

Die Bekämpfung von Fake News

**Der Vorschlag des EU Digital Services Act vor dem
Hintergrund des deutschen Netzwerkdurchsetzungs-
gesetzes**

Gerald Spindler

I. Einleitung

Fake News haben sich als Bedrohung demokratischer Meinungsbildungsprozesse spätestens seit den Wahlen zum US-Präsidenten 2017 und den zu beobachtenden Manipulationen in den sog. sozialen Medien wie Facebook, Instagram oder Twitter herausgestellt. Aber nicht nur Fake News spielen eine erhebliche Rolle, sondern auch die eher auf Mikroebene zu beobachtenden Phänomene der Hate-speech, des Mobbing und des Stalking bis hinunter auf schulische Ebenen sind zu beobachten. Umso mehr geraten natürlich auch rechtliche Regelungsmöglichkeiten in den Fokus, hier vor allem die als Gatekeeper bezeichneten Betreiber großer sozialer Netzwerke. Angesichts nach wie vor bestehender Probleme, die Urheber von Falschnachrichten oder Hass-Botschaften zu identifizieren und sie straf- oder zivilrechtlich zu verfolgen, bieten offenbar die Betreiber der sozialen Netzwerke bessere Möglichkeiten, Fake News oder Hass-Botschaften zu bekämpfen. Nicht zuletzt aufgrund ihrer eigenen Community Standards haben diese Netzwerkbetreiber bereits mehr oder minder strenge, aber rein auf privater Basis durchgeführte Inhaltskontrollen eingeführt.

Das Spannungsfeld aus verfassungsrechtlicher Sicht hinsichtlich der Bekämpfung von Fake News, insbesondere mit automatisierten Verfahren, liegt auf der Hand: Auf der einen Seite das hohe Gut der Sicherung demokratischer Meinungsbildungsprozesse, auf der anderen Seite die Gefahr einer übermäßigen Beeinträchtigung der Kommunikationsfreiheiten, insbesondere durch das sog. „overblocking“, also der überschießenden Sperrung und Löschung von Inhalten, die an sich durch die Meinungsfreiheit nach Art. 5 Abs. 1 GG gedeckt wären, aber durch automatisierte Systeme als solche – da kontextabhängig – nicht erkannt werden können.

Hinsichtlich der Plattformbetreiber waren diese bislang weitgehend von jeglicher Verantwortlichkeit befreit, da sie unter Art. 14 E-Commerce-RL bzw. § 10 TMG fielen, die jegliche Verantwortlichkeit – gleich ob zivil-, straf- oder verwaltungsrechtlich – grosso modo¹ davon abhängig machen, ob der Betreiber Kenntnis von der konkreten rechtswidrigen Tätigkeit oder dem Inhalt hat. Erst nach Kenntniserlangung war der Betreiber verpflichtet, den konkreten Inhalt zu sperren oder zu löschen (notice-and-take-down-Verfahren), wobei zahlreiche Einzelheiten nach wie vor ungeklärt sind, etwa wie präzise die Mitteilung an den Betreiber ausfallen muss.² Es ist daher nicht verwunderlich, dass angesichts dieser

¹ Genauer gesprochen genügen nach § 10 TMG bzw. Art. 14 E-Commerce-RL für zivilrechtliche Schadensersatzansprüche die Kenntnis von Umständen, die solche rechtswidrigen Tätigkeiten bzw. Inhalte nahelegen.

² *Spindler*, in: *Spindler/Schmitz*, 2. Aufl. 2018, TMG § 10 Rn 24 ff.; *Hoffmann/Volkmann*, in: *Spindler/Schuster*, *Recht der elektronischen Medien*, 4. Aufl. 2019, TMG § 10 Rn 18 ff.; zur Auslegung des Begriffs „Kenntnis“ durch den EuGH vgl. EuGH, 22.06.2021 – C-682/18, C-683/18, GRUR-RS 2021, 15191 Rn. 85 – Youtube/Peterson und Cyando/Elsevier; vgl. dazu auch die Besprechung *Spindler*, NJW 2021, 2554.

weitgehenden Freistellung von Pflichten der Plattformbetreiber zunächst vor den damaligen Bundestagswahlen 2017 der deutsche Gesetzgeber in Gestalt der Verabschiedung des Netzwerkdurchsetzungsgesetzes (NetzDG)³ und nunmehr auch die EU-Kommission durch den Vorschlag eines neuen Digital Services Act (DSA)⁴ tätig wurde; beide Normenwerke führen auf unterschiedliche Weise und Ebenen Pflichten der Plattformen ein, die die Betreiber stärker in die Pflicht nehmen sollen. Dementsprechend werden im Folgenden zunächst das NetzDG und dann der Digital Services Act mit einem Fokus auf fake news und die Einbindung der Plattformbetreiber behandelt.⁵

II. Das Netzwerkdurchsetzungsgesetz (NetzDG)

Der grundsätzliche Ansatz des NetzDG besteht darin, die Plattformbetreiber zur effizienten Behandlung von Beschwerden zu verpflichten, zum einen zur Einrichtung eines Beschwerdemanagementsystems, zum anderen zur Löschung und Sperrung von rechtswidrigen Inhalten innerhalb einer Woche, bei evident rechtswidrigen Inhalten sogar binnen 24 Stunden. Durchgesetzt werden diese Pflichten durch Bußgelder sowie Transparenz- und Publizitätspflichten. Demgegenüber hat bisher ein Anspruch des Betroffenen auf Wiederherstellung seiner Inhalte keine Berücksichtigung gefunden.

A. Der Anwendungsbereich

1. Soziale Netzwerke: von der individuellen Kommunikation zur Massenkommunikation

Der Begriff der sozialen Netzwerke ist bislang dem deutschen Recht – soweit ersichtlich – fremd. Das TMG enthält keine derartige Definition, sondern findet auf sämtliche Telemedien Anwendung, zu denen ohne Zweifel auch die sozialen Netzwerke gehören.⁶ Der Gesetzgeber versucht das Phänomen dadurch in den Griff zu bekommen, dass in § 1 Abs. 1 NetzDG als soziales Netzwerk ein Telemediendienst definiert wird, der dazu bestimmt ist, dass „beliebige Inhalte mit anderen Nutzern“ geteilt oder „der Öffentlichkeit zugänglich“ gemacht werden.⁷

³ Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 1 des Gesetzes vom 3. Juni 2021 (BGBl. I S. 1436) geändert worden ist.

⁴ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, COM/2020/825 final.

⁵ Die Ausführungen gehen auf Publikationen des Verf. in K&R 2017 zum NetzDG sowie in GRUR 2021 zum Digital Services Act zurück.

⁶ Näher dazu *Spindler*, in: *Spindler/Schmitz*, 2. Aufl. 2018, TMG § 1 Rn. 78 f.

⁷ BegrRegE BT-Drs. 18/12356, S. 19 unter Verweis auf BGH, 8.7.1993 – I ZR 124/91, GRUR 1994, 45, 46 – Verteileranlagen; BGH, 11.7.1996 – I ZR 22/94, GRUR 1996, 875, 876 – Zweibettzimmer im Krankenhaus und BGH, 22. 4. 2009 – I ZR 216/06,

Dabei versteht der Gesetzgeber den Begriff des der Öffentlichkeit Zugänglichmachens genauso wie im Urheberrecht im Rahmen der Regelung des § 19a UrhG. Mit § 1 Abs. 1 S. 3 NetzDG, der ebenfalls durch den Bundestag erst eingefügt wurde, sollen Plattformen ausgenommen werden, „die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind“. Damit versucht der Gesetzgeber der Kritik am RegE⁸ Rechnung zu tragen, dass der Anwendungsbereich viel zu breit geraten war und selbst Messaging- und Mailedienste unter die Definition der Netzwerke fielen.⁹ Allerdings ist nach wie vor fraglich, ob tatsächlich nur die sozialen Netzwerke wie Facebook oder Twitter damit erfasst werden; denn auch über Host-Provider, die ihre Plattformen zur Verfügung stellen, damit User Inhalte hochladen und dann ggf. per Hyperlink diese mit anderen teilen, fallen im Prinzip unter die Definition, bis hin zu Cloud Dienste Anbietern, bei denen ein Nutzer seinen Account mit anderen teilen kann. Auch Dienste wie Microsoft OneDrive oder Dropbox fallen deshalb nicht aus dieser Definition heraus, selbst wenn man das Merkmal „dazu bestimmt“ eng interpretiert; sie sind gerade dazu gedacht, dass Inhalte synchron bearbeitet werden können, so dass sie ebenfalls den „Netzwerken“ unterfallen. Ebenso wenig dienen diese Dienste nur der Individualkommunikation, sondern können auch von mehreren gleichzeitig genutzt werden. Selbst für Messengerdienste, die der Gesetzgeber ausdrücklich ausnehmen will, ergeben sich Zweifel: Warum sollten etwa große WhatsApp-Gruppen nicht dem Begriff der sozialen Netzwerke unterfallen (da Messengerdienst), kleine Twittergruppen bzw. Follower dagegen schon? Die Unterscheidung zwischen Individual- und Massenkommunikation ist gerade im Zeitalter des Internet schon immer fragwürdig gewesen.¹⁰ Dies wird derzeit auch am Verfahren des Bundesamtes für Justiz gegen den Messengerdienst „Telegram“ deutlich, auf dem sich zahlreiche Kanäle von zigtausenden „Followern“ finden.¹¹

Nach Auffassung des Gesetzgebers sollen in diesem Rahmen ferner berufliche Netzwerke wie XING oder LinkedIn nicht unter den Begriff des sozialen Netzwerks fallen, da sie nur darauf angelegt seien, spezifische Inhalte zu verbreiten.¹² Auch Online-Spiele, Fachportale oder Verkaufsplattformen sollen unter diese Ausnahme fallen.¹³ Offen bleibt, was „spezifische“ Inhalte sind: Wäre etwa eine rechtsextremistische Plattform auf „spezifische“ (eben rechtsextreme) Inhalte aus-

GRUR 2009, 845, 848 – Internet-Videorecorder; vgl. Begr. Rechtsausschuss BT-Drs. 18/13030 S. 19, Begr. RegE BT-Drs. 18/12727 S. 28.

⁸ Stellungnahme BITKOM vom 30. 03. 2017, S. 5; ähnlich Stellungnahme eco Verband der Internetwirtschaft e. V., 30. 3. 2017, S. 4.

⁹ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

¹⁰ Näher dazu *Spindler*, in: *Spindler/Schmitz*, 2. Aufl. 2018, TMG § 1 Rn. 44 f.; ebenfalls krit. etwa: *Roßnagel*, NVwZ 2007, 743, 745; *Bizer*, DuD 2007, 40.

¹¹ FAZ, Bundesamt für Justiz geht gegen Telegram vor, 14.6.2021, abrufbar unter: <https://s.gwdg.de/da2Nm9>.

¹² Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

¹³ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

gerichtet und würde damit nicht dem NetzDG unterfallen (was wohl kaum in der Intention des Gesetzgebers liegt)? Auch der eingegrenzte Teilnehmerkreis führt nicht recht weiter: Warum sollte dieses Merkmal bei beruflichen Plattformen gegeben sein (und damit das NetzDG nicht anwendbar), warum bei Facebook mit entsprechend eingegrenztem Freundeskreis?

Das Gesetz lässt sich nur durch eine restriktive Interpretation dergestalt retten, dass ausschließlich Plattformen mit überwiegend meinungsbildenden Inhalten gemeint sind, worauf auch die Mehrzahl der genannten Delikte hinweist – was seinerseits allerdings immer noch breit gefasst ist. Welche Form der Inhalt hat, spielt dabei keine Rolle, ob Video, Musik oder Text.¹⁴ Ferner sollte der Terminus „dazu bestimmt sind“ dahingehend interpretiert werden, dass die Plattform entsprechende Tools zur Kommunikation bereitstellt; völlig neutrale Host-Provider, bei denen aber durch die Nutzer Inhalte geteilt werden können (Cloud etc.), wären damit ausgenommen vom Begriff der sozialen Netzwerke – indes immer noch nicht Synchronisierungsdienste wie Dropbox.

Ferner beschränkt das Gesetz den Begriff auf Betreiber von Plattformen mit Gewinnerzielungsabsicht; rein private Kommunikationsplattformen oder non-profit Plattformen sind damit ausgeschlossen. Versteht man in den einschlägigen Lizenzen wie creativecommons den Begriff „non-commercial“ in der gleichen Weise, sind Plattformen wie Wikipedia vom NetzDG ausgenommen.¹⁵ Allerdings herrscht hier nach wie vor große Unsicherheit, ob der Begriff in gleicher Weise wie im deutschen Recht zu verstehen ist.¹⁶

2. Zahl der registrierten Nutzer im Inland

§ 1 Abs. 2 NetzDG schränkt den Anwendungsbereich auf große soziale Netzwerke mit mehr als 2 Mio. im Inland registrierte Nutzer ein. Ob die Nutzer ihren Wohnsitz oder gewöhnlichen Aufenthalt im Inland haben, spielt dabei keine Rolle; allein die Registrierung unter ihrer IP-Adresse ist maßgeblich. Dabei spielt es nach Auffassung des Gesetzgebers keine Rolle, „in welchem Land der jeweilige Nutzer hauptsächlich aktiv ist“.¹⁷ Abgesehen davon, dass damit Missbrauch möglich ist, indem die Registrierungen im Ausland erfolgen, ergeben sich en detail

¹⁴ Begr. RegE BT-Drs. 18/12356, S. 19.

