 Abs. 1 S. 1 RStV tritt das **Verbot unterschwelliger Technik** nach § 58 Abs. 1 S. 2 RStV, das indes wenig praktische Relevanz aufweist. Die darüber hinaus in § 58 RStV normierten Werberegeln des § 58 Abs. 2 und 3 RStV sind für die hier interessierenden Social Media nicht relevant: Denn zunächst ist der Fernsehtext (§ 58 Abs. 2 RStV) kein Thema sozialer Medien. Sodann sind Social Media auch keine fernsehähnlichen Telemedien im Sinne des § 58 Abs. 3 RStV. Unter diesen versteht der Gesetzgeber im Einklang mit der AVMD-Richtlinie allein solche Abrufdienste, bei denen fernsehähnliche Dienste wie Spielfilme, Sportberichte, Fernsehfilme und -spiele sowie Dokumentarfilme im Rahmen einer wirtschaftlichen Tätigkeit bereitgehalten werden.[160] Hierunter fallen aber rein nutzergenerierte Videoportale nicht. Denn hier übernimmt nicht der Diensteanbieter die Auswahl, sondern der Nutzer, über den keine wirksame Kontrolle ausgeübt wird.[161] Plattformen wie Vimeo oder YouTube stellen also keine fernsehähnlichen Telemedien in diesem Sinne dar. Die anderen hier relevanten sozialen Medien erfüllen bereits von der Art ihres Angebots her den Tatbestand nicht. Für Social Media hält der 2010 in Kraft getretene § 58 Abs. 3 RStV also keine weiteren Restriktionen bereit. Vor diesem Hintergrund kann das Werberecht der Telemedien im Verhältnis zu dem des Fernsehens als sehr liberal bezeichnet werden. Solange Werbung als solche erkennbar vom Programm getrennt bzw. abtrennbar ist und die Vorschriften des Jugendschutzes eingehalten werden[162], sind im Rahmen von Social Media viele, auch neue und kreative Werbekonzepte denkbar, die nicht alle auch ins Fernsehen transportiert werden könnten bzw. dürften.

---

[158] Solmecke, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 21.1 Rn. 40 f.

[159] Vgl. Smid, in: Spindler/Schuster, Recht der elektronischen Medien, § 58 RStV, Rn. 28. Ausführlicher zu den wettbewerbsrechtlichen Folgen Kreile, in: Dörr et al., Handbuch Medienrecht, Abschnitt J, Rn. 97 ff.

[160] Begründung zum 13. RÄStV, abgedruckt bei Hartstein et al., RStV, vor § 58.

[161] Begründung zum 13. RÄStV, wie vor.

[162] Verboten ist nach § 4 Abs. 1 S. 1 Nr. 11, Abs. 2 S. 1 Nr. 2 JMStV nur die Werbung für indizierte Angebote. Im Übrigen ist Werbung nur dann verboten, wenn sie selbst ein jugendmedienschutzrechtlich unzulässiges Angebot darstellt, s. zum Ganzen ausführlich Altenhain, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 20 Rn. 112 ff.

9.2.2.10 Jugendschutz

84 Bereits das Grundgesetz sieht im Jugendschutz ein Gut von Verfassungsrang, das der Ausübung der Kommunikationsfreiheiten Grenzen setzen kann. Konsequenterweise wird er daher in Art. 5 Abs. 2 GG als Schranke der Grundrechte des Art. 5 Abs. 1 GG sogar neben das „allgemeine Gesetz" gestellt, so dass zum Schutz der Jugend auch Sondergesetze gegen die Medien möglich sind. Der Jugendschutz ist insbesondere in zwei Regelwerken umgesetzt: dem Jugendschutzgesetz (**JuSchG**) und dem Jugendmedienschutzstaatsvertrag (**JMStV**). Für Social Media wird dabei in den allermeisten Fällen[163] nur der JMStV relevant, weil das JuSchG den Jugendschutz für die sogenannten Trägermedien regelt[164], d. h. für die auf einem Datenträger gespeicherten Medien. Online-Anwendungen, Downloads o. ä. fallen dagegen unter den JMStV. Dieser Staatsvertrag regelt den Jugendschutz für sämtliche elektronischen Medien, also auch für den (privaten und öffentlich-rechtlichen) Rundfunk, § 2 Abs. 1 JMStV. Einige Vorschriften gelten für alle elektronischen Mediengattungen, andere wiederum richten sich speziell an Telemedien. Daneben gelten zusätzlich die jeweils einschlägigen Vorschriften des RStV sowie des TMG, § 2 Abs. 3 JMStV.

85 Der JMStV entfaltet ein **dreistufiges Schutzinstrumentarium**[165], das grundsätzlich für alle elektronischen Medien gilt. Es sieht drei Arten von jugendschutzrechtlich relevanten Angeboten vor: So existieren zunächst absolut unzulässige Angebote, für die ein ausnahmsloses Verbreitungsverbot statuiert wird (§ 4 Abs. 1 S. 1 Nr. 1–11 JMStV), und relativ unzulässige Angebote, die unter bestimmten Voraussetzungen verbreitet werden dürfen, obwohl sie Jugendliche gefährden oder beeinträchtigen (relative Verbreitungsverbote der §§ 4 Abs. 2 S. 2 und 5 Abs. 1 JMStV). Als mildeste Eingriffsstufe sind schließlich in § 7 JMStV Instrumente der Selbstkontrolle vorgesehen.

86 Die grundsätzlich **absolut unzulässigen Angebote** der Nummern 1–6 des § 4 Abs. 1 JMStV sind dabei dem Strafrecht entnommen und transportieren Straftatbestände staatsschützender Normen bzw. Straftaten gegen Allgemeingüter in den medienspezifischen Jugendschutz; der enge Konnex zum Strafrecht wird auch durch § 4 Abs. 1 S. 2 JMStV deutlich, der die entsprechende Geltung der §§ 86 Abs. 3, 131 StGB anordnet. Die restlichen Tatbestände des § 4 Abs. 1 JMStV sichern die Menschenwürdegarantie – insoweit auch als allgemeinen Programmgrundsatz – ab und sollen dem sexuellen Missbrauch vorbeugen, indem sie Kinderpornographie ebenso verbieten wie Vorstufen und Gefährdungssituation hierzu. Die „**sonstige**" **Pornographie** (d. h. diejenige ohne strafrechtliche Relevanz und ohne Bezug zur Sexualisierung von Kindern) wird nach § 4 Abs. 2 S. 1 Nr. 1 JMStV – ebenso wie indizierte Angebote (Nr. 2) oder offensichtlich schwer jugendgefährdende Inhalte

---

[163] S. zur schwierigen Abgrenzung Cole, in: Dörr et al., Handbuch Medienrecht, Abschnitt H, Rn. 39.

[164] Vgl. dazu § 1 Abs. 2 JuSchG. Einen Überblick über die verschiedenen Regelwerke zum Jugendschutz liefert Fechner, Medienrecht, 6. Kapitel, Rn. 1 ff.

[165] Altenhain, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 20 Rn. 9 f.

(Nr. 3)[166] – von § 4 Abs. 2 S. 1 JMStV zwar eigentlich ebenfalls verboten. Für Telemedien macht § 4 Abs. 2 S. 2 JMStV aber sodann eine Ausnahme, wenn der Anbieter sicherstellt, dass das Angebot nur Erwachsenen im Sinne einer geschlossenen Benutzergruppe zugänglich ist. Sofern also ein verlässliches Altersverifikationssystem[167] besteht, darf über Telemedien Pornographie verbreitet werden; das setzt jedoch in der Regel eine „face-to-face"-Kontrolle voraus, etwa durch persönlichen Vertragsschluss oder das sogenannte Post-Ident-Verfahren der Deutschen Post AG.[168] Diese Privilegierung gilt für den Rundfunk – auch soweit das digitale Fernsehen betroffen ist – nicht, was vielfach kritisiert wurde.[169] Im Fernsehen ist Pornographie also nur in Form von Pay-TV-Abrufangeboten (Video on demand) zulässig. Dies ist einer der Hauptgründe dafür, dass Anbieter elektronischer Medien Anträge auf Feststellung der Unbedenklichkeit nach § 20 Abs. 2 RStV stellen,[170] d. h. von der Landesmedienanstalt die Feststellung begehren, dass ihr Angebot keinen Rundfunk darstellt. Erst dann ist ihnen dieser lukrative Markt eröffnet.

87 § 5 Abs. 1 JMStV regelt in der Folge die sogenannten **entwicklungsbeeinträchtigenden Angebote**. Diese Angebote, die sich unterhalb der Schwelle des § 4 Abs. 2 JMStV befinden, dürfen zugänglich gemacht und verbreitet werden, wenn der Anbieter sicherstellt, dass Kinder oder Jugendliche einer bestimmten Altersgruppe sie „üblicherweise nicht wahrnehmen". Die insofern einzuhaltenden Sicherheitsmaßnahmen und Zugangs-„Kontrollen" sind also weniger strikt als die der eben genannten Privilegierung in § 4 Abs. 2 JMStV. Die Vorsorgemaßnahmen können entweder technischer Natur sein (§ 5 Abs. 3 Nr. 1 JMStV) oder durch eine zeitliche Beschränkung wirken (§ 5 Abs. 3 Nr. 2 JMStV); Letzteres ist im Falle von Social Media freilich nur begrenzt vorstellbar. Die technische Lösung kann gem. § 11 Abs. 1 JMStV bei Telemedien auch darin bestehen, dass die jugendgefährdeten Angebote durch ein als geeignet anerkanntes Jugendschutzprogramm dergestalt abgesichert werden, dass die Angebote so programmiert werden oder dass das Jugendschutzprogramm ihnen vorgeschaltet ist. Dabei muss das Programm gem. § 11 Abs. 2 JMStV durch die zuständige Landesmedienanstalt anerkannt werden, die insoweit durch die Kommission für Jugendmedienschutz (**KJM**) handelt; auf die Erteilung besteht nach § 11 Abs. 3 JMStV ein Anspruch, wenn das Programm einen nach Altersstufen differenzierenden Zugang ermöglicht oder „vergleichbar geeignet"

---

[166] Dabei ist umstritten, ob § 4 Abs. 2 S. 1 Nr. 3 JMStV als Auffangtatbestand auch pornographische Angebote erfasst oder als selbstständige Gruppe neben die beiden anderen Nummern tritt. Vgl. zum Streitstand Hartstein et al., § 4 JMStV, Rn. 63b f.

[167] So die Begründung zum JMStV.

[168] Beispiele solcher von der KJM für zulässig erachteten Altersverifikationssysteme finden sich bei Hartstein et al., § 4 JMStV, Rn. 65a.

[169] Vgl. Cole, in: Dörr et al., Handbuch Medienrecht, Abschnitt H, Rn. 28 m. w. N.; Hartstein et al., § 4 JMStV, Rn. 65; Kreile/Diesbach, ZUM 2002, 849 (850 f.); Liesching, in: BeckOK-JMStV, § 4 Rn. 1; Hertel, in: Hahn/Vesting, Rundfunkrecht, § 4 JMStV, Rn. 4; Erdemir, in: Spindler/Schuster, Recht der elektronischen Medien, § 4 RStV, Rn. 64.

[170] Erdemir, in: Spindler/Schuster, Recht der elektronischen Medien, § 4 RStV, Rn. 63 spricht hier von einer „Flucht in die Telemedien".

ist. § 12 JMStV ordnet schließlich noch eine Hinweispflicht hinsichtlich der Altersfreigabe für die Angebote von Telemedien an, die mit solchen auf Trägermedien vergleichbar sind. Hier soll also Parallelität zwischen den Regelungen des JuSchG
88 und des JMStV hergestellt werden. Es würde den Rahmen dieses Beitrags sprengen, auf alle Details insbesondere der Zugangskontrolle einzugehen. Allgemein lässt sich mit Blick auf Social Media zweierlei feststellen: Zum einen werden sie in gleicher Weise wie das Fernsehen oder sonstige Medien in den Jugendschutz einbezogen. Auf der anderen Seite stellt der Gesetzgeber auch in diesem Bereich deutlich geringere Anforderungen bzw. deutlich weniger Restriktionen an Telemedien als an den Rundfunk. Inhalte, die im Fernsehen nicht zugänglich gemacht werden dürfen, sind in Telemedien bei Einhaltung gewisser **technischer Zugangskontrollen** zulässig. Insbesondere der Zugang zu pornographischen Inhalten kann über Telemedien einfacher gewährleistet werden als über den Rundfunk, was die Entwicklung telemedialer Angebote erheblich beschleunigt haben dürfte. Absolut wirksame Jugendschutzkonzepte gibt es in der Praxis insoweit nicht.[171] Gerade das heute übliche Abrufen sozialer Medien über Smartphones und Tablet-Computer macht technische Lösungen zunehmend schwieriger.[172] Hinzu kommt, dass die meisten Social-Media-Angebote über ausländische Seiten vorgehalten werden, womit de facto die deutschen Standards häufig unterlaufen werden.

9.2.3 Vorgaben des TMG mit Relevanz für Social Media

89 Neben die inhaltliche Regulierung der Telemedien durch das Rundfunkrecht, die im Lichte der Medienfreiheiten zu sehen und auszulegen ist, treten für alle Telemedien die Vorgaben des TMG. Dieses gilt für alle Anbieter von Telemedien, unabhängig davon, ob das Angebot gegen Entgelt erfolgt oder nicht (§ 1 Abs. 1 S. 2 TMG). Im TMG wird die Frage nach dem anwendbaren Recht hinsichtlich der telemedienrechtlichen Fragen beantwortet; insoweit gilt gem. § 3 TMG grundsätzlich das Herkunftslandprinzip.[173] Außerdem statuiert das TMG Rechte und Pflichten der Telemedien(anbieter) im Geschäftsverkehr. Es enthält also die **wirtschaftsbezogenen Regelungen**, die neben die inhaltlichen Regelungen des Rundfunkrechts treten. Die fehlende Normierung in einem Gesetz hat dabei kompetenzielle Gründe, weil der Bund die Telemedien nur soweit regeln konnte, wie die Gesetzgebungskompetenz für das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG) reicht. Für Social Media werden dabei die §§ 5 ff. TMG relevant.

---

[171] So auch Rockstroh, in: Splittgerber, Praxishandbuch Rechtsfragen Social Media, Kap. 2 Rn. 238 f.

[172] S. nur den Befund von jugendschutz.net in MMR-Aktuell 2012, 332982.

[173] Welches jedoch in anderen Bereich des IPR als Ansatzpunkt gewählt wird, wodurch sich vielfach Widersprüche ergeben, vgl. dazu Heckmann, jurisPK-Internetrecht, Kap. 1 Rn. 151 ff. m. w. N.

9.2.3.1 Besondere Impressumspflicht

So statuieren die §§ 5, 6 TMG eine **besondere Impressumspflicht**, die neben die bereits erwähnte, aus § 55 RStV folgende rundfunkrechtliche Impressumspflicht tritt.[174] Ist der Anwendungsbereich dieser besonderen Impressumspflicht eröffnet, so müssen nach § 5 TMG zusätzlich zu den spärlichen Angaben des § 55 Abs. 1 RStV (Name, Anschrift, Vertretungsberechtigter bei juristischen Personen) folgende Informationen bereitgehalten werden: Angaben über das Kapital der Gesellschaft (§ 5 Abs. 1 Nr. 1 TMG), Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der E-Mail-Adresse (§ 5 Abs. 1 Nr. 2 TMG), ggf. Angaben zu einer Aufsichtsbehörde (§ 5 Abs. 1 Nr. 3 TMG), Registereintragungen (vgl. § 5 Abs. 1 Nr. 4 TMG), berufsbezogene bzw. berufsständische Angaben (vgl. § 5 Abs. 1 Nr. 5 TMG), die Umsatzsteuer- bzw. Wirtschafts-Identifikationsnummer (§ 5 Abs. 1 Nr. 6 TMG) sowie Angaben über die Abwicklung/Liquidation von Gesellschaften (§ 5 Abs. 1 Nr. 7 TMG).[175] § 6 TMG macht sodann Vorgaben für zwingende Angaben in kommerzieller Kommunikation. Da diese Vorschrift aber wenige Berührungspunkte mit sozialen Medien aufweist, sei sie im vorliegenden Kontext ausgeklammert; sie ist zudem aus sich heraus verständlich. **90**

Diese erhebliche Ausweitung der anzugebenden Information trifft nach § 5 Abs. 1 TMG Diensteanbieter von „**geschäftsmäßigen**, **in der Regel gegen Entgelt** angebotenen Telemedien“. Dabei wird überwiegend im Einklang mit der früheren Rechtslage und dem sonstigen, auch außerhalt des Internetrechts verfolgten Begriffsverständnis unter einer geschäftsmäßigen Betätigung die bloße nachhaltige Tätigkeit verstanden, unabhängig davon, ob sie mit oder ohne Gewinnerzielungsabsicht betrieben wird.[176] Nachhaltigkeit ist bei einer – subjektiv – auf einen längeren Zeitraum ausgerichteten Tätigkeit gegeben. „Geschäftsmäßig“ ist also gerade nicht gleichzusetzen mit einer auf Gewinnerzielung gerichteten oder entgeltlichen Tätigkeit.[177] Hiernach ist die Geschäftsmäßigkeit dennoch bei den meisten selbstständigen Telemedienangeboten gegeben, und so ist es das weitere Tatbestandsmerkmal, das für eine Eingrenzung des Adressatenkreises sorgt. **91**

Denn ein geschäftsmäßiges Angebot ist nur als „**in der Regel gegen Entgelt angebotene(s)** Telemedium“ der besonderen Impressumspflicht unterworfen. Die Auslegung dieses Merkmals ist zwar im Einzelnen umstritten.[178] Weitgehende **92**

---

[174] Der Begriff des „Anbieters“ eines Telemediums ist insoweit identisch. Wie im Rahmen des § 55 Abs. 1 RStV ist also auch ein eigenes Teilangebot auf einer Social-Media-Plattform grds. von § 5 TMG erfasst, vgl. Rockstroh, in: Splittgerber, Praxishandbuch Rechtsfragen Social Media, Kap. 2 Rn. 141.

[175] Hinweise zu den Details der verpflichtenden Angaben finden sich auch im Leitfaden des BMJ unter: www.bmj.de/musterimpressum.

[176] Vgl. Held, in: Paschke et al., Hamburger Kommentar, 71. Abschnitt, Rn. 31; Brönnecke, in: Roßnagel, Telemediendienste, § 5 TMG, Rn. 40.

[177] So aber OLG Hamburg, CR 2008, 606.

[178] S. zu den einzelnen Auslegungsvarianten ausführlicher Lange, ZJS 2013, 141 (141 ff.).

Einigkeit besteht darin, dass es diese Voraussetzung ist, welche auf die Gewinnerzielungsabsicht abstellt. Durch die Einschränkung „in der Regel" wird dabei allerdings deutlich, dass die Gewinnerzielungsangebot nicht im konkreten Fall für den konkreten Anbieter mit seinem konkreten Telemedium gegeben sein muss, sondern abstrakt für die betroffene Art an Telemedien. Es erfolgt daher eine typisierende, abstrakte Betrachtung aus einer „objektiven Nutzersicht", was im Übrigen auch die Kontrolle einfacher macht – nicht zuletzt im Fall von wettbewerbsrechtlichen Konkurrentenklagen. Es genügt mithin eine „**wirtschaftliche Relevanz**"[179] der jeweiligen Seite. Wenn aber ein Telemedium vorliegt, das üblicherweise nur gegen Entgelt angeboten wird, kann sich der Anbieter nicht mit dem Argument den Pflichten der §§ 5, 6 TMG entziehen, er selbst verlange im Gegensatz zu den sonstigen Anbietern solcher Dienste kein Entgelt.[180]

93 Welches sind nun diese typischerweise gegen **Entgelt** angebotenen Telemedien? Es dürfte zu weit gehen, im Rahmen der §§ 5, 6 TMG das Entgelt für das Anlegen eines Social-Media-Profils – etwa auf einer Plattform wie Facebook – in der Preisgabe der persönlichen Daten zu Werbezwecken zu sehen.[181] Denn dieses „Entgelt" wird dem Nutzer aufgezwungen und nicht selten ohne seine Kenntnis erlangt. Jedenfalls mit Blick auf die Impressumspflicht kann diese datenschutzrechtliche Einwilligung nicht als Entgelt gedeutet werden. Denn erfasst werden sollen Telemedien mit Bezug zu einem kommerziellen Angebot, ob sich dieses nun auch im Netz finden lässt oder nicht. Anderenfalls wäre jedes nachhaltig gepflegte Facebook-Profil zu einem umfassenden Impressum verpflichtet, insbesondere auch zur Angabe der E-Mail-Adresse und einer weiteren Kontaktmöglichkeit. Eine am Sinn und Zweck der Norm orientierte Auslegung ergibt – nicht zuletzt auch mit Blick auf die Art der Angaben, zu denen § 5 TMG verpflichtet – daher, dass solche Telemedien gemeint sind, über die entweder unmittelbar beruflich-kommerzielle Kontakte abgewickelt werden[182] oder für die ein Entgelt tatsächlich verlangt wird oder die gleichsam als „Eingangsportal" zu den kommerziellen Angeboten dienen. Letzteres ist der Fall, wenn beispielsweise die Social-Media-Fanpage oder ein Unternehmensprofil dazu genutzt wird, für das Unternehmen zu werben[183] und sodann ein Link auf die kommerziellen Seiten des Unternehmens führt.[184] Solche Auftritte sind also zu dem umfassenden Impressum des § 5 TMG verpflichtet, genauso wie Seiten, die zur Generierung von Einnahmen

---

[179] Held, in: Paschke et al., Hamburger Kommentar, 71. Abschnitt, Rn. 31. Für einen „wirtschaftlichen Charakter im weitesten Sinne" Rockstroh, MMR 2013, 627 (629).

[180] Zutreffend daher Brönnecke, in: Roßnagel, Telemediendienste, § 5 TMG, Rn. 44.

[181] So für das Vertragsrecht Bräutigam, Kap. 3 Rn. 18 ff. sowie ders., MMR 2012, 635 ff. Ebenso: Lange, ZJS 2013, 141 (144 f.).

[182] So etwa bei einem nachhaltig betriebenen selbstständigen eBay-Account, vgl. OLG Brandenburg, GRUR-RR 2007, 54.

[183] S. z. B. LG Berlin, Beschluss vom 28.03.2013 – 16 O 154/13 = JurPC-Web-Dok. 102/3013 (Hinweis auf Produkte des Unternehmens). S. auch LG Aschaffenburg, MMR 2012, 38 ff. (dort Werbung für regionale Kulturangebote und Platzierung kommerzieller Werbung).

[184] Wie hier Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 5 TMG, Rn. 13a; Held, in: Paschke et al., Hamburger Kommentar, 71. Abschnitt, Rn. 31; Pießkalla, ZUM 2014, 368 (370 f.).

dienen, etwa wenn ein Blog nicht nur auf einer werbefinanzierten Plattform betrieben wird, sondern dazu genutzt wird, Anzeigen zu schalten, mit denen ein Gewinn erwirtschaftet wird.[185]

94 Einen **Grenzfall** stellen insoweit Social-Media-Profile zu beruflichen Zwecken dar, z. B. auf der in Deutschland beliebten Plattform **XING**. Diese werden von Privatpersonen dazu genutzt, berufliche Kontakte zu knüpfen und evtl. sogar nach einer neuen Arbeitsstelle zu suchen. Es handelt sich mithin – jedenfalls in der Regel – nicht um Profilseiten von Unternehmen oder solche, die für Unternehmen werben, sondern um Profilseiten Privater, welche diese aber zu beruflich veranlassten Kontaktaufnahmen und Selbstpräsentationen nutzen. Im weiteren Sinne geht es also um geschäftliche Kontaktpflege und die Anbahnung neuer Geschäftsbeziehungen bzw. Arbeitsverhältnisse. Diese Profile haben also die oben angesprochene „wirtschaftliche Relevanz" und fallen deshalb unter die Impressumspflicht des § 5 TMG.[186] XING selbst bietet im Übrigen auch die technische Möglichkeit, ein Impressum zu integrieren.

95 Das **klassische Profil** auf einer Social-Media-Seite, ein privater Blog, der keine Werbegewinne abwirft, oder auch Wissensplattformen sind hingegen nicht von der Impressumspflicht der §§ 5, 6 TMG erfasst. Gleiches gilt auch für die Seiten von Idealvereinen oder sonstigen ehrenamtlichen Organisationen, über deren Telemedium keine entgeltlichen Leistungen vermittelt werden. Dort, wo § 5 TMG anwendbar ist, hat § 55 RStV inhaltlich keine Bedeutung mehr, weil die besondere Impressumspflicht bereits alle Daten voraussetzt, welche nach der rundfunkrechtlichen Impressumspflicht zu leisten sind. § 55 RStV bewirkt dann allein, dass die Zuständigkeit der Landesmedienanstalten als Aufsichtsbehörden eröffnet wird.[187]

96 Wenn ein Social-Media-Anbieter unter § 5 TMG fällt, so stellt ein Verstoß gegen die verpflichtenden Angaben zugleich gegenüber Wettbewerbern einen **Wettbewerbsverstoß** dar, der wettbewerbsrechtliche Unterlassungsansprüche nach sich ziehen kann.[188] Neben diesen Ansprüchen des Wettbewerbsrechts – die nur von Wettbewerbern, nicht aber von Privatpersonen geltend gemacht werden können – verpflichtet ein Verstoß gegen § 5 TMG auch nach § 823 Abs. 2 BGB zum Ersatz des dadurch entstandenen Schadens. Zudem kann der Verstoß auch mit einer Geldbuße geahndet werden, § 16 Abs. 3 TMG.[189] Wettbewerbswidrig verhält sich dabei jedoch nicht nur der Anbieter einer impressumspflichtigen Unterseite, sondern auch

---

[185] Vgl. Brönnecke, in: Roßnagel, Telemediendienste, § 5 TMG, Rn. 43; Ott, MMR 2007, 355; Ott, in: Gersdorf/Paal, Informations- und Medienrecht, § 5 TMG, Rn. 11.

[186] So auch Pießkalla, ZUM 2014, 368 (373) und zuletzt das LG Dortmund (Beschl. v. 06.02.2014 – 5 O 107/14, ITRB 2014, 73).

[187] So der zutreffende Hinweis von Hoeren, NJW 2007, 801 (803). Etwas zu kritisch zum Nebeneinander der beiden Normen Micklitz/Schirmbacher, in: Spindler/Schuster, § 55 RStV, Rn. 14.

[188] BGH, GRUR 2007, 890 ff. Vgl. dazu Lorenz, WRP 2010, 1224 ff. und Held, in: Paschke et al., Hamburger Kommentar, 71. Abschnitt, Rn. 46 mit umfassenden w. N.

[189] Freilich wurden Bußgelder in der Praxis bisher kaum verhängt und sind damit wohl noch nicht zu einem wirksamen Druckmittel geworden (vgl. z. B. die Einschätzung von Ott unter: http://linksandlaw.info/Impressumspflicht-40-aufsichtsbehoerde-bussgeld.html).

ein Portalbetreiber, der in seinen Angebotsmasken o. ä. keine Möglichkeit für ein Impressum vorhält. Der Oberseitenbetreiber hat insoweit eine **Verkehrspflicht** zu erfüllen, wobei ihm das Haftungsprivileg des § 10 TMG für einen entsprechenden wettbewerbsrechtlichen Unterlassungsanspruch nach der Rechtsprechung des BGH nicht zugutekommt.[190]

97 Erwähnt sei schließlich noch, dass das in **§ 13 Abs. 6 TMG** verankerte Recht, Telemedien anonym bzw. unter einem Pseudonym nutzen zu können, weder der allgemeinen noch der besonderen Impressumspflicht entgegensteht. Denn die Impressumspflicht trifft nur den Anbieter eines Telemediums selbst, das – wie gesehen – auch in Unterseiten einer Plattform bestehen kann. In dieser Funktion ist der Seiteninhaber aber nicht Nutzer, sondern allein Anbieter und kann sich gegen die §§ 55 RStV, 5 und 6 TMG nicht mit dem Recht der anonymen Nutzung wehren.[191] Es wäre im Übrigen widersprüchlich, würde dasselbe Gesetz (TMG) in den §§ 5 und 6 spezielle Informationspflichten statuieren, die stets von einer anderen Norm (§ 13 Abs. 6) verhindert würden; das kann der Gesetzgeber ersichtlich nicht beabsichtigt haben.

9.2.3.2 Haftung

98 Die für die Praxis sehr wichtige Frage nach der Haftung des Telemedienanbieters wird im TMG nicht umfassend, sondern ergänzend zu den allgemeinen Vorschriften in den §§ 7–10 TMG geregelt. Siehe zu diesem Bereich den gesonderten Beitrag von *Spindler* (Kap. 5).

9.2.3.3 Datenschutz

99 Das Datenschutzrecht stellt einen der bedeutendsten Bereich des IT-Rechts und somit auch des Rechts der sozialen Medien dar. Weil es im vorliegenden Werk nicht zuletzt deshalb mit einem speziellen Beitrag bedacht ist (vgl. insoweit den Beitrag von *Hornung* [Kap. 4]), sollen in diesem Kapitel nur die einschlägigen speziellen Normen des Rundfunk- und Telemedienrechts genannt werden. Daneben existieren die allgemeinen Datenschutzbestimmungen (BDSG und Datenschutzgesetze der Länder) sowie – je nach Erhebungs- und Verwendungszusammenhang – weitere Regelungen in den jeweils im konkreten Kontext einschlägigen Spezialgesetzen, z. B. des Sicherheitsrechts oder des Sozialrechts.

100 Das Datenschutzrecht der Telemedien findet sich hinsichtlich des Verhältnisses zwischen Anbieter und Nutzer grundsätzlich in den **§§ 11–15a TMG**, die auf Vorgängernormen im MDStV und im Teledienstedatenschutzgesetz (TDDSG) zurückgehen. Für das daneben bestehende Verhältnis der Nutzer oder der Anbieter

---

[190] Vgl. zu dieser Haftung zuletzt OLG Düsseldorf, MMR 2013, 649.

[191] Zutreffend daher Lange, ZJS 2013, 141 (142 f.). Etwas unklar, im Ergebnis aber wohl identisch Stadler, ZD 2011, 57 (58 f.).

von Telemedien zu Dritten gelten die §§ 11 ff. TMG nicht; insoweit ist also bereits das allgemeine Datenschutzrecht angesprochen.[192] Die Regelungen des TMG transportieren dabei allgemeine datenschutzrechtliche Wertungen (z. B. Zweckbindung, Datenvermeidung) in das Telemedienrecht – ganz im Sinne der Forderung des Bundesverfassungsgerichts nach einem bereichsspezifischen Datenschutz.[193]

101 Modifiziert bzw. überlagert werden diese Vorschriften im Rundfunkrecht sodann durch **§ 57 RStV**. Diese Norm erstreckt das sogenannte Medienprivileg auch auf Telemedien, sofern diese als (Hilfs-)Unternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistischen Zwecken nutzen bzw. erheben. Um dem Grundrechtsschutz der Medientätigkeit Rechnung zu tragen, werden damit gewisse Ausnahmen vom sonst geltenden Datenschutz – zum Beispiel den Normen des TMG – gemacht, die bereits bei den klassischen Presse anerkannt und normiert sind.[194] Auch hier soll also die Wahl eines anderen Verbreitungsweges für das Presseerzeugnis nicht zu einem anderen Schutzniveau führen. Ob die Beschränkung auf Presseunternehmen mit Blick auf Blogs, die nach dem oben Gesagten durchaus journalistisch-redaktionell gestaltet sein können, gerechtfertigt ist, kann insoweit aber bezweifelt werden.[195] Im vorliegenden Rahmen kann jedoch auf den Datenschutz nur kursorisch eingegangen werden; hinsichtlich der Einzelheiten zum speziellen Datenschutzrecht der Telemedien sei nochmals auf das 4. Kapitel verwiesen.

9.2.4 Aufsichtsbehörden

102 Wer überwacht nun die rundfunk- und telemedienrechtlichen Verpflichtungen? Die zuständige Behörde wird insoweit **von den Ländern bestimmt**. § 59 Abs. 1 RStV überlässt ihnen dabei die Wahl der Behörde zur Kontrolle der datenschutzrechtlichen Bestimmungen §§ 11 ff. TMG, 57 RStV)[196], § 59 Abs. 2 RStV ermächtigt sie zur Bestimmung der Aufsichtsbehörde für die Regelungen des Rundfunkstaatsvertrages. Mehrheitlich – konkret: in 10 der 16 Bundesländer – haben die Länder hierfür die Landesmedienanstalt bestimmt, mitunter ist aber auch eine Bezirksregierung – bzw. die jeweilige dieser Kategorie entsprechende kommunalrechtliche Entsprechung –,

[192] Vgl. Müller-Broich, TMG, § 11 Rn. 3 f.
[193] S. namentlich BVerfGE 65, 1 (46) – Volkszählung.
[194] S. etwa die §§ 41 f. BDSG.
[195] Kritisch etwa auch Schmittmann, in: Schwartmann, Praxishandbuch, 10. Kapitel, Rn. 110. Für eine weniger formale, strenge Auslegung des Medienprivilegs auch Lauber-Rönsberg, ZD 2014, 177 (181).
[196] Für journalistisch-redaktionell gestaltete Telemedien ist gem. § 59 Abs. 1 S. 2 RStV die Datenschutzaufsicht der öffentlich-rechtlichen Rundfunkanstalten zuständig.

ein Ministerium oder eine spezielle Behörde zuständig[197]; am sachnächsten ist jedoch stets die Landesmedienanstalt.[198] Mit Blick auf das aus der Rundfunkfreiheit folgende Gebot der **Staatsferne** des Rundfunks wird es im Übrigen mitunter sogar für verfassungswidrig gehalten, die Telemedienaufsicht in die Hände von unmittelbarer Staatsverwaltung zu geben, wie dies beispielsweise in Bayern geschehen ist.[199]

103 Für den **Jugendschutz** ist eine spezielle Zuständigkeit in § 20 Abs. 4 JMStV geregelt, wonach die Aufsicht der jeweils zuständigen Landesmedienanstalt obliegt, die insoweit durch die KJM als Organ handelt; § 59 Abs. 2–4 RStV kann hier entsprechend angewandt werden.[200] Örtlich zuständig ist die Behörde in dem Bundesland, in welchem der Anbieter seinen Sitz hat, hilfsweise dort, wo der Anlass für die Behördenhandlung entstanden ist, § 59 Abs. 6 RStV. In einigen Bundesländern ist also die Landesmedienanstalt für alle in diesem Beitrag thematisierten Regelungen mit Ausnahme des Datenschutzes zuständig, in anderen Ländern eine andere Behörde oder die Zuständigkeiten fallen auseinander. Mehrheitlich haben die Bundesländer aber jedenfalls für den Datenschutz gesondert den Landesbeauftragten für den Datenschutz für zuständig erklärt[201]; in keinem Fall ist die Landesmedienanstalt auch für den Datenschutz zuständig.

104 Den Aufsichtsbehörden stehen zunächst die in den jeweils betroffenen Vorschriften normierten **Aufsichtsmaßnahmen** zu. Daneben regelt grundsätzlich § 59 Abs. 3–5 RStV, welche Maßnahmen ergriffen werden können. So können die Aufsichtsbehörden die aus den §§ 49 RStV, 16 TMG folgenden Bußgelder verhängen, Untersagungsverfügungen erlassen und als ultima ratio auch eine Sperrung des Angebots verfügen, § 59 Abs. 4 RStV. Stets sind dabei die §§ 7 ff. TMG zu beachten, die eine solche Maßnahme ausschließen, wenn der (vermeintliche) Anbieter hiernach nicht verantwortlich ist; gegen den Zugangsvermittler kann allein im Rahmen des § 59 Abs. 4 RStV vorgegangen werden, d. h. wenn Maßnahmen gegen den Verantwortlichen nicht durchführbar sind oder keinen Erfolg versprechen. § 59 Abs. 5 RStV geht im Übrigen von der Subsidiarität der staatlichen Aufsicht aus. Sie soll in den Fällen, in denen in Rechte Dritter eingegriffen wird, denen hiergegen der Rechtsweg offen steht, nur dann erfolgen, wenn dies „aus Gründen des Gemeinwohls“ geboten ist – eine reichlich unscharfe Kategorie, zumal zahlreiche der betroffenen

---

[197] Vgl. zu den Behörden i. S. d. § 59 Abs. 1 und 2 RStV die Übersichten bei Schulz, in: Hahn/Vesting, Rundfunkrecht, § 59 RStV, Rn. 38 (für den Datenschutz) und 41 (Behörden nach § 59 Abs. 2 RStV) sowie bei Fiedler, in: Gersdorf/Paal, Informations- und Medienrecht, § 59 RStV, Rn. 2 und 6.

[198] Hartstein et al., RStV, § 59 Rn. 16.

[199] Vgl. Kunisch, MMR 2011, 796 (798 f.) sowie dens., Rundfunk, S. 175 ff. (insb. S. 181 ff.: „Verstoß offensichtlich“).

[200] Vgl. zur Aufsicht im Jugendschutz Schmittmann, in: Schwartmann, Praxishandbuch, 10. Kapitel, Rn. 141 ff.

[201] So in Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein. Eine Ausnahme gilt gem. § 59 Abs. 1 S. 3 RStV nur für Hilfsunternehmen der Presse als Anbieter von journalistisch-redaktionellen Telemedien, die sich dem deutschen Presserat angeschlossen haben.

Vorschriften wettbewerbsrechtliche Relevanz aufweisen und so den Wettbewerbern des Telemedienanbieters entsprechende Klagen ermöglichen.[202]

Allerdings werden Verstöße gegen die §§ 54 (journalistische Grundsätze[203]), 55 Abs. 2 und 3 (Impressumspflicht bei journalistisch-redaktionell gestalteten Telemedien), 56 (Gegendarstellungsanspruch), 57 Abs. 2 RStV und gegen die Datenschutzbestimmungen des TMG von **§ 59 Abs. 3 RStV** explizit von den Maßnahmen ausgenommen. Der Datenschutz und die Vorschriften für journalistisch-redaktionell gestaltete Telemedienangebote fallen also nicht unter das Standard-Aufsichtsinstrumentarium. Der Gesetzgeber hat für diese Bereiche auf eine „Aufsicht" durch **Selbstregulierung** gesetzt, die sich des Deutschen Presserats als „Organ" bedient. Das ist hinsichtlich der Impressumspflicht nach § 55 Abs. 2 RStV etwas inkonsistent, stellt doch der Verstoß gegen diese Vorschrift eine Ordnungswidrigkeit dar.[204] Auch im Bereich des Jugendschutzes wird ein Konzept der sogenannten regulierten Selbstregulierung verfolgt.[205] Für die Aufsichtsbehörden des § 59 Abs. 2 RStV verbleiben also die Vorschriften über die unzulässige Werbung, Verstöße gegen allgemeine Gesetze i. S. d. § 54 Abs. 1 RStV und die Impressumspflicht nach § 55 Abs. 1 RStV. **105**

9.2.5 Anwendbares Recht/Herkunftslandprinzip

Mit Blick auf die zuständigen Aufsichtsbehörden und die dargestellten Regeln des nationalen Rundfunk- und Internetrechts stellt sich zum Abschluss der Vorgaben für Social Media als solche die scheinbar einfache Frage, wann diese Normen überhaupt anwendbar sind. Gelten auch bei im Ausland angesiedelten Social Media die Vorgaben aus RStV und TMG? Das „anwendbare" Recht wird für den Bereich des Telemedienrechts durch **§ 3 TMG** festgelegt. Dieser normiert das sogenannte Herkunftslandprinzip, nach dem – ganz im Sinne der *Cassis*-Rechtsprechung des Europäischen Gerichtshofs (EuGH) – davon ausgegangen wird, dass ein in einem Mitgliedstaat der Europäischen Union (EU) nach dessen Recht zulässiges Angebot auch in den anderen Mitgliedstaat zulässig sein muss.[206] Entsprechend regelt § 3 Abs. 1 TMG, dass in Deutschland niedergelassene Diensteanbieter und ihre Telemedien grundsätzlich auch dann den Anforderungen des deutschen Rechts unterliegen, **106**

---

[202] Kritisch auch Holznagel/Nolden, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 5 Rn. 167.

[203] Nicht aber die in § 54 Abs. 1 RStV in Bezug genommenen allgemeinen Gesetze; insoweit ist im Einklang mit Volkmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 54 RStV, Rn. 39 m. w. N. von einem Redaktionsversehen auszugehen bzw. die Vorschrift nach ihrem Sinn und Zweck – nämlich die Bereiche der presserechtlichen Selbstregulierung auszuklammern – entsprechend auszulegen.

[204] Zutreffender Hinweis bei Hartstein et al., RStV, § 59 Rn. 17.