¹⁵ Für eine restriktive Auslegung bei Nutzungsrechteinräumung: LG Köln, 5. 3. 2014 – 28 O 232/13, MMR 2014, 478, 480 f. m. krit. Anm. *Jaeger/Mantz*; „rein private Nutzung“; unter Anwendung des § 305c Abs. 2 BGB weitergehend: OLG Köln, 31. 10. 2014 – 6 U 60/14, K&R 2015, 57 ff. = MMR 2015, 331 Rn. 87: „keinen direkten finanziellen Vorteil“; zu den Grenzfällen und für Einzelfallauslegung plädierend: *Kreutzer*, Open Content Lizenzen, 2011, 44 ff.

¹⁶ Zu den Schwierigkeiten der Auslegung generischer Lizenzversionen etwa: OLG Köln, 31. 10. 2014 – 6 U 60/14, K&R 2015, 57 ff. = MMR 2015, 331 Rn. 74 ff., insbes. 79, 86; *Kreutzer*, Open Content Lizenzen, 2011, 42 f.; *Jaeger/Mantz*, MMR 2014, 480 f.

¹⁷ Begr. RegE BT-Drs. 18/12356, S. 20.

weitere Abgrenzungsprobleme: So definiert das Gesetz nicht, für welchen Zeitraum die Grenze von 2 Mio. Nutzern gelten soll. Hier wird man von einer halbjährlichen Durchschnittszahl von 2 Mio. Nutzern ausgehen müssen, um zu vermeiden, dass tägliche Schwankungen eintreten und damit unklar wäre, wann das Gesetz eingreift und wann nicht. Das Gesetz sieht selbst bei den Berichtspflichten einen halbjährlichen Turnus vor, so dass dies als Anhaltspunkt für die Berechnung dienen mag.

Moniert wurde auch die fehlende datenschutzrechtliche Grundlage für die Speicherung der IP-Adresse bei der Registrierung;¹⁸ dem widerspricht allerdings die Rechtfertigung nach Art. 6 Abs. 1 S. 1 lit. c DSGVO,¹⁹ da es sich um die Erfüllung gesetzlicher Pflichten handelt, für die die Speicherung der IP-Adresse erforderlich ist. Ein späterer Wechsel der IP-Adresse und der „Wegzug“ des im Inland zuvor registrierten Nutzers löst im Prinzip eine Neuberechnung der Schwelle aus, so dass die Netzwerke faktisch gezwungen sind, zumindest jährlich eine Abfrage bei den Nutzern durchzuführen.

3. Ausnahmen für journalistische Plattformen

Das NetzDG soll nicht für „Plattformen mit journalistisch-redaktionell gestalteten Angeboten (gelten), die vom Diensteanbieter selbst verantwortet werden“, § 1 Abs. 1 S. 2 NetzDG. Für diese sollten die Vorschriften der §§ 74 ff. MStV eingreifen.²⁰ Damit ist wieder – wie etwa im Leistungsschutzrecht für Presseverleger, auch bei §§ 74 ff. MStV – die Frage aufgeworfen, was man unter „journalistisch-redaktionell gestaltet“ verstehen kann. Hier wird es auf eine aktive Gestaltung und Einzelauswahl bzw. Zusammenstellung von Beiträgen ankommen; allein die Einrichtung von bestimmten Inhaltskategorien, unter denen dann Blogs oder Beiträge abgelegt werden können, reicht hierfür nicht.²¹

Zudem müssen diese Angebote vom Anbieter „selbst verantwortet“ werden – dieser sonst im NetzDG nicht verwandte Begriff ist in derselben Weise wie § 10 S. 2 TMG zu verstehen, der auf die Aufsicht des Telemedienanbieters gegenüber denjenigen, die Inhalte einstellen, abstellt. Eine reine Moderation z. B. genügt hier-

¹⁸ Stellungnahme BITKOM, 30.3.2017, S. 5; ähnlich Stellungnahme eco Verband der Internetwirtschaft e. V., 30. 3. 2017, S. 4.

¹⁹ VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 v. 4. 5. 2016, S. 1; zuvor § 4 Abs. 2 Nr. 1 BDSG a.F.

²⁰ Begr. RegE BT-Drs. 18/12356, S. 19.

²¹ Näher dazu *Spindler*, in: *Spindler/Schmitz*, 2. Aufl. 2018, TMG § 1 Rn. 66 ff.; ferner *Held*, in: *Hahn/Vesting*, *Rundfunkrecht*, 3. Aufl. 2012, RStV § 54 Rn. 38 ff.; *Fricke*, in: *Spindler/Schuster*, *Recht der elektronischen Medien*, 4. Aufl. 2019, UrhG § 87f Rn. 6; *Martini*, in: *BeckOK InfoMedienR*, 33. Ed. 2021, MStV § 2 Rn. 19; *Leitgeb*, ZUM 2009, 39, 42; *Weiner/Schmelz*, *K&R* 2006, 453, 456 f.

für nicht, da Inhalte nicht für den Anbieter bzw. in dessen Auftrag angefertigt werden.

Unklar und wichtig für die Verbreitung von hate speech und fake news ist, ob auch Gästeforen von (online) Zeitungen unter die Ausnahme des § 1 Abs. 3 NetzDG fallen: Dagegen spricht auf den ersten Blick, dass es sich hier nicht um journalistisch-redaktionelle Angebote des Diensteanbieters handelt, sondern eindeutig um fremde, nicht verantwortete Beiträge. Doch sind diese Gästeforen Teil des gesamten Angebots solcher Plattformen – und die Ausnahme bezieht sich auf die Plattform als solche und nicht auf einzelne Bestandteile der Plattform.

Da die Ausnahme sich auf die Plattform als solche bezieht, werden auch Inhalte, die von Journalisten stammen – bzw. von mehreren mit redaktioneller Gestaltung –, aber auf anderen Plattformen wie z. B. Facebook gepostet werden, nicht von der Ausnahme umfasst.²² Schwierig sind die Fälle zu erfassen, in denen eine Zeitung, ein Radiosender etc. ein eigenes Facebook-Profil, einen Twitter-Account oder einen YouTube-Kanal unterhält: Hier lässt sich nur mit einer Art inhärenten Bereichsausnahme arbeiten, da diese Profile etc. für den objektiven Nutzer als solche mit journalistisch-redaktionellen Inhalt als Gesamtangebot erkennbar sind, so dass auch sie in den Genuss der Ausnahme nach § 1 Abs. 3 NetzDG kommen, obwohl der Diensteanbieter hier nicht der eigentliche Betreiber des sozialen Netzwerks ist. In vergleichbarer Weise wird als Host Provider auch derjenige angesehen, der ein Facebook-Profil betreibt und hier die Speicherung fremder Inhalte gestattet.²³ Daher werden Plattformen, die zwar fake news vertreiben, wie etwa die offenbar von Russland unterhaltenen Inhaltsgebote wie Russia Today etc.²⁴ nicht vom NetzDG erfasst.

4. Rechtswidrige Inhalte

Die Pflichten, die das NetzDG den Betreibern sozialer Netzwerke auferlegt, greifen aber nur bezüglich bestimmter strafrechtlicher Delikte ein, die § 1 Abs. 3 NetzDG abschließend aufzählt. Der Katalog des § 1 Abs. 3 NetzDG bezieht sich im Wesentlichen auf Kommunikationsdelikte, aber auch auf Delikte gegen die öffentliche Ordnung, etwa § 130 StGB,²⁵ und nunmehr auch auf § 201 a StGB und damit der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen. Klargestellt wurde zudem, dass nur rechtswidrige Delikte bzw. solche,

²² S. auch die Kritik in der Stellungnahme BITKOM vom 30. 3. 2017, S. 4.

²³ Etwa: LG Würzburg, 7. 3. 2017 – 11 O 2338/16, MMR 2017, 347, 348; ähnlich bei Websites: LG Frankfurt a. M., 5. 8. 2015 – 2-03 O 306/15, CR 2016, 461, 462.

²⁴ S. dazu die Angaben zu fake news bei <https://euvsdisinfo.eu/>.

²⁵ Zum Eintritt eines Erfolgs im Inland (§ 9 Abs. 1 3.Var. StGB) bei Volksverhetzung auf ausländischem Server: BGH, 12. 12. 2000 – 1 StR 184/00, ZUM-RD 2001, 103, 107 – *Toeben*; nunmehr durch BGH, 3. 5. 2016 – 3 StR 449/15, NStZ 2017, 146 aufgegeben; ausführlich zur Diskussion *Schwidessen*, CR 2017, 443, 447 f.; *Handel*, MMR 2017, 227, 228 f.

die nicht gerechtfertigt sind, unter den Katalog des § 1 Abs. 3 NetzDG fallen, womit insbesondere § 193 StGB als besonderer Rechtfertigungsgrund für Kommunikationsdelikte nochmals hervorgehoben wird.²⁶ Dadurch, dass der Gesetzgeber explizit nur auf rechtswidrige Inhalte abstellt, kommt es seiner Auffassung nach nicht darauf an, ob die Delikte auch schuldhaft begangen worden sind.²⁷ Offenbar soll es auch nicht darauf ankommen, ob ein Strafantrag gestellt wurde, wie er etwa gem. § 194 StGB für die Beleidigung nach § 185 StGB erforderlich ist.²⁸

5. Verfassungsrechtliche Problematiken

Sowohl vor als auch mit der Einführung des NetzDG im Jahr 2017 wurden in der Literatur verbreitet verfassungsrechtliche Bedenken gegen das Gesetz geäußert.²⁹ Dabei standen sowohl Fragen der formellen als auch der materiellen Verfassungsmäßigkeit zur Debatte.

a) Gesetzgebungskompetenz des Bundes

Im Mittelpunkt der Diskussion um die formelle Verfassungsmäßigkeit steht die fehlende Gesetzgebungskompetenz des Bundes, die nach Art. 70 Abs. 1 GG grundsätzlich bei den Ländern liegt. Der Bund darf hingegen nur tätig werden, soweit ihm nach Art. 73, 71 GG die ausschließliche, bzw. nach Art. 74, 72 GG die konkurrierende Gesetzgebungskompetenz zugeschrieben ist.

Mit dem NetzDG reguliert der Bundesgesetzgeber soziale Netzwerke, die als inhaltsbezogene Telemediendienste i.S.d. § 1 Abs. 1 TMG einzuordnen sind. Somit scheidet die ausschließliche Gesetzgebungskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 7 GG, die sich allein auf technische Fragen der Telekommunikation bezieht,³⁰ von vornherein aus.³¹

Für das NetzDG stützt der Bundesgesetzgeber ausweislich der Gesetzesbegründung seine Kompetenz grundsätzlich auf das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG).³² Dieser Kompetenztitel kann jedoch nur Anwendung finden, wenn der Regelungsgehalt der mit NetzDG eingeführten Normen auch einen

²⁶ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 21.

²⁷ Begr. RegE BT-Drs. 18/12356, S. 20.

²⁸ Krit. daher Stellungnahme eco Verband der Internetwirtschaft e. V., 30. 3. 2017, S. 4 f.

²⁹ *Papier*, NJW 2017, 3025; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433; *Gersdorf*, MMR 2017, 439; *Liesching*, MMR 2018, 26; *Ladeur/Gostomzyk*, K&R 2017, 390; *Wimmers/Heymann*, AfP 2017, 93; *Spindler*, K&R 2017, 533; *Kalbbenn/Hemmert-Halswick*, MMR 2020, 518; *Nolte*, ZUM 2017, 552; *Heckmann/Wimmers* CR 2017, 310; *Müller-Franken* AfP 2018, 1; *Koreng* GRUR-Prax 2017, 203.

³⁰ BVerfG, 02.03.2010- 1 BvR 256/08 = BVerfGE 125, 260, 314; *Degenhart*, in: Sachs, 9. Aufl. 2021, GG Art. 73 Rn. 34.

³¹ So auch *Gersdorf*, MMR 2017, 439, 439.

³² Begr. RegE BT-Drs. 18/12356, S. 13.

sachlichen Zusammenhang zum Recht der Wirtschaft aufweist.³³ Diese Einordnung kann indessen aufgrund der außerordentlichen Bedeutung der Grundrechte des Art. 5 Abs. 1 GG nicht durchgehalten werden.³⁴

Hier steht schließlich nicht die wirtschaftliche Betätigung der Netzwerke, sondern das äußerungsrechtliche Element im öffentlichen Diskurs im Vordergrund.³⁵ Die Gesetzgebungskompetenz für Regelungen betreffend die Gewährleistung der verfassungsmäßigen Ordnung im Bereich der Telemedien – inklusive der allgemeinen Gesetze – verbleibt damit nach Art. 70 Abs. 1 GG bei den Ländern.³⁶

Schließlich überzeugt auch die vom Bundesgesetzgeber angeführte Kompetenz aus Art. 74 Abs. 1 Nr. 7 GG nicht abschließend. Mit dem NetzDG sollen auch Belange des Jugendschutzes adressiert werden, die der öffentlichen Fürsorge zuzuordnen seien. Indessen gehen die Regelungen des NetzDG weit über den originären Bereich des Jugendschutzes hinaus, indem die eingeführten Regelungen zugunsten und gegenüber sämtlichen Personengruppen Geltung beanspruchen.³⁷

Unabhängig davon, dass dem Bundesgesetzgeber damit keine Gesetzgebungskompetenz nach Art. 74 Abs. 1 Nr. 7, 11 GG zusteht, bestehen weiterführend auch Bedenken hinsichtlich der Erforderlichkeitsprüfung nach Art. 72 Abs. 2 GG.³⁸ Die Erforderlichkeit einer bundesgesetzlichen Regelung zur Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder zur Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse kann schon deshalb bezweifelt werden, da die Länder mit dem MStV eine einheitliche Regelung für das Recht der Telemediendienste gefunden haben. Nach § 17 S. 2 MStV gilt für Angebote von Telemedien einerseits die verfassungsmäßige Ordnung. Andererseits müssen diese nach § 17 S. 3 MStV auch die Vorschriften der allgemeinen Gesetze und die Bestimmungen zum Schutz der persönlichen Ehre einhalten. Inwieweit neben diesem bereits bestehenden Pflichtenkanon auf Länderebene auch noch eine Bundesregelung erforderlich sein soll, ist daher nicht ersichtlich.³⁹

³³ BVerfG, 29.04.1958 – 2 BvO 3/56 = BVerfGE 8, 143, 149f.; BVerfG, 11.02.2004 – 2 BvR 834/02 = BVerfGE 109, 190, 215.

³⁴ *Liesching*, MMR 2018, 26; *Gersdorf*, MMR 2017, 439, 441; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 434 f.; *Ladner/Gostomzyk*, K&R 2017, 390; *Wimmers/Heymann*, AfP 2017, 93, 97; *Hain*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, C. Verfassungsrecht, Rn. 164.

³⁵ *Hain*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, C. Verfassungsrecht, Rn. 164; *Liesching*, MMR 2018, 26, 26; *Gersdorf*, MMR 2017, 439, 441.

³⁶ Ebd.

³⁷ *Liesching*, in: *Liesching*, 1. Aufl. 2018, NetzDG Einleitung, Rn. 5; *Hain*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, C. Verfassungsrecht, Rn. 164; *Gersdorf*, MMR 2017, 439, 441.

³⁸ *Gersdorf*, MMR 2017, 439, 445 f.; *Liesching*, in: *Liesching*, 1. Aufl. 2018, NetzDG Einleitung, Rn. 5.

³⁹ So auch, wenn auch noch zum alten § 54 Abs. 1 RStV *Gersdorf*, MMR 2017, 439, 445 f.

Abschließend ist dem Bundesgesetzgeber lediglich mit Blick auf § 4 NetzDG, der die Einführung von Bußgeldtatbestände betrifft, die Gesetzgebungskompetenz nach Art. 74 Abs. 1 Nr. 1 GG einzuräumen. Insoweit wird zum Sachgebiet des Strafrechts i.S.d. Norm auch das Ordnungswidrigkeitenrecht gezählt.⁴⁰ Eine darüber hinaus gehende Kompetenz kann jedoch auch diesem Kompetenztitel nicht entnommen werden.⁴¹

b) Hinreichende Bestimmtheit der Normen

Neben den Bedenken bezüglich der Gesetzgebungskompetenz ist weitergehend auch ein Verstoß gegen den Bestimmtheitsgrundsatz in Betracht zu ziehen. Als spezielle Ausformung des Rechtsstaatsprinzips folgt aus Art. 20 Abs. 3 GG, dass gesetzliche Tatbestände derart präzise formuliert sein müssen, dass der jeweilige Normadressat sein Handeln kalkulieren kann, weil die Folgen der Regelung für ihn voraussehbar und berechenbar sind.⁴² Der Bestimmtheitsgrundsatz wird für den Bereich des Strafrechts, der hier aufgrund der Bußgeldvorschriften in § 4 NetzDG eröffnet ist,⁴³ schließlich in Art. 103 Abs. 2 GG nochmal explizit aufgenommen und verschärft.⁴⁴

In diesem Zusammenhang begegnet etwa der vage Begriff der „offensichtlich rechtswidrigen Inhalte“ in § 3 Abs. 2 Nr. 2 NetzDG Bedenken. Dem Wortlaut nach scheint sich die Rechtswidrigkeit auf die Inhalte zu beziehen. Somit liegt insoweit eine – zumindest sprachliche – Diskrepanz zur strafrechtlichen Dogmatik vor, wonach ausschließlich Tathandlungen dem Vorwurf der Rechtswidrigkeit ausgesetzt werden können.⁴⁵ Außerdem soll die Beurteilung der Rechtswidrigkeit zunächst durch die Netzwerkanbieter gewährleistet werden. Gerade für den Bereich der Beleidigungsdelikte hat sich indessen eine umfangreiche Kasuistik in der Rechtsprechung entwickelt, die auch unter dem Eindruck grundrechtlicher Einflüsse wie etwa der Meinungsfreiheit aus Art. 5 Abs. 1 GG steht. Einerseits die Kenntnis dieser Dogmatik sowie andererseits deren korrekte Anwendung im Einzelfall kann von den Netzwerkanbietern jedoch kaum erwartet werden.⁴⁶

⁴⁰ BVerfG, 16.07.1969 – 2 BvL 2/69 = BVerfGE 27, 18, 32 f.; *Degenhart*, in: Sachs, 9. Aufl. 2021, GG Art. 74 Rn. 11.

⁴¹ *Gersdorf*, MMR 2017, 439, 440.

⁴² BVerfG, 03.03.2004 – 1 BvF 3/92 = BVerfGE 110, 33, 53 f.; *Sachs*, in: Sachs, 9. Aufl. 2021, GG Art. 20 Rn. 129; *Huster/Rux*, in: BeckOK GG, 48. Ed. 15.8.2021, GG Art. 20 Rn. 182.

⁴³ *Liesching*, MMR 2018, 26, 27.

⁴⁴ *Degenhart*, in: Sachs, 9. Aufl. 2021, GG Art. 103 Rn. 63.

⁴⁵ *Wimmers/Heymann*, AfP 2017, 93, 101; *Liesching*, MMR 2018, 26, 26 f.; *ders.*, in: Spindler/Schmitz, 2. Aufl. 2018, NetzDG § 1 Rn. 75 f.; a.A. *Hoven/Gersdorf*, in: BeckOK Info MedienR, 33. Ed. 1.5.2021, NetzDG § 1 Rn. 41.

⁴⁶ *Liedemann*, MMR 2019, 279, 282; *Ladeur*, in: Eifert/Gostomzyk (Hrsg.), Netzwerkrecht, S. 160, 184.

Überraschend ist insoweit ebenfalls, dass es nach Auffassung des Gesetzgebers auch eine Kategorie von „rechtswidrigen Inhalten“ gibt, die „offensichtlich“ so einzuordnen ist. Welche Anforderungen an den Grad der Offensichtlichkeit zu stellen sind, ergibt sich jedoch nicht aus dem NetzDG. Für den Normadressaten ist folglich nicht kalkulierbar, welche konkreten Pflichten zu erfüllen sind.⁴⁷

Gleichermaßen vage und unbestimmt sind auch die Begriffe der „organisatorischen Unzulänglichkeit“ in § 3 Abs. 4 S. 2 NetzDG sowie der „Schulungs- und Betreuungsangebote“ in § 3 Abs. 4 S. 4 NetzDG. Für letztere sind insbesondere keine einheitlichen Vorgaben zu deren Ausgestaltung, etwa durch Zertifizierungen oder Audits, aufgestellt worden.

c) Verletzung von Grundrechten

Im Rahmen der materiellen Verfassungsmäßigkeit des NetzDG wird außerdem die Verletzung verschiedener Grundrechte kritisiert. Bei der Darstellung sind die Grundrechte der Nutzer von denen der Netzbetreiber zu unterscheiden.

Meinungs- und Informationsfreiheit der Nutzer, Art. 5 Abs. 1 GG

Zunächst sind die negativen Effekte des NetzDG auf die Meinungs- und Informationsfreiheit der Nutzer aus Art. 5 Abs. 1 GG zu untersuchen. Dabei ist zu beachten, dass sich das NetzDG seinem Anwendungsbereich nach nur an soziale Netzwerke richtet, der Einfluss der Grundrechte der Nutzer gleichwohl über die mittelbare Drittwirkung im Verhältnis zum Netzbetreiber zu berücksichtigen ist.

Mit der Pflicht zur Löschung rechtswidriger Inhalte nach § 3 Abs. 2 NetzDG wird dementsprechend mittelbar in die Kommunikationsgrundrechte der Nutzer eingegriffen.⁴⁸ Der Gewährleistungsgehalt der Meinungsfreiheit erfasst insoweit jedes im Rahmen einer Stellungnahme oder eines Dafürhaltens geäußerte Werturteil.⁴⁹ Im Kontext des NetzDG ist zu beachten, dass das Gesetz im Grundsatz neutral gegenüber Meinungsinhalten steht, jedoch dann zu Sperrung- bzw. Löschung aufruft, wenn diese Meinung mit den Mitteln der Hassrede etwa im Rahmen eines Verstoßes gegen Strafgesetze kommuniziert wird. Besonders kritisch ist insoweit anzumerken, dass die Beurteilung der Rechtswidrigkeit des Inhalts den Netzanbietern und nicht etwa den Gerichten obliegt. Aufgrund welcher Kompetenz die Netzanbieter diese auch verfassungsrechtlich komplexen Entscheidungen treffen können sollen, ist zweifelhaft. Stattdessen liegen „Zweifels-Löschungen“ und sogenannte „Chilling“-Effekte im Sinne einer systema-

⁴⁷ *Liesching*, MMR 2018, 26, 27.

⁴⁸ *Liesching*, MMR 2018, 26, 27; *Gersdorf*, MMR 2017, 439, 442.

⁴⁹ *Betge*, in: Sachs, 9. Aufl. 2021, GG Art. 5 Rn. 25 ff.; *Schulze-Fielitz*, in: Dreier, 3. Aufl. 2013, GG Art. 5 Rn 62 ff.; *Grimm*, NJW 1995, 1697, 1698.

tischen Tendenz zur Löschung von Inhalten, um Bußgelder zu vermeiden, näher.⁵⁰

Bei der Novellierung des NetzDG ist nunmehr jedoch die Einführung eines Gegenvorstellungsverfahrens zu begrüßen.⁵¹ Damit wurde ein zentraler Kritikpunkt, der auch unter dem Eindruck der besonderen Bedeutung der Meinungsfreiheit besprochen wurde, berücksichtigt.

Die Informationsfreiheit der Nutzer, also die Freiheit sich aus allgemein zugänglichen Quellen zu informieren, ist durch die Sperr- und Löschverpflichtungen der Anbieter ebenfalls beeinträchtigt. Als ein dem Meinungsbildungsprozess notwendig vorgeschalteter Vorgang der Informationsgewinnung steht die Informationsfreiheit gleichbedeutend neben der Meinungsfreiheit.

Selbstverständlich sind beide Grundrechte nicht vorbehaltlos gewährleistet, sondern finden ihre Grenzen in der Schrankentrias in Art. 5 Abs. 2 GG sowie in den verfassungsimmanenten Schranken. Ob die Ausführungen des Gesetzgebers,⁵² mit dem NetzDG der zunehmend aggressiver und hasserfüllter stattfindenden Debattenkultur im sozialen Netzwerken Rechnung tragen zu wollen, den Vorgaben des Bundesverfassungsgerichts an die Bestimmtheit eines legitimen Zwecks entsprechend, ist jedoch zu bezweifeln.⁵³

Grundrechtsbelange der Netzwerkanbieter

Auf Seiten der Netzwerkanbieter kommen insbesondere die Verletzung der Berufsfreiheit aus Art. 12 Abs. 1 GG sowie der Eigentumsfreiheit aus Art. 14 Abs. 1 GG in Betracht.⁵⁴ In diesem Zusammenhang ist der personelle Schutzbereich jedenfalls für solche Anbieter mit Sitz im Inland oder einem EU-Mitgliedsstaat eröffnet.⁵⁵ Die Einführung der weitreichenden Sperr- und Löschpflichten sowie die damit erforderliche Beurteilung im rechtlich komplexen Sachgebiet der Meinungsfreiheit unterliegen dem NetzDG nach jedoch keinerlei einschränkenden

⁵⁰ *Papier*, NJW 2017, 3025, 3030; *Feldmann*, K&R 2017, 292, 295; *Guggenberger*, ZRP 2017, 98, 100

⁵¹ *Schwartzmann*, Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) (BT-Drucksache 19/18792), S. 8; der von *Liesching*, Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) (BT-Drucksache 19/18792), S. 5 ff. vorgebrachte Einwand des geringen Anwendungsbereichs dürfte mit Einführung von § 3 Abs. 3 S. 1 NetzDG leerlaufen.

⁵² Begr. RegE BT-Drs. 18/12356, S. 11.

⁵³ BVerfG MMR 2010, 199, 200 m. Anm. *Liesching*; *Papier*, NJW 2017, 3025, 3030; *Wimmers/Heymann*, AfP 2017, 93, 98.

⁵⁴ So auch Begr. RegE BT-Drs. 18/12356, S. 20.