[205] Vgl. Petersen, Medienrecht, § 16 Rn. 15 f.; Altenhain, in: Hoeren et al., Handbuch Multimedia-Recht, Teil 20 Rn. 147 ff.

[206] Vgl. EuGH, Slg. 1979, 649 (664) – Cassis de Dijon.

wenn die Telemedien in einem anderen Staat im Geltungsbereich der zugrunde liegenden Richtlinie (E-Commerce-Richtlinie) geschäftsmäßig angeboten oder erbracht werden; umgekehrt gilt die Regelung über das jeweilige gleichlautende – da auf der Richtlinie beruhende – nationale Recht auch für andere Mitgliedstaaten, deren Angebote in Deutschland abrufbar sind bzw. abgerufen werden. § 3 Abs. 2 TMG ergänzt diese Regelung um ein Verbot der Beschränkung des freien Dienstleistungsverkehrs von Telemedien. § 3 TMG gilt – sofern die Geschäftsmäßigkeit des Angebots gegeben ist – dabei sowohl für die Vorschriften des TMG als auch für den Rundfunkstaatsvertrag (vgl. §§ 1 Abs. 4 TMG, 60 Abs. 1 RStV). Der hier ebenfalls thematisierte Jugendschutz wird jedoch vom Anwendungsbereich des Herkunftslandprinzips ausgenommen, vgl. § 3 Abs. 5 Nr. 1 TMG.

107 Über die Auslegung dieser Norm bestand lange Streit. Insbesondere war umstritten, ob es sich um eine Kollisionsnorm oder eine Norm des Sachrechts handelt.[207] Nach Vorlage durch den BGH hatte im Jahr 2011 der EuGH Gelegenheit zur Stellungnahme,[208] so dass die Auslegung der Norm in praxi nunmehr festgelegt ist: § 3 TMG enthält **keine Kollisionsnorm** – diese Funktion übernehmen z. B. die Rom-Verordnungen und (für Deutschland) ergänzend das EGBGB –, sondern ein **Beschränkungsverbot**.[209] Dies entspricht auch dem Wortlaut des TMG selbst, das in § 1 Abs. 5 TMG – entsprechend den Vorgaben der Richtlinie – ausdrücklich feststellt, dass dieses Gesetz keine Regelungen des internationalen Privatrechts enthält.[210] § 3 Abs. 1 und 2 TMG verbietet es also, an einen in einem Mitgliedstaat[211] ansässigen Telemedienanbieter in einem anderen Mitgliedstaat andere, insbesondere strengere Anforderungen zu stellen als in seinem Herkunftsland, indem sachlich stets das „Heimatrecht" des Sitzstaates Anwendung findet, wenn es günstiger ist.[212] Dogmatisch überzeugend ist diese Kategorisierung als sachrechtliche Norm freilich nicht. § 3 TMG ist normtechnisch so aufgebaut wie eine klassische Kollisionsnorm und kann als solche auch am besten gedeutet und angewendet werden. Allerdings hat sich für die Praxis durch die Vorlagefrage des BGH der Streit „erledigt", so dass mit der Auslegung des EuGH umgegangen werden muss. Sie stellt in jedem Falle Einklang mit dem Wortlaut der dem TMG zugrunde liegenden Richtlinie her.

108 Was bedeutet das für Social-Media-Anbieter, die ein Angebot in Deutschland zum Abruf bereithalten? In prozessualer Hinsicht sind die deutschen Aufsichtsbehörden i. S. d. § 59 RStV als Medienaufsicht für die Einhaltung der Vorgaben des Rundfunk- und Telemedienrechts in Deutschland zuständig. Soweit dieses Anordnungen für ihr Zuständigkeitsgebiet trifft – also Rechtsfolgen, die in dem jeweiligen

---

[207] S. zu den unterschiedlichen Ergebnissen je nach Verständnis dieser Norm Sack, WRP 2013, 1545 ff.

[208] EuGH, EuZW 2011, 962 ff. S. zu dieser Entscheidung Sack, EWS 2011, 513 ff.

[209] BGH, MMR 2012, 703 (704). Anders noch: Hain, in: MüKo-StGB, § 3 TMG, Rn. 14 mit umfassenden weiteren Nachweisen zu dieser Ansicht. Wie hier aber bereits Pfeiffer et al., in: Spindler/Schuster, § 3 TMG, Rn. 7 und Sack, WRP 2013, 1407 (1409 f.).

[210] So auch der Hinweis von Gitter, in: Roßnagel, Telemediendienste, § 3 TMG, Rn. 23.

[211] Neben den Mitgliedstaaten der EU gilt die Richtlinie auch für Island, Norwegen und die Schweiz.

[212] Vgl. auch Sack, WRP 2013, 1545 (1553).

deutschen Bundesland eintreten –, kann es entsprechende Maßnahmen gegen in Deutschland niedergelassene Anbieter und in den Grenzen des § 3 Abs. 5 TMG auch für im EU-Ausland niedergelassene Anbieter ergreifen. Wenn nun § 3 TMG keine Kollisionsnorm enthält, sondern die Frage des anwendbaren Rechts sich aus anderen Vorschriften ergeben muss, gilt insoweit das **allgemeine Kollisionsrecht**. Für das öffentliche Recht, d. h. das Recht, das öffentliche Aufsichtsbehörden anwenden, heißt das nach ganz herrschender Ansicht, dass deutsche Behörden nur deutsches öffentliches Recht anwenden; hier gilt also das Territorialitätsprinzip.[213] Die von den Behörden i. S. d. § 59 RStV kontrollierten Normen sind also stets und allein die deutschen rundfunkrechtlichen Vorschriften.

109 Welche Regelungen des Privatrechts im konkreten Fall anzuwenden sind, richtet sich nach den **Regelungen des internationalen Privatrechts**, also dem Kollisionsrecht. Für den europäischen Raum sind das insbesondere die Rom-Verordnungen, in Deutschland ergänzt durch das EGBGB. Für die meisten Rechtsverhältnisse im Zusammenhang mit Social Media dürften die Rom I- und die Rom II-Verordnung, welche die vertraglichen und gesetzlichen Schuldverhältnisse regeln, insoweit einschlägig sein. Gelangt man über diese Normen zur Anwendung des deutschen internationalen und materiellen („sachrechtlichen") Privatrechts, gehört zu den Vorschriften für Telemedien auch § 3 TMG als Vorschrift des Sachrechts. Das dort normierte Herkunftslandprinzip stellt für geschäftsmäßige Angebote dann klar, dass bei kollisionsrechtlicher Anwendung des deutschen Rechts dessen Vorgaben nicht strenger sein dürfen als diejenigen des Herkunftslandes (z. B. Irland). Auf diese Weise werden den Kollisionsregelungen inhaltliche Grenzen gesetzt.[214] Insoweit hat die Vorschrift eine gewisse Nähe zu den kollisionsrechtlichen Regelungen über Eingriffsnormen und kann so verstanden werden, dass sie gewissen nationalen Standards zur Durchsetzung verhelfen bzw. als ausreichenden Standard akzeptieren will.[215] Es ist dabei – jedenfalls außerhalb des Wettbewerbsrechts, wenn anderenfalls Wettbewerbsverfälschungen drohen[216] – also ein **Günstigkeitsvergleich** vorzunehmen.[217]

110 Denkbar ist aber auch eine andere Konstellation: Zum einen ist es möglich, dass die Parteien das für sie geltende **(Sach-)Recht wirksam vereinbart** haben, so dass ihre Vereinbarung der Rechtsordnung, die nach der Kollisionsnorm zu beachten wäre,

---

[213] Vgl. Kegel/Schurig, Internationales Privatrecht, S. 1095.

[214] Treffend insoweit bereits Martiny, in: MüKo-BGB, Anh. III zu Art. 9 Rom I-VO, § 3 TMG, Rn. 37.

[215] S. zu dieser Deutung Martiny, in: MüKo-BGB, Anh. III zu Art. 9 Rom I-VO, § 3 TMG, Rn. 34. In diese Richtung auch Weller, in: Gersdorf/Paal, Informations- und Medienrecht, § 3 TMG, Rn. 8.3. Diese Deutung würde auch der sogenannte Alternativentest nach Kahn und Schurig nahe legen, der danach fragt, was die Alternative zur Nichtgeltung der Norm ist. Ist dies – wie hier – die Geltung einer ausländischen sachrechtlichen Norm, so kann die betroffene Regelung (auch) als Eingriffsnorm im formalen Sinne ausgelegt werden. S. dazu ausführlicher Köhler, Eingriffsnormen, S. 10 ff.

[216] Sack, WRP 2013, 1545 (1552).

[217] EuGH, NJW 2012, 137 Rn. 66 ff.

vorgeht.[218] Eine solche Rechtswahl – die sowohl das Sach- als auch das Kollisionsrecht erfassen kann – sieht § 3 Abs. 3 Nr. 1 TMG ausdrücklich vor. Zum anderen ist denkbar, dass der Telemedienanbieter weder in Deutschland noch in einem EU-Mitgliedstaat ansässig ist. Für diese Fälle trifft § 3 TMG keine Aussage.[219] Dann dürfte in den meisten Fällen kollisionsrechtlich das Recht dieses Sitzstaates anwendbar sein, im Falle von Verbraucherverträgen das Recht des Staates, in dem sich der Verbraucher, mit dem der Nutzungsvertrag geschlossen wurde, befindet, vgl. insbesondere Art. 6 Abs. 1 lit. b) Rom I-VO.[220] Es ist also stets eine Einzelfallprüfung für jedes soziale Medium und das konkrete Rechtsverhältnis bzw. der betroffene Einzelaspekt des Sachverhalts erforderlich, bei der nicht nur der Sitzstaat relevant ist, sondern auch die vertraglichen Regelungen in die Betrachtung einzubeziehen sind. Pauschale Aussagen für alle sozialen Medien sind im vorliegenden Rahmen also nicht möglich. Hinzu kommt, dass das internationale Privatrecht nicht für jeden Sachverhalt dieselbe nationale Rechtsordnung vorsieht.

111 Ferner ist zu beachten, dass § 3 TMG selbst zahlreiche Bereiche **aus seinem Anwendungsbereich herausnimmt**: So gilt die Regelung nicht für Angebote, die nicht geschäftsmäßig erbracht werden. Auch bleiben gem. § 3 Abs. 3 Nr. 2 und 4 TMG die Vorschriften für vertragliche Schuldverhältnisse in Bezug auf Verbraucherverträge und das Datenschutzrecht unberührt. § 3 Abs. 4 TMG schließt weitere wichtige Bereich aus, so etwa das Urheberrecht und dem Kartellrecht unterliegende Vereinbarungen (Nrn. 6 und 8). § 3 Abs. 5 TMG macht schließlich noch eine Ausnahme für nationale Vorschriften zum Schutz der öffentlichen Sicherheit und Ordnung (Nr. 1), den Gesundheits- (Nr. 2) sowie dem Verbraucherschutz (Nr. 3). Je nach dem, welches Rechtsverhältnis in welchem Teilaspekt im Rahmen einer Social-Media-Anwendung betroffen ist, greift § 3 TMG möglicherweise gar nicht oder nur in Teilen ein.

112 Die Frage nach dem anwendbaren Recht bzw. dem im **konkreten Fall** geltenden Schutzniveau ist mithin eine diffizile, die keinesfalls pauschal allein nach dem Sitz der Plattform beantwortet werden kann.[221] Entscheidend ist dabei nämlich auch, wer der konkrete Telemedienanbieter ist, dessen Angebot es zu bewerten gilt. Anbieter ist nicht nur der Betreiber der Oberseite bzw. Plattform selbst, sondern u. U. auch einzelne Unterseiteninhaber, etwa eines gewerblichen Facebook-Profils. Dieses wiederum kann durchaus in einem anderen Staat angesiedelt sein als die übergeordnete Internetseite. Auch ist stets relevant, um welche Vorschriften bzw. welche Ansprüche es sich handelt, da nicht alle Rechtsbereiche kollisionsrechtlich gleich behandelt werden. Konkrete Aussagen zur Anwendbarkeit des RStV und des TMG,

---

[218] Die Normen des internationalen Privatrechts sehen in vielen Bereichen dem Grundsatz nach vor, dass die von den Parteien gewählte Rechtsordnung dem Kollisionsrecht vorgeht, vgl. z. B. Art. 3 Rom I-VO; 14 Rom II-VO; 5 der VO (EU) Nr. 1259/2010 („Rom III“); 42 EGBGB.

[219] BT-Drs. 14/6098, S. 17; Sack, WRP 2013, 1407 (1408); Hain, in: MüKo-StGB, § 3 TMG, Rn. 10 m. w. N.

[220] Anders aber im Delikts- und Wettbewerbsrecht, wo die Auslegung des § 3 TMG deshalb besondere Bedeutung erlangt, Pfeiffer et al., in: Spindler/Schuster, § 3 TMG, Rn. 10.

[221] In diese Richtung aber Zysk, ZUM 2012, 22 (26) für den Fall der Plattform „MyVideo“ der ProSiebenSat1-Gruppe, auf welche rumänisches Recht anwendbar ist.

aber auch der anderen rechtlichen Aspekte (wie insb. der Haftungsfragen), auf ein bestimmtes soziales Medium können an dieser Stelle deshalb nicht gemacht werden; in jedem Falle führt das Herkunftslandprinzip dazu, dass zahlreiche nationale Vorgaben leerlaufen.[222]

9.2.6 Bewertung der Regulierung der Social Media in Zeiten konvergenter Medien

Der Blick auf die medien- und internetrechtlichen Aspekte der Social Media hat – ebenso wie die übrigen Kapitel dieses Handbuchs – gezeigt, dass für diese spezielle Erscheinungsform von Internetangeboten eine Vielzahl von **speziellen Regeln** existiert, dass sie aber auch **teilweise gleich behandelt** werden die klassischen Medien bzw. die Entsprechung zur virtuellen Handlung in der realen Welt. Auch auf Social Media kann das „normale" Vertragsrecht des BGB angewandt werden; das Deliktsrecht und die Abwehrrechte bei Persönlichkeitsrechtsverletzungen greifen, genauso wie auch das Straf- und Arbeitsrecht anwendbar bleibt. In vielen Bereichen werden die allgemeinen, technikneutralen Regelungen aber ergänzt, teilweise auch überlagert durch spezielle Normen, die sich nur an Telemedien richten, so z. B. beim speziellen Datenschutz, im Falle besonderer internetspezifischer Straftaten oder der Modifizierung und Ergänzung der zivilrechtlichen Haftungsregeln für Telemedien (§§ 7 ff. TMG). **113**

9.2.6.1 Bewertung des Medienrechts für Telemedien

Was das Medienrecht betrifft, so scheint der Gesetzgeber besonders unentschlossen zu sein, wie er mit Angeboten im Internet umzugehen hat. Hier existieren keine Spezialregeln, die den allgemeinen Vorschriften in toto vorgingen. Auch werden Telemedien gerade nicht in jeder Hinsicht anders behandelt als Presse und Rundfunk. Der Gesetzgeber hat sich zwar bemüht, die Telemedien insbesondere dem Rundfunk gegenüber zu stellen und von ihm abzugrenzen. Genauso wie im Verhältnis zur klassischen Presse – d. h. dem periodischen Printprodukt – vermag er die Trennung der Telemedien vom Fernsehen aber nicht konsequent durchzuhalten. Dem Phänomen der **Medienkonvergenz** wird an den vielen aufgezeigten Stellen dadurch Rechnung getragen, dass die Regelungen für Telemedien denen des Fernsehens bzw. der Presse angeglichen werden, indem Teilbereiche der Rundfunkregulierung und des Presserechts auf die Telemedien erstreckt werden. Im Grundsatz überzeugt diese Handhabung: Dort, wo das Internetangebot in seiner Wirkweise der Presse gleichkommt, muss es sich an deren Gesetzmäßigkeiten halten – also die publizistischen **114**

[222] Holznagel, MMR 2014, 18 (23).

Grundsätze wahren oder auch Gegendarstellungen veröffentlichen. Dort, wo die Anwendung einem Fernsehprogramm ähnelt, kann sich dasselbe Bedürfnis nach einem Zulassungsverfahren ergeben wie beim klassischen Fernsehen.

115 Allerdings wird die Handhabung des Telemedienrechts durch diese **vielfältigen Binnendifferenzierungen** erheblich erschwert. Die neben den Begriff des Telemediums tretenden gesetzlichen Termini (Telemedien mit journalistisch-redaktioneller Gestaltung; Telemedien, die sich an die Allgemeinheit richten) werden in der praktischen Rechtsanwendung darüber hinaus noch ergänzt durch Begriffe wie die „elektronische Presse" oder anders bezeichnet, etwa als „fernsehähnliche Telemedien". Das macht nicht nur den Zugang des Rechtsanwenders zur Medienregulierung schwierig, sondern bringt Rechtsunsicherheit durch schwierige Subsumtionen und ein Nebeneinander verschiedener Regelungen, aber auch Aufsichtsorgane.[223] Dieses Anwendungs- und Vollzugsproblem lässt dann die grundsätzlich sinnvolle Differenzierung der verschiedenen Telemedienangebote in einem anderen Licht erscheinen und bei manchen das Bedürfnis nach einer einheitlichen Medienregulierung mit einer gemeinsamen Behörde aufkommen. Diese Überlegungen[224] durchziehen die Änderungen des Rundfunkrechts und beschäftigen Gesetzgeber[225] wie Wissenschaft seit mehr als zehn Jahren. Sie können im vorliegenden Rahmen freilich nicht in allen Facetten nachvollzogen werden – zum Teil stehen auch schlicht die unterschiedlichen Gesetzgebungskompetenzen einer einheitlichen Regulierung im Wege.

116 Zwei Aspekte der Debatte werden indes auch für die Frage, ob die **Regulierung** der sozialen Medien **de lege lata** sachgerecht ist, relevant: Zum einen steht über allen Bewertungen der Medienregulierung die Frage, ob das dogmatische Verständnis namentlich des Bundesverfassungsgerichts von der Rundfunkfreiheit (noch) seine Berechtigung hat. Zum anderen ergeben sich neue Gefährdungslagen durch marktmächtige Internetanwendungen, die gerade nicht der Regulierung für das Fernsehen unterfallen. Insbesondere Facebook und Google haben sich Marktpositionen erarbeitet, die ein Bedürfnis nach Regulierung, jedenfalls aber nach rechtlichen Regelungen wecken können.

9.2.6.2 Die anachronistische Dogmatik zur Rundfunkfreiheit

117 Die Differenzierung zwischen verschiedenen Angebotskategorien erlangt ihre Brisanz auch durch das Verfassungsrecht in seiner praktischen Handhabung. Denn das Bundesverfassungsgericht versteht – wie bereits erwähnt – die Rundfunkfreiheit nicht als natürliche Freiheit, sondern als „dienende", **normgeprägte Freiheit**, die

---

[223] S. zum alten Recht bereits die Kritik durch Gounalakis, Konvergenz, C 143, dessen Vorschlag nach einem einheitlichen einfachrechtlichen Rundfunkbegriff bei gleichzeitiger Binnendifferenzierung (C 146 f.) letztlich umgesetzt wurde. Ebenso: Schoch, JZ 2002, 798 (805); Holznagel, JZ 2001, 905 (906).

[224] Ausführlicher zu den verschiedenen Ansätzen Jungheim, Medienordnung, S. 591 ff.

[225] S. zum Grünbuch Konvergenz der Medien 2013 auf der Ebene der EU ausführlicher Holznagel, MMR 2014, 18 ff.

auf gesetzliche Ausgestaltung angewiesen ist, um in Anspruch genommen werden zu können.[226] Dieses dogmatische Verständnis begründete das Bundesverfassungsgericht ursprünglich mit der Frequenzknappheit[227], welche die Veranstaltung von Fernsehprogrammen zu einem knappen Gut werden ließ, für das es aufgrund der gesellschaftlichen Relevanz gesetzlicher Regelungen bedarf, bevor eine grundrechtlich geschützte Veranstalterfreiheit anerkannt werden konnte. Als die technische Entwicklung diese Knappheit entfallen ließ, hätte man annehmen können, dass die Berechtigung für die Sonderdogmatik der Rundfunk- gerade im Verhältnis zur Presse- und Meinungsfreiheit entfallen wäre. Das Bundesverfassungsgericht hat jedoch gleichsam die Begründung ausgetauscht und festgestellt, dass trotz der größeren Zahl an zur Verfügung stehenden Frequenzen nach wie vor von der Ausgestaltungsbedürftigkeit der Rundfunkfreiheit auszugehen ist. Diese begründet es nunmehr mit der **Aktualität, Suggestivkraft und Breitenwirkung** des klassischen Fernsehens.[228]

Ob diese Sonderdogmatik im 21. Jahrhundert noch ihre Berechtigung hat, kann **118**
indes bezweifelt werden. So ist zweifelhaft, ob das Fernsehen gerade im Verhältnis zu den Anwendungen des „Web 2.0", zu Social Media und zur elektronischen Presse über ein solches Mehr an Aktualität und **Suggestivkraft** verfügt. Auch erreichen die Hauptanwendungen im Internet wie Facebook, Twitter, Spiegel Online, YouTube und die Google-Dienste ebenfalls eine hohe Zahl an Nutzern. Zudem werden auch auf diesen Seiten bewegte Bilder zur Verfügung gestellt – jedoch nicht in einem „Einheitsprogramm" des Hauptseiteninhabers. Wenn der oben genannte Dreiklang eine grundrechtliche Sonderdogmatik begründen soll, hätte sich das Bundesverfassungsgericht um eine bessere empirische Absicherung seiner Annahmen bemühen können, denn die Austauschung der Begründung erfolgte ohne überzeugende kommunikationswissenschaftliche Fundierung. Die aktuell beliebtesten Internetanwendungen verfügen denn auch über wesentlich mehr Interaktivität, Datenmengen und Inhalte, als dies noch zu Beginn des Jahrhunderts der Fall war. Die Beeinflussung von Wahlkämpfen durch schnell lancierte Internetmeldungen, die Aktivierung von Massenbewegungen über Plattformen wie Facebook – sei es als Hochwasserhilfe im Rahmen von Flutkatastrophen oder bei politischen Umbrüchen im arabischen Raum – und das Bekanntwerden von Künstlern allein durch YouTube-Clips zeigen, dass den Angeboten im Internet ebenfalls ein hohes Maß an Suggestivkraft und Breitenwirkung zukommen kann. Was die **Aktualität** betrifft, dürften viele Angebote gar reaktionsschneller sein als das Fernsehen. Das macht die herkömmliche Rundfunkdogmatik zweifelhaft und zwingt zu einem Umdenken für die Zukunft.[229]

---

[226] BVerfGE 57, 295 (320 f.); 73, 118 (152 f.); 74, 297 (324); 90, 60 (88).

[227] Vgl. BVerfGE 31, 314 (326).

[228] BVerfGE 90, 60 (87); 119, 181 (215). Bereits in BVerfGE 57, 295 (322 ff.) wird angedeutet, dass der Wegfall der Frequenzknappheit an der besonderen Funktion des Rundfunks nichts ändere. Die aktuelle Rechtsprechung stellt also keine überraschende Wendung dar; ihr Boden war in früheren Judikaten bereits vor Auftreten des Internets bereitet worden.

[229] A.A. Dörr, K&R 2013, Beihefter 2/2013 zu Heft 5, S. 9 (11). Wie hier in der Tendenz – namentlich bezogen auf die Rundfunkregulierung – aber Kühling, in: Gersdorf/Paal, Informations- und Medienrecht, Art. 5 GG, Rn. 94 ff.

119 Die Rundfunkfreiheit als dienende, normgeprägte Freiheit sollte vor diesem Hintergrund in der herkömmlichen Dogmatik möglicherweise aufgegeben werden[230] und durch eine Interpretation der Medienfreiheiten ersetzt werden, die überzeugend vorherrschende Meinungsmacht im Rundfunk verhindert und trotzdem in diesem Bereich freiheitliche Betätigung nicht für den einen Übertragungsweg – das klassische Fernsehen – nur sehr restriktiv zulässt und für den anderen Übertragungsweg – das Internet – nur sehr wenige inhaltliche und formelle Vorgaben bereithält. Vielmehr ist hier eine Annäherung entweder der Rundfunk- an die Pressefreiheit nötig oder eine andere Bewertung des Internets im Rahmen der Rundfunkfreiheit. Eine solche **Umorientierung** muss allerdings nicht zwangsweise dazu führen, dass auch im einfachen Recht für Presse, Fernsehen und Internet dieselben Regeln gelten müssen. Bei einer besonderen Wirkungsweise des Fernsehens – oder auch gewisser Internetanwendungen – sind durchaus für einzelne Bereiche gesonderte Regulierungsformen denkbar und zulässig.[231] Entscheidendes Kriterium ist dabei die Vielfalt als Vorsorge gegen vorherrschende Meinungsmacht.[232] Das **Vielfaltsgebot** könnte dabei aber durchaus auch aus Art. 5 Abs. 1 S. 1 GG i. V. m. Art. 5 Abs. 1 S. GG hergeleitet werden, d. h. nicht auf den Rundfunk beschränkt bleiben.[233]

120 Reformbedürftig ist insoweit insbesondere das **Medienkonzentrationsrecht**. Dieses verfolgt nach wie vor in den §§ 25 ff. RStV einen fernsehzentrierten Ansatz. Entscheidend für das Eingreifen der Medienaufsicht bleiben im Wesentlichen die Zuschaueranteile im Fernsehen. Zwar werden auch die sogenannten medienrelevanten verwandten Märkte (Presse, Internetanwendungen) in die Betrachtung und Berechnung nach § 26 RStV einbezogen. Wie die Marktanteile im Internet aber in Zuschaueranteile umzurechnen sind, wenn auf dem verwandten Markt keine marktbeherrschende Stellung besteht, bleibt nach wie vor unsicher.[234] Bedauerlicherweise schweigt der Gesetzgeber zu dieser für die Medienvielfalt so wichtigen Frage und spricht in § 26 Abs. 2 S. 2 RStV von dem Fall, dass der Fernsehveranstalter über einen Zuschaueranteil von 25 % verfügt und „eine Gesamtbeurteilung seiner Aktivitäten im Fernsehen und auf medienrelevanten verwandten Märkten ergibt, dass der dadurch erzielte Meinungseinfluss dem eines Unternehmens mit einem Zuschaueranteil von 30 vom Hundert im Fernsehen entspricht“.

---

[230] Als scharfer Kritiker hat sich insbesondere Hain hervorgetan, vgl. dens., Rundfunkfreiheit, S. 31 ff.; K&R 2006, 325 (330 f.); JZ 2008, 128 (129 ff.); K&R 2012, 98 (102); K&R 2012, 313 (316 ff.) sowie dens., in: Stern et al., Neue Mediendienste, S. 7 (28 f.). In diese Richtung z. B. auch Schoch, JZ 2002, 798 (805); Bullinger, ZUM 2007, 337 (343); ders., JZ 2006, 1137 (1140 f.); Gersdorf, Legitimation, S. 55 ff.

[231] Ebenso Holznagel et al., Elektronische Medien, S. 471 f.

[232] Insoweit zutreffend Sporn, K&R 2013, Beihefter 2/2013 zu Heft 5, S. 1 (7).

[233] So der Vorschlag von Jungheim, Medienordnung, S. 156 ff., insb. S. 161 unter Verweis auf Lehrke, Pluralismus, S. 167 ff.

[234] Es wird im Übrigen auch teilweise bestritten, dass Internetanwendungen in diesem Sinne überhaupt einen verwandten Markt darstellen, vgl. Holznagel/Grünwald, in: Spindler/Schuster, Recht der elektronischen Medien, § 26 RStV, Rn. 16. S. zur Berechnungsweise durch die KEK Gounalakis/Zagouras, Medienkonzentrationsrecht, S. 146 f. und 149 f.

Auch wenn der Gesetzgeber der Meinung sein sollte, dass die bewegten Bilder des Fernsehens nach wie vor eine spezielle Dogmatik und Regulierung rechtfertigen, sollte die Meinungsmacht und **Breitenwirkung des Internets** – die von der KEK freilich bisher nur mit 28 % veranschlagt wird[235] – nicht zuletzt im Medienkonzentrationsrecht besser berücksichtigt werden.[236] Angesichts der Bedeutung für die Gesellschaft, die öffentliche Meinungsbildung und die Informationskultur wäre eine parlamentsgesetzliche Festlegung für die Behandlung der Internet-„Zuschauer" wünschenswert. Auch könnte die „Ergänzung" von 25 % Zuschaueranteil im Fernsehen durch „5 %" äquivalenten Einfluss im Internet etwas niedrig gegriffen sein. Ob die verschiedenen Reformvorschläge[237] in nächster Zukunft zu einer Umgestaltung der §§ 25 ff. RStV, insbesondere des § 26 RStV führen werden, darf jedoch momentan noch bezweifelt werden. **121**

Eine entscheidende Hürde für solche Reformpläne besteht bereits in der einfachrechtlichen **Definition des Rundfunks**. Weil diese – wie gesehen – alle nichtlinearen („Pull"-) Dienste ausschließt, lineare („Push"-) Dienste aber stets erfasst, setzt die Rundfunkregulierung grundsätzlich nicht bei der Frage nach der Meinungsrelevanz an, sondern an dieser formellen Unterscheidung. Das macht es schwer, den Vorgaben der Rundfunkfreiheit – die vorherrschende Meinungsmacht verhindern soll – widerspruchsfrei im Rahmen des einfachen Rechts zu genügen.[238] **122**

9.2.6.3 Interoperabilität und Zugang zu sozialen Netzwerken

Neben dem allgemeinen dogmatischen Verständnis der Rundfunkfreiheit und einer gebotenen Reform des Medienkonzentrationsrechts sind durch erfolgreiche Internetanwendungen aber auch neue rechtliche Fragen und regelungsbedürftige Sachverhalte aufgetaucht. Insbesondere Facebook und Google haben sich auf dem Markt eine so starke, **marktmächtige Stellung** in ihrem Segment erarbeitet, die sie nicht nur als sehr erfolgreiches Geschäftsmodell vermarkten können, sondern die es ihren Konkurrenten bisweilen unmöglich macht, überhaupt mit einem alternativen Angebot Nutzer zu gewinnen. Für Social Media ist hier insbesondere die überragende Stellung der Netzwerkplattform **Facebook** angesprochen, die momentan praktisch alle anderen Angebote in diesem Bereich ver- bzw. jedenfalls zurückgedrängt hat. Genauso, wie die Monopolstellung der Suchmaschine Google medienkartellrechtlich **123**

---

[235] Vgl. KEK 293-1 bis 5, S. 95.

[236] Kritisch z. B. auch Schmid/Kitz, ZUM 2009, 739 (741 f.).

[237] S. zuletzt die vorsichtigen Vorschläge durch Hinrichsen, Konzentration, S. 283 ff., der im Kern jedoch an dem gegenwärtigen Modell festhalten möchte, sowie der Vorschlag von Bloch, Meinungsvielfalt, S. 285 ff. Ausführlicher zu den verschiedenen Reformvorschlägen Bloch, a. a. O., S. 245 ff. und Gounalakis, Konvergenz, S. 293 ff.

[238] Sehr kritisch insoweit Kempermann, Content-Regulierung, S. 204 ff., welcher der gegenwärtigen Ausgestaltung der Rundfunkregulierung gar Verfassungswidrigkeit unterstellt.

problematische Regulierungsbedürfnisse wecken kann[239], besteht aus Sicht konkurrierender Angebote eine Situation, in der es für andere Anbieter schwer ist, Nutzer für eine neue Plattform zu gewinnen. Denn Facebook vereint so viele Nutzer, die untereinander vernetzt sind, dass es für den Einzelnen aktuell oft keine interessante Alternative darstellt, zu einer anderen Plattform zu wechseln. Auf dieser würden sich zunächst nämlich kaum Inhalte oder Vernetzungsmöglichkeiten mit neuen „Freunden" finden. Ohne entsprechende Finanzkraft zur Überbrückung einer Phase anfänglicher Verluste ist eine neue, professionell gestaltete und leicht zu bedienende Plattform daher kaum zu etablieren. Und selbst mit einem entsprechenden finanziellen Hintergrund – das zeigt der Dienst Google+ – werden neue Plattformen nicht so gut angenommen, dass sie zur Generierung größerer Werbeeinnahmen genutzt werden können.

124 In dieser Situation liegt zum einen eine wettbewerbsrechtliche Problematik begründet, geht es doch um die überragende Marktmacht auf einem (vermeintlichen) Markt. Zum anderen führt ein solches Monopol aber auch dazu, dass Internetnutzer sich in Bezug auf die soziale Vernetzung nur noch eines Angebots bedienen können, um Informationen zu erhalten, Meinungen auszutauschen und sich mit anderen Personen zu vernetzen. Dieser Aspekt tritt neben die rein kartellrechtliche Dimension und betrifft die Vielfalt der Meinungen, Informationen und Kommunikationsformen im Internet als einem entscheidenden Freiheitsraum unserer Zeit. Das nach herrschender Ansicht aus der objektiven Funktion der Rundfunkfreiheit abzuleitende Vielfaltsgebot – bzw., negativ formuliert: das Verbot vorherrschender Meinungsmacht – kann es hier gebieten, diesen „**Kommunikationsmonopolen**" vorzubeugen bzw. sie aufzubrechen.

125 Eine wirksame Lösung kann aber nicht in der bloßen Zulassung konkurrierender Netzwerkplattformen bestehen. Denn diese sind ohnehin zulassungsfrei (§§ 54 Abs. 1 S. 1 RStV, 4 TMG) und in der Einrichtung keinen größeren Hürden ausgesetzt – außer dem finanziellen Risiko. Es könnte demgegenüber an **medienrechtliche Regulierungsoptionen** gedacht werden, die einen Wechsel der bei Facebook und ähnlichen, entsprechend marktmächtigen Netzwerken der Zukunft angemeldeten Nutzer zu einem anderen Dienst möglich machen. Diese Situation ist aus dem Medienbereich in zweierlei Hinsicht bekannt: nämlich zum einen aus dem Bereich der Telekommunikation, bei der gewährleistet sein muss, dass auch zwischen verschiedenen Anbietern und in fremden Netzen telefoniert werden kann, und zum anderen aus dem Bereich der Plattformen beim Zugang zu Fernsehprogrammen.[240] An diesen Bereichen könnte man sich orientieren, um marktmächtige soziale Netzwerke dazu zu zwingen, einen einfachen technischen Zugang zu Konkurrenzangeboten zu ermöglichen.

126 *Moini* hat zuletzt in insoweit den telekommunikationsrechtlichen Aspekt der **Interoperabilität** ins Spiel gebracht und an eine Lösung gedacht, die sich an den

---

[239] S. zu dieser im vorliegenden Kontext nicht einschlägigen Thematik insb. Paal, Suchmaschinen, 2012.

[240] S. zu Letzteren in terminologischer Abgrenzung bereits oben Rn. 30 ff.

Netzzugangsregeln des Telekommunikationsrechts (§§ 16, 21 TKG) orientiert.[241] Diese interessante Lösung würde die Netzwerkanbieter dazu zwingen, über Buttons, Verlinkungen oder sonstige technische Kanäle den Zugang zu anderen Netzwerken zu eröffnen, ohne dass erhebliche Zugangserschwernisse bestehen. Ein anderer rechtlicher Ansatzpunkt wäre es, die **Plattformregulierung des RStV** (§§ 52 ff. RStV), unter welche – wie gesehen[242] – die untechnisch als Plattformen bezeichneten Netzwerkseiten gerade nicht fallen, auf selbige zu erweitern. Dieser Ansatz wurde beispielsweise für den Zugang zu Smartphone-Oberflächen[243] oder die Öffnung marktmächtiger Suchmaschinen[244] bereits angedacht und könnte auch eine Option zur Zugangsverpflichtung gegenüber marktmächtigen Social Media in inhaltlicher Hinsicht werden. Diese Ideen zur Übertragung technischer Zugangsregelungen auf inhaltliche Zugangserschwerungen stellen momentan noch bloße rechtspolitische Postulate dar. Um dem Vielfaltsgebot gerecht zu werden und der Meinungsmacht des Internets nicht nur Rechnung zu tragen, sondern für erschwernisfreie Kommunikation auch in diesem Bereich zu sorgen, bieten sie indes interessante Regulierungsoptionen einer zukünftigen Medienordnung. Nach Einführung solcher Regelungen für diese „infrastrukturähnliche[n] Einrichtungen“[245] wäre auch die momentan bestehende und vorliegend bereits kritisierte Asymmetrie zwischen einem stark regulierten Fernsehen und den kaum regulierten Telemedien verringert.

9.3 Das Engagement der öffentlich-rechtlichen Rundfunkanstalten in Social Media

Neben den weiten Bereich der bisher betrachteten Vorschriften für Social Media als **127**
solche tritt ein weiterer Aspekt sozialer Medien, der seit ungefähr einer Dekade praktisch und rechtlich relevant wurde: das Online-Engagement der öffentlich-rechtlichen Rundfunkanstalten. Sie haben sich die Medienkonvergenz zunutze gemacht und versuchen, ein zeitgemäßes Programm und eine zeitgemäße Vermarktung durch Online-Angebote zu erreichen, mit denen sie ihr Fernsehprogramm ergänzen oder „vermarkten“. Diese Ausweitung der Fernsehaktivitäten auf das Internet hat von Anfang an Fragen aufgeworfen: Dürfen die Rundfunkanstalten im Netz mehr als im Fernsehen? Schließlich stellen die online vorgehaltenen Angebote keinen Rundfunk im einfachgesetzlichen Sinne dar. Darf das Online-Engagement durch die Rundfunkgebühren bzw. (nunmehr) den Rundfunkbeitrag finanziert werden? Wird es von der Bestands- und Entwicklungsgarantie erfasst? Diese verfassungsrechtlichen,

[241] Moini, „Facebook regulieren“, FAZ v. 08.02.2013, S. 7.
[242] S. oben, Rn. 33 ff.
[243] Vgl. den Vorschlag einer Ergänzung der Plattformdefinition in § 2 Abs. 2 Nr. 13 RStV um einen „elektronischen Portalanbieter in marktbeherrschender Stellung“ von Koenig, MMR 2013, 137 f.
[244] So der Gedanke von Paal, Suchmaschinen, S. 75.
[245] Paal, GRUR 2012, 873 (880).

aber auch rechtspolitischen Fragen wurden jahrelang kontrovers diskutiert.[246] Sie haben schließlich auf europäischer Ebene zum sogenannten „**Beihilfekompromiss**“[247] geführt, der sodann die danach erfolgte einfachgesetzliche Ausgestaltung beeinflusst hat.[248] Seit dem 1. Juni 2009 finden sich seitdem im Rundfunkstaatsvertrag Regelungen dazu, was die öffentlich-rechtlichen Rundfunkanstalten im Internet anbieten dürfen.

9.3.1 Social-Media-Angebote der Rundfunkveranstalter in der Praxis

128 Die öffentlich-rechtlichen Rundfunkanstalten nutzen zunehmend Social Media dazu, Bindungen zu ihren Sendungen herzustellen, indem sie eine „Fankultur“ pflegen. Zudem werden soziale Medien dazu eingesetzt, dass sich Zuschauer über Kommentare, Anfragen oder eigene Twitter-Meldungen an den Sendungen beteiligen und Rückmeldungen zum Programm geben können. Häufig werden in den Sendungen – zumal in den zahlreichen politischen Talkshows – solche Reaktionen oder auch Fragen in das laufende Programm eingebracht und stellen auf diese Weise Interaktivität dar, die es im klassischen Fernsehen außerhalb von Telefonanrufen im Live-Programm bisher nicht gegeben hat – und die dem klassischen Fernsehen im Übrigen auch seine Eigenschaft als Rundfunk im einfachgesetzlichen Sinne nehmen würde. Gerade deshalb können die **Online-Aktivitäten** nur ein **Annex**, eine Ergänzung zum Fernsehen darstellen, um die Regulierung dieses Mediums durch die strengen Vorgaben des RStV nicht zu unterlaufen.

129 ARD und ZDF unterhalten insoweit einige Angebote über Facebook und Twitter[249], verfügen über eigene YouTube-Kanäle[250] und bieten Foren und Chats zu einzelnen Programmformaten an, teilweise in der Form von Blogs.[251] Zumeist dienen die Angebote dazu, dass Zuschauer Sendungen auf Pinnwänden, in Foren oder Blogs **kommentieren** oder über sie mit anderen Zuschauern diskutieren können. Zudem finden sich entsprechende „**Fansites**“ für einzelne Sendungen – namentlich über Facebook –, auf denen sich auch Links mit kurzen Beschreibungen finden oder auf die Mediathek, um die online verfügbaren Sendungen abzurufen. Sowohl ARD

---

[246] S. zur Diskussion vor dem 12. RÄndStV statt vieler die umfassende Untersuchung von Held, Online-Angebote, 2008.

[247] Ausführlicher zum Beihilfekompromiss Neuhoff, Rechtsprobleme, S. 47 ff.