⁵⁵ BVerfG, 19.07.2011 - 1 BvR 1916/09, BVerfGE 129, 78, 98 = NJW 2011, 3428, 3431.

Maßgaben im Sinne eines Zumutbarkeitskriteriums. Stattdessen obliegt es hier den Anbietern eigenverantwortlich und für den Fall einer „falschen“ Beurteilung auch bußgeldbewährt gegen Fake News und Hassrede im Netz vorzugehen.⁵⁶ Darüber hinaus geben außerdem die Medienfreiheiten der Anbieter aus Art. 5 Abs. 1 S. 2 GG einen verfassungsrechtlichen Rahmen, der von NetzDG jedoch nicht eingehalten wird.⁵⁷

Zwischenergebnis

Das NetzDG steht damit unter dem Eindruck vielfältiger Grundrechtseinflüsse, denen es kaum gerecht zu werden vermag. Neben den genannten Grundrechten kommen darüber hinaus auch noch die Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 GG) der sonstigen Nutzer des sozialen Netzwerks, aber auch eine Verletzung von Verfahrensgrundrechten in Betracht.⁵⁸ Insgesamt begegnet das Gesetz damit erheblichen verfassungsrechtlichen Bedenken – sowohl in formeller als auch materieller Hinsicht.

6. Internationale Anwendbarkeit (und Europarechtswidrigkeit)

Das NetzDG enthält keinerlei Norm, die die internationale Anwendbarkeit, etwa in Gestalt auf nur im Inland ansässige soziale Netzwerkanbieter, beschränkt. Da das NetzDG nur bei der Mindestzahl von 2 Mio. registrierten Nutzern im Inland anwendbar ist, stellte es offenbar allein auf die Abrufbarkeit oder das Einstellen solcher Inhalte durch Nutzer im Inland ab – vorbehaltlich der internationalen Anwendbarkeit der in § 1 Abs. 3 NetzDG aufgeführten Inhalte. Darüber hinaus stellt § 4 Abs. 3 NetzDG zudem klar, dass eine Bebußung auch dann stattfindet, wenn die Handlung (bzw. Unterlassung) des Betreibers des Netzwerkes nicht im Inland vorgenommen wurde, worunter der Gesetzgeber offenbar den Handlungs-ort versteht.⁵⁹ Das NetzDG findet mithin auf alle Anbieter Anwendung, unabhängig davon ob sie im Inland, in EU-Mitgliedstaaten oder in Drittstaaten niedergelassen sind.

Sofern das NetzDG nunmehr jedoch engere Regelungen vorsieht als das Herkunftsland des Netzwerkanbieters, kollidiert es mit dem in Art. 3 Abs. 1 ECRL

⁵⁶ Vgl. etwa zum einschränkenden Kriterium bei der Störerhaftung BGH, 1.3.2016 – VI ZR 34/15, BGHZ 209, 139 = MMR 2016, 418 Rn 22; BGH, 25.10.2011 – VI ZR 93/10, BGHZ 191, 219 = MMR 2012, 124 Rn 22 mW Nachw; sie auch *Gersdorf*, MMR 2017, 439, 446.

⁵⁷ Vgl. ausf. *Gersdorf*, MMR 2017, 439, 446, der auf BGH, 1.3.2016 - VI ZR 34/15, BGHZ 209, 139 = MMR 2016, 418 Rn 40 verweist; *Liesching*, MMR 2018, 26, 28; *Ladeur/Gostomzyk*, K&R 2017, 390, 393; *Wimmers/Heymann*, AfP 2017, 94, 98.

⁵⁸ *Nolte*, ZUM 2017, 552, 560 f.

⁵⁹ Begr. RegE BT-Drs. 18/12356, S. 28.

normierten Herkunftslandprinzip.⁶⁰ Demnach obliegt es zum Zwecke des reibungslosen, elektronischen Dienstleistungsverkehrs im Binnenmarkt allein dem Herkunftsland des Netzwerks sicherzustellen, dass dieses den in diesem Mitgliedsstaat geltenden innerstaatlichen Vorschriften entspricht.⁶¹

Dieses Vorgehen des nationalen Gesetzgebers könnte jedoch vor dem Hintergrund der Ausnahmen in Art. 3 Abs. 3-6 ECRL mit europäischem Recht vereinbar sein. Zunächst scheidet eine Rechtfertigung auf Grundlage der Ausnahmeregelung des Art. 3 Abs. 3 ECRL i.V.m. dessen Annex von vornherein aus. Das NetzDG betrifft in diesen Zusammenhang keines der im Annex genannten Rechtsgebiete.⁶²

Folglich verbleibt nur noch der Ausnahmetatbestand des Art. 3 Abs. 4 ECRL (ggf. i.V.m. Art. 3 Abs. 5 ECRL), auf den schließlich auch der nationale Gesetzgeber in der Gesetzesbegründung rekurriert.⁶³ Demnach können Mitgliedsstaaten abweichend von Art. 3 Abs. 2 ECRL Maßnahmen gegen einen bestimmten Dienst der Informationsgesellschaft ergreifen, wenn die enumerativ aufgelisteten Bedingungen vorliegen – und zwar selbst dann, wenn diese in den koordinierten Bereich i.S.v. Art. 2 lit. h ECRL fallen. Die Antwort auf die Frage der Anwendbarkeit des Art. 3 Abs. 4 ECRL – und damit auch die Antwort auf die Frage der Europarechtswidrigkeit des NetzDG – richtet sich nun maßgeblich nach der Auslegung des Begriffs der Betroffenheit „eines bestimmten Dienstes der Informationsgesellschaft“. Der nationale Gesetzgeber legt hier ein weites Begriffsverständnis an, wenn er auf einen Tätigkeitstypus abstellt und folglich mit dem NetzDG Regelungen für soziale Netzwerke als eine bestimmte Art von Diensten der Informationsgesellschaft schafft.⁶⁴ In diesem Zusammenhang soll auch auf die parallel ablaufende Diskussion zur Bestrebung des europäischen Gesetzgebers zugegriffen werden können, im Rahmen der AVMD-RL den Mitgliedsstaaten bereichsspezifische Regelungen im koordinierten Bereich zu ermöglichen. Dieser, mit Art. 28a Abs. 5 AVMD-RL zum Ausdruck kommende Gedanke, soll auf die hier zu führende Diskussion übertragbar sein.⁶⁵

Der Art. 3 Abs. 4 ECRL ist indessen restriktiv auszulegen. Der Charakter der Norm möchte den Mitgliedsstaaten nicht die Kompetenz zur Schaffung von

⁶⁰ Ausführlich dazu *Spindler*, ZUM 2017, 473, 474; deutliche Zweifel auch bei Wissenschaftlicher Dienst Bundestag, Entwurf eines Netzwerkdurchsetzungsgesetzes – Vereinbarkeit mit dem Herkunftslandprinzip, 29. 5. 2017, PE 6 - 3000 – 32/17; wie hier jetzt auch *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 434.

⁶¹ Zum Zweck des Herkunftslandprinzips vgl. EuGH, 25.10.2011, C-509/09 = EuZW 2011, 962 Rn 66 – eDate Advertising.

⁶² Vgl. *Spindler*, ZUM 2017, 473, 475.

⁶³ Begr. RegE BT-Drs. 18/12356, S. 14.

⁶⁴ Begr. RegE BT-Drs. 18/12356, S. 14.

⁶⁵ *Schwartmann*, Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) (BT-Drucksache 19/18792), S. 11.

Bereichsausnahmen für bestimmte Kategorien von Diensten der Informationsgesellschaft einräumen. Stattdessen zielt die Norm auf Maßnahmen gegen einen einzelnen Dienst und ist damit als einzelfallbezogene Schutzklausel einzuordnen.⁶⁶ Für diese Auslegung streitet auch ein systematisches Argument: Soweit dem Empfangsstaat allein schon aufgrund von Art. 3 Abs. 4 E-Commerce-RL eine Ausnahme möglich wäre, ist schlicht nicht erklärbar, warum Art. 3 Abs. 3 E-Commerce-RL mit seinem Annex ganze Rechtsgebiete vom Herkunftslandprinzip ausnimmt. Demnach wäre der eher generalklauselartig formulierte Art. 3 Abs. 4 ECRL – etwa der Schutz der öffentlichen Ordnung – überflüssig.⁶⁷ Hinzu kommt, dass auch die EU-Kommission in ihrer Mitteilung vom 15. Mai 2003⁶⁸ zwischen den allgemeinen Ausnahmen des Art. 3 Abs. 3 ECRL und den lediglich im Einzelfall zulässigen Maßnahmen gegen einen Diensteanbieter nach Art. 3 Abs. 4-6 ECRL klar unterscheidet.⁶⁹ Damit erfasst Art. 3 Abs. 4 ECRL auch weiterhin lediglich konkret-individuelle Regelungen bzw. Maßnahmen.⁷⁰ Abstrakt-generelle Regelungen – wie das hier zu besprechende NetzDG – fallen indessen nicht in den Anwendungsbereich. Soweit das NetzDG also strengere Anforderungen festlegt als das jeweilige Herkunftsland des Netzwerkanbieters, kollidiert es mit dem Herkunftslandprinzip und ist folglich europarechtswidrig.⁷¹

⁶⁶ Ausführlicher dazu *Spindler*, ZUM 2017, 473, 476 m. w. N.; wie hier *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 434.

⁶⁷ S. aber auch BGH, 30.03.2006 – I ZR 24/03, BGHZ 167, 91, 101 f. = ZUM-RD 2006, 373, 377 – Arzneimittelwerbung im Internet, der offenbar genau dies annimmt. Der Senat setzt sich allerdings nicht damit auseinander, ob und wie das Verhältnis der E-Commerce-RL mit anderen Richtlinien zu bestimmen ist, hier dem Verbot von Heilmittelwerbung; ähnlich OLG Hamburg, 08.04.2009 – 5 U 13/08, MMR 2010, 185, ebenfalls ohne Auseinandersetzung mit dem Charakter des Art. 3 Abs. 4 E-Commerce-RL.

⁶⁸ Vgl. Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank vom 14.05.2003 zur „Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM(2003) 259 endg.

⁶⁹ Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank vom 14.05.2003 zur „Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM (2003) 259 endg, S. 2 ff; *Nordmeier*, in: *Spindler/Schuster*, Recht der elektronischen Medien, 4. Aufl. 2019, TMG § 3 Rn. 22; *Heckmann*, in: *jurisPK-Internetrecht*, 5. Aufl. 2015, Kap. 1 Rn. 215 ff.; *Altenhain*, in: *MüKo StGB*, 3. Aufl. 2019, TMG § 3 Rn. 58 ff.; *Wimmers/Heymann*, AfP 2017, 93, 96; *Feldmann*, K&R 2017, 292, 296.

⁷⁰ Ausführlich auch *Liesching*, Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkungen auf die aktuelle Mediengesetzgebung in Deutschland, 2020, S. 16 ff.

⁷¹ So auch *Liesching*, Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkungen auf die aktuelle Mediengesetzgebung in Deutschland, 2020, S. 20; *ders.*, MMR 2018, 26, 29; *Feldmann*, K&R 2017, 292, 296; *Spindler*, K&R 2017, 533, 535 f.; *ders.*, ZUM 2017, 473, 474 ff.; *Wimmers/Heymann*, AfP 2017, 93, 96; anders offenbar BGH, 30.03.2006 – I ZR 24/03, BGHZ 167, 91, 101 f. = ZUM-RD 2006, 373, 377 – Arzneimittel-

B. Berichts- und Organisationspflichten, insbesondere Einrichtung eines Beschwerdemanagementsystems

Neben den Pflichten zur Löschung und Sperrung von rechtswidrigen Inhalten besteht einer der Kernpunkte des NetzDG in der Pflicht zur Einrichtung eines wirksamen und transparenten Beschwerdemanagementsystems nach § 3 Abs. 1 S. 1 NetzDG und der Veröffentlichung von diesbezüglichen Berichten gem. § 2 NetzDG.

1. Beschwerdemanagementsystem

Der Anbieter eines sozialen Netzwerks ist nach § 3 Abs. 1 S. 2 NetzDG verpflichtet für die Nutzer „ein leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte“ zur Verfügung zu stellen. Diese Pflicht besteht für alle Anbieter eines sozialen Netzwerks, die in den Anwendungsbereich des NetzDG fallen und ist – anders als die Berichtspflicht aus § 2 NetzDG – unabhängig von der Anzahl der tatsächlich eingegangenen Beschwerden. Für die leichte Erreichbarkeit und Erkennbarkeit stellt der Gesetzgeber zu Recht auf die gleichen Kriterien wie in § 5 Abs. 1 TMG ab.⁷²

§ 3 Abs. 4 NetzDG erlegt der „Leitung“ des sozialen Netzwerks eine Pflicht zur ordnungsgemäßen Organisation auf, indem monatliche Kontrollen des Beschwerdemanagements durchgeführt und „organisatorische Unzulänglichkeiten“ im Umgang mit Beschwerden sofort beseitigt werden müssen. Zudem muss wiederum die Leitung des sozialen Netzwerks für die mit dem Beschwerdemanagement betrauten Personen mindestens halbjährlich deutschsprachige Schulungs- und Betreuungsangebote machen. Dem Gesetz lässt sich nicht entnehmen, was „organisatorische Unzulänglichkeiten“ sind – da es um die Organisation als Ganzes geht, scheiden Einzelfälle (im Sinne von Ausreißern) aus, es muss sich um wiederholte Verletzungen der Pflichten handeln. Das steht letztlich auch im Einklang mit § 4 Abs. 5 NetzDG (mehrere Inhalte), der nur „systemische“, also wiederholte Verletzungen bebußt. Inhaltlich kommen sowohl Probleme im Prozessablauf als auch in personeller Hinsicht in Betracht.