[248] Der deutsche Gesetzgeber ging jedoch sogar über die Anforderungen des Unionsrechts hinaus, etwa bei der der Festlegung zeitlicher Grenzen für die zum Abruf vorgehaltenen Telemedien, vgl. Neuhoff, Rechtsprobleme, S. 83 f.

[249] Siehe für die ARD die Zusammenfassung ihres Social-Media-Engagements unter: http://www.daserste.de/community/diskutieren/foren/social-media/index.html. Allgemein zu den Online-Angeboten der Rundfunkveranstalter Amlung/Fisch, ZUM 2009, 442 (443 ff.).

[250] S. unter www.youtube.com/user/ard sowie unter www.youtube.com/user/zdf. Entsprechende Kanäle existieren für einige der „Dritten“ Programme.

[251] So etwa für die Sendung „Anne Will“, s. unter http://annewill.blog.ndr.de/.

als auch ZDF bieten daneben auch sogenannte **Apps** an, mit denen Nachrichten über Smartphones abgerufen werden können. Diese sehr umstrittene Konkurrenz für die klassische Presse und die Nachrichtenseiten im Internet[252] ist jedoch nicht als soziales Medium zu qualifizieren, weil hier keine Interaktion und Vernetzung mit anderen Internetnutzern gegeben ist. Deshalb sei dieser Problemkreis – ebenso wie die Mediatheken – im vorliegenden Kontext ausgeklammert. Im Rahmen dieser Untersuchung werden allein die „Mitmach-Angebote" über die erwähnten Kanäle relevant.

9.3.2 Die Beschränkungen des RStV für Online-Betätigungen

Die langen Diskussionen um die Frage, ob sich die öffentlich-rechtlichen Rundfunkanstalten überhaupt im Internet betätigen dürfen und wenn ja, welchen Beschränkungen sie dabei unterliegen (dürfen), haben inzwischen zu einem eigenen Abschnitt im **Rundfunkstaatsvertrag** geführt. Dieser hat zwar die vor seiner Schaffung artikulierten verfassungsrechtlichen Zweifel nicht völlig beseitigen können.[253] Nicht zuletzt auf dem Boden der – hier freilich kritisch betrachteten – herrschenden Dogmatik der Rundfunkfreiheit kommt dem Gesetzgeber bei der Ausgestaltung der Rundfunkordnung und des Programmauftrags der öffentlich-rechtlichen Rundfunkanstalten aber ein erheblicher Gestaltungsspielraum zu. Wenn aber Internetanwendungen als solche im Zweifel Rundfunk im Sinne der Verfassung darstellen[254], begegnet die grundsätzliche Öffnung des öffentlich-rechtlichen Fernsehens jedenfalls für **sendungsbezogene Telemedien** keinen durchgreifenden Bedenken. Die neu etablierten Regelungen setzen zudem für das Online-Engagement enge inhaltliche, zeitliche und formale Grenzen. Keinesfalls ist also den öffentlich-rechtlichen Rundfunkanstalten im Netz alles erlaubt, was sie im klassischen Fernsehen nicht dürfen. Wenn man die Entwicklungsgarantie des öffentlich-rechtlichen Rundfunks auch auf neue Übertragungswege und neue „Annexangebote" zum Fernsehen erstreckt,[255] dürfte der Gesetzgeber mit der Neufassung des RStV durch den 12. RÄndStV seinen weiten Gestaltungsspielraum nicht überschritten haben,[256] zumal die Mehrzahl der zulässigen Angebote Programmbezug aufweisen muss. **130**

---

[252] Siehe zum Streit um die Tagesschau-App das Urteil des LG Köln v. 27.09.2012 – 31 O 360/11 (zu diesem Hain, WRP 2012, 1495 ff.) sowie das zum selben Ergebnis gelangende Urteil des OLG Köln v. 20.12.2013 – 6 U 188/12, das jedoch das Urteil des LG Köln aufhob. Zu letztgenanntem Urteil s. Wierny, ZUM 2014, 196 ff.

[253] Nach wie vor zweifelnd etwa Degenhart, in: FS Stern, S. 1299 (1313 ff.).

[254] S. dazu oben Rn. 5 ff.

[255] Kritisch insoweit aber z. B. Ladeur, ZUM 2009, 906 (909).

[256] Wie hier mit Blick auf die damaligen Entwürfe bereits Müller-Terpitz, AfP 2008, 335 (341); a. A. aber Neuhoff, Rechtsprobleme, S. 183 ff. (S. 200), der in die andere Richtung Bedenken anmeldet: Es würden zu enge Vorgaben gemacht, die öffentlich-rechtlichen Rundfunkanstalten mithin zu sehr belastet. Diese Sichtweise überdehnt jedoch die Bestands- und Entwicklungsgarantie

9.3.2.1 Die Voraussetzungen für zulässige Onlineangebote

131 Was aber ist nun nach der einfachgesetzlichen Ausgestaltung mit Blick auf Social Media zulässig? **§ 11d Abs. 1 RStV** stellt zunächst fest, dass die öffentlich-rechtlichen Anstalten auch Telemedien anbieten können, die journalistisch-redaktionell veranlasst und journalistisch-redaktionell gestaltet sind. Sie gehören also zum **Funktionsauftrag** des öffentlich-rechtlichen Rundfunks und sind damit generell zulässig. Die dann folgenden Absätze präzisieren, welche Voraussetzungen ein solches Angebot erfüllen muss bzw. unter welchen Voraussetzungen es zum Programmauftrag gehört. Hierzu werden verschiedene Kategorien von Telemedien gebildet: § 11d Abs. 2 S. 1 Nr. 1 und 2 RStV regelt dabei den zeitlich gebundenen Abruf von Sendungen im Internet (Nr. 1) und den zeitlich gebundenen Abruf von Telemedien, „soweit auf für die jeweilige Sendung genutzte Materialien und Quellen zurückgegriffen wird und diese Telemedien thematisch und inhaltlich die Sendung unterstützend vertiefen und begleiten, ohne jedoch bereits ein eigenständiges Telemedienangebot nach § 11f Abs. 3 darzustellen“ (sendungsbezogene Telemedien, Nr. 2).

132 Die beiden anderen Kategorien betreffen zum einen sendungsbezogene Telemedien nach den Nummern 1 und 2, nachdem die Frist abgelaufen ist (Nr. 3 Alt. 1), Archive mit zeit- und kulturgeschichtlichen Inhalten (Nr. 4) sowie nichtsendungsbezogene Telemedien (Nr. 3 Alt. 2). Alle diese Angebote nach den Nummern 3 und 4 müssen jedoch den an den Vorgaben des Unionsrechts orientierten „**Dreistufentest**“ nach § 11f. RStV bestehen, um zulässig zu sein. Hiernach muss auf der ersten Stufe nachgewiesen werden, dass das Telemedienangebot demokratischen, sozialen und kulturellen Bedürfnissen entspricht; danach ist auf der zweiten Stufe zu fragen, ob es qualitativ zum publizistischen Wettbewerb beiträgt, bevor auf der dritten Stufe der Aufwand für die Erbringung des Angebots zu untersuchen ist. So sehr dieses Verfahren auch ehrenwerten materiellen Kriterien folgt, so sehr wird es doch in prozeduraler Hinsicht **kritisiert**. So wird beispielsweise angemerkt, dass die Rundfunkräte mit einer solch schwierigen kommunikationswissenschaftlichen und wettbewerbsrechtlichen Entscheidung überfordert seien bzw. als selbstregulatives Organ des öffentlich-rechtlichen Rundfunks nicht die richtige (unabhängige) Adresse für diese Entscheidung seien.[257] Auch mangelnde Transparenz der einbezogenen Gutachter und ihrer Überprüfungsmaßstäbe wird gerügt.[258] Diese Kritik kann hier nicht in vollem Umfang nachvollzogen werden. Es ist aber jedenfalls kein

und fördert eine beitragsfinanzierte Konkurrenz für private Anbieter journalistischer Telemedien im Internet. Weniger streng ders., ZUM 2012, 371 (381 ff.). In eine ähnliche Richtung aber auch das bekannte Gutachten von Papier/Schröder, das sogar eine Pflicht zur Erstreckung des Grundversorgungsauftrags auf das Internet annimmt (Papier/Schröder, Verfassungsfragen, S. 82 ff. [S. 96]).

[257] Ladeur, ZUM 2009, 906 (911 ff.) mit Hinweis darauf, dass in Großbritannien die Medienaufsichtsbehörde für den dortigen Public-Value-Test zuständig sei. In diese Richtung auch Gersdorf, Legitimation, S. 113 f.

[258] Vgl. Klickermann, MMR 2009, 740 (743 f.).

absolutes Zeichen für die Unbedenklichkeit der öffentlich-rechtlichen Telemedienangebote, dass sie bisher alle von den Rundfunkräten für zulässig gehalten wurden; ob das gegenwärtige Verfahren möglichen zukünftigen Expansionstendenzen der öffentlich-rechtlichen Anstalten im Online-Bereich wirksam Schranken setzen kann, bleibt abzuwarten.[259]

Unzulässig sind im Rahmen der sonstigen Telemedien „**presseähnliche Angebote**“, § 11d Abs. 2 S. 1 Nr. 3 Hs. 2 RStV. Dieser Ausschlussgrund stellt das umstrittenste Element der Zentralnorm für die Online-Aktivitäten dar. Nachdem der Begriff der presseähnlichen Angebote Vorschläge verdrängt hat, wonach „elektronische Presse“ ausgeschlossen sein sollte, streitet man nach wie vor darum, wann diese Ähnlichkeit gegeben ist. Während eine Extremposition hiervon letztlich nur bei Substituten für klassische Presseerzeugnisse ausgeht, also beim sogenannten E-Paper[260], fasst die herrschende Ansicht diesen Begriff zu Recht weiter. Denn es soll verhindert werden, dass die Rundfunkanstalten sich im Netz zu weit von ihrem Fernsehprogramm entfernen und die Rolle der (nicht durch Rundfunkbeiträge finanzierten) Presse übernehmen. Wenn sie also ein Angebot bereithalten, das als redaktionell gestaltetes Lesemedium bezeichnet werden muss, d. h. bei dem die bewegten Bilder und der Programmbezug zulasten eines bebilderten Textes, reinen Textes oder einer durch einer gestalteten Bilderseite völlig zurücktreten, handelt es sich um ein solches presseähnliches Telemedium.[261] **133**

Eine allgemein anerkannte und in ihrer Anwendung sichere Definition ist trotz der Begriffsbestimmung in § 2 Nr. 20 RStV, welche auf die Ähnlichkeit zu Zeitungen und Zeitschriften „nach Gestaltung und Inhalt“ abstellt, insoweit noch nicht gefunden. Social Media fallen jedoch in ihren gängigen und aktuell zu beobachtenden Erscheinungsformen nicht unter dieses Verbot. Denn sie sind durch die Möglichkeit der Interaktion unter den Nutzern des Angebots sowie durch die Mitgestaltung des Telemediums durch seine Rezipienten geprägt („**Multimedialität**“[262]). Diese Aspekte sind bei klassischen Presseangeboten nicht gegeben. Als Lesemedien sind sie vielmehr durch ihre Statik geprägt. **Social Media** sind vor diesem Hintergrund **134**

[259] Sehr kritisch Degenhart, in: FS Stern, S. 1299 (1315).

[260] Pate für diese Ansicht steht namentlich das bereits erwähnte Gutachten von Papier und Schröder (Verfassungsfragen, S. 93 f.).

[261] Auf den Charakter als Lesemedium abstellend z. B. Gersdorf, Legitimation, S. 106; ders., AfP 2010, 421 (432). Für eine Orientierung an den formalen Merkmalen von Zeitungen und Zeitschriften („Überschriften, Unterüberschriften, Kopfzeilen, spaltige Darstellung“) Schulz, in: Hahn/Vesting, Rundfunkrecht, § 2 RStV, Rn. 170 und wohl auch Hain, Einschränkungen, S. 109 und Neuhoff, Rechtsprobleme, S. 176. Monographisch zum Ganzen Wellenreuther, Presseähnliche Telemedien, 2011.

[262] Peters, Online-Angebote, S. 125.

nicht „presseähnlich“, so dass diese Ausnahme vom Onlineauftrag für sie nicht eingreift. Im Gegensatz z. B. zu Schweden[263] – ebenso aber wie in Österreich[264] – ist in Deutschland also ein Engagement der öffentlich-rechtlichen Rundfunkanstalten in sozialen Medien nicht per se ausgeschlossen.

135 **Social-Media-Angebote mit Sendungsbezug** sind demnach grundsätzlich zulässig. Die gängigen Sendungsbegleitungen durch Foren, Kommentarfunktionen und Hinweisseiten im Social Web sind – ebenso wie Foren und Chats unter Programm- oder Sendermarken – deshalb mit den §§ 11d ff. RStV vereinbar. Allerdings müssen alle diese Angebote journalistisch-redaktionell gestaltet bzw. begleitet sein. Unmoderierte Foren und reine „Mitmach“-Angebote ohne eine solche Begleitung sind nicht zulässig. Eine Social-Media-Plattform wie z. B. Facebook wäre deshalb in ihrer klassischen Funktionsweise als Telemedium des öffentlich-rechtlichen Rundfunks nicht zulässig.[265] Unter zusätzlicher Beachtung des Negativkatalogs nach § 11d Abs. 5 S. 4 RStV scheiden damit außerhalb der redaktionell begleiteten interaktiven sendungsbezogenen Angebote mögliche weitere interessante Social-Media-Konzepte aus.

136 Sehr umstritten bleibt ferner, ob die öffentlich-rechtlichen Rundfunkanstalten theoretisch auch **nicht sendungsbezogene Angebote** auf Plattformen Dritter zum Abruf bereithalten dürfen, etwa speziell für YouTube hergestellte Clips. Diese Angebote werden bisweilen unter § 11d Abs. 4 RStV gefasst, wonach die öffentlich-rechtlichen Anstalten „ihre Angebote in elektronischen Portalen“ anbieten.[266] Richtigerweise wird man dieser Norm aber einen solchen Gehalt nicht attestieren können. Sie legitimiert nicht zur Beteiligung an Download-Portalen abseits des in § 11d RStV im Übrigen geregelten Programmauftrags, stellt keinen Freibrief für die Teilnahme an einem Portal nach dessen jeweiligen Eigengesetzlichkeiten dar. Eine Ausweitung des Engagements auf diesen Portalen auf ein sendungsunabhängiges, speziell für eine Internetplattform hergestelltes Angebot

---

[263] Dem öffentlich-rechtlichen Radiosender SR und dem öffentlich-rechtlichen Fernsehsender SVT wurde von der schwedischen Rundfunkkommission Granskningsnämnden för radio och TV (GRN) mit zwei Entscheidungen vom 06.09.2010 (Az. Beslut 10/00010 und 10/00018) das Bewerben ihrer Facebook-Seiten verboten, vgl. MMR-Aktuell 2010, 309017.

[264] S. zur (vermeintlichen) Unzulässigkeit des Facebook-Angebots des öffentlich-rechtlichen österreichischen Rundfunks (ORF) die Entscheidung der österreichischen Kommunikationsbehörde Austria (KommAustria) vom 25.01.2012 (Az. KOA 11.260/11-018), MMR-Aktuell 2012, 328551 sowie die Besprechung von Wichert, JurPC Web-Dok. 49/2013. Mit Entscheidung vom 27.06.2013 erklärte der Österreichische Verfassungsgerichtshof die dem Bescheid zugrunde liegende Bestimmung wegen ihrer Unverhältnismäßigkeit teilweise für verfassungswidrig (vgl. VerfGH v. 27.06.2013 – G 34/2013-10, abrufbar unter: http://www.vfgh.gv.at/cms/vfgh-site/attachments/4/7/1/CH0006/CMS1378797883281/orf_facebook_g_34-2013entscheidung.pdf).
Daraufhin erließ der Kommissionssenat im September einen neuen Verbotsbescheid gegen den ORF wegen der Kommentarfunktion im Rahmen seines Facebook-Angebots. Dieser Bescheid wurde nunmehr vom VerfGH neuerlich aufgehoben, vgl. VerfGH v. 06.03.2014 – B1035/2013-22, abrufbar unter: http://www.heise.de/downloads/18/1/2/0/0/6/6/2/orf_facebook_foren_entscheidung_b_1035-2013.pdf.

[265] Held, in: Hahn/Vesting, Rundfunkrecht, § 11d RStV, Rn. 140.

[266] Neuhoff, Rechtsprobleme, S. 229.

ist jedoch der öffentlich-rechtlichen Rundfunkanstalten ohnehin nicht geplant; es dürfte den Dreistufentest mangels Vielfaltsbedürfnisses – anders als die YouTube-Kanäle der öffentlich-rechtlichen Rundfunkanstalten, in denen kleinere Ausschnitte des Programmes in Form kurzer Clips angesehen werden können – nicht bestehen.

9.3.2.2 Vorgaben für Werbung und kommerzielle Tätigkeiten

Neben den §§ 11d ff. RStV enthalten zwar theoretisch auch die §§ 7–8a sowie 15–18 RStV Vorgaben für **kommerzielle Betätigungen** und **Werbung**, die im Rahmen des Online-Engagements relevant werden könnten. Werbung und Sponsoring ist allerdings in den Telemedien des öffentlich-rechtlichen Rundfunks von vornherein nicht zulässig (§ 11d Abs. 5 S. 1 RStV). Daneben sind auch soziale Medien mit kommerziellem Inhalt weitestgehend ausgeschlossen. Denn in der auf § 11d Abs. 5 S. 4 RStV beruhenden Anlage[267] zum RStV („Negativliste“) sind weitere Telemedienangebote aufgelistet, die stets unzulässig sind. Hiervon werden – als verfassungskonforme[268] Ausgestaltung des Programmauftrags – einige Erscheinungsformen kommerzieller Social Media erfasst, z. B. Anzeigenportale (Nr. 1), Bewertungsportale (Nr. 4), Partner-, Kontakt-, Stellen- und Tauschbörsen (Nr. 5), Ratgeberportale ohne Sendungsbezug (Nr. 6), Business-Networks (Nr. 7), Downloads von Musik, Spielen und Fotos ohne Sendungsbezug (Nrn. 13–16) sowie Foren und Chats ohne Sendungsbezug und redaktionelle Prüfung (Nr. 17). **137**

Richtigerweise ist **§ 11d Abs. 2 S. 2 RStV**, wonach die Vorschriften über die kommerziellen Betätigungen unberührt bleiben, so auszulegen, dass ein stets unzulässiges Telemedium nicht als kommerzielles Angebot erlaubt sein kann. § 16a RStV mag Telemedien ermöglich, die z. B. den Dreistufentest nicht bestanden haben oder für welche die Siebentagesfrist abgelaufen ist.[269] Wenn aber systematisch nach § 11d Abs. 2 S. 2 RStV in Absatz 5 derselben Norm Verbote für bestimmte Angebote statuiert werden, hat dies nicht nur Auswirkung auf den beitragsfinanzierten Bereich, sondern begrenzt generell die Tätigkeit der öffentlich-rechtlichen Rundfunkanstalten, und zwar auch als kommerzielle Tätigkeit, die von einem anderen Rechtsträger durchzuführen ist.[270] **138**

Die enge Bindung an den Sendungsbezug und der Ausschluss der meisten im Internet bisher kommerziell marktfähigen Angebote lässt die **§§ 15 ff. RStV** für den hier interessierenden Bereich damit **weitestgehend ohne Anwendungsbereich** bleiben. Denn übrig bliebe aktuell allein eine nichtsendungsbezogene Netzwerkplattform des Zuschnitts von Facebook; dass diese aber den Drei-Stufen-Test besteht, dürfte auf **139**

---

[267] Die Anlage ist abgedruckt und ausführlicher kommentiert bei Peters, Online-Angebote, S. 66 ff. und bei Held, in: Hahn/Vesting, Rundfunkrecht, § 11d RStV, Rn. 116 ff.

[268] A.A. Neuhoff, Rechtsprobleme, S. 189 f.

[269] So auch Neuhoff, Rechtsprobleme, S. 205.

[270] Wie hier Eifert, in: Hahn/Vesting, Rundfunkrecht, § 16a RStV, Rn. 22 und Hartstein et al., RStV, § 16a Rn. 5 („versteht sich von selbst“). Etwas weiter aber Held, in: Hahn/Vesting, § 11d RStV, Rn. 76 f. A.A. Neuhoff, Rechtsprobleme, S. 218.

lange Zeit angesichts der pluralistischen Entwicklung des Internets, für welches kein Defizit an Vielfalt besteht, ausgeschlossen bleiben.[271]

9.3.2.3 Resümee zur Zulässigkeit des Online-Engagements

140 Der Gesetzgeber hat mit der Etablierung der §§ 11d ff. RStV die langen Diskussionen um die Entwicklungsgarantie des öffentlich-rechtlichen Rundfunks im Online-Bereich mit Blick auf das „Ob" beendet. Abseits der verbleibenden rechtspolitischen Fragen und den dargestellten Einzelproblemen sind jedenfalls die **bestehenden** Social-Media-Eskapaden der öffentlich-rechtlichen Rundfunkanstalten zulässig. Eine signifikante **Ausdehnung** des Angebots im „Web 2.0" stößt indes auf erhebliche Hürden. Zum einen schließt der Negativkatalog bereits einige Varianten denkbarer Social-Media-Angebote der öffentlich-rechtlichen Rundfunkanstalten aus; hinzu kommt das Erfordernis journalistisch-redaktioneller Gestaltung, das de facto weitere interessante „Mitmach"-Techniken ausschließt. Zum anderen dürfte es für nicht-sendungsbezogene Social Media schwierig sein, den erforderlichen Dreistufentest zu bestehen. Außerhalb der bestehenden, verfassungs- wie einfachrechtlich zulässigen Sendungsbegleitungen, Hinweise und moderierten Foren wird es vor diesem Hintergrund vorerst keine rechtskonformen Social-Media-Angebote des öffentlich-rechtlichen Rundfunks geben.

9.4 Fazit/Ausblick

141 Social Media genießen grundrechtlich den Schutz der **Rundfunkfreiheit**. Einfachgesetzlich sind sie als „Telemedien" in verschiedenen Vorschriften einem speziellen Regelungsregime unterworfen. Die bestehenden Regelungen haben zwar die ehemals bestehenden Abgrenzungsschwierigkeiten zwischen Rundfunk auf der einen sowie Tele- und Mediendiensten auf der anderen Seite auf das Begriffspaar „Rundfunk" versus „Telemedien" reduziert. Allerdings werden die Telemedien weiter in einzelne Kategorien unterteilt und je nach Meinungsrelevanz an die Vorschriften für Presse und Rundfunk (i. S. d. RStV) angenähert. Diese sachlich passenden **Differenzierungen** machen die Subsumtion mitunter schwierig; hinzu kommen verschiedene Aufsichtsbehörden. Insgesamt ist allerdings dem Phänomen der Medienkonvergenz durch die aktuellen Regelungen ausreichend Rechnung getragen worden. Das gilt auch für die detailliert ausgestaltete Öffnung des Funktionsbereichs der öffentlich-rechtlichen Rundfunkanstalten für die Betätigung im Netz.

142 Gleichwohl haben gerade die **marktmächtigen Telemedien** wie Google und – für den Bereich der Social Media – Facebook auch neue Fragen aufgeworfen. Deren markt- und meinungsmächtige Angebote wirken als „bottle necks" für Information und Kommunikation in einem zentralen Freiheitsbereich des 21. Jahrhunderts.

[271] Vgl. Müller-Terpitz, AfP 2008, 335 (341).

Den hierdurch drohenden Gefahren und Missständen begegnet das Recht bisher möglicherweise noch nicht in ausreichendem Maße. Es ist deshalb nicht die Regulierung der öffentlich-rechtlichen Rundfunkanstalten, welche in den nächsten Jahren die größten Rechtsfragen aufwerfen wird, sondern die Verhinderung von monopolisierter Kommunikations- und Informationsstruktur im Internet. Ansätze dazu sind vorhanden; die hier nur angerissenen Lösungsansätze – insbesondere die Übertragung der für den technischen Zugang etablierten Regeln auf die Regulierung der Inhalte – werden jedoch eines der entscheidenden Themen zukünftiger Reformen des Medienrechts sein. Die Regulierung der Social Media steht also eventuell erst am Anfang.

Literatur

Altenhain, K. (2006). Jugendschutz. In T. Hoeren, U. Sieber, B. Holznagel (Hrsg.), *Handbuch Multimedia-Recht* (Teil 20). München: C.H. Beck.

Amlung, R., Fisch, M. (2009). Digitale Rundfunkangebote im Netz. Bewegtbild in der der digitalen Welt. *ZUM*, 442 ff.

Beater, A. (2007). *Medienrecht*. Tübingen: Mohr Siebeck.

Bloch, A. (2013). *Meinungsvielfalt contra Medienmacht. Aktuelle Entwicklungen und Reformbestrebungen im Medienkonzentrationsrecht*. Berlin: Logos.

Bonner Kommentar zum Grundgesetz → siehe unter Kahl et al.

Boos, C. (2012). Divergenter Rechtsrahmen für Inhalte im konvergenten Fernsehgerät. Vorschläge zum gesetzlichen Umgang mit dem Hybrid-TV. *MMR*, 364 ff.

Brand, T. (2002). *Rundfunk im Sinne des Artikel 5 Abs. 1 Satz 2 GG. Eine Analyse der Reichweite des verfassungsrechtlichen Rundfunkbegriffs unter besonderer Berücksichtigung neuerer medialer Angebotsformen*. Berlin: Duncker & Humblot.

Brand, P.-A. (2012). Persönlichkeitsrechtsverletzungen im Internet, E-Commerce und „Fliegender Gerichtsstand". *NJW*, 127 ff.

Bräutigam, P. (2012). Das Nutzerverhältnis bei sozialen Netzwerken. Zivilrechtlicher Austausch von IT-Leistungen gegen personenbezogene Daten. *MMR*, 635 ff.

Broemel, R. (2012). Hybrid-TV als Regulierungsproblem? Medien-, urheber- und wettbewerbsrechtliche Rahmenbedingungen hybriden Fernsehens. *ZUM*, S. 866 ff.

Brunst, P. W. (2004). Umsetzungsprobleme der Impressumspflicht bei Webangeboten. *MMR*, 8 ff.

Bullinger, M. (2006). Von presseferner zu pressenaher Rundfunkfreiheit. *JZ*, 1137 ff.

Bullinger, M. (2007). Private Rundfunkfreiheit auf dem Weg zur Pressefreiheit. *ZUM*, 337 ff.

Degenhart, C. (2011). Verfassungsfragen der Internet-Kommunikation. Wie die Rundfunkfreiheit in die Online-Welt hineinstrahlt. *CR*, 231 ff.

Degenhart, C. (2011). Rundfunkfreiheit. In D. Merten, H.-J. Papier, (Hrsg.), *Handbuch der Grundrechte in Deutschland und Europa, Bd. IV: Grundrechte in Deutschland: Einzelgrundrechte I* (§ 105, S. 1065 ff.). Heidelberg: C. F. Müller.

Degenhart, C. (2012). Medienkonvergenz zwischen Rundfunk- und Pressefreiheit. In M. Sachs, H. Siekmann (Hrsg.), *Der grundrechtsgeprägte Verfassungsstaat. Festschrift für Klaus Stern zum 80. Geburtstag* (S. 1299 ff.). Berlin: Duncker & Humblot.

Dörr, D. (2013). Ein Grundrecht der Medienfreiheit – Gleiches Recht für alle? *K&R*, Beihefter 2/2013 zu Heft 5, 9 ff.

Dörr, D., Schwartmann, R. (2012). *Medienrecht*. 4. Aufl. Heidelberg: C. F. Müller.

Dörr, D., Kreile, J., Cole, M. D. (2011). *Handbuch Medienrecht. Recht der elektronischen Massenmedien*. 2. Aufl. Frankfurt a. M.: Verlag Recht und Wirtschaft.

Dreier, H. (Hrsg.) (2013). *Grundgesetz. Kommentar, Band 1: Präambel, Artikel 1–19*. 3. Aufl. Tübingen: Mohr Siebeck.

Fechner, F. (2012). *Medienrecht*. 13. Aufl. Tübingen: Mohr Siebeck.

Gersdorf, H. (1995). *Der verfassungsrechtliche Rundfunkbegriff im Lichte der Digitalisierung der Telekommunikation. Ein Rechtsgutachten im Auftrag der Hamburgischen Anstalt für neue Medien*. Berlin: Vistas.

Gersdorf, H. (2009). *Legitimation und Limitierung von Onlineangeboten des öffentlich-rechtlichen Rundfunks. Konzeption der Kommunikationsverfassung des 21. Jahrhunderts*. Berlin: Duncker & Humblot.

Gersdorf, H. (2010). Verbot presseähnlicher Angebote des öffentlich-rechtlichen Rundfunks. *AfP*, 421 ff.

Gersdorf, H., Paal, B. (2014). *Informations- und Medienrecht Kommentar*. München: C. H. Beck.

Gounalakis, G. (2002). Konvergenz der Medien – Sollte das Recht der Medien harmonisiert werden? Gutachten C für den 64. Deutschen Juristentag Berlin 2002. In *Verhandlungen des 64. Deutschen Juristentages*. München: C. H. Beck.

Hahn, W., Vesting, T. (Hrsg.) (2012). *Beck'scher Kommentar zum Rundfunkrecht*. 3. Aufl. München: C. H. Beck.

Hain, K.-E. (2006). Regulierung in den Zeiten der Konvergenz. Wirtschaftsrechtliche und/oder medienrechtliche Steuerung? *K&R*, 325 ff.

Hain, K.-E. (2008). Die zweite Gebührenentscheidung des Bundesverfassungsgerichts – Kontinuität in den Zeiten der Konvergenz. *JZ*, 128 ff.

Hain, K.-E. (2009a). Die öffentlich-rechtlichen Anstalten auf dem Weg in die digitale Welt. In K. Stern, H. Prütting, K.-N. Peifer (Hrsg.), *Neue Mediendienste und öffentlich-rechtlicher Rundfunk. Vortragsveranstaltung des Instituts für Rundfunkrecht an der Universität zu Köln vom 30. Mai 2008* (S. 7 ff.). München: C. H. Beck.

Hain, K.-E. (2009b). *Die zeitlichen und inhaltlichen Einschränkungen der Telemedienangebote von ARD, ZDF und Deutschlandradio nach dem 12. RÄndStV. Rechtsgutachten für ARD, ZDF und Deutschlandradio*. Baden-Baden: Nomos.

Hain, K.-E. (2012). Die Tagesschau-App vor Gericht. *WRP*, 1495 ff.

Hain, K.-E. (2012). Ist die Etablierung einer Internetdienstefreiheit sinnvoll? *K&R*, 98 ff.

Hain, K.-E. (2012). Medienmarkt im Wandel: Technischer Konvergenz und Anbieterkonkurrenz als Herausforderung an Verfassungsrecht und Regulierung. *AfP*, 313 ff.

Hartstein, R., Ring, W.-D., Kreile, J., Dörr, D. Stettner, R. (2012). *Rundfunkstaatsvertrag. Kommentar*, Loseblatt (Stand: 54. Aktualisierung Dezember 2012). Heidelberg u. a.: Rehm.

Haug, V. (2010). *Internetrecht*. 2. Aufl. Stuttgart: Kohlhammer.

Heckmann, D. (2011). *juris PraxisKommentar Internetrecht*. 3. Aufl. Saarbrücken: Juris.

Heckmann, D. (2012). Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz. *NJW*, 2631 ff.

Heinze, C. (2011). Surf global, sue local! Der europäische Klägergerichtsstand bei Persönlichkeitsrechtsverletzungen im Internet. *EuZW*, 947 ff.

Held, T. (2008). *Online-Angebote öffentlich-rechtlicher Rundfunkanstalten. Eine Untersuchung des verfassungsrechtlich geprägten und einfachgesetzlich ausgestalteten Funktionsauftrags öffentlich-rechtlichen Rundfunks im Hinblick auf Internet-Dienste*. Baden-Baden: Nomos.

Hoeren, T. (2007). Das Telemediengesetz. *NJW*, 801 ff.

Hoeren, T., Sieber, U., Holznagel, B. (Hrsg.) (2013). *Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs*, Loseblatt (Stand: 34. EL April 2013). München: C. H. Beck.

Hoffmann-Riem, W., Schulz, W., Held, T. (2000). *Konvergenz und Regulierung. Optionen für rechtliche Regelungen und Aufsichtsstrukturen im Bereich Information, Kommunikation und Medien*. Baden-Baden: Nomos.

Holznagel, B. (2011). Internetdienstefreiheit und Netzneutralität. *AfP*, 532 ff.

Holznagel, B. (2014). Grünbuch Konvergenz der Medien 2013. Verpasste Chance oder gangbarer Weg aus dem Globalisierungsdilemma?. *MMR*, 18 ff.

Holznagel, B., Schumacher, P. (2011a). Kommunikationsfreiheiten und Netzneutralität. In M. Kloepfer (Hrsg.), *Netzneutralität in der Informationsgesellschaft* (S. 47 ff.). Berlin: Duncker & Humblot.

Holznagel, B., Schumacher, P. (2011b). Netzpolitik reloaded. Pflichten und Grenzen staatlicher Internetpolitik. *ZRP*, 74 ff.

Holznagel, B., Dörr, D., Hildebrand, D. (2008). *Elektronische Medien. Entwicklung und Regulierungsbedarf*. München: Vahlen.

Joecks, W., Miebach, K. (Hrsg.) (2010). *Münchener Kommentar zum Strafgesetzbuch. Kommentar*, Band 6/1: Nebenstrafrecht II, herausgegeben von W. Joecks und R. Schmitz, München: Verlag [zitiert: Bearbeiter, in: MüKo-StGB].

Jungheim, S. (2012). *Medienordnung und Wettbewerbsrecht im Zeitalter der Digitalisierung und Globalisierung*. Tübingen: Mohr Siebeck.

Kahl, W., Waldhoff, C. & Walter, C. (2013). *Bonner Kommentar zum Grundgesetz*, Band 2: Art. 4–6 I. Loseblatt (Stand: 160. EL März 2013). Heidelberg: C. F. Müller [zitiert: Bearbeiter, in: BK-GG].

Kegel, G., Schurig, K. (2004). *Internationales Privatrecht*. 9. Aufl. München: C. H. Beck.

Kempermann, P. (2010). *Content-Regulierung in konvergierenden Medien*. Frankfurt a. M.: Peter Lang.

Kitz, V. (2007). Das neue Recht der elektronischen Medien in Deutschland – sein Charme, seine Fallstricke. *ZUM*, 368 ff.

Klaes, R. (2009). Verfassungsrechtlicher Rundfunkbegriff und Internet. Eine dogmatische Bestandsaufnahme vor dem Hintergrund des 12. Rundfunkänderungsstaatsvertrages. *ZUM*, 135 ff.

Klickermann, P. H. (2009). Telemedienangebote von ARD und ZDF im Fokus des Dreistufentests. *MMR*, 740 ff.

Koenig, C. (2013). Zugang von Inhalteanbietern zu Smartphone-Oberflächen! *MMR*, 137 f.

Köhler, A. (2013). *Eingriffsnormen – Der „unfertige Teil" des europäischen IPR*. Tübingen: Mohr Siebeck.

Kreile, J., Diesbach, M. (2002). Der neue Jugendmedienschutz-Staatsvertrag – was ändert sich für den Rundfunk? *ZUM*, 849 ff.

Krieg, H. (2010). Twitter und Recht. Kurze Tweets, große Wirkung – die rechtlichen Stolperfallen beim Twittern. *K&R*, 73 ff.

Krieg, H., Roggenkamp, J. D. (2010). Astroturfing – rechtliche Probleme bei gefälschten Kundenbewertungen im Internet. *K&R*, 689 ff.

Kube, H. (2006). Neue Medien – Internet. In J. Isensee, P. Kirchhof (Hrsg.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band IV: Aufgaben des Staates*. 3. Aufl. (§ 91, S. 843 ff.). Heidelberg: C. F. Müller.

Kunisch, J. K. (2011). *Rundfunk im Internet und der Grundsatz der Staatsfreiheit des Rundfunks. Eine Untersuchung zur Rundfunkqualität von Internetdiensten und der Einhaltung des Staatsfreiheitsgrundsatzes bei der Aufsicht über Internetdienste im Schutzbereich der Rundfunkfreiheit*. München: C. H. Beck.

Kunisch, J. K. (2011). Verfassungswidrige Telemedienaufsicht durch Regierungsstellen. Aufsicht über Internetdienste im Schutzbereich der Rundfunkfreiheit. *MMR*, 796 ff.

Kuper, E.-S. (2009). *Internet Protocol Television – IPTV. Rechtlicher Rahmen und Besonderheiten im Rundfunk- und Medienrecht, Telekommunikationsrecht, Urheberrecht und im Wettbewerbs- und Kartellrecht*. Hamburg: Verlag Dr. Kovač.

Lange, C. (2013). Impressumspflicht in sozialen Netzwerken. *ZJS*, 141 ff.

Lauber-Rönsberg, A. (2014). Internetveröffentlichungen und Medienprivileg. *ZD*, 177 ff.

Lehrke, A. (2006). *Pluralismus in den Medien. Verfassungsrechtliche Aspekte von Meinungsbildungsrelevanz als medienübergreifendem Kriterium der Vielfaltsregulierung*. Münster: LIT Verlag.

Lent, W. (2001). *Rundfunk-, Medien-, Teledienste. Eine verfassungsrechtliche Untersuchung des Rundfunkbegriffs und der Gewährleistungsbereiche öffentlich-rechtlicher Rundfunkanstalten*

unter Berücksichtigung einfachrechtlicher Abgrenzungsfragen zwischen Rundfunkstaatsvertrag, Mediendienstestaatsvertrag und Teledienstegesetz. Frankfurt a. M. u. a.: Peter Lang.
Lichtnecker, F. (2013). Die Werbung in sozialen Netzwerken und mögliche hierbei auftretende Probleme. *GRUR*, 135 ff.
Liesching, M. (2013). *Beck'scher Online-Kommentar JMStV*, München: C. H. Beck (Stand: Mai 2013) [zitiert: Liesching, in: BeckOK JMStV].
Lorenz, B. (2008). Die Anbieterkennzeichnung nach dem TMG und RStV. *K&R*, 340 ff.
Lorenz, B. (2010). Die Wettbewerbswidrigkeit einer mangelhaften Anbieterkennzeichnung. *WRP*, 1224 ff.
Luch, A. D., Schulz, S. E. (2013). Die digitale Dimension der Grundrechte. Die Bedeutung der speziellen Grundrechte im Internet. *MMR*, 88 ff.
von Mangoldt, H., Klein, F., Starck, C. (2010). *Kommentar zum Grundgesetz, Band 1: Präambel, Artikel 1 bis 19*. 6. Aufl. München: Verlag Vahlen.
Mecklenburg, W. (1997). Internetfreiheit. *ZUM*, 525 ff.
Moini, B. (2013). Facebook regulieren. *Frankfurter Allgemeine Zeitung (FAZ)* vom 08.02.2013, S. 7.
Müller-Broich, J. D. (2012). *Telemediengesetz. Kommentar*. Baden-Baden: Nomos.
Müller-Terpitz, R. (2008). Öffentlich-rechtliche Rundfunk und Neue Medien – Eine gemeinschafts- und verfassungsrechtliche Betrachtung. *AfP*, 335 ff.
Müller-Terpitz, R., Rauchhaus, A. (2011). „Hybrid-TV". Eine neue Technik als Herausforderung für das Recht. In Institut für interdisziplinäre Medienforschung (Hrsg.), *Medien und Wandel* (S. 309 ff.). Berlin: Logos.
Münchener Kommentar zum Strafgesetzbuch → siehe unter Joecks.
Neuhoff, H. (2012). Die Dynamik der Medienfreiheit am Beispiel von Presse und Rundfunk. Zur Operationalisierung des Verbots nichtsendungsbezogener presseähnlicher Telemedienangebote der Rundfunkanstalten. *ZUM*, 371 ff.
Neuhoff, H. (2013). *Rechtsprobleme der Ausgestaltung des Auftrags des öffentlich-rechtlichen Rundfunks im Online-Bereich*. Baden-Baden: Nomos.
Oster, J. (2009). Rechtsfragen der Medienkonvergenz am Beispiel der Internet-Telefonie. In F. Fechner (Hrsg.), *Konvergenz – Datenschutz – Meinungsforen: Fragestellungen des Internetrechts*. Ilmenau: Universitätsverlag Ilmenau, 8 ff.
Ott, S. (2007). Impressumspflicht für Webseiten. Die Neuregelungen des § 5 TMG, § 55 RStV. *MMR*, 354 ff.
Paal, B. P. (2010). *Medienvielfalt und Wettbewerbsrecht*. Tübingen: Mohr Siebeck.
Paal, B. P. (2012). *Suchmaschinen, Marktmacht und Meinungsbildung*. Baden-Baden: Nomos.
Papier, H.-J., Schröder, M. (2011). *Verfassungsfragen des Dreistufentests. Inhaltliche und verfahrensrechtliche Herausforderungen*. Baden-Baden: Verlag.
Paschke, M. (2009). *Medienrecht*. 3. Aufl. Berlin: Springer.
Paschke, M., Berlit, W., Meyer, C. (Hrsg.) (2012). *Hamburger Kommentar Gesamtes Medienrecht*. 2. Aufl. Baden-Baden: Nomos.
Peters, B. (2009). Der „Drei-Stufen-Test": Die Zukunft der öffentlich-rechtlichen Onlineangebote. *K&R*, 26 ff.
Peters, B. (2010). *Öffentlich-rechtliche Online-Angebote. Was dürfen die Rundfunkanstalten im Netz*? Baden-Baden: Nomos.
Petersen, J. (2010). *Medienrecht*. 5. Aufl. München: C. H. Beck.
Pießkalla, M. (2014). Zur Reichweite der Impressumspflicht in sozialen Netzwerken. *ZUM*, 368 ff.
Ricker, R., Schiwy, P. (1997). *Rundfunkverfassungsrecht*. München: C. H. Beck.
Ricker, R., Weberling, J. (2012). *Handbuch des Pressrechts*. 6. Aufl. München: C. H. Beck.
Rockstroh, S. (2013). Impressumspflicht auf Facebook-Seiten. Wann werden Telemedien „in der Regel gegen Entgelt" angeboten? *MMR*, 627 ff.
Roßnagel, A. (2007). Das Telemediengesetz. Neuordnung für Informations- und Kommunikationsdienste. *NVwZ*, 743 ff.

Roßnagel, A. (Hrsg.) (2013). *Beck'scher Kommentar zum Recht der Telemediendienste*. München: C. H. Beck.

Rossen-Stadtfeld, H. (2009). *Audiovisuelle Bewegtbildangebote im Internet: Presse oder Rundfunk*? Baden-Baden: Nomos.

Rumyantsev, A. (2008). Journalistisch-redaktionelle Gestaltung: Eine verfassungswidrige Forderung? „Wiedergeburt" des wertbezogenen Medienbegriffs. *ZUM*, 33 ff.

Sachs, M. (2011). *Grundgesetz. Kommentar*. 6. Aufl. München: C. H. Beck.

Sack, R. (2011). Der EuGH zu Art. 3 E-Commerce-Richtlinie – die Entscheidung „eDate-Advertising". *EWS*, 513 ff.

Sack, R. (2013). Internetwerbung – ihre Rechtskontrolle außerhalb des Herkunftslands des Werbenden. *WPR*, 1407 ff.

Sack, R. (2013). Internetwerbung – ihre Rechtskontrolle im Herkunftsland des Werbenden. *WRP*, 1545 ff.

Schmid, T., Kitz, V. (2009). Von der Begriffs- zur Gefährdungsregulierung im Medienrecht. Möglichkeiten und Grenzen von Fiktionen in einer modernen Medienordnung. *ZUM*, 739 ff.

Schmidtmann, K. (2013). *Die verfassungsrechtliche Einordnung konvergenter Massenmedien. Eine* Analyse *der Auswirkungen des Medienwandels auf Presse und Rundfunk aus verfassungsrechtlicher Sicht*. Hamburg: Verlag Dr. Kovač.

Schoch, F. (2002). Konvergenz der Medien – Sollte das Recht der Medien harmonisiert werden? *JZ*, 798 ff.

Schwartmann, R. (Hrsg.) (2011). *Praxishandbuch Medien-, IT- und Urheberrecht*. 2. Aufl. Heidelberg u. a.: C. F. Müller.

Schwenke, T. (2012). Social Media Marketing und Recht. Cambridge u. a.: O'Reilley Verlag.

Seitz, W. (2012). Zivilrechtlicher Persönlichkeitsschutz gegenüber Äußerungen im Internet. In T. Hoeren, U. Sieber, B. Holznagel, *Handbuch Multimedia-Recht* (Teil 8). München: C. H. Beck.

Solmecke, C. (2012). Social Media. In T. Hoeren, U. Sieber, B. Holznagel, *Handbuch Multimedia-Recht* (Teil 21.1). München: C. H. Beck.

Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien*. Kommentar, 2. Aufl. München: C. H. Beck.

Splittgerber, A. (Hrsg.) (2014). *Praxishandbuch Rechtsfragen Social Media*. Berlin: De Gruyter.

Sporn, S. (2013). Ein Grundrecht der Medienfreiheit – Gleiches Recht für alle!? *K&R*, Beihefter 2/2013 zu Heft 5, 1 ff.

Stadler, T. (2011). Verstoßen Facebook und Google Plus gegen deutsches Recht? Ausschluss von Pseudonymen auf Social-Media-Plattformen. *ZD*, 57 ff.

Stenner, D. (2009). *Die Zulässigkeit interaktiver und individualisierter Werbung in Fernsehen und in audiovisuellen Telemedien*. Hamburg: Verlag Dr. Kovač.

Trute, H.-H. (1998). Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung. *VVDStRL* 57, 216 ff.

Venzke, S. (2011). Social Media Marketing. Eine datenschutzrechtliche Orientierungshilfe. *DuD*, 387 ff.

Weigl, M. (2011). *Meinungsfreiheit contra Persönlichkeitsschutz am Beispiel von Web 2.0-Applikationen*. Hamburg: Verlag Dr. Kovač.

Weiner, C., Schmelz, C. (2006). Die elektronische Presse und andere neue Kommunikationsformen im neuen rechtlichen Regulierungsrahmen. Regierungsentwurf zum Telemediengesetz und 9. Rundfunkänderungsstaatsvertrag. *K&R*, 453 ff.

Wellenreuther, M. (2011). *Presseähnliche Telemedien öffentlich-rechtlicher Rundfunkanstalten*. Berlin: Logos.

Wichert, G. (2013). Nutzung sozialer Netzwerke durch Rundfunkanstalten – Zugleich Besprechung der Erkenntnis des Österreichischen Verwaltungsgerichtshofs vom 22.10.2012. JurPC-Web-Dok. 49/2013, Abs. 1–18, abrufbar unter: http://www.jurpc.de/jurpc/show?id=20130049.

Wierny, T. (2014). App-Streit Runde zwei. Was das Oberlandesgericht Köln konsequenter, aber nicht richtiger gemacht hat. *ZUM*, 196 ff.

Witt, J. (2007). *Internet-Aktivitäten öffentlich-rechtliche Rundfunkanstalten*. Berlin: Duncker & Humblot.

Zagouras, G. (2002). *Konvergenz und Kartellrecht. Die Regulierung des Wettbewerbs im Bereich der Medien und Kommunikationsplattformen nach GWG, TKG und RStV sowie Optionen für eine Umstrukturierung*. München: C. H. Beck.

Zoebisch, M. (2011). Der Gegendarstellungsanspruch im Internet. *ZUM*, 390 ff.

Zysk, H. (2012). Compliance im Jugendmedienschutz. Herausforderung an Medienunternehmen im Kontext multimedialer Angebote. *ZUM*, 22 ff.

Kapitel 10
Einsatz von Social Media durch die öffentliche Verwaltung

Sönke E. Schulz

Inhalt

S. E. Schulz (✉)
Geschäftsführender wissenschaftlicher Mitarbeiter, Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Olshausenstraße 40, 24098 Kiel, Deutschland
E-Mail: sschulz@lvstein.uni-kiel.de

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8_10

10.1 Einleitung

1 **Social Media** beschreibt eine Reihe miteinander verbundener Entwicklungen: Der Begriff bezeichnet die Interaktion der Nutzer, welche auf digitalen Plattformen zu neuen Formen der Zusammenarbeit und des Datenaustauschs zusammen finden. Das soziale Netz bezieht seine Nutzer aktiv in lebendige Wertschöpfungsprozesse ein – sei es durch die erleichterte Produktion eigener Inhalte, Kommentare, Tags oder auch nur durch virtuelle Präsenz. Social Media erlaubt einem zuvor auf passiven Konsum beschränkten Publikum, zum Schöpfer vielfältiger multimedialer Inhalte zu werden, und stellt Plattformen wie bspw. Blogs, Wikis und soziale Netzwerke für deren Verbreitung zur Verfügung.

2 Aufgrund der veränderten Gewohnheiten der Internet-Nutzung im privaten wie im geschäftlichen Kontakt wird zunehmend von der öffentlichen Verwaltung verlangt, dass diese die gleichen Kanäle nutzt. Für die Generation der sog. **Digital Natives**[1] sind das Internet und soziale Netzwerke mittlerweile das primäre Kommunikationsmittel. Insofern ist ein Trend feststellbar, dass auch öffentliche Verwaltungen Social-Media-Anwendungen und -Dienste nutzen[2] – in welcher Art und Weise auch immer, ob man diese Entwicklung nun begrüßt oder für entbehrlich hält.

3 Offiziell wird Social Media insbesondere für die **Öffentlichkeits- und Pressearbeit** eingesetzt. Insofern kommt es vor allem zu einer Zweitverwertung der auch auf anderem Wege verbreiteten Informationen. Parallel dazu haben einzelne Verwaltungsmitarbeiter begonnen, diese Angebote im Kontext ihrer dienstlichen Tätigkeit zu nutzen. Die Erscheinungsformen reichen von Handlungsweisen, bei denen der Bezug zur dienstlichen Tätigkeit kaum erkennbar ist, über die Nutzung als bloße Informationsquelle bis hin zu einer offenen Diskussion beruflicher Themen in sozialen Netzwerken (fachlicher Diskurs).[3]

---

[1] S. zum Begriff der Digital Natives Deutsches Institut für Vertrauen und Sicherheit im Internet (Hrsg.), DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2012, abrufbar unter www.divsi.de.

[2] Übersicht der in den sozialen Medien vertretenen Kommunen, Behörden und Organisationen auf www.pluragraph.de.

[3] Zum Einsatz sozialer Medien durch die öffentliche Verwaltung ausführlich Schliesky/Schulz, Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung, 2012; vgl. auch Schulz/Hoffmann, Rechtsrahmen ermöglicht Teilnahme an sozialen Netzwerken, innovative Verwaltung, 5/2013, 16 ff.

Diese Entwicklungen haben sich bisher weitgehend **unreglementiert** vollzogen. Zum Teil existieren keine Absprachen der Beteiligten, zum Teil werden die Social-Media-Aktivitäten der Mitarbeiter geduldet oder gefördert. Weiterhin gibt es bilaterale Absprachen, die bestimmte Einsatzformen von Social Media erlauben oder (einschränkende) Vorgaben machen. Nur selten gehen dem Einsatz strategische Überlegungen voraus, zu welchen Zwecken man Social-Media-Dienste nutzen kann und welche Vorgaben gelten.[4] 4

Aufgrund der **Besonderheiten der Web 2.0-Kommunikation** ist der Rückgriff auf bestehende handlungsleitende Vorgaben (sei es in Form von Verwaltungsvorschriften zur Behördenkommunikation oder des ohnehin Geltung beanspruchenden gesetzlichen Rahmens, bspw. des Beamten- und Dienstrechts) nicht geeignet, die Nutzung vollständig zu erfassen und die mit dem Einsatz einhergehenden Risiken für Mitarbeiter und Organisation sachgerecht zu minimieren.[5] Die Kommunikation über soziale Medien vollzieht sich in der Regel nicht-hierarchisch, d. h. die Kommunikation findet auf allen Ebenen der öffentlichen Verwaltung statt bzw. es wird eine Reaktion aller Ebenen erwartet. Auch sind Reaktionszeiten der Regelfall, die die bisherige Behördenorganisation nicht abbilden kann. Zudem entstehen aus der leichteren Durchsuchbarkeit und Verknüpfbarkeit von Einzeläußerungen sowie der langfristigen Verfügbarkeit besondere Gefahren – bspw. in Form einer deutlich größeren Streuwirkung von Einzelmeinungen oder einer fälschlicherweise vorgenommenen Zurechnung zur Gesamtorganisation.[6] Neue, diesen Besonderheiten gerecht werdende Regelwerke existieren noch nicht bzw. kommen über allgemeine Ausführungen und bloß empfehlenden Charakter nicht hinaus.[7] 5

Im Folgenden wird der **Rechtsrahmen** des Einsatzes von Social Media durch die öffentliche Verwaltung umschrieben, wobei die in den anderen Kapiteln dargestellten allgemeinen rechtlichen Vorgaben selbstverständlich auch für behördliche Nutzer gelten. Insofern ist vor allem auf die Besonderheiten einzugehen, die sich aus der Funktion der öffentlichen Verwaltung und speziellen rechtlichen Vorgaben ergeben. Im Mittelpunkt stehen die Einsatzoptionen für die allgemeine Verwaltung; soweit bspw. für Polizei- und Sicherheitsbehörden, Sozial- und Jugendämter abweichende Nutzungsanlässe und damit rechtliche Vorgaben existieren, wird darauf hingewiesen. 6

10.2 Abgrenzungen und Nutzungsanlässe

Der Einsatz von Social Media durch und in der öffentlichen Verwaltung lässt sich nach verschiedenen **Kriterien** abgrenzen und differenzieren: 7

[4] Vgl. dazu auch Müller/Schulz, Die drei Dimensionen von Social Media Policy, Blogbeitrag v. 06.10.2011; abrufbar unter www.government2020.de.

[5] Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (124).

[6] So bspw. im Kontext der Frage, ob ein Arbeitgeber für private Äußerungen seiner Mitarbeiter verantwortlich gemacht werden kann; s. dazu LG Freiburg, MMR 2014, 118 ff.

[7] So insbesondere die Empfehlungen für die Hamburgische Verwaltung; s. Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, 2011.

- danach, ob der Einsatz der Dienste durch die Behörde oder die Nutzung durch die Mitarbeiter bewertet werden soll,
- ob der Mitarbeiter in dienstlicher Eigenschaft, als Privatperson oder in einer anderen offiziellen Rolle, bspw. als kommunaler Mandatsträger, agiert,
- ob die Nutzung externer Dienste in Rede steht oder interne Kommunikationsprozesse mithilfe von Social-Media-Anwendungen realisiert werden sollen,
- und schließlich danach, welche Zielsetzungen konkret verfolgt werden sollen.

10.2.1 Behördliche Nutzung und Nutzung durch die Mitarbeiter

8 Erste maßgebliche **Abgrenzung** ist die Frage, ob das Verhalten der Behörde (also eines ihr zurechenbaren Mitarbeiters) in den sozialen Medien, also rechtliche Vorgaben, die an die Behörde adressiert sind, oder ob die Nutzung durch die Mitarbeiter bewertet werden soll. So betreffen bspw. Vorgaben aus dem Vergabe-, Datenschutz- und Verfassungsrecht nicht unmittelbar den Mitarbeiter, sondern die gem. Art. 20 Abs. 3 GG an Recht und Gesetz gebundene öffentliche Verwaltung. Die Nutzung durch den Mitarbeiter lässt sich weitergehend danach differenzieren, ob dieser dienstlich – also im Rahmen der behördlichen Nutzung – oder in sonstiger Funktion und Rolle agiert. In beiden Fällen sind rechtliche, an den Mitarbeiter gerichtete Vorgaben denkbar, die sein Handeln determinieren.

10.2.2 Unterschiedliche Rollen bei der Nutzung durch die Mitarbeiter

9 Personen nehmen im Netz zunehmend **verschiedene Rollen** ein – so verfügen Mitarbeiter der öffentlichen Verwaltung zum Teil neben ihrer dienstlichen (als Verwaltung), ihrer privaten (als Privatperson) ebenfalls über eine Parteirolle (bspw. als Kandidat für ein Bürgermeisteramt) oder sind zugleich kommunale Mandatsträger. Die Abgrenzung ist durch Web 2.0-Dienste und soziale Netzwerke wesentlich komplexer geworden. Hinsichtlich des Einsatzes durch die Mitarbeiter ist aber gleichwohl zwischen diesen Rollen zu differenzieren, für sie gelten unterschiedliche rechtliche Rahmenbedingungen und es bestehen unterschiedlich ausgeprägte Möglichkeiten des Dienstherrn, auf das Verhalten einzuwirken.

10 Die ***dienstliche Nutzung*** korrespondiert mit den behördlichen Einsatzformen. Nur dort, wo die Behörde überhaupt als solche aktiv wird, kann das Verhalten des Mitarbeiters dienstlichen Charakter haben. Verzichtet bspw. eine Behörde gänzlich auf Social-Media-Aktivitäten, ist nur privates Handeln der Mitarbeiter (selbst wenn ein Bezug zum Aufgabenbestand der Behörde und dem Geschäftsbereich des

Mitarbeiters besteht) denkbar.[8] Abgrenzung und Abgrenzbarkeit von dienstlicher und sonstiger Nutzung bereiten insbesondere dann Schwierigkeiten, wenn Regelungen zur Social-Media-Nutzung durch die Behörde und ihre Mitarbeiter vollständig fehlen. Daher bieten verbindliche interne Anweisungen (bspw. in Form einer Social-Media-Guideline[9]) die Möglichkeit, die dienstlichen Aktivitäten zu definieren und diese im Interesse der Rechtssicherheit von sonstigen Handlungsweisen abzugrenzen. Dabei besteht ein großer Gestaltungsspielraum des Dienstherrn, zumal die denkbaren Nutzungsformen je nach Aufgabe der Behörde und Zielgruppe variieren sowie einem zeitlichen Wandel unterliegen. Sind explizite Vorgaben vorhanden oder die Nutzung allgemein zu dienstlichen Zwecken gestattet, lässt sich eine Abgrenzung relativ einfach umschreiben: Als dienstliche Nutzung kann nur diejenige Tätigkeit eingestuft werden, die von den Vorgaben der Social-Media-Guideline abgedeckt ist. Dies bedeutet bspw., dass wenn eine Behörde den fachlichen Diskurs nicht gestattet, es sich bei entsprechenden Diskussionsbeiträgen eines Mitarbeiters schon aus diesem Grund um private Äußerungen handelt[10].

11 Neben der Option, durch eine Social-Media-Guideline explizit dienstliche und sonstige (nicht nur private) Handlungsweisen abzugrenzen, kann zusätzliche Rechtssicherheit geschaffen werden, indem für dienstliche Aktivitäten ausschließlich behördliche **„Funktions-Accounts"** genutzt werden. Persönliche Accounts sind für die dienstliche Kommunikation weniger geeignet und könnten interessierte Bürger ggf. sogar verwirren. Funktions-Accounts widersprechen hingegen den Grundgedanken der auf persönliche Kommunikation angelegten sozialen (!) Medien.[11]

12 Fehlen Vorgaben, ist im Interesse der Adressaten der dienstliche Charakter ausgehend vom **objektiven Empfängerhorizont** zu bestimmen. Gleiches gilt beim Handeln einzelner Mitarbeitern, welches von internen Vorgaben abweicht. Selbst wenn Mitarbeitern der öffentlichen Verwaltung die Beantwortung von Bürgeranfragen (intern) nicht gestattet ist, ein Mitarbeiter dies dennoch tut, muss diese – wenn das Verhalten nach außen der Behörde zurechenbar erscheint – bspw. auch für Fehlinformationen haften.[12]

13 Alle Handlungen, die nicht explizit oder konkludent vom Dienstherrn als dienstliche Nutzungen vorgesehen und legitimiert sind, sind als *privat* einzustufen. Im Außenverhältnis kann dies aufgrund des objektiven Empfängerhorizonts anders zu beurteilen sein. Die private Nutzung ist grundsätzlich – mit Einschränkungen während der Dienstzeit – nicht nur gestattet, sondern wird durch die Meinungsfreiheit aus Art. 5 GG auch verfassungsrechtlich gesichert. Einschränkende Regelungen, bspw. aus dem Beamtenrecht (§ 60 Abs. 2 BBG), müssen sich daher rechtfertigen lassen.[13] Eine weitergehende Unterscheidung zwischen der Vielzahl der Rollen, die

[8] Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (145).
[9] Ausführlich dazu Schulz, Social Media Guidelines, ISPRAT-Whitepaper, herausgegeben von Matthias Kammer, Huppertz und Westerfeld, 2011; abrufbar unter www.isprat.net.
[10] Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (133).
[11] Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (141).
[12] Zur Zurechnung im Rahmen der Amtshaftung Papier, in: MüKo-BGB, § 839 Rn. 129 ff.
[13] Battis, Bundesbeamtengesetz, § 60 Rn. 17.

ein Mitarbeiter der öffentlichen Verwaltung in seiner Freizeit (in Abgrenzung vom dienstlichen Handeln) einnehmen kann und in denen er in den sozialen Medien aktiv wird, ist nicht erforderlich. Auch das Agieren in einer Parteirolle oder im Rahmen einer erlaubten Nebentätigkeit ist insofern privat, also **nicht-dienstlich**. Inwiefern solche nicht-dienstlichen Aktivitäten während der Dienstzeit zugelassen sind – unabhängig davon, ob über dienstliche oder private Geräte –, richtet sich nach den allgemeinen Grundsätzen zur privaten Internetnutzung.[14] Eine besondere Konstellation entsteht bei der Nutzung sozialer Medien durch (kommunale) Mandatsträger: Da das Verhalten einzelner Mitglieder nicht der Kommune zugerechnet werden kann, bleiben diese Aktivitäten außerhalb der behördlichen Nutzung der Kommune und sie haben keinen dienstlichen Charakter.[15]

10.2.3 Externe und interne Einsatzformen

14 Eine auch unter rechtlichen Gesichtspunkten relevante Unterscheidung betrifft den Umstand, ob Social Media lediglich zur internen Kommunikation eingesetzt wird oder ob es zu einer **Interaktion mit Externen** kommt. So kann der Austausch zwischen Behördenmitarbeitern unter Umständen dienstliche Angelegenheiten betreffen, die von der Verschwiegenheitspflicht erfasst werden, während solche schon von vornherein nicht Gegenstand einer wie auch immer gearteten Außenkommunikation sein können. Der *interne* Einsatz von Social Media hat vor allem Effizienzgründe. Schwerpunkte liegen im Bereich der Kommunikation und des Wissensmanagements. So kann die Nutzung von Sharepoints, also die gemeinsame Bearbeitung von Dokumenten, Abstimmungsprozesse beschleunigen. Die Terminfindung wird durch Tools wie Doodle auch für die öffentliche Verwaltung erleichtert, soziale Netzwerke können das Auffinden eines Experten zu einem bestimmten Thema beschleunigen. Hinzu kommt die damit einhergehende Attraktivität der öffentlichen Verwaltung für (neue) Mitarbeiter, da es vielfach als Vorzug gesehen wird, privat und dienstlich die gleichen Anwendungen zu nutzen. Insbesondere bei der internen Nutzung stellt sich die Frage, ob aufgrund des internen Charakters lediglich eigene Dienste zum Einsatz kommen sollen oder ob auch auf externe Anbieter zurückgegriffen werden kann.

15 Zu den *externen* Nutzungen mit Außenwirkung sollen nicht nur diejenigen gezählt werden, bei denen mit außerhalb der Verwaltung stehenden Personen aktiv kommuniziert wird (Bürgeranfragen und -kommunikation, fachlicher Diskurs, Presse- und Öffentlichkeitsarbeit, Online-Fahndung), sondern auch all diejenigen Einsatzformen, die auf eine Erhebung und **Nutzung von Daten aus den sozialen Netzwerken** abzielen (Online-Streife, Social Media Monitoring).

---

[14] Dazu Rn. 122.
[15] Dazu Rn. 101 ff.

10.2.4 Eigene behördliche Homepages oder Dienste privater Anbieter

Zusätzlich ist zu differenzieren, ob eine Behörde Social-Media-Anwendungen auf der eigenen Homepage – und damit weitgehend unter eigener Verantwortung – betreibt und nutzt oder auf (kommerzielle und nicht-kommerzielle) **Angebote privater Unternehmen** zurückgreifen will. Während es sich bei Foren, Wikis und Blogs anbietet, diese selbst zu realisieren, sind Microblogging, soziale Netzwerke und Umfragetools kaum selbst realisierbar. Fotos und Videos lassen sich zwar auf der eigenen behördlichen Homepage einstellen, ein Mehrwert folgt aber erst aus der Integration in Video- und Fotoplattformen mit zahlreichen Zusatzfunktionen. Selbst wenn vollständig eigene Lösungen realisiert werden, kommen zum Teil – um die Reichweite zu erhöhen – Social Plugins in Betracht, mit denen Inhalte von den Nutzern leicht in den sozialen Netzen verbreitet werden können. Diese sind mit ähnlichen Rechtsfragen verbunden wie der unmittelbare Rückgriff auf Dienstleistungen von privaten Anbietern.[16] **16**

Angesichts des fehlenden Erfordernisses, eine breite Öffentlichkeit zu erreichen, was vor allem die großen Dienste privater Anbieter gewährleisten, wird vor allem bei der internen Behördenkommunikation über **interne Alternativen** diskutiert.[17] Grundsätzlich erscheinen eine interne Ausgestaltung, verbunden mit dem eigenen Betrieb der Anwendung und einer stärkeren Beherrschung bspw. der Datenverarbeitung, sowie der Rückgriff auf die Dienste externer Anbieter möglich. Intern sind perspektivisch soziale Netzwerke denkbar, die exklusiv für Mitarbeiter der öffentlichen Verwaltung zugänglich sind[18] und dem fachlichen Austausch gerade über Ebenengrenzen hinweg dienen (Beispiele aus dem Ausland: Ambtenaar 2.0[19], Govloop[20]). Es stellt sich aber die Frage, ob man ausreichend Nutzer gewinnt, ein weiteres internes Profil anzulegen, zu pflegen und aktiv am Netzwerk zu partizipieren. Diejenigen Mitarbeiter der öffentlichen Verwaltung, die eine gewisse Social-Media-Affinität aufweisen, dürften schon in kommerziellen Angeboten aktiv sein, sodass ein Zusatzaufwand entsteht, während skeptische Mitarbeiter nur zu einem geringen Anteil zur Mitwirkung an einem internen Netzwerk motiviert werden könnten. Denkbar erscheint aber eine Integration von Social-Media-Tools in die gewohnte Arbeitsoberfläche, bspw. die Software zur Bearbeitung elektronischer Akten. Auch kommerzielle Dienste bieten mit der Option, geschlossene Gruppen einzurichten (vor allem im beruflichen Netzwerk Xing), einen Raum für den fachlichen Austausch. Allerdings erweisen sich die Datenhaltung beim Anbieter **17**

---

[16] Dazu Rn. 89 ff.
[17] Ausführlich Müller et al., Ein soziales Netzwerk als internes Kommunikationsmittel für die öffentliche Verwaltung, 2014, abrufbar unter www.isprat.net.
[18] S. dazu Hoffmann, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 87 ff.
[19] www.ambtenaar20.nl.
[20] www.govloop.com.

sowie die fehlende Möglichkeit der sicheren Identifizierung der Teilnehmer (und damit der Beschränkung auf Verwaltungsmitarbeiter) als problematisch. Gleiches gilt auch für Angebote, die ausschließlich an Verwaltungsmitarbeiter gerichtet sind, aber gleichwohl privat betrieben werden, so das Verwaltungs- und Beschaffernetzwerk.[21]

10.2.5 Behördliche Nutzungsanlässe

18 Angesichts der kurzen Innovationszyklen und des schnellen Wandels der Social-Media-Dienste dürften sich auch die denkbaren Nutzungsoptionen für die öffentliche Verwaltung verändern. Während zunächst fast ausschließlich die Presse- und Öffentlichkeitsarbeit auf die sozialen Medien zurückgriff und allgemeine Informationen zur Verfügung gestellt wurden, haben sich die **Nutzungsanlässe** mittlerweile ausdifferenziert: Denkbar sind vor allem:

- Presse- und Öffentlichkeitsarbeit,
- Bürgerinformation und andere allgemeine Informationstätigkeit,
- die Beantwortung von Bürgeranfragen,
- der fachliche Diskurs,
- die Nutzung im Kontext interner Arbeitsprozesse,
- eine Online-Fahndung,
- die Nutzung zu Ermittlungszwecken (Online-Streife) sowie
- das sog. Social-Media-Monitoring.

Feststellbar ist zudem ein Übergang von der Nutzung von Angeboten, die in eigener Verantwortung liegen, hin zu Diensten von privaten Anbietern, deren Nutzung mit zusätzlichen Rechtsfragen verbunden ist.

10.2.5.1 Presse- und Öffentlichkeitsarbeit/allgemeine Informationstätigkeit

19 Der Einsatz sozialer Medien zur Presse- und Öffentlichkeitsarbeit dient dazu, interessierte Bürger und Medienvertreter besser und schneller mit relevanten Informationen zu versorgen und diejenigen Kanäle zu bedienen, die aufgrund ihrer Zusatzfunktionalitäten (bspw. leichtere Durchsuchbarkeit, schnellere Verfügbarkeit) auch von Journalisten mittlerweile primär genutzt werden. Die **Zielsetzungen** decken sich mit der klassischen Presse- und Öffentlichkeitsarbeit bzw. allgemein der Informationstätigkeit der öffentlichen Verwaltung. Erkennbar ist derzeit ein Trend, nicht nur aufbereitete Informationen, sondern auch die zugrunde liegenden Daten transparent zu machen und zu veröffentlichen. Soweit dies auch über Social Media erfolgt bzw. durch entsprechende Maßnahmen begleitet wird, müssen die rechtlichen Aspekte

[21] www.vubn.de.

des Einsatzes sozialer Medien und von „Open Data“[22] gleichermaßen berücksichtigt werden.

Bei der Presse- und Öffentlichkeitsarbeit und Informationstätigkeit handelt es überwiegend um eine **freiwillige Aufgabe** der öffentlichen Verwaltung. Daraus folgt, dass die Verlagerung auf andere Medien weitaus unkritischer sein dürfte als bspw. ausschließlich elektronisch durchführbare Verwaltungsverfahren.[23] Dennoch wird das Angebot in der Regel so auszugestalten sein[24], dass die relevanten Informationen auch über andere Kanäle verbreitet werden. **20**

10.2.5.2 Bürgerinformation und Bürgeranfragen

Soweit Social Media zur Bürgerinformation genutzt wird, kann dies die Bürgernähe und damit die Identifikation bspw. mit einer Kommune steigern. Die Abgrenzung zur Presse- und Öffentlichkeitsarbeit ist vielfach fließend. Der einfache, schnelle und ungefilterte **Rückkanal** des Bürgers zur Verwaltung kann eingesetzt werden, um Stimmungen auf- und konkrete Wünsche im Sinne eines zentralen Beschwerdemanagements entgegenzunehmen (Beispiel: Maerker Brandenburg[25]). Die Möglichkeit, mit dem Bürger in direkte Kommunikation einzutreten, ermöglicht es auch, neben allgemeinen Informationen konkrete Bürgeranfragen, soweit diese keinen Bezug zu einem Verwaltungsverfahren haben, bspw. zu Ansprechpartnern, Öffnungszeiten usw., zu beantworten. Insofern muss über geeignete organisatorische Maßnahmen vor allem die Richtigkeit der Informationen gesichert sein[26], sowie der Umgang mit eingehenden Anfragen zu Verwaltungsverfahren oder gar Anträgen geregelt werden. **21**

10.2.5.3 Fachlicher Diskurs

Fachlicher Diskurs meint die Teilnahme von Mitarbeitern der öffentlichen Verwaltung an öffentlichen Diskussionen zu Themenstellungen, die in ihren Geschäftsbereich und ihre konkrete Zuständigkeit fallen.[27] Er ist abzugrenzen von der Beantwortung von allgemeinen Bürgeranfragen, solchen mit Verfahrensbezug und **22**

---

[22] Dazu aus rechtlicher Perspektive Schulz, in: Dix et al., Jahrbuch für Informationsfreiheit und Informationsrecht 2012, S. 247 ff.; ders., VerwArch 104 (2013), 327 ff.; Hoffmann/Klessmann, VM 2011, 306 ff.; dies., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 41 ff.; Martini/Damm, DVBl 2013, 1 ff.; s. auch dies., NJW 2014, 130 ff.; Hofmann/Schulz, KommJur 2014, 126 ff.

[23] Dazu Hoffmann et al., Die Verwaltung 45 (2012), 207 ff.

[24] Vom rheinland-pfälzischen Landesdatenschutzbeauftragten explizit als Zulässigkeitsvoraussetzung für behördliche Facebook-Auftritte formuliert; vgl. http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013012401; dazu auch Rn. 49 ff.

[25] www.maerker.brandenburg.de.

[26] Dazu Rn. 84 f.

[27] Ausführlich Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (148 ff.).

der Presse- und Öffentlichkeitsarbeit, die der Pressestelle und/oder der Behördenleitung vorbehalten ist. In der Regel wird im Rahmen des fachlichen Diskurses darauf hinzuweisen sein, dass es sich nicht um eine abgestimmte „Hausmeinung", sondern eine vorläufige Einschätzung eines einzelnen Mitarbeiters handelt. Während es sachgerecht ist, die **dienstliche Kommunikation** über soziale Medien bspw. in einer Abteilung, die netzpolitische, internetbezogene Themen oder solche, die einen starken Bürgerbezug aufweisen (bspw. im Sozialbereich) oder diskursive Prozesse betreffen (z. B. Planungsabteilungen im kommunalen Bereich), bearbeitet, aktiv einzufordern, existieren in jeder Verwaltung auch Bereiche, für die sich dies weit weniger eignet (Zentralabteilungen, Abteilungen mit weitgehend internen Aufgabenstellungen etc.).

23 Der fachliche Diskurs dient, wie die reine Informationsbeschaffung, der Erweiterung der staatlichen Wissensbasis als Grundlage rationaler Entscheidungen.[28] Den Diskussionen in Foren, Blogs und sozialen Medien vergleichbar sind die aus der analogen Welt bekannten Formen des fachlichen Austauschs mit der Wissenschaft, Wirtschaftsvertretern, anderen Behörden und interessierten Bürgern auf Konferenzen, Vorträgen, Podiumsdiskussionen und Ähnlichem. Die Einbindung verschiedener gesellschaftlicher Gruppen, die bspw. von einem Gesetzgebungsverfahren oder einem administrativen Vorhaben betroffen sind, kann auch – insbesondere wenn sich dies ergänzend zu den formellen Beteiligungsverfahren vollzieht – als wesentlicher Teilaspekt des **Open Government**[29] verstanden werden, der insofern dazu dienen kann, einerseits die Akzeptanz behördlicher Entscheidungen zu verbessern, andererseits der Verwaltung neue Erkenntnisquellen zu erschließen. Die Verwaltung bekommt die Gelegenheit, relevante Themen bereits im Anfangsstadium zu erkennen, in bestehende Diskussionen einzusteigen und diese aktiv mitzugestalten. Ein weiterer Anwendungsfall sind Mitteilungen an die Öffentlichkeit, die nicht eine derart hohe Relevanz besitzen, dass die Einschaltung der Presseabteilung und die Erstellung einer Pressemitteilung geboten erscheint.

10.2.5.4 Online-Fahndung

24 Ein relativ neues Anwendungsfeld der Nutzung sozialer Medien zur Erfüllung öffentlicher Aufgaben ist der Einsatz zu Fahndungszwecken, insbesondere durch Polizeibehörden.[30] Hierbei werden Fahndungsaufrufe über soziale Netzwerke verbreitet. Während dies in der Anfangszeit noch unmittelbar im sozialen Netzwerk erfolgte, sind die Behörden, die dementsprechend aktiv sind, mittlerweile dazu übergegangen, lediglich **Links** zu posten und auf die eigene behördliche Online-Präsenz

---

[28] Zur Wissensgenerierung in der öffentlichen Verwaltung Kluth, in: Collin/Spiecker gen. Döhmann, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, S. 73 ff.
[29] Graudenz et al., Vom Open Government zur Digitalen Agora, ISPRAT-Whitepaper, 2010; abrufbar unter www.isprat.net; s. auch Janda, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 11 ff.; Schulz et al., in: Hill, Verwaltungskommunikation, S. 9 ff.
[30] Ausführlich zum Einsatz der Social Media zur Strafermittlung Esser, Kap. 7 Rn. 327 ff.

zu verweisen.[31] Dies hat den Vorteil, dass die – personenbezogenen – Daten auf den Servern der Behörde und damit in ihrem Einflussbereich verbleiben.

10.2.5.5 Online-Streife

Denkbar ist es auch, das Internet als Informationsquelle für staatliche Stellen und zur staatlichen Aufgabenerfüllung zu nutzen. Dies erfolgt vorrangig durch Polizei- und andere Sicherheitsbehörden.[32] In Betracht kommen dabei nicht nur offen zugängliche Websites, sondern zwangsläufig rücken auch die sozialen Netzwerke in den Mittelpunkt des Interesses, zumal diese einen **enormen Datenbestand** aus allgemeinen und personenbezogenen Daten, Fotos, Statusmeldungen, Beziehungsinformationen und vielem mehr bereit halten. Auch andere (kommunale) Behörden können soziale Netzwerke zur Beschaffung von Informationen für ihre tägliche Verwaltungsarbeit einsetzen. Selbst wenn derartige Fälle – soweit ersichtlich, zumindest in Deutschland – noch nicht bekannt geworden sind, scheint es nicht ausgeschlossen, dass Mitarbeiter in Jobcentern Informationen aus sozialen Netzwerken heranziehen, um die tatsächlichen Wohnverhältnisse der Leistungsempfänger oder nicht angegebene Arbeitsverhältnisse zu ermitteln. **25**

10.2.5.6 Social-Media-Monitoring/-Analytics

Angesichts der Tatsache, dass Verwaltungsthemen in vielen sozialen Medien diskutiert werden, auch wenn sich die öffentliche Verwaltung nicht selbst äußert, kommen der Beobachtung und Analyse der Stimmung in den sozialen Netzen erhebliche Bedeutung zu. Unter Social-Media-Monitoring ist die **systematische Sammlung und Filterung** relevanter, meist nutzergenerierter Inhalte im Web 2.0-Umfeld zu verstehen.[33] Texte, wie sie bspw. in Foren, Blogs oder Portalen von Bürgern oder Konsumenten verfasst werden, lassen sich bestimmten Themen zuordnen und in ihrer Tonalität (positiv, negativ, neutral usw.) einschätzen – etwa um Stimmungsbilder zu ermitteln. Social-Media-Monitoring wird in erster Linie von Unternehmen genutzt, um unmittelbare Meinungen, Kritik und Anregungen zu Produkten oder Dienstleistungen zu erhalten. Insofern ist die Situation in der öffentlichen Verwaltung aber vergleichbar. Um Social-Media-Monitoring zu betreiben, stehen sowohl kostenlose Werkzeuge als auch professionelle, kostenpflichtige Dienstleistungen zur Verfügung. Unternehmen, die diese Dienstleistung anbieten, konzipieren häufig zusätzliche Marketingmaßnahmen, die sich aus den Beobachtungen ableiten und zu einem positiveren Bild innerhalb von Social Media verhelfen sollen. **26**

---

[31] Roggenkamp, K&R 1/2013, Editorial.
[32] Ausführlich Schulz/Hoffmann, CR 2010, 131 ff.; dies., DuD 2012, 7 ff.
[33] S. auch Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 42 ff.

10.3 (Datenschutzrechtliche) Zulässigkeit der Nutzung von Social Media

27 Hinsichtlich der generellen Zulässigkeit des Einsatzes von Social Media durch die öffentliche Verwaltung ist zu differenzieren, ob die Behörde auf Dienste eines Dritten zurückgreift oder sein behördliches Internetangebot entsprechend weiterentwickelt. Letzteres ist in der Regel ohne größere Einschränkungen zulässig – es sind einerseits diejenigen Vorgaben zu beachten, die ganz allgemein für eine (behördliche) Homepage gelten, andererseits muss das konkrete „Web 2.0-typische" Verhalten, wie auch bei der Nutzung externer Dienste, rechtskonform ausgestaltet werden. Demgegenüber wird, insbesondere aufgrund einer datenschutzrechtlichen und technischen Analyse der Angebote von Facebook durch das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) im August 2011[34] und die damit verbundene Aufforderung an öffentliche Stellen und private Unternehmen (in Schleswig-Holstein), ihre Facebook-Auftritte einzustellen, die grundsätzliche Zulässigkeit der Nutzung sozialer Netzwerke durch die öffentliche Verwaltung kritisch diskutiert.[35] Die Ausführungen des ULD beziehen sich zwar lediglich auf die Dienste von Facebook, dennoch ist aufgrund vergleichbarer Funktionalitäten davon auszugehen, dass die rechtliche Bewertung anderer Dienste ähnlich ausfallen würde. Mit einer Entscheidung des OVG Schleswig vom 04.09.2014[36] hat die Debatte um **Facebook-Seiten** nunmehr einen vorläufigen Abschluss gefunden – es ist aber nicht absehbar, ob vergleichbare Dienste entsprechend von den Datenschutzbehörden angegriffen werden. Zudem vertreten das ULD und andere Datenschutzbeauftragte der Länder weiterhin ihre kritische Meinung zu den Facebook-Seiten; das ULD hat angekündigt, Revision zum BVerwG einzulegen und verweist darauf, dass die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Hinblick auf das Internet nicht ausreichend berücksichtigt werde und dass das Betreiben einer Fanseite ein rechtlich und technisch einheitlicher Vorgang ist, bei dem sich Betreiber und Facebook gegenseitig ergänzen und voneinander abhängig sind.[37] Der Fortgang des Verfahrens bleibt abzuwarten.