Generell verbietet das NetzDG nicht, dass die Aufgaben an Dritte vergeben werden – solange nur die Leitung hierfür verantwortlich bleibt. Die Kernaufgaben der Leitung und Kontrolle können daher nicht ausgelagert werden, wohl aber das

werbung im Internet: Heilmittelwerbeverbot fällt generell unter die Ausnahme (Rn. 30), wenn die einschlägige EU-Richtlinie (hier zu Werbung über Humanarzneimittel) keine Einzelfallprüfung vorsieht; ähnlich OLG Hamburg, 8. 4. 2009 – 5 U 13/08, MMR 2010, 185 – gratis-SMS für wettbewerbsrechtliches Verbot der Irreführung von Verbrauchern; a.A. *Schwartmann/Mühlenbeck*, ZRP 2020, 170, 172; *Nölscher*, ZUM 2020, 301, 306 ff.

⁷² Begr. RegE BT-Drs. 18/12356, S. 22; krit. dazu Stellungnahme eco Verband der Internetwirtschaft e. V., 30. 3. 2017, S. 6: zu großer Eingriff in Gestaltungsfreiheit.

Beschwerdemanagementsystem selbst, solange die Leitung des Netzbetreibers in der Lage ist, sofort einzugreifen und die nötigen Informationen zu erhalten.⁷³

Schließlich sollten nach Auffassung des nationalen Gesetzgebers die Berichts- und Organisationspflichten durch Audits und Zertifizierungen flankiert werden, deren Voraussetzungen vom BMJV mit den Beteiligten bis 2018 erarbeitet werden sollten – soweit ersichtlich, sind hier noch keine Ergebnisse vorgetragen worden. Demnach sollen entsprechende Zertifizierungen eine positive Vermutungswirkung für die Bewertung des Beschwerdemanagementsystems entfalten.⁷⁴

2. Berichtspflicht

Nach § 2 Abs. 1 NetzDG muss halbjährlich in deutscher Sprache über den Umgang mit Beschwerden im Bundesanzeiger sowie (kumulativ) auf der eigenen Homepage berichtet werden. Die im Bericht anzusprechenden Aspekte sind in § 2 Abs. 2 NetzDG näher aufgeschlüsselt und entsprechen quasi spiegelbildlich den materiellen Organisationspflichten, enthalten aber auch die Pflicht zur Angabe, wie viele und welche Beschwerden anhängig waren (§ 2 Abs. 2 Nr. 3 NetzDG). Auch muss der Bericht Angaben über die Löschung oder Sperrung von rechtswidrigen Inhalten innerhalb der jeweiligen Fristen (§ 2 Abs. 2 Nr. 8) sowie einer eventuellen Abgabe an die unabhängige Stelle nach § 3 Abs. 2 Nr. 3 b NetzDG enthalten, § 2 Abs. 2 Nr. 7 NetzDG.

C. Pflichten zur Löschung und Sperrungen

Teil des Beschwerdemanagementsystems, aber nicht nur rein organisatorischer Natur sind die von § 3 Abs. 2 Nr. 2, 3 NetzDG vorgesehenen Pflichten zur Löschung und Sperrung der von § 1 Abs. 3 NetzDG in Bezug genommenen Inhalte. Diese Pflichten trennen sich auf in die Pflicht zur Löschung offensichtlich rechtswidriger Inhalte innerhalb von 24 Stunden nach Eingang der Beschwerde gem. § 3 Abs. 2 Nr. 2 NetzDG, und anderen rechtswidrigen Inhalten, für die eine Frist von 7 Tagen oder unter bestimmten Bedingungen auch ein längerer, nicht spezifizierter Zeitraum gilt. Für alle Beschwerden hat der Gesetzgeber aber im parlamentarischen Verfahren noch für eine wichtige Präzisierung in § 3 Abs. 2 Nr. 1 NetzDG gesorgt, dass nämlich für die Auslösung der Pflichten nach § 3 Abs. 2 Nr. 2, 3 NetzDG nur eine Beschwerde mit konkretem Inhalt geeignet ist; damit sollen allgemein gehaltene Beschwerden, die den Netzbetreiber nicht in die Lage versetzen, einen konkreten Inhalt zu löschen bzw. zu sperren, aus dem NetzDG ausgenommen werden.⁷⁵ Damit erreicht der Gesetzgeber nunmehr einen Gleichklang mit Art. 14 E-Commerce-RL, der ebenfalls nur auf einen konkreten

⁷³ In diese Richtung Begr. RegE BT-Drs. 18/12356, S. 23.

⁷⁴ Begr. Rechtsausschuss BT-Drs. 18/13013 S. 18.

⁷⁵ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

Inhalt bezogen ist;⁷⁶ allgemeine Benachrichtigungen eines Providers lösen auch in Art. 14 E-Commerce-RL (bzw. § 10 TMG) keine Pflichten zur Löschung aus.⁷⁷

1. Pflicht zur Löschung offensichtlich rechtswidriger Inhalte

§ 3 Abs. 2 Nr. 2 NetzDG enthält die Pflicht zur Löschung bzw. Sperrung ab Eingang der Beschwerde innerhalb von 24 Stunden. Diese Pflicht ist in mehrfacher Hinsicht problematisch: Zum einen ist nach wie vor schwer zu beantworten, wann es sich um offensichtlich rechtswidrige Inhalte handelt; wie bekannt, sind gerade Kommunikationsdelikte immer unter Berücksichtigung der Meinungsfreiheit auszulegen und eine praktische Konkordanz der betroffenen Grundrechte herbeizuführen, was nicht selten zu langwierigen Verfahren und völlig unterschiedlichen Entscheidungen der jeweiligen Gerichte führt.⁷⁸

Das Gesetz legt letztlich nach wie vor – trotz Nachbesserungen im parlamentarischen Verfahren – das Risiko einer richtigen rechtlichen Beurteilung dem Betreiber des Netzwerkes auf; die Erleichterungen des § 3 Abs. 1 Nr. 3 NetzDG beziehen sich nur auf die nicht-offensichtlich rechtswidrigen Inhalte. Der Gesetzgeber zieht hier neben dem Verweis auf § 101 Abs. 2 UrhG eine Art tautologischen Rückschluss: Wenn geschultes Personal bei zumutbarem Aufwand nicht in der Lage sei, innerhalb von 24 Stunden zu entscheiden, handele es sich eben nicht um eine offensichtliche Rechtswidrigkeit.⁷⁹ Dabei darf man nicht auf die subjektive Lage des Netzbetreibers abstellen, vielmehr wird ein objektiver Maßstab eines sorgfältig handelnden und organisierten Netzbetreibers anzulegen sein.

Um Bedenken gegen eine unverhältnismäßige Beeinträchtigung der Meinungsfreiheit, insbesondere des „overblocking“, Rechnung zu tragen, hat der Gesetzgeber im Rahmen der Novellierung des NetzDG 2021 ein Gegenvorstellungsverfahren eingeführt.⁸⁰ Dies folgt grosso modo dem bereits im Bereich der Störerhaftung vom BGH eingeschlagenem Weg bei Blogs, indem der Provider den Blogger nach Eingang einer Beschwerde zur Stellungnahme auffordern muss, um-

⁷⁶ S. zur noch im RegE vorhandenen Diskrepanz zu Art. 14 E-Commerce-RL *Spindler*, ZUM 2017, 473, 481.

⁷⁷ Wohl allg., s. dazu etwa BGH, 17.08.2011 – I ZR 57/09, K&R 2011, 727 ff. = BGHZ 191, 19, Rn. 28 = GRUR 2011, 1038 – Stiftparfüm; *Spindler*, in: *Spindler/Schmitz*, 2. Aufl. 2018, TMG § 10 Rn. 24; *Paal*, in: BeckOK InfoMedienR, 33. Ed. 2021, TMG § 10 Rn. 40.

⁷⁸ S. etwa die verschiedenen Caroline -Entscheidungen: BGH, 6. 3. 2007 – VI ZR 51/06, BGHZ 171, 275 = ZUM 2007, 651; BVerfG, 26. 2. 2008 – 1 BvR 1602/07, BVerfGE 120, 180 = ZUM 2008, 420 – Caroline von Monaco III; hingegen EGMR, 7. 2. 2012 – 40660/08, 60641/08, K&R 2012, 179 = ZUM 2012, 551 – Caroline von Hannover II.

⁷⁹ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

⁸⁰ Zu kritischen Anmerkungen in der Literatur vgl. etwa *Peukert*, MMR 2018, 572; *Kettmann*, Stellungnahme zum NetzDG, Ausschuss für Recht und Verbraucherschutz, 15. Mai 2019, abrufbar unter <https://s.gwdg.de/MLdPKi> (zuletzt abgerufen am 11. Oktober 2021).

gekehrt der Blogger nach der Stellungnahme seinerseits den Beschwerdeführer um eine Replik.⁸¹ Der Anwendungsbereich des Gegenvorstellungsverfahrens ist nach § 3b Abs. 3 NetzDG nicht auf die Überprüfung von Beschwerden beschränkt, die sich gegen rechtswidrige Inhalte i.S.d. § 1 Abs. 3 NetzDG wenden. Stattdessen soll es auch zur Anwendung kommen, wenn mit der Beschwerde die Verletzung von Gemeinschaftsstandards gerügt wird oder i.R.e. Conten-Moderation eingelegt wurde.⁸²

Sowohl der Beschwerdeführer, dessen Beschwerde vom Netzwerkanbieter negativ beschieden wurde als auch der Nutzer der Plattform, dessen Inhalte aufgrund einer Beschwerde gesperrt oder entfernt wurden, erhalten mit Einführung des Verfahrens die Möglichkeit eines plattforminternen Rechtsbehelfsverfahrens. Das Verfahren wird gem. § 3b Abs. 1 S. 1 NetzDG nur auf Initiative des Beschwerdeführers bzw. des Nutzers eingeleitet, die dazu einen begründeten Antrag auf Einleitung des Gegenvorstellungsverfahrens binnen zwei Wochen nach der Information über die ursprüngliche Entscheidung beim Netzwerkanbieter einreichen müssen. Wie schon für das Beschwerdeverfahren nach § 3 NetzDG, muss der Netzwerkanbieter auch für das Gegenvorstellungsverfahren ein leicht erkennbares Verfahren zur Verfügung stellen, das eine einfache elektronische Kontaktaufnahme und eine unmittelbare Kommunikation mit ihm ermöglicht (§ 3b Abs. 1 S. 4 NetzDG). Nach der Antragstellung muss der Netzwerkbetreiber der Gegenseite die Möglichkeit zur Stellungnahme binnen einer angemessenen Frist gem. § 3b Abs. 2 Nr. 1 NetzDG geben und den Inhalt dieser Stellungnahme dem Antragsteller übermitteln (§ 3b Abs. 2 Nr. 2 NetzDG). Die daraufhin zu erfolgende Überprüfungsentscheidung durch den Netzwerkanbieter ist schließlich beiden Verfahrensbeteiligten zu übermitteln und bedarf gem. § 3b Abs. 2 Nr. 4 NetzDG einer einzelfallbezogenen Begründung. Während des gesamten Verfahrens hat der Netzwerkanbieter nach § 3b Abs. 2 Nr. 5 NetzDG außerdem die Identität der Verfahrensbeteiligten zu wahren.

Die Möglichkeit, den Rechtsweg zu beschreiten, bleibt von diesem plattforminternen Gegenvorstellungsverfahren gem. § 3b Abs. 4 NetzDG unberührt.

⁸¹ BGH, 25. 10. 2011 – VI ZR 93/10, K&R 2012, 110 ff. = BGHZ 191, 219 = ZUM-RD 2012, 82 Rn. 27 ff. – Blog-Eintrag; zu dem Procedere bei Bewertungsportalen s. BGH, 23. 9. 2014 – VI ZR 358/13, K&R 2014, 802 ff. = BGHZ 202, 242 Rn. 36 = ZUM-RD 2015, 154 – Ärztebewertung II; darüber hinaus hat der BGH im Hinblick auf rechtswidrige Inhalte auf Online-Bewertungsportalen einen Auskunftsanspruch des Betroffenen gegen den Portalbetreiber diskutiert, diesen jedoch aufgrund von § 12 Abs. 2 TMG verneint, BGH, 1. 7. 2014 – VI ZR 354/13, BGHZ 201, 380 Rn. 9 ff. = ZUM 2014, 793 – Ärztebewertung I; hierzu *Spindler*, in: FS Bamberger 2017, S. 313, 316 ff., 318.

⁸² Vgl. auch *Cornils*, NJW 2021, 2465, 2468.