28 Während die Verlinkung aus sozialen Netzwerken auf eigene Inhalte außerhalb unproblematisch ist, ist der umgekehrte Verweis mit weiteren Rechtsfragen verbunden – vor allem, wenn auf der behördlichen Homepage Verlinkungsmechanismen genutzt werden, die vom Anbieter eines sozialen Netzwerks zur Verfügung gestellt werden.[38] Diese **Social Plugins** erfreuen sich immer größerer Beliebtheit; der bekannteste

---

[34] Karg/Thomsen, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook vom 19.08.2011, abrufbar unter www.datenschutzzentrum.de.

[35] S. auch Hoffmann et al., ZD 2013, 122 ff.

[36] OVG Schleswig, Urt. v. 04.09.2014, 4 LB 20/13; vorhergehend VG Schleswig, DuD 2014, 120 ff.; dazu Karg, ZD 2014, 54 ff.; Albrecht, jurisPR-ITR 24/2013 Anm. 6.

[37] Pressemitteilungen von 01.11.2013 (zur Einlegung der Berufung) und vom 29.09.2014 (zur Revision); abrufbar unter www.datenschutzzentrum.de.

[38] Dazu Rn. 89 ff.

dürfte der Gefällt-Mir-Button des Anbieters Facebook sein. Zu einer gerichtlichen Klärung ist es hier, anders als hinsichtlich der Fanseiten, bisher nicht gekommen.

10.3.1 Relevante Datenverarbeitungsprozesse

Soziale Netzwerke basieren auf der Idee, dass die **Interaktion** der Mitglieder dadurch ermöglicht wird, dass diese eine Profilseite anlegen. Für juristische Personen des privaten und des öffentlichen Rechts stehen bei Facebook sog. Fanseiten zur Verfügung. Im Gegensatz zu natürlichen Personen kann man mit diesen Seiten nicht „befreundet" sein, vielmehr wird man lediglich „Fan" der Seite. Dabei handelt es sich um eine einseitige Vernetzung, d. h. die privaten Nutzer können die Fanseite komplett einsehen und erhalten die neuesten Aktivitäten sowie Statusupdates der Seite angezeigt, die Seitenbetreiber (auch aus der öffentlichen Verwaltung) können lediglich die öffentliche Ansicht der Profile ihrer Fans sehen. **29**

Vom Anbieter bekommen Seitenbetreiber statistische Auswertungen zur Verfügung gestellt. So ist **„Facebook Insights"** ein kostenloses Analyse-Tool für die eigene Facebook-Fanseite. Es stellt detaillierte Statistikinformationen über die Nutzer zur Verfügung. So kann anhand der Statistik bspw. nachvollzogen werden, wie viele aktive Nutzer die Seite angeklickt haben und welchen Geschlechts und welchen Alters diese sind. Inhalte der Nutzer und personenbezogene Daten werden den Seitenbetreibern bei „Facebook Insights" nicht zur Verfügung gestellt, sondern lediglich anonymisiert. Eine Verknüpfung der Daten mit den Pseudonymen der Nutzer (den Facebook-Profilen) ist dem Seitenbetreiber nicht möglich. **30**

10.3.2 Anwendbarkeit deutschen Rechts

Die Anwendbarkeit des deutschen Datenschutzrechts im Sinne des BDSG sowie der datenschutzrechtlichen Vorschriften des TMG ist im Falle des Rückgriffs **deutscher Behörden** auf Fanseiten oder vergleichbare Dienste anderer Anbieter (mit Sitz außerhalb Deutschlands bzw. der Europäischen Union) gegeben. Sie und nicht der Bereitsteller des Netzwerks sind Betreiber der Fanseite und damit Gegenstand einer datenschutzrechtlichen Bewertung.[39] **31**

[39] Insofern muss auf die Frage der Anwendbarkeit des deutschen Rechts auf Facebook nicht eingegangen werden; dazu VG Schleswig, K&R 2013, 280 ff.; Piltz, K&R 2013, 283 f.; Karg, ZD 2013, 247 f.; Steinrötter, MMR 2013, 691 ff.

10.3.3 Verstoß gegen das TMG

32 Ob Behörden mit dem Anlegen einer Facebook-Seite (dies ist der einzig rechtlich relevante Anknüpfungspunkt[40]), verbunden mit der Möglichkeit, über den Dienst Facebook Insights statistische Daten zu nutzen, das deutsche Datenschutzrecht verletzen, ist strittig. Rechtlicher Maßstab ist vor allem das TMG, welches für Telemedien **bereichsspezifische datenschutzrechtliche Regelungen** enthält und deshalb vorrangig Anwendung findet (vgl. § 12 Abs. 1 TMG).[41] Es ist gem. § 1 Abs. 1 Satz 1 TMG auf alle Telemediendienste anwendbar. Dies gilt uneingeschränkt auch für öffentliche Stellen der Länder und Kommunen, unabhängig davon, ob für die Nutzung der bereitgestellten Dienste ein Entgelt erhoben wird oder nicht.[42]

10.3.3.1 Relevante Normen

33 Der Diensteanbieter hat gem. § 13 Abs. 1 TMG den Nutzer zu Beginn des Nutzungsvorgangs bspw. in allgemein verständlicher Form über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu unterrichten.[43] Gegen eine Nutzung von Fanseiten oder vergleichbarer Dienste externer Anbieter könnte daher der Umstand sprechen, dass die Behörde diesen Pflichten nicht (zumindest nicht vollständig) nachkommen kann, da sie weder maßgeblichen Einfluss auf die entsprechende Datenverarbeitung noch Kenntnis von den konkreten Prozessen hat. Zudem müsste sie gem. § 13 Abs. 4 TMG durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer die Nutzung des Dienstes jederzeit beenden kann, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden[44], und dass **Nutzungsprofile** nach § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

34 Nach § 15 Abs. 3 TMG darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer nicht widerspricht.[45] Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen. Derartige Nutzungsprofile dürfen nach § 15 Abs. 3 Satz 3 TMG aber nicht mit Daten über den Träger des

---

[40] So zutreffend das VG Schleswig, DuD 2014, 120 (121): „durch das Betreiben einer Fanpage bei Facebook als solches".
[41] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 12 TMG, Rn. 11 f.
[42] Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG, Rn. 13.
[43] Ausführlich zum Inhalt Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 13 TMG, Rn. 2 ff.
[44] Dazu Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 13 TMG, Rn. 8 ff.
[45] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG, Rn. 7 ff.

Pseudonyms zusammengeführt werden (**Trennungsgebot**). Gegen diese Regelung könnte die mit Facebook Insights verbundene sog. Reichweitenanalyse verstoßen.

10.3.3.2 Seitenbetreiber als Diensteanbieter i. S. d. TMG

Um Verstöße einer Behörde gegen die Pflichten aus §§ 13 und 15 TMG durch den Betrieb einer Fanseite oder eines vergleichbaren Profils feststellen zu können, muss daher geklärt werden, ob (auch) der Betreiber einer solchen Seite **Telemediendiensteanbieter** im Sinne des TMG ist. Telemedien sind gem. § 1 Abs. 1 Satz 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 RStV sind. Zur Ausfüllung des Begriffs wird vor allem auf Einzelbeispiele zurückgegriffen. Bspw. werden Weblogs unter den Begriff der Telemedien subsumiert[46], sodass eine Verwaltung, die einen Blog auf ihren eigenen Internetseiten betreibt, ein Impressum nach § 5 Abs. 1 TMG vorhalten muss. Gleiches gilt für behördliche Webseiten und andere im Internet verfügbare Inhaltsangebote.[47] **35**

Unproblematisch können die sozialen Netzwerke als Ganzes als Telemediendienst eingestuft werden[48], sodass die jeweiligen Betreiber – die Anwendbarkeit des deutschen Rechts vorausgesetzt – den Vorgaben des TMG unterliegen. Fraglich ist jedoch, ob einzelne Twitter-Profile, einzelne Tweets, Facebook-Seiten und vergleichbare **Auftritte von Behörden in den sozialen Netzwerken** bzw. im Web 2.0 als eigenständige Dienste eingestuft werden können.[49] Das VG Schleswig scheint dies zu bejahen[50], vertieft diese Fragestellung angesichts der fehlenden (Mit-)Verantwortlichkeit des Seitenbetreibers nicht. **36**

Dem Argument, dass eine restriktive Auslegung des Begriffs der Telemedien geboten sei, da diejenigen, die ein solches Profil einrichten, Nutzer eines Dienstes und gerade keine Anbieter seien, kann entgegnet werden, dass es durchaus möglich ist, dass ein Nutzer durch die Art und Weise der konkreten Nutzung selbst zum Anbieter eines weiteren Dienstes werden kann.[51] Vergleichbar ist die Rechtsprechung[52], dass sich Unterseiten einer Domain zu eigenständigen Telemedien entwickeln können.[53] Letztlich sind kaum Unterschiede zwischen einem Twitter-Profil, einer Facebook-Seite bzw. eines vergleichbaren Dienstes und einer herkömmlichen **37**

---

[46] Krieg, AnwZert ITR 10/2009, Anm. 3.
[47] Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG, Rn. 4.
[48] Krieg, AnwZert ITR 10/2009, Anm. 3.
[49] Krieg, AnwZert ITR 10/2009, Anm. 3.
[50] VG Schleswig, DuD 2014, 120 (121).
[51] Krieg, AnwZert ITR 10/2009, Anm. 3.
[52] OLG Frankfurt a. M., MMR 2007, 379 f.; OLG Hamm, MMR 2010, 29 f.; OLG Düsseldorf, MMR 2008, 682 f.
[53] Krieg, K&R 2010, 73 (74).

Behörden-Webseite zu erkennen.[54] Diese sind in der Regel hinsichtlich des Inhalts und des Erscheinungsbilds mit Facebook-Fanseiten vergleichbar. Auch die Nutzung ist weitgehend identisch. Profile in sozialen Medien lassen sich im Grundsatz als **ausgelagerte Behörden-Homepage** ansehen.[55] Eine wertende Betrachtung im Einzelfall[56] begründet daher in der Regel die Eigenschaft der Behörde, die mit Profilen und Seiten in den sozialen Netzwerken aktiv wird, als Anbieter von Telemediendiensten. Dies gilt in jedem Fall, wenn diese Profile mit dem Willen genutzt werden, durch die Gesamtheit der „Postings" und anderer Aktivitäten ein dauerhaftes inhaltliches Angebot zu schaffen.

38 Für die Anwendbarkeit des TMG auf derartige Behördenaktivitäten ist zudem erforderlich, dass die Mediendienste **geschäftsmäßig** angeboten werden. Ein Diensteanbieter handelt geschäftsmäßig, wenn er Telemedien aufgrund einer nachhaltigen Tätigkeit mit oder ohne Gewinnerzielungsabsicht erbringt. Ausgeschlossen werden aufgrund der fehlenden Nachhaltigkeit nur private Gelegenheitsgeschäfte.[57] Als nachhaltig ist eine Tätigkeit anzusehen, wenn sie auf einen längeren Zeitraum ausgerichtet ist und sich nicht auf einen Einzelfall beschränkt. Dies trifft in der Regel zu, wenn die öffentliche Verwaltung Twitter, Facebook oder einen Blog nutzt.

10.3.4 Verantwortlichkeit des Seitenbetreibers

39 Darüber hinaus müssten (auch) die Fanseiten- oder Profil-Betreiber aus der öffentlichen Verwaltung personenbezogene Daten verarbeiten – unzulässig wäre dies in der Form, dass entgegen § 15 Abs. 3 Satz 3 TMG zulässig erstellte **Nutzungsprofile** mit den Daten über den Träger des Pseudonyms zusammengeführt werden.

10.3.4.1 Diensteanbieter (TMG) und verantwortliche Stelle (BDSG)

40 Mit dem Begriff „Diensteanbieter" im Sinne des TMG ist hinsichtlich der Verarbeitung personenbezogener Daten **keine spezialgesetzliche Verantwortlichkeit** abweichend von dem Begriff der verantwortlichen Stelle gem. § 3 Abs. 7 BDSG bzw. Verantwortlicher im Sinne von Art. 2 d) der RL 95/46/EG geregelt worden.[58] Mangels spezieller Vorschriften zur datenschutzrechtlichen Verantwortlichkeit im TMG ist es daher sachgerecht, auf die allgemeinen Vorschriften des Datenschutzrechts zurückzugreifen.[59] Grundsätzlich genießt das TMG als bereichsspezifische Regelung zwar Anwendungsvorrang, wenn jedoch keine Vorschriften im TMG existieren, so kann

[54] Krieg, K&R 2010, 73 (77 f.).
[55] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (196 ff.).
[56] Krieg, AnwZert ITR 10/2009, Anm. 3.
[57] Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 5 TMG, Rn. 8.
[58] VG Schleswig, DuD 2014, 120 (121).
[59] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 12 TMG, Rn. 1.

lückenfüllend auf die allgemeinen Vorschriften des BDSG zurückgegriffen werden (vgl. auch § 12 Abs. 3 TMG). Die Vorschriften über die Auftragsdatenverarbeitung des § 11 BDSG und zur Verantwortlichkeit des § 3 Abs. 7 BDSG sind im Rahmen des § 15 Abs. 3 Satz 3 TMG also entsprechend anzuwenden.[60]

10.3.4.2 Unmittelbare eigene Verantwortlichkeit nach BDSG

Gem. § 3 Abs. 7 BDSG ist jede Person oder Stelle, die Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 11 BDSG), als verantwortliche Stelle zu qualifizieren. Verantwortlich ist, wer maßgeblich die inhaltlichen Entscheidungen über die **Art**, den **Umfang und** vor allem **Zweck der Datenverarbeitung** trifft.[61] Der Betreiber einer Fanseite oder eines vergleichbaren Profils in sozialen Netzwerken erhebt, verarbeitet oder nutzt die (personenbezogenen) Daten jedoch nicht selbst.[62] Der Nutzer einer Fanpage bei Facebook ruft unmittelbar eine Facebook-Seite auf, sodass personenbezogene Daten ausschließlich vom Nutzer direkt zu Facebook gelangen.[63] Der Betreiber einer Fanseite aus der öffentlichen Verwaltung kommt mit seinem operativen Instrumentarium in keinerlei direkten Kontakt zu dem Nutzer der Fanpage und dessen personenbezogenen Daten.[64] Soweit Facebook dem Seitenbetreiber aus der öffentlichen Verwaltung den kostenlosen Dienst „Insights" zur Verfügung stellt, handelt es sich lediglich um eine unabhängig von einem Auftrag ausgeführte statistische Auswertung der Nutzung der Fanpage mit dem Ergebnis anonymisierten Statistikmaterials.[65] **41**

10.3.4.3 Auftragsdatenverarbeitung

Weiterhin käme eine Auftragsdatenverarbeitung nach § 11 Abs. 1 Satz 1 BDSG in Betracht, für die der Auftraggeber, also der Fanseiten-Betreiber, verantwortlich bliebe. Das Auftragsverhältnis einer Auftragsdatenverarbeitung i. S. d. § 11 BDSG ist zwar an keine bestimmte Rechtsform gebunden[66], dennoch beauftragt die öffentliche Verwaltung den Betreiber eines sozialen Netzwerks durch den Nutzungsvertrag in der Regel nicht, für ihn Daten zu erheben und/oder zu verarbeiten.[67] Das für die Annahme eines Auftragsverhältnisses wesentliche Element eines vertraglichen **42**

[60] Piltz, CR 2011, 657 (662).
[61] Statt Vieler Gola/Schomerus, BDSG, § 32 Rn. 48 ff.
[62] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (182).
[63] VG Schleswig, DuD 2014, 120 (121).
[64] VG Schleswig, DuD 2014, 120 (121).
[65] VG Schleswig, DuD 2014, 120 (122).
[66] Spindler, in: Spindler/Schuster, Recht der elektronischen Medien, § 11 BDSG, Rn. 6.
[67] Ausführlich Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (182 f.).

Weisungsrechtes fehlt im Vertragsverhältnis zwischen Fanseitenbetreiber und Anbieter.[68] Die Entscheidung des Seitenbetreibers beschränkt sich auf die Annahme eines für ihn unabänderlichen Angebotes, die Fanpage einzurichten und mit Inhalten zu füllen oder nicht. Durch die Annahme dieses Angebotes und die Einrichtung einer Fanpage bestimmt er nicht Zweck und Mittel der Verarbeitung von personenbezogenen Daten der Nutzer der Fanpage.[69] Der Social-Media-Anbieter führt die Datenerhebungen vielmehr grundsätzlich und in eigenem Interesse durch, ohne dass der Fanseiten-Betreiber daran etwas ändern könnte. Er kann sich bloß entschließen, die ihm zur Verfügung gestellten anonymisierten Daten nicht zu nutzen. Von einem Auftrag, Daten für den Fanseiten-Betreiber zu verarbeiten, kann mithin keine Rede sein, da der Fanseiten-Betreiber keine Entscheidungsgewalt über die Datenerhebung besitzt. Eine Auftragsdatenverarbeitung setzt den Willen voraus, im fremden Namen zu handeln bzw. einen anderen zu beauftragen.[70] Des Weiteren werden dem Fanseiten-Betreiber das Ausmaß und der Umfang der Datenerhebung und -verarbeitung nur unzureichend bekannt sein, sodass er kaum steuernden Einfluss haben kann.

10.3.4.4 Gemeinsame Verantwortlichkeiten

43 Ein anderes Ergebnis lässt sich auch nicht mithilfe der Figur einer geteilten oder gemeinsamen datenschutzrechtlichen Verantwortlichkeit begründen.[71] Den maßgeblichen Arbeitspapieren **der Art. 29-Datenschutzgruppe** kann nur entnommen werden, dass (auch) im Rahmen von sozialen Netzwerken differenzierte Verantwortlichkeiten bestehen (können). Eine Zuordnung bestimmter Datenverarbeitungsprozesse zum Plattformbetreiber oder zum Nutzer ist nicht enthalten.[72] Ableitbar ist, dass allein die Nutzung eines sozialen Netzwerks, welches von einem Dritten betrieben wird, nicht zum Ausschluss jeglicher Verantwortlichkeit führt. Die Verantwortlichkeit für eigene Inhalte und selbst initiierte Datenerhebungen bleibt unverändert: „Das Datenschutzrecht hebt bei der Zuordnung der Verantwortlichkeit auf die einzelnen Verarbeitungsschritte bzw. Aktivitäten ab. Dies hat zur Folge, dass die Verantwortung nicht notwendigerweise gebündelt zu beurteilen ist, sondern je nach technischer und organisatorischer Gestaltung auf verschiedene Stellen verteilt sein kann. Möglich ist auch, dass die Verantwortlichkeit für einen konkreten Umgang mit Daten nicht umfassend besteht, sondern nur im Hinblick auf bestimmte Aspekte [. . .] In solchen Fällen ist die Verantwortlichkeit eingeschränkt, aber nicht aufgehoben“.[73] Bei der

---

[68] VG Schleswig, DuD 2014, 120 (122).
[69] VG Schleswig, DuD 2014, 120 (122); anders Polenz, VuR 2012, 207 ff.
[70] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (182).
[71] VG Schleswig, DuD 2014, 120 (122); ausführlich Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (182).
[72] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (184).
[73] Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein, Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social Plugins?, 30.09.2011, abrufbar unter www.datenschutzzentrum.de.

Fanseite besteht keinerlei Einfluss des Seitenbetreibers als Minimalbedingung auch einer gemeinsamen Verantwortlichkeit. Der Seitenbetreiber entscheidet mit dem Bereitstellen einer Fanpage bei in einem sozialen Netzwerk nicht gemeinsam mit dessen Betreiber über Zweck und Mittel der Verarbeitung von personenbezogenen Daten.[74] Diese werden ausschließlich vom Anbieter bestimmt.[75]

10.3.4.5 Rückgriff auf allgemeine Rechtsgrundsätze

Auch über andere – allgemeine – Rechtsgrundsätze außerhalb des Datenschutzrechts lässt sich keine (gemeinsame) Verantwortlichkeit der Seitenbetreiber konstruieren. Zutreffend gehen das OVG und VG Schleswig davon aus, dass die Verantwortlichkeit nicht durch den Rückgriff auf Zurechnungsnormen des Privatrechtes oder des allgemeinen Polizei- und Ordnungsrechtes ausgeweitet werden kann.[76] Damit scheiden Normen über die Störereigenschaft (ggf. mithilfe der Rechtsfigur des **Zweckveranlassers**) und zur deliktischen Mittäterschaft als Ansatzpunkte von vornherein aus. Zudem erscheint fraglich, ob deren Voraussetzungen überhaupt vorliegen. Eine Inanspruchnahme als Nichtstörer scheitert an den gesetzlichen hohen Hürden. **44**

10.3.4.6 Mittelbare Verantwortlichkeit als Korrektiv

Eine (unmittelbare) Verantwortlichkeit von Fanseiten- oder Profil-Betreibern aus der öffentlichen Verwaltung nach dem TMG und dem BDSG scheidet somit aus. Erforderlich ist eine **einzelfallbezogene Abgrenzung** zwischen der Verantwortlichkeit für nutzergenerierte Inhalte und der Verantwortlichkeit für die Plattform. Die besondere Verantwortung des Staates gebietet es jedoch – trotz der fehlenden unmittelbaren Verantwortlichkeit –, aus Rücksicht auf die beeinträchtigten personenbezogenen Daten zumindest eine Abwägung vorzunehmen, ob die Nutzung bestimmter Dienste vor diesem Hintergrund vertretbar ist.[77] **45**

Relevant für die rechtliche Einordnung der Fanseiten oder ähnlicher Angebote im Rahmen sozialer Medien ist deren tatsächliche Ausgestaltung und Funktionsweise. Ursprünglich basierte das Internet – und von diesem Grundverständnis geht insbesondere das TMG aus – auf einer Differenzierung zwischen der technischen Infrastrukturebene und den darauf angebotenen Diensten. Dies führte dazu, dass ein Homepage-Betreiber und damit auch Diensteanbieter im Sinne des TMG alle Datenverarbeitungsprozesse, die mit seiner Homepage verbunden waren, auch vollständig beherrschte (bzw. beherrschen konnte). Insofern war die Verantwortlichkeit, selbst **46**

---

[74] Zu Facebook VG Schleswig, DuD 2014, 120 (122).
[75] Zu Facebook VG Schleswig, DuD 2014, 120 (122).
[76] VG Schleswig, DuD 2014, 120 (122 f.).
[77] Auf diesen Ansatz, der zuvor in der Literatur entwickelt wurde, gehen weder das VG noch das OVG Schleswig ein; ausführlich dazu Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (185 ff.), dies., ZD 2013, 122 (124 f.).

wenn sich der Diensteanbieter eines Dritten bediente, letztlich ungeteilt. Durch die Social-Media-Plattformen ist aber eine **weitere Infrastrukturebene** hinzugetreten, die dazu führt, dass der Anbieter von Inhalten die Datenverarbeitungsprozesse nicht mehr allein gestaltet (gestalten kann bzw. gestalten muss).[78]

47 Diese **Ausdifferenzierung der Verantwortlichkeiten** muss bei der Auslegung der maßgeblichen Vorschriften Berücksichtigung finden. Lediglich für den Fall der inhaltlichen Entscheidung über die Art, den Umfang und den Zweck der Datenverarbeitung handelt es sich um eine unmittelbare Verantwortlichkeit im Sinne von TMG und BDSG, für alle anderen Prozesse allenfalls um eine mittelbare Verantwortung. Dies führt zu folgender ausdifferenzierter Betrachtungsweise:

- Der Nutzer eines sozialen Netzwerks, bspw. der Betreiber einer Fanseite oder eine Verwaltung, die ein Profil anlegt, erstellt eigene sog. nutzergenerierte Inhalte auf einer von einem Dritten bereitgestellten Plattform. Diesbezüglich besteht eine unmittelbare rechtliche Verpflichtung.
- Nehmen weitere Nutzer wiederum dieses Profil in Anspruch, indem dort bspw. Kommentare hinterlassen oder Fotos hochgeladen werden, besteht für den Betreiber eines Auftritts in den sozialen Netzwerken nur eine mittelbare Verantwortlichkeit – rechtlich konkretisiert durch die Vorschriften und insbesondere die Rechtsprechung zur Haftung für Fremdinhalte.[79]
- Und schließlich existiert die Plattform-Ebene des sozialen Netzwerks, für deren Verarbeitungsprozesse und Inhalte ein Nutzer aus der öffentlichen Verwaltung lediglich mittelbar verantwortlich ist. Eine unmittelbare Verantwortung nach deutschem oder europäischem Datenschutzrecht trifft ausschließlich den Plattformbetreiber selbst. Die mittelbare Verantwortlichkeit der öffentlichen Verwaltung bewirkt, dass der Einsatz von Plattformen, die über bestimmte rechtlich problematische Funktionalitäten oder Inhalte verfügen, ausgehend von allgemeinen Rechtsgrundsätzen nur aufgrund einer Abwägung der widerstreitenden Interessen legitimiert werden kann.

48 Diese Unterteilung zugrunde gelegt, lassen sich sachgerechte Ergebnisse erzielen, die sowohl rechtsstaatlichen Grundsätzen genügen als auch eine Überdehnung der Haftung der öffentlichen Stellen für Drittinhalte und -aktivitäten verhindern. Angesichts der Rechtsbindung der deutschen Verwaltung aus Art. 20 Abs. 3 GG und der **Schutzverpflichtung** gegenüber den Persönlichkeitsrechten der Nutzer muss analysiert werden, ob eine Nutzung von Diensten zugelassen werden kann, bei denen die öffentliche Verwaltung für bestimmte Datenverarbeitungen zwar nicht verantwortlich (im Sinne der deutschen Datenschutzregeln aus BDSG und TMG) ist, bei denen jedoch Gewissheit besteht, dass unzulässige Datenverarbeitungsprozesse – auch unter Rückgriff auf die von der öffentlichen Verwaltung nutzergenerierten Inhalte – seitens des (verantwortlichen) Betreibers initiiert werden. Da das derzeit geltende Recht keine Maßstäbe bereithält, anhand derer die Zulässigkeit der Nutzung beurteilt werden kann, verlagert sich die Diskussion auf eine andere Ebene. Es müssen

[78] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (185).
[79] Dazu Rn. 86 f.

allgemeine Rechtsgrundsätze beachtet und sichergestellt werden, dass deutsche Datenschutzvorgaben bei der Nutzung soweit wie möglich eingehalten werden, zugleich aber die grundsätzliche Nutzbarkeit nicht prinzipiell infrage gestellt wird. Letztlich muss die Nutzung dieser Angebote vor dem Hintergrund staatlicher Schutzpflichten vertretbar und verhältnismäßig sein. Deshalb bedarf es einer Abwägung von Risiko und Nutzen, die sowohl die seitens des Plattform-Betreibers beeinträchtigten Grundrechte der Nutzer als auch die entgegenstehenden Interessen der Fanseiten-Betreiber (öffentlicher Informationsauftrag) einbezieht. Die Nutzung lässt sich bspw. mit der besonderen Reichweite eines sozialen Netzwerks, gerade bei bestimmten Zielgruppen, mit bestimmten Funktionen und auch der Überlegung, dass die Nutzer sich (auch wenn die Einwilligung deutschen Datenschutz-Standards nicht genügt) freiwillig in dem sozialen Netzwerk bewegen, rechtfertigen.

10.3.5 Handlungsempfehlungen für die öffentliche Verwaltung

Ob bzw. inwieweit die Nutzung von sozialen Netzwerken durch die öffentliche Verwaltung unter datenschutzrechtlichen Aspekten zugelassen werden kann, lässt sich vor diesem Hintergrund und der bisher nicht abschließenden gerichtlichen Klärung nicht sagen. Das ULD hat gegen das Berufungsurteil des OVG Schleswig v. 04.09.2014 **Revision** eingelegt.[80] Es argumentiert, dass grundlegende Regelungen des deutschen Telemedienrechts nicht ausreichend beachtet werden, dass das Betreiben einer Fanseite ein rechtlich und technisch einheitlicher Vorgang ist, bei dem sich Betreiber und Facebook gegenseitig ergänzen und voneinander abhängig sind und insbesondere, dass das Urteil grundrechtliche Schutzpflichten des Staates für das Recht auf informationelle Selbstbestimmung im Hinblick auf das Internet ignoriert.[81] Insofern ist aber darauf hinzuweisen, dass eine staatliche Schutzpflicht von der dargestellten Ansicht nicht negiert wird, sondern als Faktor in eine Güterabwägung einbezogen wird. Mit welchen Maßnahmen der grundrechtlichen Schutz- und Gewährleistungspflicht seitens Gesetzgebung und Verwaltung nachgekommen wird, steht weitgehend in ihrem Ermessen. Die den Staat treffende Schutzpflicht sieht das BVerfG erst als verletzt an, „wenn die öffentliche Gewalt Schutzvorkehrungen überhaupt nicht getroffen hat oder die getroffenen Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen oder erheblich dahinter zurückbleiben".[82] Der Staat muss seine Pflichten mithin evident verfehlen.[83] Eine solche Konstellation ist hier nicht zu sehen. **49**

[80] Pressemitteilung v. 01.11.2013; abrufbar unter www.datenschutzzentrum.de.
[81] Umfassend zu staatlichen Schutzpflichten bei Internetsachverhalten Schliesky et al., Schutzpflichten und Drittwirkung im Internet.
[82] BVerfGE 88, 203 (263).
[83] Epping, Grundrechte, Rn. 121.

50 Andere Landesdatenschutzbeauftragte scheinen ebenfalls eine differenzierte Sichtweise zugrunde zu legen: Auch wenn die Facebook-Nutzung durch öffentliche Stellen überwiegend zwar nach wie vor für rechtswidrig gehalten wird, soll ein Einsatz unter bestimmten Prämissen tolerierbar sein.[84] Diese Sichtweise ist inkonsequent, dennoch enthalten die genannten Hinweise zur Art und Weise der zugelassenen Nutzung Elemente, die der zuvor dargestellten **Güterabwägung** entsprechen. Lässt sich vor diesem Hintergrund der Einsatz rechtfertigen, handelt die Behörde aber nicht rechtswidrig. Folgende handlungsleitende Faktoren sollten bei einer Prüfung, ob, in welchem Ausmaß und zu welchen Zwecken Social-Media-Angebote genutzt werden, berücksichtigt werden. Zudem kommt ggf. auch eine Differenzierung zwischen den unterschiedlichen Angeboten in Betracht – auch wenn die grundlegenden Datenverarbeitungsprozesse übereinstimmen dürften:

51 *Prüfung der **Erforderlichkeit***: Social Media darf nur eingesetzt werden, wenn dies für klar festgelegte, anders nicht erreichbare Zwecke und ggf. bestimmte Zielgruppen unabdingbar ist. Diese Forderung ist inhaltlich gleichbedeutend mit der dargestellten Abwägung zwischen Risiko und Nutzen, da ein Einsatz durch öffentliche Stellen vor dem Hintergrund staatlicher Schutzpflichten vertretbar und verhältnismäßig sein muss. Auch der staatliche Informationsauftrag ist ein Gut von Verfassungsrang[85], wobei Wertigkeit und Bedeutung nach Art der Behörde und ihrem Aufgabenprofil variieren können. Die Unabdingbarkeit der Nutzung wird sich in vielen Fällen mit der Tatsache begründen lassen, dass anders große Teile der Bevölkerung, insbesondere die sog. Digital Natives, nicht (mehr) erreicht werden können.

52 Welchen Hintergrund eine Güterabwägung besitzt, lässt sich bspw. im Kontext von **Katastrophenwarnungen** verdeutlichen. Social Media kann – vor allem aufgrund der „viralen" Verbreitung von Informationen – zur Bewältigung von besonderen Krisensituationen eingesetzt werden. Entsprechende Anwendungen, z. B. in Form mobiler und ortsbasierter Apps, bieten eine komfortable und oft kostengünstige Möglichkeit, einer besonderen Nachfrage – bspw. in Krisensituationen – zu begegnen und viele Personen zugleich zu erreichen. Wollte man nun die Nutzung aufgrund der datenschutzrechtlichen Bedenken nicht zulassen, bliebe der erzielbare Vorteil, ebenfalls für im Gemeinwohlinteresse stehende staatliche Aufgaben, unberücksichtigt. Gleiches kann auch im Bereich polizeilicher Tätigkeit gelten.

53 *Keine Nutzung sozialer Netzwerke in Kernbereichen der Verwaltung*: Die Datenschutzbeauftragten fordern, dass soziale Netzwerke nicht zur Durchführung hoheitlicher Maßnahmen oder zur Erbringung behördlicher Leistungen (über die Bereitstellung von Informationen hinaus) genutzt werden dürfen. Dem Grunde nach ist dieser Auffassung zuzustimmen, wobei die Abgrenzung des **„Kernbereichs"** kaum trennscharf gelingen wird. Selbstverständlich können über soziale Netzwerke keine rechtsverbindlichen Verwaltungsverfahren abgewickelt oder Anträge gestellt

---

[84] Vgl. bspw. die vom rheinland-pfälzischen Landesdatenschutzbeauftragten formulierten einschränkenden Voraussetzungen http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013012401.

[85] Exemplarisch BVerfGE 105, 252 ff.; s. auch Rn. 93 f.

werden. Vielmehr dürfte sich der Einsatz auf eine zeitgemäße und effektive Presse- und Öffentlichkeitsarbeit, fachlichen Diskurs oder allgemeine Bürgerinformationen beschränken. Die Information in Krisenfällen, im Rahmen der Gefahrenabwehr oder zu Fahndungszwecken ließe sich aber auch dem Kernbereich zuordnen; eine generelle Unzulässigkeit dieser Einsatzformen kann – bspw. bei Beachtung der Grenzen der Öffentlichkeitsfahndung[86] – aber nicht angenommen werden.

Datenschutzhinweise und Impressum: Nutzer sollten zudem darauf hingewiesen **54**
werden, in welchem Umfang ihre Daten durch die Netzwerkanbieter verarbeitet werden. Auch wenn sich diese Forderung in der Praxis oftmals aufgrund der Unkenntnis über die genauen Datenerhebungen der Netzwerkanbieter kaum vollständig umsetzen lassen wird, bedarf es eines derartigen Hinweises. Er sollte – auch wenn nicht unmittelbar gesetzlich vorgeschrieben – den gleichen Kriterien folgen wie das erforderliche Impressum, also leicht erreichbar sowie einfach und verständlich formuliert sein.[87] In diesem Zusammenhang müssen immer die Veränderungen der eingesetzten Dienste durch den Anbieter verfolgt werden, um **Datenschutzhinweise** anzupassen oder bspw. eine leichtere Erreichbarkeit zu sichern.[88]

Keine Inhalte ausschließlich in Social Media: Die Datenschutzbeauftragten wei- **55**
sen darauf hin, dass durch die Bereitstellung exklusiver Informationen Bürger faktisch gezwungen werden könnten, sich in einem sozialen Netzwerk anzumelden.[89] Zu beachten ist aber, dass es sich zumindest bei Presse- und Öffentlichkeitsarbeit und bestimmten Informationstätigkeiten um freiwillige Aufgaben bzw. **zusätzliche Services** der öffentlichen Verwaltung handelt. Auch wenn es daher denkbar und zulässig erscheint, bestimmte Angebote ausschließlich in sozialen Medien zu platzieren, dürfte der Forderung, keine Inhalte ausschließlich in den sozialen Medien zu veröffentlichen, in der Verwaltungspraxis weitgehend entsprochen werden. Soweit mit vertretbarem Ressourceneinsatz realisierbar, kommt auch die Nutzung verschiedener Social-Media-Dienste in Betracht.

Brückenfunktion von Social Media: Um möglichst wenig Nutzerdaten entstehen **56**
zu lassen, sollen nach den Empfehlungen der Datenschutzbeauftragten in den sozialen Netzwerken möglichst wenig **Inhaltsinformationen** bereitgestellt werden. Diese sollten auf den behördlichen Internetauftritten zur Verfügung stehen, auf die aus den sozialen Netzwerken verlinkt werden kann. Zurückhaltung mag zwar bei bestimmten sensiblen Daten geboten sein, die unter staatlicher „Herrschaft" gehalten werden müssen (bspw. im Kontext von Fahndungsmaßnahmen im Internet), eine generelle Zurückhaltung würde aber den Einsatz grundsätzlich infrage stellen. Da die Güterabwägung, die einem Einsatz voranzugehen hat, auch Umfang und Art der zu veröffentlichenden Daten einbeziehen muss, ergibt sich bereits ein ausreichendes Korrektiv gegenüber allzu extensiven Auftritten in den sozialen Medien.

---

[86] Dazu Rn. 95 f.
[87] Dazu Rn. 79.
[88] Vgl. dazu, ob es bspw. ausreichend ist, das Impressum unter „Info" bzw. „Kontakt" zu verlinken, ebenfalls Rn. 78 f. mit weiteren Nachweisen.
[89] Zu diesem Aspekt ausführlich Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (190).

57 *Verlagerung des Dialogs auf datenschutzgerechte Kanäle*: Lebensfern erscheinen die Forderungen der Datenschutzbeauftragten, innerhalb des sozialen Netzwerks nicht auf Fragen und Kommentare der Nutzer zu antworten (sog. **Rückkanalverbot**). Das Verbot ist nicht zielführend, konterkariert es doch den besonderen Zusatznutzen, den die sozialen Netzwerke im Vergleich zu reinen Informationsdiensten haben. Der Verweis auf behördliche Foren ist einerseits mit erheblichen Zusatzaufwand verbunden, andererseits wollen die Bürger dort kommunizieren, wo sie ohnehin präsent sind, und nicht weitere – behördliche – Dienste nutzen.

58 Gleiches gilt für die Förderung datenschutzfreundlicher Netzwerke. Angesichts mangelnder Angebote dieser Art steht die Verwaltung vor der Herausforderung, die knappen Zeitressourcen auf solche Netzwerke zu beschränken, mit denen eine Vielzahl der Nutzer erreicht werden können. Diese entsprechen jedoch derzeit vielfach nicht dem deutschen Datenschutzrecht. Ähnlich kritisch ist der **Aufbau eigener sozialer Netzwerke** für die öffentliche Verwaltung zu sehen; auch hier stellt sich die Frage, ob man ausreichend Nutzer motiviert, ein weiteres internes Profil anzulegen, zu pflegen und aktiv am Netzwerk zu partizipieren.

10.4 Vorgaben für die behördliche Nutzung

59 Soweit sich eine öffentliche Verwaltung grundsätzlich für die Nutzung von Social Media bzw. einzelner Anwendungen oder für bestimmte Zielsetzungen entschieden hat, müssen im Rahmen der Umsetzung dieser Entscheidung zahlreiche Rechtsfragen betrachtet werden. Hinsichtlich der Vorgaben für die behördliche Nutzung kann zwischen Regeln, die für alle Behörden, insbesondere die „allgemeine Verwaltung", gleichermaßen gelten und den spezifischen Anforderungen, bspw. für Polizei- und Sicherheitsbehörden, oberste Landesbehörden, Sozial- und Jugendämter sowie Mandatsträger, differenziert werden. Angesichts der kurzen Innovationszyklen handelt es sich um ein Rechtsgebiet, welches sich ständig verändert. Insofern ist es zielführend, die technischen Entwicklungen und Veränderungen der Dienste aufmerksam zu beobachten. Zur Ermittlung der relevanten Aspekte erscheint es zielführend, sich den **Lebenszyklus** der Nutzung, beginnend bei der Auswahlentscheidung (vorgelagert noch die strategische Entscheidung, überhaupt zu nutzen) über den Vertragsschluss, das Agieren im Netz bis hin zur Einstellung der Aktivitäten zu betrachten. Zudem kann als handlungsleitende Grundaussage gelten, dass die nutzer- (also behörden-) generierten Inhalte, die gerade das Charakteristikum von Social Media darstellen, im Zweifel als ausgelagerte Behördenhomepage zu behandeln sind.

60 Neben gesetzlichen Vorgaben existieren zum Teil **interne Regelwerke**, in Form von Dienstvorschriften, Betriebsvereinbarungen, Verwaltungsvorschriften und Ähnlichem, die sich zum Teil mit den gesetzlichen Vorgaben überschneiden und diese untergesetzlich konkretisieren. Sie können Regelungen sowohl zum behördlichen bzw. dienstlichen als auch zum privaten Einsatz von Social Media durch Beamte und Mitarbeiter der öffentlichen Verwaltung enthalten. In Betracht kommen:[90]

[90] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (194 f.).