2. Lösch- und Sperrpflichten bei anderen Inhalten

Bei Inhalten, die nicht offensichtlich rechtswidrig sind, sieht § 3 Abs. 2 Nr. 3 NetzDG grundsätzlich eine unverzügliche Löschung bzw. Sperrung vor, die aber „in der Regel“ innerhalb von 7 Tagen bewerkstelligt werden soll. Mit diesem im parlamentarischen Verfahren gefundenen Kompromiss wollte der Gesetzgeber die Gefahren eines „overblockings“ bzw. allzu rascher Löschung vermeiden und nähert sich wieder § 10 TMG bzw. Art. 14 E-Commerce-RL an – allerdings ist nach wie vor mehr als zweifelhaft, ob ein nationaler Gesetzgeber das Kriterium der Unverzüglichkeit selbst mit einer Art „Regelvermutung“ präzisieren kann.

Das Gesetz sieht aber auch eine Überschreitung der „Regel“frist von 7 Tagen in zwei Fällen vor, einmal nach § 3 Abs. 2 Nr. 3 a) NetzDG wenn die Rechtswidrigkeit von unwahren Tatsachenbehauptungen oder „anderen tatsächlichen Umständen“ abhängt, zum anderen wenn die Beschwerde zur Entscheidung an eine anerkannte Einrichtung der regulierten Selbstregulierung abgegeben wird. Die Notwendigkeit einer komplexen rechtlichen Würdigung vermag daher den Betreiber sozialer Netzwerke nach § 3 Abs. 2 Nr. 3 a) NetzDG nicht zu entlasten – lediglich tatsächliche Umstände bzw. Zweifel sowie die Stellungnahme des Äußernden sind hier fristverlängernd. Das NetzDG lehnt sich hier an die Blogger-Entscheidung des BGH an,⁸³ indem der Gesetzgeber davon ausgeht, dass bei einer fehlenden Stellungnahme des Nutzers in der Regel von der Glaubhaftigkeit des Beschwerdevorbringens auszugehen sei, bei einer Stellungnahme dagegen abgewogen werden müsse. Der Gesetzgeber will in diesen Fällen aber kein Bußgeld gegen den Netzbetreibler verhängen, wenn sich dessen Einschätzung ex post als falsch herausstellt.⁸⁴

Für schwierige rechtliche Abwägungen bei Kommunikationsdelikten ohne Bezug zu Tatsachen oder äußeren Umständen wird der Betreiber des sozialen Netzwerkes dagegen faktisch gezwungen sein, die Beschwerde an die anerkannte Einrichtung der regulierten Selbstregulierung abzugeben; Fälle, in denen es sich um offensichtlich rechtswidrige Inhalte handelt, können dagegen nicht (befreiend) an die Einrichtung übertragen werden.⁸⁵ In welcher Frist diese Einrichtung dann zu entscheiden hat, schreibt das NetzDG nur indirekt vor, indem in § 3 Abs. 6 Nr. 2 NetzDG für die Anerkennung der Einrichtung gefordert wird, dass sie über eine sachgerechte Ausstattung verfügt und eine „zügige Prüfung innerhalb von 7 Tagen sichergestellt ist“.

Der Betreiber des Netzwerkes ist an die Entscheidung der Einrichtung gebunden, ob zu löschen ist oder nicht. Interessanterweise – und in Parallele zum JMStV und der die KJM bindenden Einschätzungsprärogative der Einrichtungen

⁸³ BGH, 25. 10. 2011 – VI ZR 93/10, K&R 2012, 110 ff. = BGHZ 191, 219 = ZUM-RD 2012, 82 – Blog-Eintrag.

⁸⁴ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 21.

⁸⁵ So ist wohl Begr. Rechtsausschuss BT-Drs. 18/13013, S. 23 zu verstehen.

der freiwilligen Selbstkontrolle (der FSM)⁸⁶ – gilt die Bindung aber auch gegenüber der Bußgeldbehörde, der es verwehrt ist, zu einer anderen Einschätzung als die Einrichtung zu kommen.⁸⁷ Umgekehrt sieht das NetzDG nicht vor, dass die Einrichtung die Annahme der Beschwerde verweigern kann, z. B. bei evident rechtswidrigen Fällen; in Betracht kommt hier aber auch, dass ein Anbieter eines sozialen Netzwerks nicht seinen finanziellen Pflichten aus der Unterhaltung der Einrichtung nachgekommen ist. Da das NetzDG die Ausgestaltung der Rechtsverhältnisse der Einrichtung den Beteiligten überlässt, muss es auch die Möglichkeit der Einrichtung geben, die Überweisung einer Beschwerde zurückzuweisen.

Hinsichtlich des Verhältnisses der Einrichtung zur FSM selbst, etwa bei jugendgefährdenden Inhalten, hat die (vorherige) Einschätzung der FSM bzw. dann der KJM als *lex specialis* natürlich Vorrang. Hat die FSM einen Inhalt als jugendgefährdend qualifiziert, handelt es sich sogar um einen evident rechtswidrigen Inhalt, sofern er unter eines der in § 1 Abs. 3 NetzDG genannten Delikte fällt. Nur in Sonder- bzw. Einzelfällen, z. B. der Zitierung eines solchen Inhalts für die eigene Gedankenführung, kann die Einrichtung nach dem NetzDG hier zu einer anderen Einschätzung im Hinblick auf einen spezifischen Inhalt kommen. So verständlich (und rechtspolitisch wünschenswert)⁸⁸ dieser nunmehr eingeführte Mechanismus sein mag – auch hier kann das NetzDG nicht an Art. 14 E-Commerce-RL vorbei, der weder eine Fristverlängerung gegenüber dem „unverzüglichen“ Tätigwerden noch die befreiende Abgabe an einen Dritten vorsieht.

D. Auskunftsrecht

Der jeweils Betroffene möchte aber unter Umständen nicht nur eine Sperrung bzw. Löschung eines ehrverletzenden Beitrags oder einer falschen Behauptung erreichen, sondern auch den Rechtsverletzer persönlich in Anspruch nehmen. Voraussetzung ist naturgemäß hier immer die Identifizierung des Rechtsverletzers, mithin die Auskunft über die jeweiligen Daten durch den sozialen Netzwerkbetreiber. Gerade hier bestand aber lange Zeit eine – auch verfassungsrechtlich

⁸⁶ *Erdemir*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, JMStV § 20 Rn. 26 ff.; ferner *Nell*, Beurteilungsspielraum zugunsten Privater, 2010, 95, 309 ff.; *Bornemann*, in: Bornemann/Erdemir, 2. Aufl. 2021, JMStV § 20 Rn. 44; *Hopf/Braml*, MMR 2009, 153, 156 f.; zur Parallelvorschrift im Rundfunk (§ 20 Abs. 3): ausführlich *Pritting*, K&R 2013, 775, 778; *Cole*, ZUM 2005, 462, 469.

⁸⁷ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 23 spricht hier ausdrücklich von einer Begrenzung des „Einschätzungsspielraums“ der Bußgeldbehörde. Allerdings bleibt unklar, warum die Bußgeldbehörde einen solchen Spielraum genießen sollte, ist doch ihre Entscheidung gerichtlich in Gänze nachprüfbar.

⁸⁸ Zu den Vorteilen der regulierten Selbstregulierung s. *Spindler/Thorun*, MMR 2016, Beil. 6/2016, 1, 9 ff.

höchst bedenkliche⁸⁹ – Benachteiligung der Geschädigten im Verhältnis zu Inhabern von Rechten des geistigen Eigentums. Letztere profitierten seit der Umsetzung der Enforcement-RL⁹⁰ durch den deutschen Gesetzgeber etwa in § 101 UrhG von breitflächigen Auskunftsansprüchen gegenüber Providern, allerdings zu Recht aufgrund von datenschutzrechtlichen Bedenken nur unter Richtervorbehalt. Für Persönlichkeitsrechte bestanden solche unmittelbaren Auskunftsansprüche und Durchbrechungen des Datenschutzes bislang nicht. Der BGH sah sich aufgrund der schon vom Bundesrat geforderten Erweiterung der Auskunftsansprüche,⁹¹ die vom Gesetzgeber im Hinblick auf die kommende DSGVO aber aufgeschoben wurde, zu Recht daran gehindert, im Wege einer Analogie die Auskunftsmöglichkeiten zu erweitern.⁹² Schon zuvor wurden auch in der rechtswissenschaftlichen Diskussion das Defizit und die Ungleichbehandlung moniert.⁹³

Mit dem durch das NetzDG geänderten § 14 Abs. 3 bis 5 TMG (jetzt § 21 Abs. 2 bis 4 TTDSG) trägt der Gesetzgeber dieser Situation endlich Rechnung und erlaubt Auskünfte durch Telemediendiensteanbieter über Bestands- und Nutzungsdaten (§ 15 TMG; jetzt § 2 Abs. 2 Nr. 3 TTDSG) für Verletzungen der Persönlichkeitsrechte, bezogen auf die in § 1 Abs. 3 NetzDG genannten Delikte. Allerdings erfasst die Auskunftserteilung nur Fälle schwerwiegender Persönlichkeitsrechtsverletzung, wenn die Straftatbestände nach § 1 Abs. 3 NetzDG erfüllt sind;⁹⁴ eine fahrlässige Persönlichkeitsrechtsverletzung wird damit nicht von der Auskunftserteilung abgedeckt.

Allerdings hat der Gesetzgeber davon abgesehen, einen eigenständigen Auskunftsanspruch nach dem Vorbild des § 101 UrhG zu schaffen, obwohl der Rechtsausschuss hierfür deutliche Sympathien erkennen lässt; vielmehr belässt es der Gesetzgeber bei dem Hinweis auf den von der Rechtsprechung bislang in der Regel angenommenen Anspruch aus § 242 BGB auf Auskunftserteilung.⁹⁵ Der Gesetzgeber beschränkt sich insoweit auf die die Parallelen zu § 101 Abs. 9 UrhG, indem die Auskünfte durch den Networkbetreiber unter einen Richtervorbehalt gestellt werden.⁹⁶ Ebenso wenig werden Networkbetreiber zur Identitätsfest-

⁸⁹ S. bereits *Spindler*, Persönlichkeitsrechte im Internet, DJT 2012, Gutachten F, S. 58 ff.; jüngst ebenso *Gersdorf*, MMR 2017, 439, 440 f.

⁹⁰ RL 2004/48/EU des Europäischen Parlaments vom 29. 4. 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. Nr. L 157 v. 30. 4. 2004, S. 45; corrigendum ABl. Nr. L 195 v. 2. 6. 2004, S. 16.

⁹¹ Stellungnahme des Bundesrats zum 2. TMG-Änderungsgesetz, 6. 11. 2015, BT-Drs. 18/6745 Anlage 2, S. 13, 17 (Nr. 5 zur Erweiterung des § 14 Abs. 2 TMG).

⁹² BGH, 1. 7. 2014 – VI ZR 354/13, BGHZ 201, 380 Rn. 9 ff., 15 = ZUM 2014, 793 – Ärztebewertung I.

⁹³ S. *Spindler*, Persönlichkeitsrechte im Internet, DJT 2012, Gutachten F, S. 58 ff. m. w. N.

⁹⁴ S. Begr. Rechtsausschuss BT-Drs. 18/13013, S. 23.

⁹⁵ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 23.

⁹⁶ S. dazu *Spindler*, ZUM 2017, 473, 486; in diese Richtung auch *Feldmann*, K&R 2017, 292, 293.

stellung verpflichtet.⁹⁷ Die weitergehenden Auskunftsbefugnisse nach § 14 Abs. 2 TMG für Immaterialgüterrechtsverletzungen werden nicht berührt; Auskünfte können daher nach wie vor bei Verletzungen des geistigen Eigentums auch ohne Richtervorbehalt erteilt werden. Der betroffene Nutzer wird in aller Regel schon aufgrund der vertraglichen Pflichten des Networkbetreibers von der bevorstehenden Auskunftserteilung zu unterrichten sein.⁹⁸

Diese Vorgaben entsprechen denjenigen aus europarechtlicher Sicht: So hat der EuGH deutlich die datenschutzrechtlichen Anforderungen selbst bei nationalen Gesetzen betont,⁹⁹ indem der Gerichtshof im Verfahren *Promusicae*¹⁰⁰ zwar feststellte, dass die Mitgliedstaaten im Rahmen von Art 15 Abs. 1 ePrivacy-RL die Möglichkeit haben, zu Zwecken der zivilrechtlichen Rechtsverfolgung die Übermittlung von persönlichen Daten von Nutzern an Dritte zu erlauben.¹⁰¹ Doch machte der EuGH auch deutlich, dass diese Einschränkungen ihrerseits verfassungsrechtliche Grundsätze, insbesondere eine gerechte Abwägung der Interessen im Rahmen des Verhältnismäßigkeitsgrundsatzes einzuhalten haben. Dabei müssen nach dem Gerichtshof vor allem die Rechte aus Art. 7 EU-GrCh (Achtung des Privat- und Familienlebens) sowie Art 8 EU-GrCh (Datenschutz) berücksichtigt werden,¹⁰² was der EuGH auch später gerade für soziale Netzwerke bekräftigte.¹⁰³ Deutlich betonte das Gericht den Stellenwert der entgegenstehenden Grundrechte der Datensubjekte und die Bedeutung des Verhältnismäßigkeits-tests in den Entscheidungen zur Vorratsdatenspeicherung, insbesondere, dass gerade verfahrensrechtliche Vorkehrungen erforderlich sind, um die Grundrechte der Betroffenen zu schützen. Im Verfahren *Tele2 Sverige* hat der EuGH die Wertungen aus seiner Entscheidung¹⁰⁴ zur EU-Vorratsdatenspeicher-RL¹⁰⁵ auch

⁹⁷ Krit. daher *Feldmann*, K&R 2017, 292, 294.