- Regelungen zum Umgang mit Presseanfragen und zur Öffentlichkeitsarbeit im Allgemeinen,
- weitere Vorgaben der Geschäftsordnungen zum Umgang mit Bürgeranfragen, zur Frage, welcher Mitarbeiter – bspw. bei der klassischen Schriftkommunikation – nach außen auftritt und zeichnet, wie Adressaten außerhalb der Verwaltung anzusprechen sind oder Ähnliches,
- Geheimschutzordnungen,
- datenschutzrechtliche Regelungen zum Umgang mit personenbezogenen Daten,
- Informationspflichten aus dem TMG, dem Rundfunkstaatsvertrag oder eine verwaltungsinterne Konkretisierung dieser Pflichten,
- „Styleguides", also Vorgaben, die die äußere Gestaltung behördlicher Kommunikation, z. B. die Verwendung von Wappen und Logos, betreffen,
- Vorgaben zur privaten Nutzung des Internets[91],
- zur barrierefreien Gestaltung von Internetauftritten,
- über Werbung[92] und Sponsoring[93] sowie
- allgemein die bestehenden Regelungen zum IT-Einsatz, insbesondere auch zur IT-Sicherheit und zum Einsatz eigener Endgeräte (Stichwort: „bring your own device").

---

[91] Dazu auch Rn. 122.

[92] Ausführlich Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 99 f., wobei diesbezüglich auf eine Besonderheit hinzuweisen ist, die von den existenten Vorgaben zur „Werbung" nicht hinreichend berücksichtigt wird (bzw. werden konnte): „Besondere Aufmerksamkeit erfordert die Prüfung der Einhaltung der Werbegrundsätze bei Social Media Auftritten der Verwaltung dann, wenn die Werbung durch Dritte (z. B. facebook) geschaltet wird und der Inhalt der Werbung somit außerhalb des Einflussbereichs der Hamburgischen Verwaltung liegt. Gerade bei den überwiegend kostenlosen Social Media Tools ist das Platzieren von Werbung ein wichtiger Refinanzierungsfaktor für die Toolbetreiber. Nicht selten werden dabei Methoden intelligenter Werbung eingesetzt, die einen Zuschnitt speziell auf den Account-Inhaber und/oder auf seine Kontakte ermöglichen (sogenannte personalisierte Werbung). Vor dem Hintergrund der Werbegrundsätze wäre dies zum Beispiel dann bedenklich, wenn aufgrund derartiger Werbemethoden ein offenkundiger Bezug zwischen Werbung und behördlichen Inhalten hergestellt wird. Weil bei Werbung durch Dritte die Verwaltung nicht agieren, sondern nur reagieren kann, empfiehlt es sich, die Werbemaßnahmen genau zu beobachten, um dann gegebenenfalls unverzüglich und adäquat reagieren zu können (z. B. Upgrade auf kostenpflichtigen und werbefreien Account). Notfalls muss auf die Nutzung eines Tools verzichtet werden, wenn die Platzierung inhaltlich unzulässiger Werbung (s. o.) nicht verhindert werden kann." Unter Bezugnahme auf die Argumentation zur datenschutzrechtlichen Zulässigkeit des Einsatzes von Social Media ist jedoch zu beachten, dass die Werbung nicht Teil der Behördenseite wird, sondern „daneben" als Bestandteil der Plattform eingeblendet wird (wie im Übrigen auch zahlreiche andere Informationen), sodass die Behörde nicht unmittelbar verantwortlich wird, da sie diesen Teil gar nicht ausgestalten kann. Insofern gelten die obigen Grundsätze entsprechend. Daneben sind aber auch Fälle denkbar, in denen die Behörde selbst Einfluss nehmen kann und daher unmittelbar an die bisherigen Grundsätze gebunden ist. So ist es einer „Facebook-Seite" möglich, nach außen zu erkennen zu geben, dass ihr (also der Behörde) bestimmte andere Facebook-Seiten „gefallen", was eindeutig als Werbung (für die entsprechenden anderen Facebook-Seiten bzw. das dahinter stehende Unternehmen) zu klassifizieren ist; allgemein zur Werbung auf behördlichen Internet-Auftritten Frevert/Wagner, NVwZ 2011, 76 (79).

[93] Dazu Rn. 92.

10.4.1 Rechtliche Vorgaben für die Auswahlentscheidung

61 Ist die Nutzung bestimmter Social-Media-Dienste – vor allem datenschutzrechtlich – zulässig, stellt sich die Frage, nach welchen Kriterien die Auswahl eines Angebots erfolgt, wenn damit zugleich eine Beeinträchtigung der Rechte der Mitbewerber einhergehen könnte. Aus Kapazitätsgründen und aufgrund begrenzter Ressourcen wird es nicht möglich sein, alle denkbaren Kanäle gleichermaßen zu bedienen, da ohnehin zusätzlich der eigene behördliche Internetauftritt gepflegt werden muss. Wird ein transparentes **Auswahl- bzw. Vergabeverfahren** durchgeführt, sind die Anforderungen, die aus dem verfassungsrechtlichen und einfachgesetzlichen Wettbewerbsrecht ableitbar sind, in jedem Fall gewahrt.

10.4.1.1 Gleichheitssatz und Wettbewerbsfreiheit

62 Nicht berücksichtigten Anbietern von Social-Media-Diensten, die dem ausgewählten Dienst vergleichbar sind, steht grundsätzlich ein Abwehranspruch gegenüber begünstigenden hoheitlichen Maßnahmen (also bspw. auch einer Auswahlentscheidung) zu, wenn diese einen nicht gerechtfertigten Eingriff in die grundrechtlich geschützte Wettbewerbsfreiheit als „die Freiheit der Teilhabe am Markt nach Maßgabe seiner Funktionsbedingungen“[94] (aus Art. 12 GG i. V. m. Art. 14 GG bzw. Art. 2 Abs. 1 GG i. V. m. Art. 3 Abs. 1 GG)[95] darstellen.[96] Ein Eingriff liegt aber nur dann vor, wenn es der öffentlichen Hand auf eine Veränderung des Konkurrenzverhältnisses unmittelbar ankommt oder die Wettbewerbsnachteile in ihren tatsächlichen Auswirkungen so schwerwiegend sind, dass von einem Grundrechtseingriff gesprochen werden muss.[97] Maßgeblich sind also die Kriterien des mittelbaren Grundrechtseingriffs: Intention, Intensität, Typizität.[98] Es ist davon auszugehen, dass selbst eine intensive Nutzung durch Bundes-, Landes- oder Kommunalbehörden nicht dazu geeignet sein dürfte, hinreichend schwerwiegende Wettbewerbsnachteile für die Konkurrenten hervorzurufen[99], selbst wenn der Dienst durch die Nutzung durch die öffentliche Verwaltung einen **„Nimbus der Seriosität“** für sich beanspruchen kann.[100]

63 Aufgrund des verfassungsrechtlichen Gleichheitssatzes ist die öffentliche Hand verpflichtet, nicht nur bei hoheitlichem Handeln, sondern auch im Bereich der fiskalischen Hilfsgeschäfte (z. B. beim Abschluss von zivilrechtlichen Verträgen)

---

[94] BVerfGE 105, 252 (265).
[95] Zu Rechtsgrundlage und Reichweite Schliesky, Öffentliches Wirtschaftsrecht, S. 99.
[96] Allgemein zur Wettbewerbsfreiheit statt Vieler Di Fabio, in: Maunz/Dürig, GG, Art. 2 Abs. 1 Rn. 116 ff.
[97] Frevert/Wagner, NVwZ 2011, 76 (80).
[98] Dazu statt Vieler BVerfGE 105, 252 (273) zum „funktionalen Äquivalent eines Eingriffs“; 105, 279 (300 f.) zur „mittelbar-faktischen“ Grundrechtsbeeinträchtigung; Lübbe-Wolff, Die Grundrechte als Eingriffsabwehrrechte: Struktur und Reichweite der Eingriffsdogmatik im Bereich staatlicher Leistungen, S. 25 ff.; Gallwas, Faktische Beeinträchtigungen im Bereich der Grundrechte, S. 49 f.
[99] Frevert/Wagner, NVwZ 2011, 76 (80).
[100] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).

verschiedene Anbieter nicht ohne sachlichen Grund ungleich zu behandeln.[101] Der Anbieter eines ebenfalls kostenlosen Angebots könnte sich benachteiligt fühlen, weil die Verwaltung für ihren Social-Media-Auftritt nicht seinen Dienst, sondern jenen eines Mitbewerbers öffentlichkeitswirksam einsetzt. Als sachlicher Grund einer Ungleichbehandlung können u. a. die besondere Reichweite eines Angebots, bestimmte erforderliche Funktionen, der Umgang mit personenbezogenen Daten der Nutzer, die Kosten des Dienstes oder für Premiumfunktionen dienen. Insofern sind die Auswahlkriterien, die einem einfachrechtlich notwendigen Vergabe- oder Auswahlverfahren zugrunde liegen (bzw. diejenigen, die ausnahmsweise einen Verzicht auf ein solches rechtfertigen), zugleich **sachlicher Grund** im Rahmen des Art. 3 Abs. 1 GG.

10.4.1.2 Wettbewerbsrecht

Die Anwendbarkeit des UWG auf einen behördlichen Auftritt in sozialen Netzen setzt voraus, dass mit dem Vertragsschluss eine geschäftliche Handlung i. S. d. § 2 Abs. 1 Nr. 1 UWG einhergeht. Darunter ist jedes Verhalten einer Person zugunsten des eigenen oder eines fremden Unternehmens bei oder nach einem Geschäftsabschluss zu verstehen, das mit der Förderung des Absatzes von Waren oder Dienstleistungen objektiv zusammenhängt.[102] Der Umstand, dass die Behörde mit ihrem Auftritt eine allgemeine öffentliche Aufgabe erfüllt, schließt die Anwendung des Wettbewerbsrechts nicht aus.[103] Allerdings ist das Vorliegen einer geschäftlichen Handlung fraglich: Dass es durch einen Behördenauftritt in einem sozialen Netzwerk zu einem Anstieg der Neuregistrierungen bei diesem Anbieter kommen wird, erscheint eher unwahrscheinlich. Der Anbieter kann sich lediglich einer besonderen **Vertrauenswürdigkeit und Attraktivität** rühmen.[104] **64**

Allerdings führt erst die **Zielgerichtetheit** des Handelns zu einer unlauteren Behinderung. Die Behörde ist gehalten, das wettbewerbsrechtliche Gebot der Neutralität und Objektivität zu beachten. Wenn die öffentliche Verwaltung sich bspw. ausschließlich für das soziale Netzwerk mit der größten Anzahl an privaten Nutzern oder bestimmten Funktionen[105] entscheidet, ist dies Folge des Wettbewerbs und keine zielgerichtete Behinderung eines anderen Anbieters. Insbesondere wenn kein Vergabeverfahren vorab durchzuführen war, muss die Auswahlentscheidung aber aufgrund sachlicher Kriterien und aufgrund eines transparenten Verfahrens erfolgen. **65**

---

[101] Zur Geltung des Gleichheitsgrundsatzes bei fiskalischen Hilfsgeschäften statt Vieler Osterloh, in: Sachs, Grundgesetz, Art. 3 Rn. 76.

[102] Hasselblatt, in: Götting/Nordemann, UWG Handkommentar, § 4 UWG Rn. 3.15.

[103] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (192). Zu einem anderen Ergebnis kommen Frevert/Wagner, NVwZ 2011, 76 (81), die das früher einschlägige subjektive Merkmal der „Wettbewerbsförderungsabsicht" prüfen und verneinen.

[104] Frevert/Wagner, NVwZ 2011, 76 (80); Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.), spricht vom „Nimbus der Seriosität".

[105] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 97.

10.4.1.3 Vergaberecht

66 Auch wenn die Nutzung eines sozialen Netzwerks kostenlos ist, kommt es zu einem Vertragsschluss, sodass zu prüfen ist, ob mit dem Vertragsschluss vergaberechtlich relevante Leistungsbeziehungen zwischen der öffentlichen Verwaltung und dem Anbieter entstehen.[106] Hierzu müsste es sich um einen entgeltlichen Vertrag im Sinne des Vergaberechts handeln. Dies setzt nicht zwingend eine Geldleistung voraus; auch andere geldwerte Gegenleistungen, bspw. die Einräumung von Verwertungsrechten, können dieses Merkmal erfüllen.[107] Ein Entgelt kann in der Überlassung von Gütern durch den öffentlichen Auftraggeber liegen, durch deren Verwertung der Auftragnehmer Einnahmen erzielt.[108] Die Möglichkeit des Anbieters, Nutzerdaten zu erheben und für eigene Zwecke einzusetzen, könnte als ein solches Verwertungsrecht angesehen werden. Allerdings ist der (behördliche) Nutzungsvertrag nicht als Überlassung eines **Erhebungs- und Verwertungsrechts** von Daten zu sehen, da die Betreiber die Daten in der Regel nicht an Dritte veräußern, sondern hauptsächlich mit gezielter Werbung Einnahmen generieren. Zudem fehlt es der eine Fanseite oder ein anderes Profil betreibenden Verwaltung an einem Recht, über „Drittdaten" zu verfügen. Die Anzahl der insgesamt vorhandenen Profile und Seiten kann die Einnahmen zwar erhöhen. Dennoch werden die Einnahmen nicht durch die einzelne Seite, sondern durch das Bestehen des Angebots als Ganzes erzielt.[109]

67 Die Entgeltlichkeit ist in jedem Fall anders zu beurteilen, wenn es sich bei den genutzten Diensten um sog. **Premiumangebote** mit Zusatzleistungen zu den kostenfreien Nutzungsmöglichkeiten handelt, die mit einem Aufpreis verbunden sind.[110] In diesem Fall wäre der Vertrag als entgeltlich einzustufen, grundsätzlich vergabepflichtig, wobei die weitere Behandlung abhängig vom Auftragswert ist. Ein Vergabeverfahren kann allenfalls entbehrlich sein, wenn aus bestimmten Gründen (bspw. erforderliche Funktionalität, angestrebte Zielgruppe) nur ein privatwirtschaftliches Angebot in Betracht kommt.[111]

68 Hinzu kommt, dass der Social-Media-Anbieter, der die Verwaltung unentgeltlich mit seinen Diensten unterstützt und sich davon eine Werbewirkung erhofft, ggf. ein **Verwaltungssponsoring** vornimmt.[112] Die Nutzung solcher Angebote erfüllt zwar nicht die tatbestandlichen Voraussetzungen einer Dienstleistungskonzession. Denn die Behörde kann und will dem privaten Dritten kein ausschließliches Nutzungsrecht zur Datennutzung verleihen. Beide Fälle sind aber wertungsmäßig vergleichbar.[113]

---

[106] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96.
[107] Zum Begriff der Entgeltlichkeit ausführlich Dreher, in: Immenga/Mestmäcker, Wettbewerbsrecht, Bd. 2: GWB, § 99 GWB, Rn. 20 ff. Relevant ist dies vor allem im Kontext der Dienstleistungskonzessionen; dazu ausführlich Ruhland, Die Dienstleistungskonzession, 2006.
[108] BGHZ 162, 116 ff.
[109] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (170).
[110] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96 f.
[111] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (171).
[112] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).
[113] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).

Im Hinblick auf die bestehende Regelungslücke ist daher eine analoge Anwendung der für Dienstleistungskonzessionen geltenden Vorschriften gerechtfertigt. Es besteht daher wie bei der Vergabe von Dienstleistungskonzessionen grundsätzlich keine Ausschreibungspflicht; es sind aber die unionsrechtlichen Grundfreiheiten sowie das Diskriminierungsverbot zu beachten und eine hinreichende öffentliche Transparenz zu wahren.[114] Die Auswahl der Anbieter muss insbesondere sachgerechten Auswahlkriterien folgen.[115]

10.4.2 Zustandekommen eines Nutzungsvertrages zwischen Behörde und Anbieter

Die Auswahlentscheidung muss durch einen Vertragsabschluss umgesetzt werden. **69**
Dabei gelten die allgemeinen Grundsätze, vor allem zur Frage, wer befugt ist, für die Behörde und in ihrem Namen zu handeln und so die Behörde (bzw. ihren Rechtsträger) wirksam gegenüber Dritten zu verpflichten. Diese Kompetenz steht in der Regel originär der Behördenleitung, anderen Mitarbeitern nur abgeleitet im Rahmen ihrer Vollmacht zu. Handelt der Mitarbeiter bei der Eröffnung eines Accounts im Auftrag seines Dienstherrn, ist dieser Vorgang (und nicht erst die Erstellung des behördlichen Auftritts) als **Vertragsschluss** zwischen der Behörde (bzw. ihrem Rechtsträger) und dem Betreiber eines sozialen Netzwerks anzusehen. Sind behördliche Profile zwingend mit einem privaten Account (eines Mitarbeiters) verknüpft, wird die Seite (bzw. genauer die Administrationsrechte) von diesem Mitarbeiter treuhänderisch verwaltet – was bedeutet, dass mit dem Ende des Arbeitsverhältnisses ein Herausgabeanspruch des Dienstherrn existiert.[116] Insofern besteht eine Parallele zur Herausgabe von Internet-Domains: Bei treuhänderischer Registrierung richtet sich der Herausgabeanspruch des Treugebers aus § 667 BGB auf Übertragung oder Umschreibung des Domainnamens.[117] Wird ein privater Account erst zu einem späteren Zeitpunkt auch für dienstliche Zwecke eingesetzt, stellt der Mitarbeiter seine ohnehin vorhandene private Infrastruktur zur Verfügung – die Vertragspartner des ursprünglichen Vertrages bleiben aber unverändert.

Der **Benutzer- oder Profilname** ist beim Anlegen eines Auftritts in den sozialen **70**
Netzwerken grundsätzlich frei wählbar. Es existieren kaum verifizierte Identitäten, sodass in der Regel nicht sicherzustellen ist, ob sich hinter einem Account mit dem Namen einer Stadt auch die Stadtverwaltung verbirgt. Soweit (ebenfalls kostenfrei) möglich, sollte die öffentliche Verwaltung auf sog. *verified accounts* zurückgreifen. Aufgrund des Prioritätsprinzips empfiehlt es sich zudem, Accounts für die jeweilige

---

[114] Wegener, in: Pünder/Schellenberg, Vergaberecht, § 99 GWB, Rn. 51 ff.
[115] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).
[116] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (169); dazu ausführlich Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 52 ff.; s. auch Ulbricht, Social Media und Recht, S. 225 ff.
[117] BGH, NJW 2010, 3440 f.; dazu Terhaag, K&R 2010, 662 f.

Verwaltung schon anzumelden, wenn noch keine konkreten Pläne bestehen, einen Dienst in nächster Zeit aktiv zu nutzen.[118] Bei der Wahl des Account-Namens sind darüber hinaus zum Teil Vorgaben des jeweiligen Social-Media-Anbieters zu berücksichtigen, die dieser im Rahmen seiner Nutzungsbedingungen macht. So sind bei Facebook generische Seitennamen für Orte (d. h. reine geografische Ortsbezeichnung von Städten, Regionen etc.) nicht erlaubt (bspw. „Berlin", „Stadt Berlin", „Land Berlin"; zulässig hingegen: „Stadtverwaltung Berlin").

71 Wird die öffentliche Verwaltung durch einen anderen Nutzer durch sog. **Grabbing**[119], d. h. das Reservieren des entsprechenden Account-Namens eines Konkurrenten oder mit der Zielsetzung der Gewinnerzielung, in ihren Namensrechten verletzt, ist eine Abmahnung möglich. Unterlassungsansprüche folgen für Gemeindenamen, die im geschäftlichen Verkehr genutzt werden, aus §§ 5, 15 MarkenG[120] sowie aus § 12 BGB. Sie können aber nur durchgesetzt werden, wenn die Identität des Störers ermittelt werden kann, was in der Regel kaum gelingen dürfte, da die Nutzer nicht verifiziert werden. Denkbar ist daher auch ein Vorgehen gegen den Betreiber der Social-Media-Plattform, da dieser bei Kenntnis der Rechtsverletzungen haftbar gemacht werden kann (sog. Notice-and-take-down-Prinzip[121]).

10.4.2.1 Rechtsnatur des Vertrages

72 Der Nutzungsvertrag über einen Social-Media-Dienst ist nicht formgebunden. Der Vertragsschluss muss daher nicht ausdrücklich erfolgen, sondern kann sich auch konkludent durch Eröffnen eines Kontos, durch Herunterladen der zum Betrieb erforderlichen Software oder durch bloße Nutzung vollziehen.[122] Die vertragstypologische Einordnung hängt davon ab, ob die Nutzung **entgeltlich oder kostenlos** erfolgt.

73 Das Leistungspaket sozialer Netzwerke besteht in der Regel aus verschiedenen Komponenten. Neben der Möglichkeit, mit anderen Nutzern innerhalb des Netzwerks durch Nachrichten zu kommunizieren, geht es vor allem darum, auf der Plattform eigene Inhalte zu verbreiten. Als Schwerpunkt der Leistung wird man daher die Bereitstellung einer technischen Plattform, die es ermöglicht, sich selbst darzustellen und mit anderen Teilnehmern des Netzwerks in Kontakt zu treten, sehen müssen. Soweit hierfür seitens des Anbieters ein Entgelt verlangt wird, schuldet dieser den Erfolg der technischen Erreichbarkeit der Plattform. Damit handelt es sich um einen **Werkvertrag** i. S. d. § 631 BGB.[123] Auch bei kostenlosen Diensten spricht bereits die Tatsache, dass in den meisten Netzwerken eine vorherige Registrierung

---

[118] Krieg, K&R 2010, 73 (76 f.); Ulbricht, KommunalPraxis spezial 2012, 101 ff.
[119] Ausführlich Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 9 ff.
[120] Ingerl/Rohnke, Markengesetz, § 5 Rn. 20.
[121] Dazu Rücker, CR 2005, 347 ff.; im Kontext von Social Media Redeker, IT-Recht, Rn. 1289; OLG Hamburg, ITRB 2011, 73.
[122] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96.
[123] Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 421.

erforderlich ist, die meist mit einer Einverständniserklärung zu den AGB nach den §§ 307 ff. BGB einhergeht, für das Vorliegen des Rechtsbindungswillens. Mangels Entgeltlichkeit scheidet ein Werkvertrag jedoch aus. Vielmehr handelt es sich am ehesten um einen Auftrag i. S. d. § 662 BGB.[124]

74 Hinzu kommt die Möglichkeit, bestimmte Inhalte (Fotos, Dokumente etc.) zu speichern. Der Anbieter stellt also zusätzlich Speicherplatz zur Verfügung. Ein solcher Vertrag ist im Falle der Entgeltlichkeit als Miete zu qualifizieren, bei kostenlosen Diensten am ehesten der Leihe vergleichbar.[125] Aufgrund der Zusammenfassung verschiedener Dienstleistungen kann in der Regel von **typengemischten Verträgen** ausgegangen werden.

10.4.2.2 Allgemeine Nutzungsbestimmungen des Anbieters

75 Mit dem Vertragsschluss stimmt der Nutzer den allgemeinen Nutzungsbedingungen und zumeist auch weiteren Regelwerken (bspw. zur Privatsphäre, zum Datenschutz oder für bestimmte weitere Funktionalitäten) zu. Die öffentliche Verwaltung muss sich als Nutzer bewusst machen, dass diese vom Betreiber gestellten Vertragsbedingungen faktisch **nicht verhandelbar** sind und somit nur die Möglichkeit besteht, diese zu akzeptieren oder vom Einsatz des Angebots Abstand zu nehmen.[126] In anderen Staaten sind die Betreiber bestimmter Dienste dazu übergegangen, spezielle auf die Nutzer aus der öffentlichen Verwaltung zugeschnittene Bedingungen zu verwenden.[127] Bisher ist ein solches Vorgehen in Deutschland bzw. auf europäischer Ebene nicht ersichtlich. Verständigungen mit den Datenschutzbeauftragten können jedoch eine vergleichbare Funktion haben.[128]

76 Bei den Nutzungsbestimmungen handelt es sich um **allgemeine Geschäftsbedingungen**. Hinsichtlich etwaiger Verstöße gegen deutsches AGB-Recht der §§ 307 ff. BGB – deren Anwendbarkeit vorausgesetzt[129] – ist zu berücksichtigen, dass eine Inhaltskontrolle zwischen staatlichen Stellen (als juristische Personen des öffentlichen Rechts) und Unternehmen nur eingeschränkt erfolgt (vgl. § 310 Abs. 1 Satz 1 BGB).[130] Dennoch können sich einzelne Regelungen als nicht AGB-Recht-konform

---

[124] Redeker, in: Hoeren et al., Multimedia-Recht, Teil 12 Rn. 424.

[125] Vgl. im Kontext der Speicherung in Cloud-Angeboten Bosesky et al., Datenhoheit in der Cloud, S. 99 f.

[126] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96.

[127] Mergel et al., Praxishandbuch Soziale Medien in der öffentlichen Verwaltung, S. 142 f.

[128] So wurde bspw. auch der Dienst Google Analytics zunächst datenschutzrechtlich kritisch bewertet (dazu Hoeren, ZD 2012, 3 ff.). Mittlerweile wird jedoch ein (modifizierter) Einsatz von den Landesdatenschutzbeauftragten toleriert (MMR-Aktuell 2011, 323860): Google hat das Verfahren dahin gehend geändert, dass den Nutzern die Möglichkeit zum Widerspruch gegen die Erfassung von Nutzungsdaten eingeräumt wird, dass auf Anforderung des Webseitenbetreibers das letzte Oktett der IP-Adresse vor jeglicher Speicherung gelöscht wird, sodass darüber keine Identifizierung des Nutzers mehr möglich ist, wobei die Löschung innerhalb Europas erfolgt, und dass mit den Webseitenbetreibern ein Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG geschlossen wird.

[129] Dazu Jotzo, MMR 2009, 232 ff.

[130] Zum Umfang der Kontrolle Basedow, in: MüKo-BGB, § 310 Rn. 7 ff.

herausstellen, insbesondere wenn es sich um überraschende Klauseln handelt. Ein solcher Verstoß führt aber nicht zur Unwirksamkeit des gesamten Vertrages, sondern lediglich zur Nichtanwendbarkeit der entsprechenden Klauseln und ggf. ihrer Ersetzung durch allgemeine Rechtsgrundsätze und gesetzliche Grundwertungen.[131] Sollte sich in den Nutzungsbedingungen eine Rechtswahl- und Gerichtsstandsklausel zugunsten eines anderen Rechtssystems finden, ist zusätzlich zu prüfen, ob eine Unterwerfung unter eine solche Klausel seitens der öffentlichen Verwaltung zulässig ist.[132]

77 Um eine abschließende Prüfung konkreter Nutzungsbedingungen zu ermöglichen, daran ausgerichtet die Grundsatzentscheidung über die Nutzung zu treffen und ggf. Anhaltspunkte für **die Modalitäten der (zulässigen) Nutzung** zu erhalten, müssen also folgende Aspekte geprüft werden: 1) Unterfallen die Nutzungsbedingungen überhaupt dem deutschen AGB-Recht?[133] 2) Kann ein Verstoß gegen das (anwendbare) deutsche AGB-Recht festgestellt werden? 3) Ist der Verstoß so gravierend, dass eine Nutzung eines Angebots grundsätzlich ausscheidet, oder hat er lediglich Auswirkungen auf die konkrete Nutzung des Angebots durch die öffentliche Verwaltung? In diesem Kontext muss dann ggf. auch eine Abwägung zwischen den Vorteilen, die mit einem bestimmten Angebot verbunden sind (z. B. Erreichbarkeit einer Vielzahl von Bürgern), und den negativen Begleiterscheinungen vorgenommen werden. Können diese durch gezielte Maßnahmen reduziert werden, kommt eine Nutzung dennoch in Betracht. Anhand eines Beispiels lässt sich dies verdeutlichen: Unterstellt man die Unzulässigkeit, Urheberrechte an nutzergenerierten Inhalten auf Grundlage von AGB-Klauseln auf einen Seitenbetreiber zu übertragen[134], führt dies nicht dazu, dass eine Behörde dieses Angebot gar nicht nutzen kann, sondern verpflichtet lediglich dazu, jeweils zu prüfen, ob der Verlust des Urheberrechts an Statusmeldungen, Fotos und anderen Inhalten unzulässig bzw. nicht opportun ist, um dann das Handeln in diesem sozialen Netzwerk daran auszurichten. So wird die Weiterverwendung der Inhalte von Pressemitteilungen seit jeher gestattet.

10.4.3 Pflichten von Seitenbetreibern aus dem TMG

78 Das TMG enthält für Telemediendienste bereichsspezifische datenschutzrechtliche Regelungen sowie sonstige Vorgaben, die gem. § 1 Abs. 1 Satz 2 TMG auch von

---

[131] Basedow, in: MüKo-BGB, § 306 Rn. 10 ff.

[132] Dies lässt sich jedenfalls nicht pauschal unterstellen, zumal die öffentliche Hand im Rahmen fiskalischer Hilfsgeschäfte (Beschaffung) sich grundsätzlich dem (internationalen) Privatrecht unterwerfen kann.

[133] Hinzuweisen ist jedoch darauf, dass die Anwendbarkeit deutschen AGB-Rechts nicht der allein maßgebliche Anknüpfungspunkt sein kann. Verstößt eine nicht nach deutschem Recht zu beurteilende Nutzungsbedingung gegen allgemeine Grundgedanken des deutschen Rechts, muss die Verwaltung in gleicher Weise prüfen, ob dieser Umstand einer Nutzung entgegensteht.

[134] Berberich, MMR 2010, 736 ff.; dazu auch Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 5 ff.

öffentlichen Stellen, unabhängig davon, ob für die Nutzung der bereitgestellten Dienste ein Entgelt erhoben wird, zu beachten sind. Aufgrund der Tatsache, dass behördliche Social-Media-Auftritte als ausgelagerte Behördenhomepage zu klassifizieren sind, zumal der Inhalt überwiegend eigenverantwortlich vom Nutzer gestaltet werden kann, beanspruchen bspw. auch die **Impressumspflichten** aus dem TMG Geltung. So ist bspw. die Fanseite bei Facebook ein eigener Telemediendienst.[135] Geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien werden von § 5 Abs. 1 TMG geregelt. Die besonderen Informationspflichten bei kommerzieller Kommunikation (§ 6 TMG)[136] dürften für die Verwaltung hingegen eher nicht in Betracht kommen. Außerhalb des Anwendungsbereichs des TMG gilt, sofern das Internetangebot nicht allein persönlichen oder familiären Zwecken dient, § 55 Abs. 1 RStV, nach dem in jedem Fall Name, Anschrift und ggf. vertretungsberechtigte Personen anzugeben sind. Weitere Pflichtangaben kommen hinzu bei journalistisch-redaktionell gestalteten Angeboten, vgl. § 55 Abs. 2 RStV. In der Regel bedarf es der Angabe des vollständigen Namens (bspw. der Fachbehörde), der vollständigen Anschrift, einer vertretungsberechtigten Person sowie von Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen.[137]

Alle Pflichtinformationen sind leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten. Sie müssen **ohne wesentliche Zwischenschritte** aufgerufen werden können, wobei von der Rechtsprechung das Erreichen der Angaben mittels zweier Links noch als unmittelbar erreichbar angenommen wird.[138] Der Link muss dauerhaft funktionstüchtig und ohne Einsatz zusätzlicher Leseprogramme einsehbar sein.[139] Auch Nutzer von Social Media-Anwendungen wie Facebook-Seiten müssen eine eigene Anbieterkennung vorhalten, wenn diese zu Marketingzwecken benutzt werden und nicht nur eine reine private Nutzung vorliegt.[140] Es besteht keine Notwendigkeit, dass sich das Impressum unter der gleichen Domäne befindet wie das angebotene Telemedium. Es ist zulässig, auf das Impressum der eigenen Website zu verlinken.[141] Um die Anzahl der Zwischenschritte klein zu halten, dürfte insofern aber nur eine direkte Verlinkung auf die Impressumsangaben der Homepage ausreichen. Es muss zudem deutlich werden, dass dieses Impressum auch für einen bestimmten Social-Media- (bspw. Facebook-) Auftritt gelten soll.[142] Verbirgt sich **79**

[135] Siehe bereits Rn. 35 ff.
[136] Zum Begriff der kommerziellen Kommunikation Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 6 TMG, Rn. 15 ff.
[137] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96.
[138] OLG München, MMR 2004, 36; s. dazu auch Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 5 TMG, Rn. 25 ff. m. w. N. auch zu anderen Ansichten.
[139] Freie und Hansestadt Hamburg, Social Media in der Hamburgischen Verwaltung, S. 96.
[140] Vgl. LG Köln v. 28.12.2010 – 28 O 402/10; OLG Düsseldorf, MMR 2008, 682 f.
[141] Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 5 TMG, Rn. 28a.
[142] Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 3.

ein solcher Link hinter der von Facebook zunächst standardmäßig angebotenen Bezeichnung „Info“, soll dies nicht ausreichend sein.[143] Dass die Sicherstellung dieser Anforderungen beim Abruf der Seiten auf mobilen Endgeräten oder in Form sog. Apps nicht immer vollständig zu gewährleisten ist und kein Einfluss auf die Gestaltung seitens des Netzwerkbetreibers besteht, entbindet den Anbieter gleichwohl nicht von seinen Pflichten.[144]

10.4.4 Umgang der öffentlichen Verwaltung mit personenbezogener Daten

80 Hinsichtlich des Datenschutzes (und des Schutzes von Betriebs- und Geschäftsgeheimnissen Dritter bzw. von Amtsgeheimnissen) stellt sich die Situation letztlich nicht anders dar als bei behördlichen Internetauftritten. Auch bei diesen wird eine entsprechende Offenbarung personenbezogener Daten im Regelfall unzulässig sein[145], es sei denn, es liegt eine (auch mutmaßliche) Einwilligung in diese spezielle Verwertung oder eine gesetzliche Legitimation – bspw. im Kontext der Öffentlichkeitsfahndung[146] – vor. Für die Veröffentlichung von Fotos (bspw. von behördlichen Veranstaltungen) gilt, dass es grundsätzlich einer **Einverständniserklärung** der abgebildeten Personen bedarf (Ausnahme: Überblicksaufnahmen nach § 23 Abs. 1 Nr. 2 und 3 KunstUrhG). Da bei der Veröffentlichung in einem sozialen Netzwerk der Verbreitungsgrad ggf. ein anderer ist als etwa in der lokalen Presse und zusätzliche Funktionen existieren, bspw. eine Gesichtserkennung mit Zuordnung von Namen, muss die explizit abgefragte Einwilligung alle beabsichtigten Veröffentlichungswege abdecken[147]. Ob ein Markieren („Taggen“) von Personen durch die öffentliche Verwaltung zulässig ist, muss ebenfalls isoliert geprüft werden.

10.4.5 Umgang mit fremden Namens- und Urheberrechten

81 Die öffentliche Verwaltung muss auch bei Social-Media-Auftritten fremde Namensrechte beachten. Dies gilt sowohl bei der Wahl des Namens für den behördlichen

---

[143] LG Aschaffenburg, MMR 2012, 38 f., OLG Düsseldorf v. 13.8.2013 – I-20 U 75/13; s. auch Micklitz/Schirmbacher, in: Spindler/Schuster, Recht der elektronischen Medien, § 5 TMG, Rn. 21. Mittlerweile hat Facebook eine Impressumsrubrik eingeführt, die den rechtlichen Anforderungen entsprechen dürfte; vgl. Schwenke, Endlich rechtssicher? Facebook führt eine Impressumsrubrik für Seiten ein, Blogbeitrag v. 26.03.2014; abrufbar unter http://rechtsanwalt-schwenke.de/facebook-fuehrt-impressumsrubrik-fuer-seiten-ein/.

[144] Speziell zum sog. M-Government Hoffmann, MMR 2013, 631 (633).

[145] Frevert/Wagner, NVwZ 2011, 76 (76).

[146] Dazu Rn. 95 f.

[147] Ulbricht, Social Media und Recht, S. 29 f.

Auftritt[148] als auch im Rahmen von Tweets, Postings und Eintragungen in Blogs. Soweit nutzergenerierte Inhalte aus den sozialen Netzwerken ihrerseits urheberrechtlichen Schutz genießen, dürfen diese nicht ohne Einwilligung des Rechteinhabers genutzt werden. Das Kopieren von Tweets, Statusmeldungen oder anderer Inhalte ist zwar in gewisser Weise typisch für Social Media, von der Beachtung rechtlicher Grenzen sind die Beteiligten dennoch nicht entbunden. In Betracht kommen vor allem aber die mutmaßliche und konkludente Einwilligung als Rechtfertigungsgrund. Ein urheberrechtlicher Schutz gilt bspw. nicht für sog. **Re-Tweets**. So wird die Wiederveröffentlichung eines fremden Tweets, um diesen zu bestätigen oder zu verbreiten, im Rahmen des Dienstes Twitter bezeichnet. Wäre dieses Verhalten durch den Urheberrechtsschutz der einzelnen Tweets untersagt, wären die für Twitter typischen schnellen Verbreitungseffekte (sog. virale Effekte) nicht denkbar.[149]

10.4.6 Barrierefreiheit behördlicher Angebote

Mit der Einhaltung der einfachgesetzlichen Vorgaben zur Barrierefreiheit (§ 11 BGG i. V. m. der Anlage zur Barrierefreien Informationstechnik-Verordnung – BITV), die sich bspw. auf die einfache Wahrnehmbarkeit der Informationen oder die Kompatibilität der Webseite mit Vorleseprogrammen und anderen technischen Hilfsmitteln beziehen, soll sichergestellt werden, dass Nutzer mit Behinderungen möglichst uneingeschränkt auf die bereitgestellten Informationen zugreifen können.[150] Aufgrund der Eigenschaft der meisten behördlichen Auftritte in sozialen Medien als ausgelagerte Behördenhomepages ist von einer grundsätzlichen Anwendbarkeit der entsprechenden Vorschriften auszugehen.[151] Da umfassende Anpassungen der Social-Media-Auftritte in sozialen Netzwerken (vor allem in ihren mobilen Varianten[152]) in der Regel nicht möglich sind, kann von einzelnen Anforderungen oder Bedingungen abgewichen werden, wenn die Gestaltung in Bezug auf den quantitativen und qualitativen Nutzwert für eine Zielgruppe wegen der besonderen sachlichen Anforderungen mit einem unverhältnismäßig hohen technischen und finanziellen Aufwand verbunden wäre.[153] Diese Voraussetzungen dürften regelmäßig vorliegen – dennoch muss auf die größtmögliche Realisierung, bspw. durch Verweise auf **barrierefreie Alternativangebote** etc., geachtet werden. **82**

[148] Dazu Rn. 70.
[149] Krieg, K&R 2010, 73 (75 f.).
[150] Frevert/Wagner, NVwZ 2011, 76 (78).
[151] Speziell zum barrierefreien E-Government vgl. Roggenkamp, NVwZ 2006, 1239 ff.
[152] Hoffmann, MMR 2013, 631 (635).
[153] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 163 (200 f.).