⁹⁸ Begr. Rechtsausschuss BT-Drs. 18/13013, S. 24.

⁹⁹ Ausführlich dazu *Spindler*, ZUM 2017, 473, 485.

¹⁰⁰ EuGH, 29.01.2008 – C-275/06, Slg. 2008, I-271, K&R 2008, 165 ff. = ZUM 2008, 288 – *Promusicae*.

¹⁰¹ EuGH, 29.01.2008 – C-275/06, Slg. 2008, I-271 Rn. 53, K&R 2008, 165 ff. = ZUM 2008, 288 – *Promusicae*.

¹⁰² EuGH, 29.01.2008 – C-275/06, Slg. 2008, I-271 Rn. 64, 65, K&R 2008, 165 ff. = ZUM 2008, 288 – *Promusicae*.

¹⁰³ EuGH, 16.02.2012 – C-360/10, K&R 2012, 269 ff. = ZUM 2012, 307 Rn. 48 – *SABAM/Netlog*.

¹⁰⁴ EuGH, 21.12.2016 – C-203/15, C-698/15, K&R 2017, 105 ff. = EuZW 2017, 153 – *Tele2 Sverige*.

¹⁰⁵ RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der RL 2002/58/EG, ABl. Nr. L 105 v. 13.04.2006, S. 54.

auf die auf rein nationaler Ebene vorgesehenen Vorratsdatenspeicherungsgesetze erstreckt.¹⁰⁶

Bedeutsam ist auch die ausdrückliche Betonung der Meinungsfreiheit, Art. 11 EU-GrCh, die durch die Preisgabe persönlicher Daten der Nutzer gefährdet werden kann,¹⁰⁷ zumal die Verfahren wiederum die den Mitgliedstaaten eingeräumten Beschränkungsbefugnisse nach Art. 15 Abs. 1 ePrivacy-RL betrafen, der auch hier in Rede steht. Der EuGH betont (wiederum)¹⁰⁸ ausdrücklich, dass auch die Ausnahmen nach Art. 15 Abs. 1 ePrivacy-RL die Grundrechte der EU-GrCh zu respektieren haben, da sie zu den generellen Prinzipien des EU-Rechts gehören.¹⁰⁹ Von Interesse ist hier vor allem die Forderung des EuGHs, dass die Preisgabe persönlicher Daten der Vorabkontrolle durch ein Gericht oder einer unabhängigen Behörde unterliegen, um die Wahrung der Grundrechte der Betroffenen zu sichern.¹¹⁰

E. DasNetzDG – Novellierung

Mit der Novellierung des NetzDG hat der Gesetzgeber einigen Kritikpunkten Rechnung getragen, gleichzeitig aber auch für eine Verschärfung gesorgt. So sieht § 3a NetzDG nunmehr eine verstärkte Zusammenarbeit zwischen den sozialen Netzbetreibern und den Strafverfolgungsbehörden in Gestalt einer Meldepflicht über bestimmte schwerwiegende Delikte vor, die eine gefährliche Wirkung auf das demokratische System und die öffentliche Ordnung haben können, nicht aber etwa die Antragsdelikte; denn bislang erlangten Strafverfolgungsbehörden von den wenigsten Taten auf sozialen Netzwerken Kenntnis.¹¹¹ Kritisch wird dazu angemerkt, dass die sozialen Netzbetreiber immer mehr sich in der Rolle von Gehilfen der Strafverfolgungsbehörden befinden.¹¹²

Den bereits beschriebenen Fragen zum Verfahren vor einer Löschung bzw. deren Defiziten versucht der Gesetzgeber nunmehr durch § 3b NetzDG Rechnung zu tragen, indem ein Gegenvorstellungsverfahren durch betroffene Nutzer

¹⁰⁶ EuGH, 21.12.2016 – C-203/15, C-698/15, K&R 2017, 105 ff. = EuZW 2017, 153 – Tele2 Sverige.

¹⁰⁷ EuGH, 21.12.2016 – C-203/15, C-698/15, K&R 2017, 105 ff. = EuZW 2017, 153 Rn. 92 f. – Tele2 Sverige.

¹⁰⁸ S. etwa auch EuGH, 6. 12. 2015 – C-362/14, K&R 2015, 710 ff. = ZUM-RD 2015, 709 Rn. 38 – Schrems/Digital Rights Ireland.

¹⁰⁹ EuGH, 21.12.2016 – C-203/15, C-698/15, K&R 2017, 105 ff. = EuZW 2017, 153 Rn. 91 – Tele2 Sverige.

¹¹⁰ EuGH, 21.12.2016 – C-203/15, C-698/15, K&R 2017, 105 ff. = EuZW 2017, 153 Rn. 120 – Tele2 Sverige; ebenso EGMR, 02.01.2016, 37138/14, Rn. 77, 80 – Szabó and Vissy v. Hungary, eine Kurzwiedergabe findet sich in OstEuR 2016, 263.

¹¹¹ Begr. RegE, BR-Drs. 87/20, 1 f.

¹¹² Höjerlein/Widlok, MMR 2021, 277 f.; Stellungnahme Direktorenkonferenz der Landesmedienanstalten v. 17.1.2020, S. 4; Stellungnahme Bitkom v. 17.1.2020, S. 7 f.

eingeführt wurde. Allerdings greift dieses Verfahren erst nach der Löschung ein, mithin wird der Inhalt zunächst gelöscht, was den verfassungsrechtlichen Vorgaben des BVerfG¹¹³ kaum entsprechend dürfte, was zum Schutz der Meinungsfreiheit eine vorherige Gelegenheit zur Stellungnahme erfordert.¹¹⁴ Auch wird damit der Plattformbetreiber noch stärker in die Rolle eines privaten Richters gedrängt.¹¹⁵

Verschärft wurden ferner die Publizitätspflichten, indem nunmehr in § 1 Abs. 4 NetzDG Bericht über jede (!) Beanstandung eines Inhalts erstattet werden muss, um zu verhindern, dass die Plattformbetreiber Beschwerden gegen Gemeinschaftsrichtlinien nicht mit in den anzufertigenden Bericht aufnehmen.¹¹⁶

Bedeutsamer erscheint allerdings die nunmehr in § 2 Abs. 2 Nr. 2 NetzDG aufgenommene Pflicht für die Netzwerkbetreiber, Informationen zum Einsatz künstlicher Intelligenz zu geben, und zwar über „Art, Grundzüge der Funktionsweise und Reichweite von gegebenenfalls eingesetzten Verfahren zur automatisierten Erkennung von Inhalten“. Nicht aufgehoben wird damit allerdings der Schutz, den die Algorithmen über das Geschäftsgeheimnis-Gesetz bzw. die entsprechende Richtlinie genießen.¹¹⁷

III. Haftung von Plattformen – der Vorschlag eines EU Digital Services Act

Vor dem Hintergrund des deutschen NetzDG und vergleichbaren Vorschlägen bzw. Gesetzen in anderen EU-Mitgliedstaaten sowie dem Reformbedarf für die nunmehr fast 20 Jahre alte E-Commerce-RL erklärt sich auch der groß angelegte Vorschlag der EU-Kommission für einen neuen Digital Service Act – der bewußt gerade Risiken durch fake news und Hass-Botschaften und die Rolle der Plattformbetreiber adressiert:

A. Pflichten und Haftungsprivilegierungen für Host-Provider

1. Notice-and-action Systeme

Im Sinne der zunehmenden Ausdifferenzierung von Pflichten der Provider spezifizieren Art. 14 und 15 DSA konkret Pflichten für ein Beschwerdesystem nur für Host-Provider, um dem eigentlich schon unter Art. 12 E-Commerce-RL bestehenden Pflichten zur Entgegennahme von Benachrichtigungen über Rechtsverlet-

¹¹³ BVerfG, 11.04.2018 - 1 BvR 3080/09 = BVerfGE 148, 267, 285 f. – Stadionverbot.

¹¹⁴ *Ladeur/Gostomzyk*, K&R 2017, 390, 393; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 435.

¹¹⁵ a.A: *Kalbhenn/Hemmert-Halsnick*, MMR 2020, 518, 520 f.

¹¹⁶ Begr. FragE, BT-Drs. 19/17741, 42; *Kalbhenn/Hemmert-Halsnick*, MMR 2021, 518, 521; *Hoven/Gersdorf*, in: BeckOK InfoMedienR, 33. Ed. 01.05.2021, NetzDG § 1 Rn. 48.

¹¹⁷ Begr. RegE, BT-Drs. 19/18792, 43; *Kalbhenn/Hemmert-Halsnick*, MMR 2021, 518, 521.

zungen schärfere Konturen zu verleihen („notice-and-take-down“-Systeme), zumal sich doch erhebliche Unterschiede in den Mitgliedstaaten hinsichtlich der Anforderungen an Benachrichtigungen gezeigt hatten.¹¹⁸ Zu den eigentlichen Entscheidungskriterien verhalten sich Art. 14, 15 DSA dagegen unmittelbar nicht; jedoch machen zum einen die Anforderungen an die Benachrichtigung des betroffenen Nutzers sowie des Beschwerdeführers, zum anderen die in ErwGr 41 explizit geforderte umfassende Abwägung die vom DSA intendierte Rückbindung der Entscheidung an die Grundrechte der Beteiligten deutlich, indem ErwGr 41 vom Recht auf freie Meinungsäußerung über die Unternehmensfreiheit bis hin zum Schutz des geistigen Eigentums das gesamte Kaleidoskop benennt. Keine näheren Anhaltspunkte enthält Art. 14, 15 DSA dagegen hinsichtlich der Frage, ob und wie lange der Provider Zeit erhält, um die Berechtigung einer Nachricht zu überprüfen, ebenso, ob ihn Nachforschungspflichten treffen.¹¹⁹

Die Benachrichtigung an den Beschwerdeführer muss auch die Information über die Verwendung von automatisierten Verfahren zur Entscheidungsfindung durch den Provider enthalten, Art. 14 Abs. 6 S. 2 DSA. Damit lässt der DSA indirekt auch den Einsatz von automatisierten Entscheidungsverfahren zu, eine menschliche Kontrolle wird vom DSA nicht gefordert. Ferner muss der Beschwerdeführer über die vom Provider getroffene Entscheidung nach Art. 14 Abs. 5 DSA unverzüglich von diesem informiert werden, einschließlich der Abhilfemöglichkeiten gegenüber dieser Entscheidung. Schließlich legt Art. 14 Abs. 6 DSA generell fest, dass Provider zeitnah und objektiv über die Behandlung der Beschwerden zu entscheiden haben – was im Vergleich mit Art. 19 DSA, der Nachrichten von trustedflaggern priorisiert, doch einen zeitlichen Unterschied markiert; eine feste zeitliche Grenze wie etwa in § 3 Abs. 2 Nr. 2, Nr. 3 NetzDG ist nicht vorgesehen.

¹¹⁸ Rechtsvergleich bei *Schweizerisches Institut für Rechtsvergleichung*, Gutachten zur zivilrechtlichen Verantwortung von Internet-Service-Providern, 2015; *Holznapel*, Notice and Take-Down-Verfahren als Teil der Providerhaftung, 2013, S. 75 ff; *Götze*, Aktuelle Fragen der strafrechtlichen Providerhaftung, 2015, S. 143 ff; zu Unterschieden zwischen Deutschland und Frankreich *Matulionytė/Nérison*, IIC 2011, 55 umfassend auch *Spindler/Verbiest/Riccio*, Study on the Liability of internet intermediaries, 2007, S. 106 ff., abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069, zuletzt abgerufen am 09.10.2021.

¹¹⁹ *Rössel* ITRB 2021, 35, 39; dazu in Grundzügen BGH, GRUR 2012, 311, 313 Rn. 27 – Blogbeitrag; es sei innerhalb einer „angemessenen Frist“ zu reagieren und ggf. „Nachweise“ zu verlangen; anders BGH, GRUR 2016, 855, 856 f.Rn. 48 – www.jameda.de II: „zumutbare Nachforschungen“ sind anzustellen; ähnlich BGH, GRUR 2014, 657, 658 Rn. 18 – BearShare; anders BGH, GRUR 2011, 1038, 1040 Rn. 28 – Stiftparfüm „ohne eingehende Überprüfung“; für Suchmaschinenanbieter sollen solche Nachforschungspflichten jedenfalls nicht bestehen, BGH, GRUR 2020, 1338, 1342 Rn. 38 – Recht auf Vergessenwerden.

Insgesamt konkretisiert damit der DSA die Anforderungen an das notice-and-take-down System des Art. 5 DSA bzw. früheren Art. 14 E-Commerce-RL in deutlicherer Weise als zuvor, so dass Provider in Zukunft nicht mehr nur versteckte Hinweise auf die Empfangnahme von Beschwerden in ihren Systemen verwenden können. Auch wird klargestellt, dass jedermann derartige Beschwerden an den Provider richten können muss – und nicht nur staatliche Stellen, wie dies vereinzelt in der EU der Fall war.¹²⁰

Allerdings ist eine zivilrechtliche Umsetzung bzw. Sanktionierung dieser Pflichten schwerer vorstellbar, da anders als beim Nutzer hier kein vertragliches Verhältnis zwischen Beschwerdeführer und Provider besteht. Eine Verletzung der Pflichten nach Art. 14 DSA dürfte daher allenfalls als Indiz für ein generell gefahrgeneigtes „aktives“ System, das zu Rechtsverletzungen quasi einlädt, angesehen werden, so dass die Anwendung der Haftungsprivilegierungen eher zu verneinen ist.