10.4.7 Behördliche Haftung im Rahmen von Social Media

83 In den sozialen Medien werden Inhalte nicht mehr einseitig von einem Webseiteninhaber erstellt, sondern es besteht die Möglichkeit der Verwaltung, auf einfache Weise in Plattformen von Drittanbietern Seiten anzulegen, zudem aber auch vielfältige Möglichkeiten der Nutzer, nutzergenerierte Inhalte auf diesen Seiten der Verwaltung zu erstellen – bspw. auf der Pinnwand einer Facebook-Seite der Verwaltung Kommentare oder Fotos zu hinterlassen. Es entsteht ein System gestufter nutzergenerierter Inhalte mit unterschiedlichen – mittelbaren und unmittelbaren – **Verantwortlichkeiten** der Beteiligten.[154]

10.4.7.1 Unmittelbare Verantwortlichkeit für eigene Inhalte

84 Für eigene nutzergenerierte Inhalte eines behördlichen Auftritts in sozialen Netzwerken ist die öffentliche Stelle als Diensteanbieter gem. § 7 Abs. 1 TMG **nach den allgemeinen Gesetzen** verantwortlich.[155] Somit haftet sie für bspw. nach Urheberrecht oder den Regeln über die Amtshaftung.[156] Als eigene Informationen i. S. d. § 7 Abs. 1 TMG gelten dabei auch fremde Inhalte, die sich die öffentliche Stelle so zu eigen gemacht hat, dass sie nach außen als originär von ihr stammend erscheinen.[157] Die Abgrenzung von fremden und eigenen Inhalten beurteilt sich ebenso wie von solchen, die als eigene übernommen werden, unter Würdigung aller Umstände des Einzelfalles aus der Sicht eines objektiv verständigen Nutzers.[158] Auch das (private) Verhalten einzelner Mitarbeiter, welches von internen Vorgaben abweicht und daher eigentlich keinen dienstlichen Charakter hat, kann zurechenbar sein. So hat das LG Freiburg festgestellt, dass das wettbewerbswidrige Verhalten eines Mitarbeiters auf seiner privaten Facebook-Seite unter Hinweis auf seine dienstliche Telefonnummer dem Arbeitgeber zugerechnet werden kann, selbst wenn dieser keine Kenntnis von der Handlung des Mitarbeiters hatte.[159] Die Verwendung von Disclaimern ist im Regelfall nicht geeignet, eine Haftung auszuschließen, genauso wie umgekehrt vom Fehlen eines Disclaimers nicht darauf geschlossen werden darf, dass ein Zueigenmachen vorliegt.[160]

85 Unter dem Gesichtspunkt der Amtshaftung kommt vor allem die (fehlerhafte) Information als haftungsauslösendes Ereignis in Betracht, da Social Media vorrangig

---

[154] Siehe bereits Rn. 45 ff. Allgemein zur Verantwortlichkeit Spindler, Kap. 5, sowie – aus datenschutzrechtlicher Sicht – Hornung, Kap. 4 Rn. 42 ff.
[155] Speziell für Social Media Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 60 ff.
[156] Zu Einzelheiten Hoffmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 7 TMG, Rn. 27.
[157] Frevert/Wagner, NVwZ 2011, 76 (77); zum Zueigenmachen Hoffmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 7 TMG, Rn. 15 ff. m. w. N.
[158] Müller-Broich, Telemediengesetz, § 7 Rn. 2.
[159] LG Freiburg, MMR 2014, 118 ff.; dazu Roggenkamp, jurisPR-ITR 25/2013 Anm. 6.
[160] Müller-Broich, Telemediengesetz, § 7 Rn. 3.

zu Informationszwecken eingesetzt wird. Die **Fehlinformation** seitens eines Trägers hoheitlicher Gewalt ist seit jeher geeignet, einen Anspruch aus Staatshaftung auszulösen.[161] Sowohl bei freiwilliger als auch gesetzlich zwingend vorgegebener Informationserteilung sind Auskünfte richtig, klar, unmissverständlich, eindeutig und vollständig zu erteilen und müssen auf dem aktuellen Erkenntnisstand beruhen.[162] Diese Anforderungen gelten selbstverständlich auch für die Verbreitung von Informationen in sozialen Netzwerken. Richtig ist die Information, wenn sie mit der Wirklichkeit übereinstimmt. Eine Amtspflichtverletzung ist daher gegeben, wenn eine falsche Information verbreitet wird, insbesondere weil nicht richtig ermittelt wurde[163] oder wenn eine Information sich nachträglich als falsch herausstellt und eine falsche Information nicht richtig gestellt oder sogar weiterverbreitet wird. Zur Richtigstellung sind die gleichen Informationswege zu nutzen wie bei der ursprünglichen Informationsverbreitung, soweit damit der gleiche Verbreitungsgrad erreicht werden kann. Somit sollte die Richtigstellung innerhalb des gleichen Netzwerkes in der Regel ausreichend sein.

10.4.7.2 Mittelbare Verantwortung für Fremdinhalte

Auch hinsichtlich der Möglichkeit für weitere Nutzer, auf den behördlichen Auftritten in sozialen Netzwerken zu interagieren und dort z. B. Fotos, Statusmeldungen, Kommentare zu veröffentlichen, und der Verantwortlichkeit für Fremdinhalte kann auf die bisherige Praxis bei behördlichen Homepages zurückgegriffen werden. Rechtlicher Ausgangspunkt ist § 7 Abs. 2 TMG, der auf die allgemeinen Gesetze verweist. In Betracht kommt eine Haftung als Mitstörer[164], da der Account-Inhaber verpflichtet ist, offensichtlich rechtswidrige Inhalte unverzüglich zu entfernen und den Zugang hierzu zu sperren, sobald er hiervon Kenntnis erlangt (Beseitigungspflicht bzw. Notice-and-take-down-Prinzip). Daneben kann auch eine in die Zukunft gerichtete Unterlassungspflicht treten.[165] Jeweils muss Beachtung finden, dass die Verwaltung als Hoheitsträger besonderes Vertrauen der Bürger genießt und grundgesetzlich verpflichtet ist, rechtmäßig zu handeln. Deshalb kann mit guten Gründen vertreten werden, dass der Verwaltung höhere und umfassendere Prüfungspflichten auferlegt sind als wirtschaftlichen Unternehmen.[166] **86**

Die Löschung einzelner Beiträge ist kein Mittel, um kritische Beiträge zu entfernen. Äußerungen, die von **der Meinungsfreiheit** geschützt sind, dürfen nicht **87**

[161] Ossenbühl, Staatshaftungsrecht, S. 47 f.
[162] Baldus et al., Staatshaftungsrecht, Rn. 119.
[163] Murswiek, NVwZ 2003, 1 (8).
[164] Nieland, NJW 2010, 1494 ff.; Roggenkamp, Web 2.0 Plattformen im kommunalen E-Government, S. 255 f.; speziell für Social Media Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 63 ff.
[165] Zu Einzelheiten Hoffmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 7 TMG, Rn. 33 f.; Müller-Broich, Telemediengesetz, § 7 Rn. 4 ff.
[166] Frevert/Wagner, NVwZ 2011, 76 (78).

gelöscht werden. Denn sonst droht eine Verletzung der Meinungsfreiheit (Art. 5 Abs. 1 GG) oder des Gleichbehandlungsgrundsatzes (Art. 3 Abs. 1 GG). Im Rahmen der Moderation behördlicher Seiten muss daher die Grundrechtsbindung Beachtung finden, die dem virtuellen Hausrecht[167], das auch der Verwaltung zukommt, Grenzen setzen kann.[168]

10.4.7.3 Verantwortlichkeit für Links

88 Von den Fremdinhalten sind Links auf andere Homepages und auf Inhalte in den sozialen Netzen abzugrenzen, die eigenes Verhalten der Behörde darstellen und mithin eigenen Grundsätzen und Regeln unterliegen.[169] Das Setzen eines Links stellt zwar grundsätzlich ein **sozialadäquates Verhalten** ohne Haftungsfolgen dar. Auch das Setzen eines Links auf einen urheberrechtlich geschützten Inhalt ohne Einwilligung des Rechteinhabers ist zulässig, da weder eine Vervielfältigung noch eine öffentliche Zugänglichmachung vorliegt. Wenn der Inhalt der verlinkten Seite aber nach den Gesamtumständen auch dem Verlinkenden zuzurechnen ist, kommt eine Haftung als Mitstörer in Betracht.[170] Grundsätzlich wird man dies annehmen können, wenn der Link mit einem zustimmenden Kommentar versehen wird.[171] Der Umfang der Prüfungspflicht richtet sich nach dem Gesamtzusammenhang, dem Zweck der Linksetzung, der Kenntnis von Umständen, die auf eine Rechtswidrigkeit hindeuten und der Erkennbarkeit der Rechtsverletzung[172], wobei von Hoheitsträgern eine umfassendere Prüfung von verlinkten Inhalten erwartet werden kann als von privatwirtschaftlichen Unternehmen.

89 Bei Verlinkungen auf Unternehmensseiten sowie von politischen und weltanschaulichen Vereinigungen sind zudem die für Werbung geltenden Grundsätze sowie das staatliche **Neutralitätsgebot** zu beachten. Aufgrund der Vergleichbarkeit einer Twitter- bzw. Facebook-Seite mit einer klassischen Webseite im Bezug auf Nutzung und Erscheinungsbild muss diese Rechtsprechung zu behördlichen (und anderen) Homepages übertragen werden.

10.4.7.4 Nutzung von Social Plug-ins durch die öffentliche Verwaltung

89 Die Erstellung von Profilen oder Seiten in sozialen Netzwerken geht oft mit der Integration sog. Social Plug-ins auf der eigenen behördlichen Homepage einher. Hierbei

---

[167] S. zu den Rechten gegenüber Störern in Chats und Foren LG München, CR 2007, 264 f.; OLG Köln, CR 2000, 843. ausführlich Karavas, Digitale Grundrechte, S. 18 ff.

[168] Roggenkamp, Web 2.0 Plattformen im kommunalen E-Government, S. 236 ff.; s. auch Hoffmann et al., Die digitale Dimension der Grundrechte, S. 129 ff.

[169] Speziell für Social Media Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 67 ff.

[170] Grundlegend BGH, NJW-RR 2003, 1685 ff.

[171] Wie etwa bei Twitter „sehr interessant", vgl. dazu LG Frankfurt/M., Beschl. v. 20.4.2010 – 3-08 O 46/10.

[172] BGHZ 158, 343 ff.

handelt es sich um eine besondere Form der **Verlinkung** – einerseits auf das soziale Netzwerk als solches, andererseits auf die eigene Präsenz, zudem verbunden mit besonderen Datenverarbeitungsprozessen, die auch rechtlich relevant sind.[173] Diese sog. Social Plug-ins erfreuen sich großer Beliebtheit. Der bekannteste dürfte der Gefällt-Mir-Button des Anbieters Facebook sein, der sich auf einer Vielzahl von Homepages befindet. Ein Vorteil derartiger Social Plug-ins ist die einfache Möglichkeit, sich als Besucher der behördlichen Homepage durch das Aktivieren der Schaltfläche unmittelbar mit dem behördlichen Auftritt im sozialen Netzwerk zu verbinden, um so zukünftig weitere Informationen innerhalb des Netzwerks zu beziehen. Zudem bieten die Social Plug-ins die Option, bestimmte Artikel, Beiträge oder Links der eigenen (behördliche) Homepage im sozialen Netzwerk zu empfehlen oder zu teilen und somit wiederum einem größeren Publikum zugänglich zu machen.

90 Problematisch ist, dass es – zum Teil, um diese Funktionen überhaupt zu ermöglichen – zu Datenübermittlungen an den Anbieter des sozialen Netzwerks kommt. Der von Facebook für die Anbieter anderer Webseiten bereitgestellte Gefällt-Mir-Button geriet in die Kritik, da beim Besuch von Seiten, auf denen sich dieses Social Plug-in befindet, automatisch ein Cookie ausgelesen wird, das dem Nutzer ohne seine Zustimmung vorher beim Anschauen von Facebook-Seiten auf seinen Computer übertragen wurde. Dieses Auslesen findet dabei unabhängig vom Anklicken des Gefällt-Mir-Buttons statt und unabhängig davon, ob der Besucher einer Homepage Mitglied bei Facebook ist oder nicht. Von Besuchern einer Seite mit dem Gefällt-Mir-Button, die zuvor noch keine Facebook-Seite besucht haben, kann das Social Plug-in Informationen wie IP-Adresse und Browsertyp auslesen. Bei Personen, die selbst Facebook-Mitglieder sind und eine Seite mit Social Plugin besuchen, können die Informationen über das Aufrufen der Seite mittels des Cookies mit ihrem Facebook-Nutzerprofil zusammengeführt werden. Ausgehend von den ausdifferenzierten datenschutzrechtlichen Verantwortlichkeiten in geteilten Social-Media-Systemen[174] muss bewertet werden, wer steuernden Einfluss auf die relevanten **Datenverarbeitungsprozesse** hat. Bei Social Plug-ins, die auf der eigenen (Behörden-)Homepage implementiert werden und bei denen es zu einer Übermittlung personenbezogener Daten von (Facebook-)Mitgliedern (und ggf. auch Nichtmitgliedern) kommt, ist diese Datenübermittlung unmittelbar von der Behörde durch die Einbindung auf der eigenen Homepage und nicht vom Betreiber des sozialen Netzwerks initiiert. Die Rechtslage stellt sich insofern anders dar als bei den Fanseiten. Die einbindende Verwaltung ist unmittelbar verantwortlich und handelt, da sie die Einhaltung der Vorgaben des § 15 Abs. 3 TMG nicht sichern kann, rechtswidrig.

[173] Vgl. auch Ernst, NJW 2011, 3541 ff.; Piltz, CR 2011, 657 (663); Müller-Riemenschneider/Specht, K&R 2014, 77 ff.; speziell zur öffentlichen (Kommunal-)Verwaltung Schmucker, DVP 2013, 319 ff.

[174] Dazu Rn. 47.

91 Um den Verstoß gegen datenschutz- und telemedienrechtliche Vorschriften zu vermeiden, sind sog. **Zwei-Klick-Lösungen** im Einsatz.[175] Denkbar – und aus datenschutzrechtlicher Sicht noch unproblematischer (allerdings dann ohne jegliche Zusatzfunktionalität) – ist es, eine Verlinkung auf den behördlichen Auftritt im sozialen Netzwerk in die eigene Homepage zu integrieren, bspw. in Form einer Grafik. In diesem Fall werden (wenn nicht schon die Grafik als Social Plug-in vom Anbieter zur Verfügung gestellt wird) keine Daten an den Betreiber des sozialen Netzwerks übertragen.

92 Des Weiteren ist auch die „werbende Wirkung", die von solchen Verlinkungen ebenso wie von dem Auftritt in einem sozialen Netzwerk als solchem ausgeht, zu berücksichtigen.[176] Staatliche Stellen sind zur Beachtung behördeninterner Grundsätze zu Werbung und zu staatlicher **Neutralität** verpflichtet. Durch die Einbindung eines Social Plug-in entsteht zudem ggf. eine (vergabe)rechtlich relevante Leistungsbeziehung zum Betreiber des sozialen Netzwerks. Es fließt zwar keine Geldleistung, bezahlt wird aber auch hier – insbesondere mit der Währung des Informationszeitalters: den Daten der Nutzer. Über diese Daten darf die Behördenhomepage, die ein Social Plug-in integriert, nicht selbst verfügen. Die dafür erforderlichen Einwilligungen können nur die Nutzer selbst erteilen. Die Verwaltung vermittelt dem externen Dienstleister immerhin aber den Zugang zu diesen Daten, indem sie ihr eigenes Angebot mit dem Drittangebot verquickt.[177] Insofern dürften die Grundsätze zum Verwaltungssponsoring entsprechend gelten.[178]

10.4.8 Grenzen staatlicher Informationstätigkeit

93 Social-Media-Aktivitäten der öffentlichen Verwaltung in sozialen Netzwerken sind überwiegend auf die Verbreitung von Informationen gerichtet. Je nach Einsatzgebiet, Zweck und Art des Netzwerks variiert der Inhalt der jeweiligen Informationen. Denkbar sind neben Warnungen vor bestimmten Produkten oder Unternehmen, Empfehlungen und Hinweise. Inwieweit für die Verbreitung von Informationen und Warnungen der **Gesetzesvorbehalt** gilt bzw. ob eine einfachgesetzliche Ermächtigungsgrundlage erforderlich ist, wird seit jeher differenziert bewertet. Nach der (umstrittenen)[179] Ansicht des BVerfG ist für das regierungsamtliche Informationshandeln grundsätzlich keine ausdrückliche Gesetzesgrundlage erforderlich, vielmehr genüge die Kompetenz der Regierung zur Öffentlichkeitsarbeit (abgeleitet aus Art. 65

[175] Die entsprechenden technischen Lösungen sind frei im Internet verfügbar. zu diesem Ansatz Venzke, DuD 2011, 387 ff.; Piltz, CR 2011, 657 (663).
[176] Siehe bereits Rn. 62 f.
[177] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).
[178] Martini, in: Hill/Schliesky, Die Neubestimmung der Privatheit, S. 193 (233 f.).
[179] Vgl. etwa Hellmann, NVwZ 2005, 163 ff.; Knitsch, ZRP 2003, 113 ff.; Murswiek, NVwZ 2003, 1 ff.

GG). Die Aufgabe der Staatsleitung der Regierung ergebe sich danach aus der Verfassung selbst und enthalte eine Ermächtigung zum Informationshandeln. Auch bei mittelbar-faktischen Grundrechtseingriffen, die beim Informationshandeln möglicherweise gegeben seien, sei keine besondere gesetzliche Ermächtigungsgrundlage erforderlich. Anders ist die Situation dagegen zu bewerten, wenn sich die staatliche Tätigkeit nicht auf die Bereitstellung von marktrelevanten Informationen zur selbstständigen Entscheidung der Marktteilnehmer beschränkt. In diesem Fall sei die staatliche Öffentlichkeitsarbeit ein funktionales Äquivalent für einen klassischen Eingriff und damit eine Umgehung des Gesetzesvorbehalts.[180] Die „rechtlichen Vorgaben für staatliches Informationshandeln" sieht das Bundesverfassungsgericht daher nur als erfüllt an, soweit eine staatliche Aufgabe vorliegt, die Zuständigkeitsordnung eingehalten wird und die Informationen richtig und sachlich sind.[181] Diese Grundsätze gelten für Regierungshandeln, nicht jedoch für Aktivitäten der Verwaltung. Hier ist das Vorliegen einer einfachgesetzlichen Ermächtigungsgrundlage zu fordern, sobald die Veröffentlichung der Informationen grundrechtliche Belastungswirkungen mit sich bringt.[182] Dies ist jedoch bei vielen über Social Media verbreiteten allgemeinen Informationen nicht der Fall; es handelt sich um einen Teilbereich gesetzesfreier Verwaltung, noch dazu oft um freiwillige Aufgaben der Behörden.

Grundrechtsbeeinträchtigende Veröffentlichungen müssen stets dem Grundsatz der Verhältnismäßigkeit genügen. Es hat eine Abwägung zwischen dem Interesse der Öffentlichkeit an der Veröffentlichung und den für die Betroffenen damit verbundenen negativen Folgen zu erfolgen. Insbesondere bei Veröffentlichungen von Informationen im Internet und damit auch in sozialen Netzwerken muss bedacht werden, dass diese zum einen große Streuwirkung entfalten und zum anderen meist dauerhaft abrufbar sind („das Internet vergisst nicht") und daher für die Betroffenen teilweise erhebliche Nachteile mit sich bringen können. Hinzu kommt, dass staatlichen Informationen per se hohes Gewicht beigemessen wird, da dem Staat stets Sachverstand, Unabhängigkeit und Neutralität zugesprochen wird.[183] Darüber hinaus müssen die Informationen dem Gebot der Sachlichkeit entsprechen. Dies ist immer dann gewahrt, wenn die Information sich an den Funktionserfordernissen der Marktverhältnisse orientiert, zur Krisenbewältigung geeignet ist und sich unter Berücksichtigung möglicher nachteiliger Wirkungen für die betroffenen Wettbewerber auf das zur Informationsgewährung Erforderliche beschränkt.[184] **94**

[180] BVerfGE 105, 252 (273).
[181] Grundlegend BVerfGE 105, 252 ff.; ausführlich zu diesem Themenkomplex, insbesondere auch zu neueren Entwicklungen, Manssen, in: v. Mangoldt et al., GG, Art. 12 Rn. 86 ff. m. w. N.
[182] Ossenbühl, NVwZ 2011, 1357 (1360).
[183] Ossenbühl, NVwZ 2011, 1357 (1357); zum Problemkreis, insbesondere bei Internet-Veröffentlichungen, auch Becker/Blackstein, NJW 2011, 490 ff.
[184] BVerfGE 105, 252 (273); jüngst betont vom OVG Schleswig, Beschl. 28.02.2014, 4 MB 82/13, im Kontext von Äußerungen eines Landesdatenschutzbeauftragten zum fragwürdigen Umgang von Unternehmen mit personenbezogenen Daten; vgl. auch Härting, WhatsApp Weichert?, Blogbeitrag v. 21.02.2014; abrufbar unter www.cr-online.de/blog/.

10.4.9 Besonderheiten bei Polizei- und Sicherheitsbehörden

95 Neben den für alle Behörden denkbaren Nutzungsanlässen, die bei Einhaltung der genannten rechtlichen Vorgaben auch im Kontext von Polizei- und Sicherheitsbehörden zum Einsatz kommen können (bspw. zu Marketingzwecken im Rahmen der Nachwuchsgewinnung[185]), existieren spezifische Fragestellungen. Gerade die sog. viralen Effekte, also die schnelle Verbreitung, machen Social-Media-Dienste für Polizei- und andere Sicherheitsbehörden attraktiv. Dies gilt bspw. für den Einsatz im Rahmen besonderer Krisensituationen[186], die **Online-Fahndung** sowie Recherchen in den sozialen Netzen.[187]

96 Während die Online-Fahndung, also die Veröffentlichung von Fahndungsaufrufen, in der Anfangszeit noch unmittelbar in sozialen Netzwerken erfolgte, sind die Behörden, die dementsprechend aktiv sind, nun dazu übergegangen, lediglich Links zu posten und auf die eigene behördliche Online-Präsenz zu verweisen.[188] Dies hat den Vorteil, dass die – personenbezogenen – Daten auf den Servern der Behörde und damit in ihrem Einflussbereich verbleiben. Angesichts der Unschuldsvermutung ist bei diesem Vorgehen besondere Zurückhaltung geboten, wie seit jeher Pressemeldungen der Polizei mit äußerster Sorgfalt verfasst und in der Regel anonymisiert wurden. Aus §§ 161, 163 StPO ergibt sich der Grundsatz der freien Gestaltung des Ermittlungsverfahrens, wonach alle zulässigen Maßnahmen zu ergreifen sind, die geeignet und erforderlich sind, zur Aufklärung einer Straftat beizutragen.[189] Dazu ist auch die Fahndung und insbesondere die Inanspruchnahme der Öffentlichkeit bei der Straftatenaufklärung zu rechnen. Bei Einhaltung der allgemeinen **Grenzen der Öffentlichkeitsfahndung**[190] dürfte daher auch der Einsatz von Social Media legitim sein.[191] Sicherzustellen ist, dass die Kommentarfunktion nicht dazu genutzt wird, konkrete Hinweise zu geben, da hier ggf. Persönlichkeitsrechte betroffen sein können. Da Kommentare aber von anderen Nutzern und nicht der Behörde selbst stammen, ist die Behörde nicht unmittelbar verantwortlich, sie trifft in jedem Fall aber eine – gegenüber der allgemeinen erhöhte – besondere Sorgfalts- und Beobachtungspflicht.[192]

---

[185] Ulbricht, Social Media und Recht, S. 231 ff.
[186] Dazu bereits Rn. 52.
[187] Dazu sogleich Rn. 97 f.
[188] Roggenkamp, K&R 1/2013, Editorial.
[189] Griesbaum, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 161 Rn. 18.
[190] Ausführlich Soiné, NStZ 1997, 166 ff., 321 ff.
[191] S. auch Zilkens/Cavin, ZD 2013, 603 ff.
[192] Dazu Rn. 86 f.

10.4.10 Besonderheiten bei Sozial-, Jugendämtern und vergleichbaren Institutionen

Denkbar ist es, das Internet und vor allem Social Media als Informationsquelle für staatliche Stellen und zur staatlichen Aufgabenerfüllung zu nutzen.[193] Dies erfolgt vorrangig durch Polizei- und andere Sicherheitsbehörden[194] und ist – soweit allgemein zugängliche Quellen betroffen sind – rechtlich unbedenklich. Allerdings sind viele der „interessanten" Inhalte von Social Media (Fotos, Freundesbeziehungen etc.) nur nach einer vorherigen Registrierung oder aufgrund einer Freundesbeziehung verfügbar. Auch wenn derartige Nutzungszwecke nicht großflächig im Einsatz sind, so scheint es nicht ausgeschlossen, dass Mitarbeiter in Jobcentern Informationen aus sozialen Netzwerken heranziehen, um die tatsächlichen Wohnverhältnisse der Leistungsempfänger zu ermitteln. Gleiches gilt für etwaige nicht angegebene Arbeitsverhältnisse, die möglicherweise in einem sozialen Netzwerk erwähnt werden. Der Bundesbeauftragte für den Datenschutz verlangt in diesem Zusammenhang, dass die Behörden zunächst versuchen müssten, die erforderlichen Angaben direkt bei den Betroffenen zu erheben (**Vorrang der Direkterhebung**[195]). Nur wenn diese sich weigern, könnte auch das Internet zurate gezogen werden. In jedem Fall sei der Betroffene aber von einer Datenerhebung zu informieren.[196] Inwieweit dies auch für allgemein zugängliche Daten i. S. d. § 28 Abs. 1 Satz 1 Nr. 3 BDSG gilt[197], erscheint allerdings fraglich, wobei noch nicht abschließend geklärt ist, welche Datenbestände eines sozialen Netzwerkes „allgemein zugänglich" sind und welche nur einem geschlossenen Personenkreis. So soll es nach dem BVerfG zur offenen Zugänglichkeit genügen, dass jedermann nach Registrierung zugelassen wird.[198] **97**

Ohne auf weitere Details der rechtlichen Zulässigkeit derartiger Recherchen eingehen zu können, sei zumindest darauf hingewiesen, dass im Aufruf von Webseiten, die für jedermann ohne Einschränkung **frei zugänglich** sind (bspw. Angebote von Zeitschriften, private Homepages, Unternehmensprofile o. Ä.), durch staatliche Stellen kein Grundrechtseingriff gesehen werden kann.[199] Gleiches gilt für die frei verfügbaren Inhalte eines sozialen Netzwerks. Ein Grundrechtseingriff, insbesondere **98**

---

[193] S. dazu auch Esser, Kap. 7 Rn. 327 ff.

[194] Ausführlich Schulz/Hoffmann, CR 2010, 131 ff.; dies., DuD 2012, 7 ff., Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 209 ff.; s. auch Brenneisen/Staack, Kriminalistik 2012, 627 ff.; Zilkens/Cavin, ZD 2013, 603 ff.; Irlbauer, Kriminalistik 2012, 764 ff.

[195] Gola/Schomerus, BDSG, § 4 Rn. 19 ff.

[196] http://www.n-tv.de/politik/Facebook-Recherche-nicht-erlaubt-article10699336.html.

[197] S. auch OLG Hamburg, MMR 2010, 62 (63); zu sozialen Netzwerken Bergmann et al., Datenschutzrecht, § 28 BDSG, Rn. 263.

[198] Es soll ausreichen, dass sich die auf der Website angezeigten Inhalte an „einen nicht weiter abgegrenzten Personenkreis richten" (BVerfGE 120, 274 (344 f.). Erfasst würden auch Angebote, die zwar eine vorherige Registrierung erfordern, bei denen aber eine Kontrolle der Identität durch den Betreiber der Seite nicht stattfindet, sodass auch Ermittlungsbehörden das Anmelden unter einer fiktiven Identität möglich ist; s. auch Böckenförde, Die Ermittlung im Netz, S. 250.

[199] Hoffmann et al., in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 209 (229 ff.).

in Art. 10 Abs. 1 GG und in das Recht auf informationelle Selbstbestimmung, entfällt aufgrund einer wirksamen Einwilligung selbst dann, wenn im Einzelfall personenbezogene Daten erhoben werden. Einfachgesetzlich findet sich dieser Grundgedanke in § 28 Abs. 1 Satz 1 Nr. 3 BDSG.

10.4.11 Besonderheiten bei obersten Landes- und Bundesbehörden

99 Das Handeln oberster Landes- und Bundesbehörden, also vorrangig der Ministerien, weist einige Besonderheiten auf, da nicht der administrative Vollzug – und die damit im Zusammenhang stehende Presse- und Öffentlichkeitsarbeit sowie Informationstätigkeit – im Mittelpunkt steht, sondern **regierungsamtliches Handeln**. Insofern ist vor allem zu berücksichtigen, dass die Abgrenzung zwischen dienstlichem Handeln (des Ministers für die Behörde) und sonstigen Äußerungen in den sozialen Medien (bspw. in der Parteirolle) strikt gehandhabt wird. Soweit Warnungen und Hinweise im Rahmen der staatsleitenden Tätigkeit gegeben werden dürfen[200], kann auch auf die Mittel von Social Media zur Verbreitung zurückgegriffen werden.

100 Wird der sog. **fachliche Diskurs** durch einzelne Mitarbeiter ermöglicht, sollten Mechanismen etabliert werden, die sicherstellen, dass Einzelmeinungen nicht fälschlicherweise als offizielle Verlautbarungen des Ministeriums erscheinen. Zwar ist es möglich, die Befugnis, für eine Behörde zu sprechen, zu delegieren, gleichwohl ist es zielführend, die Mitarbeiter zu verpflichten, in der Außenkommunikation auf eine „nicht abgestimmte" Meinung, einen Arbeitsstand o. Ä. hinzuweisen. Gerade in diesem Bereich können Social-Media-Guidelines helfen, die Rechtssicherheit im Umgang mit Social Media sowohl für die Mitarbeiter als auch die betroffene Organisation zu erhöhen.[201]

10.4.12 (Kommunale) Amts- und Mandatsträger und Social Media

101 Auch hinsichtlich des Einsatzes von Social Media durch (kommunale) Mandatsträger, die insofern Teile eines Kollegialorgans der Exekutive sind, sind einige Besonderheiten zu berücksichtigen. Zwar ist das Verhalten der Gemeindevertretung der Gemeinde zurechenbar, nicht jedoch das Verhalten der einzelnen Mitglieder. Soweit nicht für die gesamte Vertretungskörperschaft gehandelt wird (bspw. durch den Vorsitzenden) – eine eher theoretische Möglichkeit –, ist die Nutzung durch

[200] Dazu bereits Rn. 93 f.
[201] Dazu Rn. 105.

einzelne Gemeindevertreter in Ausübung des Mandats nicht durch die Gemeinde reglementierbar, sondern **Ausdruck des freien Mandats**.

102 Entscheidet sich eine Gemeindeverwaltung, den dienstlichen Einsatz von Social Media durch eine interne Verhaltensrichtlinie zu legitimieren und zu reglementieren, erfasst dies zunächst alle Mitarbeiter der jeweiligen Verwaltung, einschließlich der **(politischen) Leitungsebenen**. Zu berücksichtigen ist, dass gewählten Bürgermeistern aufgrund der eigenverantwortlichen Leitung der Gemeinde(verwaltung) weitergehende Freiheiten zukommen, sie zum Teil über ein kommunales Mandat verfügen und zudem in der Regel auch eine Parteifunktion einnehmen. Nur soweit echtes Verwaltungshandeln Gegenstand der Aktivitäten in den sozialen Medien ist, gelten also die allgemeinen Regeln für dienstliches Verhalten oder die in einer Guideline konkretisierten Vorgaben.

103 Demgegenüber wird es in der Regel nicht zulässig sein, kommunale Mandatsträger hinsichtlich ihrer Tätigkeit als Gemeindevertreter zu reglementieren. Die Ausübung des freien Mandats steht externen Bindungen, vor allem solchen der Gemeindeverwaltung entgegen. Wenn überhaupt kommt eine Reglementierung durch Selbstbindung in Form einer **Geschäftsordnung** in Betracht. Diese beschränkt sich dann aber in der Regel auf das Verhalten in Gremiensitzungen. Zu beachten ist auch, dass, anders als bei Mitarbeitern der öffentlichen Verwaltung, das besondere Rechtsverhältnis weniger stark in die private Sphäre ausstrahlt. Verschwiegenheitspflichten bestehen zwar ebenfalls[202], die Meinungsäußerungsfreiheit ist aber nicht eingeschränkt; Gemeindevertreter sind nicht verpflichtet, sich gemeindeverträglich zu äußern.[203]

104 Hinsichtlich der **Nutzung von Social Media in Gremiensitzungen**[204] ist – wie bei vergleichbaren Maßnahmen (z. B. Rauchverboten[205]) – abzugrenzen, ob die Gemeindevertreter in ihren Mitgliedschaftsrechten oder als Bürger in ihren Grundrechten beeinträchtigt werden. Zumindest soweit die Nutzung von Social-Media-Diensten einen Bezug zur Tätigkeit als Gemeindevertreter aufweist, sind die Mitgliedschaftsrechte betroffen. Die Gemeindevertreter können sich auf ihr freies Mandat berufen, sodass einschränkende Maßnahmen, bspw. das Verbot, Laptops, Smartphones o. Ä. in Gremiensitzungen zu benutzen, durch die Aufrechterhaltung der Ordnung gerechtfertigt sein müssen. Das Recht, derartige Vorgaben in Form der Geschäftsordnung festzulegen, folgt aus der Geschäftsordnungsautonomie; Einzelmaßnahmen kann der Vorsitzende in Ausübung der Sitzungs- bzw. Ordnungsgewalt ergreifen.[206]

---

[202] Dazu Rn. 144 ff.

[203] VGH Mannheim, NVwZ-RR 2001 S. 262.

[204] S. auch Papsthart, BayVBl 2013, 645 ff.; Schulz et al., Die Gemeinde SH 2014, i. E. Eine Orientierung kann insofern auch das Vorgehen in den Landtagen bieten. So wollte man sich im Schleswig-Holsteinischen Landtag auf entsprechende Verhaltensregeln verständigen; abrufbar unter http://landesblog.de/blog/2012/09/23/laptopverbot-in-plenartagungen-des-landtags/.

[205] Statt Vieler VGH Mannheim, NVwZ 1983, 485 ff.; dazu Pitschas, JA 1983, 668 ff.

[206] S. auch Schmidt-Aßmann/Röhl, in: Schmidt-Aßmann/Schoch, Besonderes Verwaltungsrecht, 1. Kap. Rn. 62 ff.

10.5 Vorgaben für die dienstliche Nutzung/Social-Media-Guidelines

105 Vorgaben für den einzelnen Mitarbeiter im Rahmen der dienstlichen Nutzung von Social Media ergeben sich mittelbar aus den Vorgaben, die für die Behörde gelten. Da der Mitarbeiter für die Behörde nach außen handelt, muss er sicherstellen, dass diesen Anforderungen genüge getan wird. Denkbar ist es aber auch, den Mitarbeitern weitergehende Hinweise zu geben, die zwischen dienstlichen Einsatzformen und ergänzenden Hinweisen zur privaten Nutzung differenzieren können. Ohne eine Aussage zur Rechtsform zu treffen, werden diese oft als Social-Media-Guideline oder als **Social-Media-Policy** bezeichnet. Während eine Policy eher die strategische Ebene (Zielsetzungen, Nutzungsformen, Verhältnis zur Gemeinwohlorientierung der Verwaltung, Risikomanagement) adressiert, handelt es sich bei Guidelines um konkrete Handlungsvorgaben für die Mitarbeiter.[207]

10.5.1 Rechtsnatur und Erlassverfahren

106 Dem geltenden Recht lässt sich keine zwingende Vorgabe entnehmen, welche Rechtsform eine Social-Media-Guideline haben muss. In Betracht kommen **Dienstvereinbarungen**, Erlasse, Verwaltungsvorschriften, die Ergänzung von Geschäftsordnungen, der allgemeinen Dienstanweisung, der Regelungen zum Umgang mit Presseanfragen und zum Bürgerkontakt oder Ähnliches, bis hin zu individuellen Absprachen in sehr kleinen (Gemeinde-)Verwaltungen. Die Wahl einer Rechtsform bedingt in der Regel auch eine bestimmte Erlassform und ein bestimmtes Erlassverfahren, bspw. bestimmte Mitwirkungsrechte, die im Erarbeitungsprozess zu beachten sind. Davon losgelöst sollte eine Social-Media-Guideline je nach Zielsetzung insbesondere mit Vertretern der Presse- und Öffentlichkeitsarbeit, dem behördeneigenen Datenschutzbeauftragten, ggf. auch der jeweiligen Aufsichtsbehörde, und dem Personalrat abgestimmt werden.[208]

10.5.2 Denkbare Inhalte einer Social-Media-Guideline

107 Der Inhalt einer Social-Media-Guideline variiert in Abhängigkeit von den verfolgten **Zielsetzungen** und Anwendungsszenarien. Hinsichtlich des Einsatzes zur Presse- und Öffentlichkeitsarbeit dürfte der geringste Handlungsbedarf entstehen, da es sich

---

[207] S. auch Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 57 ff.

[208] Zur Beteiligung des Betriebsrates Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 59; nicht erforderlich bei unverbindlichen Empfehlungen; so Schwenke, Social Media Marketing & Recht, S. 419.

bei dieser Art der Kommunikation um eine geübte Praxis handelt (lediglich das Medium variiert), das eingesetzte Personal in der Regel eine gewisse Affinität zu neuen Arten der Informationsbeschaffung und -verbreitung besitzen dürfte und oft ein in sich kohärentes Regelungs- und Verantwortlichkeitenregime existiert.

Zu Beginn einer Guideline kann eine Beschreibung der **allgemeinen Rahmenbedingungen** stehen. Diese hat den Zweck, Mitarbeitern, für die der Umgang mit sozialen Medien nicht (oder: noch nicht) zum alltäglichen Handwerkszeug gehört, eine erste Orientierung zu geben. Angesichts des Umstandes, dass selbst Kommunikationsformen, die in der Privatwirtschaft schon seit Längerem im Einsatz sind, nur langsam Einzug in die öffentliche Verwaltung halten, erscheint ein solches Vorgehen zielführend. In den allgemeinen Rahmenbedingungen lassen sich folgende Aspekte verorten:[209] **108**

- die Definition der sozialen Medien, des Web 2.0 sowie die Beschreibung der Funktionsweise einzelner Anwendungen,
- die mit dem Einsatz von der Behörde konkret verfolgten Zielsetzungen,
- der Bezug zu den Unternehmenszielen (bzw. in der öffentlichen Verwaltung: zum öffentlichen Auftrag, den gesetzlichen Aufgaben der jeweiligen Behörde),
- Hinweise auf allgemeine arbeits-, dienst- und beamtenrechtliche Grundsätze und deren Fortgeltung[210],
- die Beziehung zu weiteren Regelwerden[211],
- zum Geltungs- und Anwendungsbereich (vor allem, wenn auch Personen oder Personengruppen einbezogen werden, die über besondere Rechte verfügen, bspw. kommunale Mandatsträger[212]).

Da explizite Vorgaben für das private, also nicht-dienstliche, Verhalten neben den geltenden Restriktionen aus dem Beamten- und Arbeitsrecht in der Regel nicht erforderlich sind, beschränkt sich der Geltungsbereich der getroffenen Regelungen auf das dienstliche Agieren in sozialen Medien. Daher kommt der **Abgrenzung** und Abgrenzbarkeit von dienstlicher und privater (nicht-dienstlicher) Nutzung ein enormer Stellenwert zu. Diese lässt sich mithilfe einer expliziten Definition im Rahmen einer Social-Media-Guideline erleichtern. **109**

Bei Regelungen, die für alle Nutzungsformen gleichermaßen gelten, stehen die **Besonderheiten von Social Media** und die zur Abfederung der daraus resultierenden Risiken zu ergreifenden organisatorischen Maßnahmen im Mittelpunkt. Daher erscheint es in diesem Kontext angezeigt, auf die Besonderheiten der Online-Kommunikation (bspw. größere Reichweite, leichtere Durchsuchbarkeit, eingeschränkte Möglichkeit zur Löschung, unbegrenzter Adressatenkreis, kontinuierliche Pflege, 24/7-Verfügbarkeit), insbesondere über soziale Medien, hinzuweisen. Aus diesen Besonderheiten lassen sich allgemeine Benutzungsregeln, Vorgaben zur Art **110**

---

[209] Ausführlich mit Formulierungsvorschlägen jeweils Schulz, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 121 (133 ff.).
[210] Dazu Rn. 144 ff. und Rn. 120 f.
[211] Dazu Rn. 60.
[212] Dazu Rn. 101 ff.

und Weise der Kommunikation ableiten, in der Online-Kommunikation oft auch „Netiquette“ bezeichnet (bspw. Einhaltung einer höflichen Kommunikationsform, auch in kontroversen Diskussionen, trotz eines weitaus informaleren Umgangs Verzicht auf übertrieben lässige Kommunikationsformen, adressatengerechte Aufbereitung). Zielführend ist auch eine Pflicht der Mitarbeiter zur Kennzeichnung ihrer Beiträge. In Abhängigkeit davon, ob Funktions- oder Mitarbeiter-Accounts zugelassen und welche Nutzungsarten verwirklicht werden, sind dabei verschiedene Varianten denkbar:

- die Kennzeichnung aller Beiträge mit der Urheberschaft der Behörde,
- ein Auftreten des Mitarbeiters als natürliche Person, was weitaus mehr dem Grundprinzip von Social Media entsprechen dürfte, aber zugleich unter Hinweis **auf** die Behördenzugehörigkeit,
- und vor allem bei der Nutzung von Funktionsaccounts, unter denen mehrere Mitarbeiter kommunizieren, der Hinweis auf den aktuell Handelnden.

111 Des Weiteren bedarf es einer Entscheidung darüber, welchem Personenkreis innerhalb der Verwaltung die Interaktion in sozialen Medien, insbesondere der fachliche Diskurs, freigestellt werden soll. Während die Ermöglichung der Nutzung durch eine Vielzahl der Mitarbeiter die Chance bietet, die Erreichung der Ziele zu optimieren, ist damit das Risiko eines weitergehenden Kontrollverlusts für Behördenleitung oder Presse- und Öffentlichkeitsarbeit verbunden. In jedem Fall sollten so viele Mitarbeiter eingebunden werden, dass eine angemessene Reaktionsgeschwindigkeit garantiert werden kann. In Betracht zu ziehen sind folgende **Begrenzungen des Mitarbeiterkreises**, der über soziale Medien kommuniziert:

- Die Option, ausschließlich einer bestimmten Hierarchieebene den fachlichen Diskurs (allgemein) zu ermöglichen. Dies garantiert einerseits ein gewisses fachliches Niveau, andererseits ist so ein bestimmter hausinterner Abstimmungsgrad gewährleistet.
- Eine Zuweisung der Kompetenz begrenzt auf bestimmte Themengebiete, wobei dann gleichfalls zu klären ist, ob alle Mitarbeiter dieser Organisationseinheit entsprechend handeln dürfen oder ob wiederum eine Begrenzung auf eine Hierarchieebene oder nach anderen Kriterien angezeigt ist.
- Denkbar sind zudem Registrierungs- und Anzeigeverfahren, bis hin zu einer Genehmigungspflicht, die entweder dem direkten Vorgesetzten, einer anderen Hierarchieebene oder der Abteilung für Presse- und Öffentlichkeitsarbeit bzw. einer Kombination zugewiesen werden kann.
- Eine personenbezogene Beschränkung, vergleichbar der Zuweisung an eine bestimmte Hierarchieebene, ließe sich zudem in Form des Erfordernisses einer speziellen Schulung im Umgang mit sozialen Medien realisieren.
- Schließlich ist es denkbar, auf eine Begrenzung zu verzichten und allen Mitarbeitern den fachlichen Diskurs zu gestatten. Dieses Modell empfiehlt sich in der Regel nur in Verbindung mit der Begrenzung auf eine bestimmte Thematik und auf die dieser zugeordneten Mitarbeiter.

Im Kontext von Bürgeranfragen existieren in vielen Verwaltungen Regelungen, die eine Weiterleitung an die entsprechend zuständige Stelle vorsehen – sei es in Form expliziter Handlungsanweisungen oder als geübte Verwaltungspraxis. Die Vorgaben einer Social-Media-Guideline können darauf aufbauen. Im Rahmen von Social Media sind allgemeine Anfragen (bspw. zu Öffnungszeiten, Rechtsgrundlagen, Zuständigkeiten o. Ä.) denkbar, die entweder – soweit existent – an eine speziell geschaffene Stelle, die in den sozialen Medien derartige Anfragen beantworten soll, ansonsten an eine vergleichbare Einrichtung (Bürgertelefon 115[213], Bürgerbüro o. Ä.) weitergeleitet werden müssen. Bei Anfragen mit Bezug zu einem konkreten Verwaltungsverfahren muss eine **Weiterleitung** an die fachlich zuständige Stelle initiiert werden. Der Bürger sollte von der Stelle, an die er seine Anfrage (fälschlicherweise) gerichtet hat, in jedem Fall über die Weiterleitung und das weitere Prozedere informiert werden. Zudem sollte die Rückantwort (der fachlich zuständigen Stelle) über das Eingangsmedium erfolgen, soweit dieses auch für derartige Anfragen durch die zuständige Stelle bedient wird und der Inhalt der Anfrage bzw. Antwort (bspw. aufgrund der personenbezogenen Daten bei Anfragen zu einem laufenden Verwaltungsverfahren) nicht entgegensteht. **112**

10.6 Vorgaben für die private Nutzung

Wie für den behördlichen und dienstlichen Einsatz von Social Media als Grundsatz festgehalten werden kann, dass sich dieser als ausgelagerte Behörden-Homepage verstehen lässt und daher die allgemeinen Vorgaben Geltung beanspruchen, gilt dies auch für die private Nutzung durch die Mitarbeiter der öffentlichen Verwaltung[214]: Deren Aktivitäten müssen sich an den auch in der analogen Welt bzw. bei der herkömmlichen Kommunikation mit einzelnen Bürgern oder einer breiteren Öffentlichkeit geltenden (allgemeinen) rechtlichen Vorgaben orientieren. Fehlen Regelungen zum dienstlichen Einsatz sozialer Medien, ist im Zweifel davon auszugehen, dass sich Mitarbeiter **als Privatperson** äußern. **113**

10.6.1 Beamten- und Dienstrecht

Die Geltung des allgemeinen Rechtsrahmens bedeutet zunächst die Anwendbarkeit derjenigen Regelungen des Beamten- und Dienstrechts, die auch in die private Sphäre des Beamten bzw. Arbeitnehmers hineinreichen. Hervorzuheben sind u. a. folgende **114**

[213] Siehe zu Ausbaumöglichkeiten im Sinne eines Mehrkanalansatzes Warnecke, in: Schliesky/Schulz, Transparenz, Partizipation, Kollaboration, S. 57 ff.
[214] S. zur arbeitsrechtlichen Problematik der Privatnutzung des Internets während der Arbeitszeit Bayreuther, Kap. 8 Rn. 16 ff.

Aspekte, die (auch) die private Kommunikation in sozialen Medien betreffen können und für **Beamte und Tarifbeschäftigte** gleichermaßen gelten:

- die Verschwiegenheitspflicht (§ 67 BBG),
- der Dienstwegvorbehalt (§ 125 BBG),
- die Pflicht zu berufserforderlicher Achtung und zu vertrauensgerechtem Verhalten (§ 61 Abs. 1 Satz 3 BBG),
- die Einschränkungen bei politischer Betätigung (§ 60 Abs. 2 BBG).

115 Untersagt ist eine **Offenbarung von dienstlichen Geheimnissen**, wobei dies mündlich, schriftlich, über elektronische Medien und durch sinngemäße Andeutungen, Gesten und konkludentes Verhalten erfolgen kann[215], also auch durch Äußerungen in sozialen Netzwerken etc. Die Verschwiegenheitspflicht gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Offenkundig sind Ereignisse oder Zustände, die von einer beliebigen Zahl von Personen ohne besondere Sachkunde jederzeit wahrgenommen werden können[216], sei es unmittelbar oder sei es durch Zugriff auf allgemein zugängliche, zuverlässige Quellen. Allgemein zugängliche, zuverlässige Quellen sind insbesondere amtliche Bekanntmachungen oder Statistiken. Weiterhin kommen Veröffentlichungen in Büchern, Lexika, in Zeitungen und Zeitschriften und vor allem im Internet in Betracht.[217] „Ihrer Bedeutung nach keiner Geheimhaltung" bedürfen Tatsachen, deren Bekanntwerden unter keinem vernünftigen Gesichtspunkt zum Zeitpunkt der Offenbarung oder später öffentliche oder private Belange beeinträchtigen kann. Dies ist der Fall, wenn keine schutzwürdigen Interessen Dritter oder der Allgemeinheit an der Geheimhaltung bestehen, wobei dies in zeitlicher Perspektive variieren kann.[218]

116 Ein allgemeiner Grundsatz, nach dem sich die Verschwiegenheitspflicht nicht auf Umstände bezieht, die der Mitarbeiter für rechtswidrig oder gar strafbewehrt hält, existiert nicht[219]. Es ist der Dienstweg einzuhalten und ggf. zu remonstrieren. Die **internen Abhilfemöglichkeiten** der Grundsätze des öffentlichen Dienstrechts sind vorrangig.[220] Demgegenüber gehen die gesetzlich begründeten Pflichten, Straftaten anzuzeigen (§ 138 StGB) und bei Gefährdung der freiheitlich demokratischen Grundordnung für deren Erhaltung einzutreten (entsprechend § 60 Abs. 1 Satz 3 BBG), der Verschwiegenheitspflicht vor.[221] Innerdienstliche Meinungsverschiedenheiten rechtfertigen in keinem Fall eine „Flucht in die Öffentlichkeit". Eine Verletzung der Verschwiegenheitspflichten kann neben disziplinarrechtlichen Konsequenzen auch

---

[215] Kastner, in: Fehling et al., Verwaltungsrecht, Handkommentar, § 84 VwVfG, Rn. 3.
[216] Bonk/Kallerhoff, in: Stelkens et al., VwVfG, § 84 Rn. 8.
[217] An einer Offenkundigkeit soll es bei Internet-Quellen fehlen, wenn eine Registrierung etc. erforderlich ist, so Kastner, in: Fehling et al., Verwaltungsrecht, Handkommentar, § 84 VwVfG, Rn. 5; anders Schulz, in: Mann et al., VwVfG, § 84 Rn. 24.
[218] BVerwG, NJW 1983, 2343 (2344); Battis, Bundesbeamtengesetz, § 61 Rn. 2.
[219] Schulz, in: Mann et al., VwVfG, § 84 Rn. 15.
[220] Bonk/Kallerhoff, in: Stelkens et al., VwVfG, § 83 Rn. 4.
[221] Bonk/Kallerhoff, in: Stelkens et al., VwVfG, § 83 Rn. 7.

eine strafrechtliche Verantwortlichkeit des Beamten nach den §§ 203, 353b, 355 StGB begründen. Gerade die Veröffentlichung in sozialen Medien, selbst in (vermeintlich) geschlossenen Gruppen, erfüllt den Tatbestand des „Offenbarens". Auch beim internen Einsatz von Social Media ist zu prüfen, inwieweit eine Offenbarung bspw. dem dienstlichen Verkehr zugehörig und daher gestattet ist. **117**

Nach § 125 BBG sind interne Streitigkeiten innerhalb der Behörde und nicht in der Öffentlichkeit beizulegen. Beamten wird das Recht zuerkannt, Anträge und Beschwerden vorzubringen; allerdings nur bei **Einhaltung des Dienstwegs**. Der Beschwerdeweg bis zur obersten Dienstbehörde steht offen. Gerade bei internen sozialen Netzwerken ist daher darauf zu achten, dass nicht vom Dienstweg abgewichen wird und andere Hierarchieebenen oder ein (wenn auch interner) größerer Personenkreis unmittelbar informiert werden. Nur wenn solche Netzwerke auch „private" Nachrichten an einzelne Mitarbeiter und Vorgesetzte vorsehen, können sie in diesem Kontext zum Einsatz kommen.

Die Pflicht zu **berufserforderlicher Achtung** und zu vertrauensgerechtem Verhalten (vgl. § 61 Abs. 1 Satz 3 BBG) ist auch beim Auftreten in sozialen Medien und Äußerungen im Internet zu beachten. Dabei ist zwischen dienstlichem und außerdienstlichem Verhalten des Beamten zu differenzieren. Ein Verhalten des Beamten außerhalb des Dienstes ist nur dann ein Dienstvergehen, wenn es nach den Umständen des Einzelfalles in besonderem Maße geeignet ist, das Vertrauen in einer für sein Amt oder das Ansehen des Beamtentums bedeutsamen Weise zu beeinträchtigen.[222] Dies können gerade auch private Äußerungen in sozialen Netzwerken sein. Entscheidend ist die Amtsbezogenheit dieser Amtswalterpflicht.[223] Die Amtsbezogenheit der Verhaltenspflicht erfordert, zwischen verschiedenen Beamtengruppen zu differenzieren. Ein leitendes Amt stellt höhere Anforderungen als ein niedriges. Außer nach der Bedeutung und dem Gehalt des konkreten Amtes können die Anforderungen abhängen vom Wechsel der öffentlichen Meinung und von örtlichen Verhältnissen, bspw. ob der Beamte seinem Publikum persönlich bekannt ist oder anonym bleibt.[224] Zu den Pflichten innerhalb des Dienstes gehören bspw. die Achtung und Höflichkeit gegenüber Vorgesetzten, die bspw. verletzt wird durch Äußerungen der Nichtachtung oder herabsetzende Kritik an Vorgesetzten, insbesondere, wenn statt des Dienstweges die Flucht in die Öffentlichkeit gewählt wird.[225] Die Pflicht zu Offenheit und Vertrauen sowie zur unbedingten Wahrhaftigkeit gegenüber dem Vorgesetzten in dienstlichen Angelegenheiten kann u. U. eine Mitteilung ohne Befragen fordern. Mobbing, auch im Internet, verstößt gegen die Pflicht zur kollegialen Zusammenarbeit, die auch durch leichtfertige, nicht nachprüfbare Beschuldigungen und hinterhältiges Verhalten verletzt wird.[226] **118**

---

[222] Battis, Bundesbeamtengesetz, § 61 Rn. 10.
[223] Battis, Bundesbeamtengesetz, § 61 Rn. 9 f.
[224] Battis, Bundesbeamtengesetz, § 61 Rn. 10.
[225] Battis, Bundesbeamtengesetz, § 61 Rn. 11.
[226] Battis, Bundesbeamtengesetz, § 61 Rn. 12.

119 Die Pflicht des Beamten, hinsichtlich seiner politischen Tätigkeiten und Äußerungen die amtsangemessene Mäßigung und Zurückhaltung zu wahren, besteht insbesondere im Hinblick auf das Vertrauen der Bürger in die Funktionsfähigkeit der öffentlichen Verwaltung (vgl. § 60 Abs. 2 BBG). Die Meinungsäußerungsfreiheit besteht aber im Grundsatz fort.[227] Bei der Vornahme von Amtshandlungen hat sich der Beamte einer **politischen Meinungsäußerung** ganz zu enthalten, denn er handelt als Amtswalter und nicht als Privatperson und Grundrechtsträger.[228] Dies gilt also auch für Aktivitäten in den sozialen Netzwerken, soweit diese dienstlichen Charakter haben. Außerhalb des Dienstes (also bei privatem Auftreten in sozialen Medien) sind politische Meinungen inhaltlich nur durch die Verfassungstreuepflicht beschränkt. Inwieweit die Betätigung in der Form beschränkt ist, richtet sich vornehmlich nach der amtlichen Stellung des Beamten.[229] Erheblich ist auch, ob die Meinungsäußerung im privaten Kreis oder in der Öffentlichkeit, bspw. auf einer Parteiversammlung unter Erwähnung des bekleideten Amtes erfolgt. Unter politische Betätigung fallen außer Meinungsäußerungen bei parteipolitischer Betätigung auch solche in Gewerkschaften, Verbänden, Bürgerinitiativen, und auch im Internet.

10.6.2 Verhaltensregeln für Angestellte

120 Diese Verpflichtungen gelten im Wesentlichen für Angestellte des öffentlichen Dienstes entsprechend. Die im Kontext von sozialen Medien besonders relevante Verschwiegenheitspflicht findet sich einerseits in § 3 Abs. 1 TVöD bzw. § 3 Abs. 2 TVL und wird andererseits durch die besondere, förmliche Verpflichtung nach dem Verpflichtungsgesetz[230] bekräftigt. Die inhaltliche Reichweite entspricht derjenigen von Beamten.[231] Die besondere Verpflichtung führt dazu, dass auch nicht-verbeamtete Personen als Amtsträger im Sinne des § 11 Abs. 1 Nr. 4 StGB für eine Verletzung von **Verschwiegenheitspflichten** strafrechtlich verantwortlich sind, vor allem nach den §§ 203, 353b, 355 StGB.

121 Auch für Angestellte lässt sich ein allgemeines **Zurückhaltungsgebot**, insbesondere hinsichtlich kritischer Ansichten über den Arbeitgeber bzw. sein konkretes Verhalten, aus allgemeinen arbeitsrechtlichen Pflichten begründen. Insbesondere bei Arbeitnehmern in leitender Position oder Arbeitnehmern, die mit ihrer Tätigkeit spezifische Vertragspflichten übernommen haben, hat deren Stellung unmittelbaren

---

[227] Ausführlich zu privaten Arbeitsverhältnissen und Social Media Solmecke, in: Hoeren et al., Multimedia-Recht, Teil 21.1 Rn. 47 ff.

[228] Battis, Bundesbeamtengesetz, § 60 Rn. 18.

[229] Battis, Bundesbeamtengesetz, § 60 Rn. 21.

[230] Gesetz über die förmliche Verpflichtung nicht beamteter Personen v. 2.3.1974 (BGBl. I S. 547), zuletzt geändert durch § 1 Nr. 4 d. G. zur Änderung des EinführungsG zum Strafgesetzbuch vom 15.8.1974 (BGBl. I S. 1942).

[231] Ausführlich zur arbeitsrechtlichen Verschwiegenheitspflicht Müller-Glöge, in: MüKo-BGB, § 611 Rn. 1088 ff.

Einfluss auf die vertragliche Pflichtenstruktur. Dies gilt umso mehr, wenn berechtigte Belange des Arbeitgebers erheblich gestört werden, weil das Verhalten des Arbeitnehmers geeignet ist, den Ruf des Arbeitgebers zu gefährden. Ansonsten darf der außerdienstliche, private Bereich des Arbeitnehmers nur insoweit arbeitsvertraglichen Bindungen unterworfen werden, als die Arbeitsaufgabe des Arbeitnehmers unmittelbar berührt wird.[232] Meinungsäußerungsfreiheit und politische Betätigung des Arbeitnehmers sind gewährleistet, doch braucht der Arbeitgeber das Arbeitsverhältnis bspw. nicht fortzusetzen, wenn er selbst, seine Produkte, seine Leistungen oder andere Aspekte der Tätigkeit vom Arbeitnehmer öffentlich angegriffen werden.[233] Eine weitergehendes dem Beamtenrecht angenähertes Zurückhaltungsgebot für das „gesamte", also auch private Verhalten, findet sich für die Ausübung hoheitlicher Tätigkeiten in § 41 Satz 2 TVöD-BT-V: „Beschäftigte des Bundes und anderer Arbeitgeber, in deren Aufgabenbereichen auch hoheitliche Tätigkeiten wahrgenommen werden, müssen sich durch ihr gesamtes Verhalten zur freiheitlich demokratischen Grundordnung im Sinne des Grundgesetzes bekennen.", vgl. auch § 3 Abs. 1 Satz 2 TVL.

10.6.3 Vorgaben zur privaten Internetnutzung

Oftmals ist die private Nutzung sozialer Medien während der Dienstzeit untersagt (**Verbot der Internetnutzung für private Zwecke**).[234] Das Recht, die Kommunikationsmittel für diese Zwecke vollständig zu untersagen, steht dem Arbeitgeber als Eigentümer der Betriebsmittel und Inhaber des Direktionsrechts zu. Die Beschäftigten haben keinen Anspruch auf die Gestattung der Privatnutzung. Es kann aber auch festgelegt werden, dass Medien während der Arbeitszeit genutzt werden dürfen, welche Plattformen besucht werden dürfen und in welchem zeitlichen Rahmen dies geschehen darf.[235] Fehlt eine explizite Vorgabe, bspw. in Form einer Dienstvereinbarung[236], gelten die allgemeinen Pflichten des Arbeitsvertrages.[237] Da auch private Aktivitäten der Mitarbeiter in den sozialen Netzwerken außerhalb des Dienstes einen dienstlichen Bezug haben können, werden teilweise auch diesbezüglich Vorgaben gemacht. Eine Teilnahme mit eigenem Bild und Namen der Bediensteten wird dabei meist nicht gänzlich untersagt, was arbeitsrechtlich auch kaum zulässig sein dürfte. Denn im außerdienstlichen Bereich ist es dem Arbeitgeber normalerweise verwehrt, **122**

[232] Müller-Glöge, in: MüKo-BGB, § 611 Rn. 1079.
[233] Müller-Glöge, in: MüKo-BGB, § 611 Rn. 1079; speziell zu Fällen im Kontext der Social-Media-Nutzung Pawlak/Smeyers, öAT 2013, 26 ff.
[234] S. BAG, NJW 2013, 104 ff.; dazu Kramer, NZA 2013, 311 ff.
[235] Zu den Rechtsfolgen bei Gestattung Seel, öAT 2013, 4 ff.
[236] Ausführlich Block, Regelung privater E-Mail- und Internetnutzung am Arbeitsplatz durch Betriebsvereinbarung, 2011.
[237] S. auch Bissels/Domke, AuA 2013, 82 ff.

Weisungen zu erteilen.[238] Dies gilt jedoch nicht, soweit auch durch die außerdienstliche Nutzung die Interessen des Arbeitgebers berührt sein können. So erweist sich das Gebot, bei einer außerdienstlichen Nutzung darauf zu achten, dass keine dienstlichen Äußerungen erfolgen, als zulässig (so etwa die Vorgaben des Niedersächsischen Ministeriums für Inneres und Sport[239]). Bei Angehörigen von Sicherheitsbehörden wird auf die erheblichen Risiken hingewiesen, die die Veröffentlichung eines Profilfotos haben kann (insbesondere durch die Verwendung von Gesichtserkennungssoftware). Zudem wird teilweise empfohlen, keine oder nur allgemeine Berufsangaben (wie zum Beispiel „öffentlicher Dienst“) zu machen. Auf diese Weise soll verhindert werden, dass persönliche Meinungsäußerung als Stellungnahmen der Behörde verstanden werden.

10.7 Fazit

123 Geänderte Kommunikationsbedingungen und veränderte Erwartungshaltungen der (jüngeren) Bürger wirken zwangsläufig auf die öffentliche Verwaltung ein. Open Government und kollaborative Verwaltung sind nur einige Stichworte dieser Diskussion. Unbestritten können die sozialen Medien einen wesentlichen Beitrag im Rahmen einer gewandelten Staatskommunikation leisten. Mehr als in der Vergangenheit geht es um die Gestaltung von Entscheidungsprozessen mit verschiedenen Interessen, auch im Sinne einer Kanalisierung des Gemeinwohls, mit dem Ziel der **Akzeptanzsteigerung**. Vor diesem Hintergrund wirken zahlreiche Vorgaben aus dem überkommenen rechtlichen Rahmen und Forderungen der Datenschutzbeauftragten anachronistisch. Eine Fortentwicklung des Rechtsrahmens ist überfällig; die öffentliche Verwaltung sollte dort präsent sein, wo der Großteil der Bevölkerung kommuniziert. Die Darstellung des Rechtsrahmens zeigt aber auch, dass vielfach geäußerte Vorbehalte nicht durchdringen: Die allgemeinen Vorgaben für Social Media gelten auch für Nutzer der öffentlichen Verwaltung, es existieren nur wenige Besonderheiten. Vergegenwärtigt man sich, dass Auftritte in den sozialen Medien überwiegend wie eine ausgelagerte Behördenhomepage anzusehen sind, steht ein Rechtsrahmen zur Verfügung, der von vielen Behörden professionell gehandhabt wird. Zudem ist das überkommene Rechtsregime für das Verhalten der Mitarbeiter der öffentlichen Verwaltung so flexibel, um auch auf neue Herausforderungen zu reagieren. Die vermeintliche Rechtsunsicherheit kann also kein Argument gegen eine Nutzung sein. Sie ist für die öffentliche Verwaltung nicht größer als für andere Nutzer – und bei innovativen Technologien und gesellschaftlichen Entwicklungen schlicht nicht zu vermeiden.

---

[238] Vgl. z. B. BAG, NZA 1994, 180.

[239] Bek. d. MI v. 18.10.2012 – 42.02840/1100-0003 (Nds. MBl. Nr. 39/2012 S.885).

Literatur

Albrecht, F. (2013). Keine Untersagung einer Facebook-Fanseite durch Datenschutzaufsicht. *JurisPR-ITR 24/2013*, Anm. 6.

Baldus, M., Grzeszick, B. & Wienhues, S. (2013). *Staatshaftungsrecht*. 4. Aufl. Heidelberg: C. F. Müller.

Battis, U. (2009). *Bundesbeamtengesetz*. 4. Aufl. München: C. H. Beck.

Becker F., Blackstein, Y. (2011). Der transparente Staat – Staatliche Verbraucherinformation über das Internet. *NJW*, 490 ff.

Berberich, M. (2010). Der Content „gehört" nicht Facebook! – AGB-Kontrolle der Rechteeinräumung an nutzergenerierten Inhalten. *MMR*, 736 ff.

Bergmann, L., Möhrle, R. & Herb, A. (2013). *Datenschutzrecht, Loseblatt-Sammlung* (Stand: 46. EL April 2013). Stuttgart: Boorberg.

Bissels, A., Domke, C. (2013). Social Media am Arbeitsplatz. *AuA*, 82 ff.

Block, T. (2011). *Regelung privater E-Mail- und Internetnutzung am Arbeitsplatz durch Betriebsvereinbarung*. Frankfurt: Peter Lang.

Böckenförde, T. (2003). *Die Ermittlung im Netz*. Tübingen: Mohr Siebeck.

Bosesky, P. et al (2013). *Datenhoheit in der Cloud*. Kiel: Lorenz-von-Stein-Inst.

Brenneisen, H., Staack, D. (2012). Die virtuelle Streife in der Welt der Social Media, *Kriminalistik*, 627 ff.

Deutsches Institut für Vertrauen und Sicherheit im Internet (Hrsg.) (2012). *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, abrufbar unter www.divsi.de.

Ernst, S. (2010). Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem. *NJOZ*, 1917 ff.

Fehling, M., Kastner, B. & Störmer, R. (Hrsg.) (2013). *Verwaltungsrecht, Handkommentar*. 3. Aufl. Baden-Baden: Nomos.

Freie und Hansestadt Hamburg. (2011). *Social Media in der Hamburgischen Verwaltung*, abrufbar unter www.hamburg.de.

Frevert, T., Wagner, O. (2011). Rechtliche Rahmenbedingungen behördlicher Internetauftritte. *NVwZ*, 76 ff.

Gallwas, H.-U. (1970). *Faktische Beeinträchtigungen im Bereich der Grundrechte*. Berlin: Duncker & Humblot.

Gola, P., Schomerus, R. (2012). *BDSG*. 11. Aufl. München: C. H. Beck.

Götting, H.-P., Nordemann, A. (Hrsg.) (2010). *UWG Handkommentar*. Baden-Baden: Nomos.

Graudenz, D. et al. (2010). Vom Open Government zur Digitalen Agora. *ISPRAT-Whitepaper*, abrufbar unter www.isprat.net.

Hannich, R. (Hrsg.) (2013). *Karlsruher Kommentar zur Strafprozessordnung*. 7. Aufl. München: C. H. Beck.

Härting, N. (2014). *WhatsApp Weichert*?. Blogbeitrag v. 21.02.2014; abrufbar unter www.cr-online.de/blog/.

Hellmann, V. (2005). Eine Warnung vor dem Bundesverfassungsgericht – Die Glykol- Entscheidung des BVerfG vom 26. 6. 2002. *NVwZ*, 163 ff.

Hoeren, T. (2012). Google Analytics – datenschutzrechtlich unbedenklich? – Verwendbarkeit von Webtracking-Tools nach BDSG und TMG. *ZD*, 3 ff.

Hoeren, T., Sieber, U. & Holznagel, B. (Hrsg.) (2013). *Multimedia-Recht, Loseblatt-Sammlung* (Stand: 36. EL 2013).

Hoffmann, C. (2012). Optimierung des behördeninternen Wissensmanagements durch kollaborative Web 2.0-Anwendungen. In: Schliesky, U., Schulz, S. E. (Hrsg.) *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 87 ff. Kiel: Lorenz-von-Stein-Inst.

Hoffmann, C. (2013). Apps der öffentlichen Verwaltung – Rechtsfragen des Mobile Government. *MMR*, 631 ff.

Hoffmann, C., Klessmann, J. (2011). Open Data in der öffentlichen Verwaltung – Chancen und Herausforderungen bei der Veröffentlichung von Verwaltungsdaten. *VM*, 306 ff.

Hoffmann, C., Klessmann, J. (2012). Open Data in der öffentlichen Verwaltung – Chancen und Herausforderungen bei der Veröffentlichung von Verwaltungsdaten. In: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 41 ff. Kiel: Lorenz-von-Stein-Inst.

Hoffmann, C., Luch, A. D. & Schulz, S. E. (2012). Das Internet, insbesondere das Web 2.0, soziale Medien und Netzwerke als Informationsquelle staatlicher Stellen, in: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 209 ff. Kiel: Lorenz-von-Stein-Inst.

Hoffmann, C., Schulz, S. E. & Tallich, M. (2012). Anreizsysteme und Instrumente zur Nutzen- und Nutzersteigerung. *Die Verwaltung 45*, 207 ff.

Hoffmann, C., Schulz, S. E. & Brackmann, F. (2012). Web 2.0 in der öffentlichen Verwaltung: Twitter, Facebook und „Blogs" aus rechtlicher Perspektive. In: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 163 ff. Kiel: Lorenz-von-Stein-Inst.

Hoffmann, C., Schulz, S. E. & Brackmann, F. (2013). Die öffentliche Verwaltung in den sozialen Medien? – zur Zulässigkeit behördlicher Facebook-Fan-Seiten. *ZD*, 122 ff.

Hoffmann, C., Schulz, S. E. (2014). Open Data für Kommunen, KommJur, 126 ff.

Hoffmann C. et al (2014). *Die digitale Dimension der Grundrechte*, Baden-Baden: Nomos.

Imenga, U., Mestmäcker, E.-J. (Hrsg.) (2007). *Wettbewerbsrecht, Bd. 2: GWB*. 4. Aufl. München: C. H. Beck.

Ingerl, R., Rohnke, C. (2010). *Markengesetz*. 3. Aufl. München: C. H. Beck.

Irlbauer, R. (2012). Gehört der Facebook-Fahndung die Zukunft? *Kriminalistik*, 764 ff.

Janda, T. C. (2012). Open Government – Transparenz, Partizipation und Kollaboration als Staatsleitbild. In: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 11 ff. Kiel: Lorenz-von-Stein-Inst.

Jotzo, F. (2009). Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr? *MMR*, 232 ff.

Karavas, V. (2007). *Digitale Grundrechte*. Baden-Baden: Nomos.

Karg, M. (2013). Anmerkung zur Entscheidung des VG Schleswig vom 14.2.2013 (8 B 60/12; ZD 2013, 245) – Zur Frage der Anwendbarkeit des deutschen Datenschutzrechtes auf Facebook. *ZD*, 247 f.

Karg, M. (2014). Anmerkung zu einer Entscheidung des VG Schleswig (Urteil vom 09.10.2013- 8 A 14/12, ZD 2014, 51) zum Verbot von Facebook-Fanseiten. *ZD*, 54 ff.

Karg, M., Thomsen, S. (2011). *Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook vom 19.08.2011*, abrufbar unter www.datenschutzzentrum.de.

Kluth, W. (2008). Die Strukturierung von Wissensgenerierung durch das Verwaltungsorganisationsrecht, In: Collin, P., Spiecker gen. Döhmann, I. (Hrsg.). *Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts*, S. 73 ff.

Knitsch, P. (2003). Die Rolle des Staates im Rahmen der Produktinformation – Zugleich ein Plädoyer für ein Verbraucherinformationsgesetz. *ZRP*, 113 ff.

Kramer, S. (2013). Kündigung eines leitenden Angestellten wegen privater Internetnutzung. *NZA*, 311 ff.

Krieg, H. (2009). Impressumspflicht bei Twitter? *AnwZert ITR 10*.

Krieg, H. (2010). Twitter und Recht. *K&R*, 73 ff.

Lübbe-Wolff, G. (1988). *Die Grundrechte als Eingriffsabwehrrechte: Struktur und Reichweite der Eingriffsdogmatik im Bereich staatlicher Leistungen*. Baden-Baden: Nomos.

Mann, T., Sennekamp, C. & Uechtritz, M. (Hrsg.) (2014). *VwVfG*. Baden-Baden: Nomos.

Martini, M. (2014). Vom heimischen Sofa in die digitale Agora: E-Partizipation als Instrument einer lebendigen Demokratie? In: Hill, H., Schliesky, U. (Hrsg.) *Die Neubestimmung der Privatheit*, S. 193 ff. Baden-Baden: Nomos.

Martini, M., Damm, M. (2013). Auf dem Weg zum Open Government: Zum Regimewechsel im Geodatenrecht. *DVBl*, 1 ff.

Martini, M., Damm, M. (2014). Der Zugang der Öffentlichkeit zu hochauflösenden Satellitenbildern. *NJW*, 130 ff.
Maunz, T., Dürig, G. (2013). *Grundgesetz-Kommentar, Loseblatt-Sammlung* (Stand: 69. EL).
Mergel, I. u. a. (2013). *Praxishandbuch Soziale Medien in der öffentlichen Verwaltung*. Heidelberg: Springer.
Müller, P., Schulz, S. E. (2011). *Die drei Dimensionen von Social Media Policy, Blogbeitrag v. 06.10.2011*, abrufbar unter www.government2020.de.
Müller, L.-S. u. a. (2014). *Ein soziales Netzwerk als internes Kommunikationsmittel für die öffentliche Verwaltung*, abrufbar unter www.isprat.net.
Müller-Broich, J. D. (2012). *Telemediengesetz*. Baden-Baden: Nomos.
Müller-Riemenschneider, S., Specht, L. (2014). Share oder Like? – Zur Reichweite der Einwilligung bei der Einbindung von Facebook-Buttons. *K&R*, 77 ff.
Murswiek, D. (2003). Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe Zu der Glykol- und der Osho- Entscheidung vom 26. 6. 2002. *NVwZ*, 1 ff.
Nieland, H. (2010). Störerhaftung bei Meinungsforen im Internet – Nachträgliche Löschungspflicht oder Pflicht zur Eingangskontrolle? *NJW*, 1494 ff.
Ossenbühl, F. (1998). *Staatshaftungsrecht*. 5. Aufl. München: C. H. Beck.
Ossenbühl, F. (2011). Verbraucherschutz durch Information. *NVwZ*, 1357 ff.
Papsthart, S. (2013). „Tweets" aus der Sitzung, „Stadtrat-TV". *BayVBl*, 645 ff.
Pawlak, K., Smeyers, L. (2013). Außerdienstliche Aktivitäten in sozialen Netzwerken – Gefahr für den Arbeitsplatz? *öAT*, 26 ff.
Piltz, C. (2011). Der Like-Button von Facebook. *CR*, 657 ff.
Piltz, C. (2013). Anmerkung zur Entscheidung des Schleswig-Holsteinischen VG vom 14.02.2013 (8 B 60/12) – Zur Rechtmäßigkeit der Sperrung von Nutzerkonten ohne Klarnamen in sozialen Netzwerken. *K&R*, 283 f.
Pitschas, R. (1983). Zur Anordnung eines Rauchverbots sowie zu Verhaltensregeln im Kommunalparlament. *JA*, 668 ff.
Polenz, S. (2012). Die Datenverarbeitung durch und via Facebook auf dem Prüfstand. *VuR*, 207 ff.
Pünder, H., Schellenberg, M. (Hrsg.) (2011). *Vergaberecht*. Baden-Baden: Nomos.
Redeker, H. (2012). *IT-Recht*. 5. Aufl. München: C. H. Beck.
Roggenkamp, J. D. (2010). *Web 2.0 Plattformen im kommunalen E-Government*. Stuttgart: Boorberg.
Roggenkamp, J. D. (2013). Facebook-Fahndung – Gefällt mir? *K&R 1/2013, Editorial*.
Roggenkamp, J. D. (2013). Wettbewerbsrechtliche Verantwortlichkeit für Mitarbeiterpostings bei Facebook. *JurisPR-ITR 25/2013 Anm. 6*.
Rücker, D. (2005). Notice and take down-Verfahren für die deutsche Providerhaftung? *CR*, 347 ff.
Ruhland, B. (2006). *Die Dienstleistungskonzession*. Baden-Baden: Nomos.
Sachs, M. (Hrsg.) (2011). *Grundgesetz – Kommentar*. 6. Aufl. München: C. H. Beck.
Säcker, F. J., Rixecker, R. (Hrsg.) (2012). *Münchener Kommentar zum BGB, Bd. 2*. 6. Aufl. München: C. H. Beck.
Säcker, F. J., Rixecker, R. (Hrsg.) (2013). *Münchener Kommentar zum BGB, Bd. 4*. 6. Aufl. München: C. H. Beck.
Schliesky, U. (2013). *Öffentliches Wirtschaftsrecht*. 4. Aufl. Heidelberg: C. F. Müller.
Schliesky, U. et al. (2014). *Schutzpflichten und Drittwirkung im Internet*. Baden-Baden: Nomos.
Schliesky, U., Schulz, S. E. (Hrsg.) (2012). *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*. Kiel: Lorenz-von-Stein-Inst.
Schmidt-Aßmann, E., Schoch, F. (Hrsg.) (2008). *Besonderes Verwaltungsrecht*. 14. Aufl. Berlin: De Gruyter.
Schmucker, J. (2013). Facebook kommunal. *DVP*, 319 ff.
Schulz, S. E. (2011). Social Media Guidelines. *ISPRAT Whitepaper*, herausgegeben von Kammer, M., Huppertz, M.-T. & Westerfeld, H., abrufbar unter www.isprat.net.

Schulz, S. E. (2012). Social Media Guidelines für die öffentliche Verwaltung. In: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 121 ff. Kiel: Lorenz-von-Stein-Inst.

Schulz, S. E., (2013). Ebenenübergreifendes Wissens- und Informationsmanagement der öffentlichen Verwaltung als Basis von Open Government Data. In: Dix, A. et al. (Hrsg.) *Jahrbuch für Informationsfreiheit und Informationsrecht 2012*, S. 247 ff. Berlin: Lexxion Verlagsgesellschaft.

Schulz, S. E. (2013). Aktuelle Entwicklungen im Informationszugangsrecht – erreicht ‚Open Data' den Gesetzgeber? *VerwArch 104*, 327 ff.

Schulz, S. E., Hoffmann, C. (2010). Grundrechtsrelevanz staatlicher Beobachtungen im Internet – Internet-Streifen der Ermittlungsbehörden und das Autorisierungskonzept des BVerfG. *CR*, 131 ff.

Schulz, S. E., Hoffmann, C. (2012). Staatliche Datenerhebung in sozialen Netzwerken. *DuD*, 7 ff.

Schulz, S. E., Hoffmann, C. (2013). Rechtsrahmen ermöglicht Teilnahme an sozialen Netzwerken. *Innovative Verwaltung 5/2013*, 16 ff.

Schulz, S. E., Janda, T. C. & Tischer, J. (2013). Alles „open" – oder: wie offen sind die Kommunikationsbeziehungen zwischen Staat und Gesellschaft ausgestaltet? In: Hill, H. (Hrsg.) *Verwaltungskommunikation*, S. 9 ff. Baden-Baden: Nomos.

Schulz, S. E., Jöns, J., Kuhlmann, F. (2014). Selbstorganisation der Gemeindevertretung: Medienöffentlichkeit und Mediennutzung, Die Gemeinde SH, i. E.

Schwenke, T. (2012). *Social Media Marketing & Recht*. Köln: O'Reilly.

Schwenke, T. (2014). Endlich rechtssicher? Facebook führt eine Impressumsrubrik für Seiten ein, Blogbeitrag v. 26.3.2014. http://rechtsanwalt-schwenke.de/facebook-fuehrt-impressumsrubrik-fuer-seiten-ein/.

Seel, H.-A. (2013). Aktuelles zum Umgang mit Emails und Internet im Arbeitsverhältnis – Was sind die Folgen privater Nutzungsmöglichkeit? *öAT*, 4 ff.

Soiné, M. (1997). Fahndung via Internet. *NStZ*, 166 ff., 321 ff.

Spindler, G., Schuster, F. (Hrsg.) (2011). *Recht der elektronischen Medien*. 2 Aufl. München: C. H. Beck.

Steinrötter, B. (2013). Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern. *MMR*, 691 ff.

Stelkens, P., Bonk, H. J. & Sachs, M. (Hrsg.) (2014). *VwVfG*. 8. Aufl. München: C. H. Beck.

Terhaag, M. (2010). Anmerkung zu einem Urteil des BGH vom 25.03.2010 (I ZR 197/08; K&R 2010, 660) – Zur Frage des Herausgabeanspruchs des Treugebers aus § 667 BGB auf Übertragung oder Umschreibung des Domainnamens. *K&R*, 662 f.

Ulbricht, C. (2012). Social Media & Recht – Praktische Handlungsempfehlungen für Kommunen. *KommunalPraxis spezial*, 101 ff.

Ulbricht, C. (2013). *Social Media und Recht*. 2. Aufl. Freiburg: Haufe-Gruppe.

Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein. (2011). *Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social Plugins?*, abrufbar unter www.datenschutzzentrum.de.

Voigt, P., Alich, S. (2011). Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber. *NJW*, 3541 ff.

Warnecke, T. (2012). Das Bürgertelefon 115 mit Mehrkanalzugang – Rechtsfragen und Lösungsvorschläge. In: Schliesky, U., Schulz, S. E. *Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung*, S. 57 ff. Kiel: Lorenz-von-Stein-Inst.

Zilkens, M., Cavin, A., Soziale Netzwerke im Umfeld kommunaler Aufgabenerfüllung, ZD 2013, 603 ff.

Sachverzeichnis

G. Hornung, R. Müller-Terpitz (Hrsg.), *Rechtshandbuch Social Media,*
DOI 10.1007/978-3-642-38192-8

T