2. Begründungspflichten bei Löschen oder Sperren von Inhalten

Nicht nur das Verfahren zur Behandlung von Beschwerden wird näher ausgeformt, sondern auch das Verhältnis zum betroffenen Nutzer. Löscht oder blockiert ein Provider einen Inhalt, muss er den betroffenen Nutzer spätestens zu diesem Zeitpunkt über die Gründe unterrichten, die den Provider zu dieser Entscheidung bewogen haben, Art. 15 Abs. 1 DSA. Wiederum konkretisiert Art. 15 Abs. 2 DSA die Anforderungen an diese Benachrichtigung des Nutzers, indem u.a. die territoriale Reichweite der Maßnahme anzugeben ist, zudem die Angabe der Tatsachen und Umstände, die der Entscheidung zugrunde liegen, einschließlich der Information darüber, ob die Entscheidung aufgrund einer Beschwerde getroffen wurde sowie die Unterrichtung darüber, ob automatisierte Verfahren zur Entscheidung und zur Identifizierung der Inhalte verwandt wurden. Im Fall rechtswidriger Inhalte ist zudem die Rechtsgrundlage anzugeben und einer Erklärung, warum der konkrete Inhalt darunterfallen soll, ebenso im Falle des Verstoßes gegen die vertraglichen Nutzungsbedingungen. Schließlich ist über Abhilfemöglichkeiten für den betroffenen Nutzer aufzuklären, sei es durch interne Beschwerdemanagementsysteme, außergerichtliche Streitbeilegungsmöglichkeiten oder gerichtliche Rechtsbehelfe. Gerade in Bezug auf die Möglichkeit, Rechtsschutz nachzusuchen, verlangt Art. 15 Abs. 3, ErwGr 42 DSA, dass die dem Nutzer erteilte Information ihn in die Lage versetzen muss, die in der Information genannten Rechtsbehelfe zu ergreifen.

¹²⁰ So etwa in Spanien nach Art. 16 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, abrufbar unter <https://s.gwdg.de/eGFdQ5>, zuletzt abgerufen am 09.10.2021; dazu auch *Spindler/Verbiest/Riccio*, Study on the Liability of internet intermediaries, 2007, S. 49, abrufbar unter <https://s.gwdg.de/FsnnKY>, zuletzt abgerufen am 09.10.2021.

Gerade diese Pflichten können aber die vertragsrechtlichen Pflichten aus dem Teilnahmevertrag mit den Nutzern konkretisieren und stellen mindestens gesetzliche Leitbilder, eher sogar zwingende öffentlich-rechtliche Normen dar, die nicht abbedungen werden können.

Dagegen sieht Art. 15 DSA kein rechtliches Gehör für den betroffenen Nutzer vor einer Entscheidung des Providers über die Löschung oder Sperrung des Inhalts vor – was sich indirekt auch aus dem explizit geregelten Verfahren für Online-Plattformen nach Art. 17 DSA ergibt.¹²¹ Ebenso wenig enthält Art. 15 DSA einen unmittelbaren Anspruch des Nutzers auf Wiederherstellung seines Inhalts; insoweit bleibt es beim nationalen Recht, hier vor allem des Vertragsrechts, dass Nutzer ihre Ansprüche auf Wiederherstellung der Inhalte geltend machen können.¹²² Allenfalls kann aus Art. 15 Abs. 3 DSA implizit ein solcher Anspruch abgeleitet werden. Ob dies verfassungsrechtlichen Anforderungen standhält, kann hier nicht vertieft werden, kann aber mit Fug und Recht sehr bezweifelt werden.

B. Dritte Stufe: Erhöhte Pflichten für Online-Plattformen

Eine der zentralen Neuerungen des DSA betrifft die Regulierung von Online-Plattformen, die erhöhten Pflichten gegenüber den „normalen“ Host-Providern unterworfen werden. Diese Pflichten richten sich zum einen auf Verschärfungen des Beschwerdemanagements und Berichtspflichten gegenüber Aufsichtsbehörden, ebenso auf die Einrichtung außergerichtlicher Streitschlichtungsmechanismen bis hin zur Einführung von trustedflaggers und Vorkehrungen gegen den Missbrauch von Beschwerden. Inwiefern diese Pflichten alle nur öffentlich-rechtlicher Natur sind und keine Auswirkungen auf zivilrechtliche und ggf. auch strafrechtliche Pflichten haben, erscheint offen und kann nur im Hinblick auf die jeweilige Norm beantwortet werden, insbesondere ob sie auch vertragsrechtliche Pflichten konkretisieren oder als Schutzgesetze im Hinblick auf § 823 Abs. 2 BGB qualifiziert werden können, vergleichbar der Diskussion um die finanzmarktrechtlichen Pflichten nach der MiFiD II.¹²³ Jedenfalls sieht der DSA keine auf die in Kapitel III und IV genannten Pflichten bezogenen Schadensersatzansprüche vor, sondern belässt es vielmehr bei Bußgeldern in Art. 42 DSA.

¹²¹ S. auch *Rüssel*, ITRB 2021, 35, 40.

¹²² Für Anspruch aus Vertrag sui generis OLG München, GRUR-RS 2020, 2103 Rn. 61, 117; ähnlich OLG München, NJW 2018, 3115, 3116 Rn. 12, 18; OLG Oldenburg, GRUR-RS 2019, 16526 Rn. 7; für Qualifizierung des Anspruchs als Erfüllungsanspruch OLG Düsseldorf, GRUR-RS 2020, 41440 Rn. 23; ähnlich *Beurskens*, NJW 2018, 3418, 3419 f; zur ähnlichen Diskussion zum NetzDG *Spindler*, CR 2019, 238, 239; *Peukert*, MMR 2018, 572; *Friebe*, NJW 2020, 1697, 1698 f; *Niggemann*, CR 2020, 326, 329.

¹²³ Wiederum *Spindler*, in: Langenbucher/Bliesener/Spindler, Bankenrecht-Kommentar, § 63 WpHG Rn. 8 ff.; *Kasper*, WM 2021, 60; vgl. *Müllert*, ZHR 172 (2008), 170, 176, 183; *Lehmann*, in: MüKo BGB, Band 13, Teil 12 A. Rn. 181.

1. Anwendungsbereich

Online-Plattformen sind nach Art. 2 h) und i) DSA eine Unterkategorie der Host-Provider, die Informationen auf Anforderung durch einen Nutzer an die Öffentlichkeit verbreiten und zugänglich machen, ganz im Sinne der Definition des öffentlichen Zugänglichmachens in Art. 3 Abs. 1 InfoSoc-RL. ErwGr 14 DSA stellt hierzu klar, dass geschlossene Gruppen von Nutzern nicht unter den Begriff der Öffentlichkeit fallen, ebenso wenig die individuelle Kommunikation etwa durch Emails oder Messenger-Dienste, wie sie durch Art. 2 Nr. 4, 5 Elektronische Kommunikationskodex-RL¹²⁴ definiert werden. Wie schon zum NetzDG erscheint gerade im Fall von Messenger-Diensten diese Abgrenzung aber mehr als zweifelhaft, etwa bei offenen Telegramm- oder Whatsapp-Gruppen.

Art. 2 h) DSA hält in diesem Rahmen ferner fest, dass untergeordnete Dienste oder solche, die aus objektiven und technischen Gründen in einen anderen Dienst integriert sind, nicht unter die Definition fallen, solange diese nicht der Umgehung des DSA dienen. Als Anwendungsbeispiel nennt ErwGr 13 DSA die Kommentarfunktion einer elektronischen Presse, die nur eine untergeordnete Funktion erfülle. Damit könnte aber eine empfindliche Anwendungslücke in der Bekämpfung von hate speech entstehen, da gerade derartige Kommentarfunktionen genutzt werden, um fake news etc. zu verbreiten, zumal die elektronische Presse nicht unter die AVM-RL fällt, ErwGr 28 AVM-RL.

2. Beschwerdemanagementsysteme für Nutzer und außergerichtliche Streitschlichtung

Online-Plattformen unterliegen gegenüber „normalen“ Host-Providern verschärften Anforderungen an Beschwerdemanagementsystemen: Diese müssen zunächst „intern“ sein, anders als nach Art. 14 DSA, der nur „Mechanismen“ verlangt, die auch von Drittanbietern stammen können. Das Beschwerdemanagementsystem nach Art. 17 DSA richtet sich aber im Gegensatz zu dem notice-and-action System nach Art. 14 DSA allein auf Beschwerden von Nutzern, deren Inhalte durch entsprechende Entscheidungen der Online-Plattformbetreiber entfernt oder gesperrt wurden oder deren Zugang zur Plattform bzw. deren Benutzerkonto gesperrt wurde, Art. 17 Abs. 1 DSA. Solche Beschwerden müssen für 6 Monate nach der Entscheidung des Providers elektronisch und kostenfrei eingereicht werden können. Ähnlich wie Art. 14 DSA – aber wiederum bezogen auf die Beschwerden betroffener Nutzer – verlangt Art. 17 Abs. 2 DSA die nutzerfreundliche Ausgestaltung des Systems, ebenso wie nach Art. 17 Abs. 3 DSA die Pflicht zur zeitnahen und objektiven Behandlung der Beschwerde sowie zur Rücknahme der Entscheidung durch den Provider, wenn die Beschwerde darlegt,

¹²⁴ Richtlinie (EU) 2018/1825 des europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), ABl. L 321 vom 17.12.2018, S. 36-214.

dass keine rechtswidrigen Informationen oder Verstöße gegen die Vertragsbedingungen etc. vorlagen. Die Entscheidung über die Beschwerde darf nicht allein durch automatisierte Verfahren getroffen werden, Art. 17 Abs. 5 DSA, aber offenbar mit ihrer Unterstützung. Eigenartigerweise enthält Art. 17 DSA keine Hinweise darauf, dass die betroffenen Dritten in dem Verfahren gehört werden – wie es etwa der EuGH in der UPC Telekabel-Entscheidung zur Wahrung der Grundrechte der Betroffenen deutlich gefordert hatte, auch wenn diese Entscheidung eine Sperrverfügung gegenüber Access-Provider betraf.¹²⁵

Ebenso wenig enthält auch Art. 17 DSA keinen ausdrücklichen Anspruch der Nutzer auf Wiederherstellung der Inhalte; auch hier lässt sich dies entweder nur vertragsrechtlich aus den Nutzerteilnahmeverträgen ableiten oder mittelbar aus Art. 17 DSA, da ein derartiges Beschwerdemanagementsystem letztlich nur Sinn macht, wenn der Nutzer im Grunde auch einen Anspruch auf die Wiederherstellung der Inhalte hat.

Eine der größten Herausforderungen für die Wahrung von Persönlichkeitsrechten auf Online-Plattformen besteht mit Sicherheit in der Gewährleistung effektiven und schnellen Rechtsschutzes.¹²⁶ Denn ein Provider ist in aller Regel nicht geeignet, um in die Rolle eines Richter zu schlüpfen, zumal gerade Auseinandersetzungen um rechtswidrige Inhalte bei Persönlichkeitsrechten kaum einer Automatisierung zugänglich sein dürften. Daher ist der Vorschlag des Art. 18 DSA zu begrüßen, der Provider von Online-Plattformen dazu verpflichtet, mit nach Art. 18 Abs. 2 DSA zertifizierten außergerichtlichen Streitschlichtungsstellen zu kooperieren und sich ihren Entscheidungen zu unterwerfen. Allerdings haben nur Nutzer, deren Inhalte nach Art. 17 Abs. 1 DSA blockiert, gelöscht oder deren Benutzerkonten gesperrt wurden, nach Art. 18 Abs. 1 DSA Zugang zu diesen außergerichtlichen Streitschlichtungsstellen (unter denen sie aber auswählen können); warum diese Möglichkeit nicht anderen Betroffenen, z.B. in ihren Persönlichkeitsrechten Verletzten zur Verfügung steht, bleibt unklar. Das Recht, staatliche Gerichte anzurufen, wird nach Art. 18 Abs. 1 UAbs. 2 DSA für die betroffenen Nutzer nicht berührt.

In zivilrechtlicher Hinsicht ist wiederum fraglich, inwiefern Art. 18 DSA auch die Pflichten aus dem Teilnahmevertrag mit den Nutzern konkretisieren kann – was uneingeschränkt zu bejahen ist, da gerade die Bereitstellung solcher Streitschlichtungsmechanismen essentiell für die Nutzer sein kann, um Abhilfe gegenüber entsprechenden Entscheidungen der Provider zu erhalten. Allerdings stellt sich wiederum die Frage, welche Sanktion zivilrechtlich bei einer Pflichtverletzung offenstünde: Hier kann zwar ein Erfüllungsanspruch theoretisch zur Verfügung

¹²⁵ EuGH, 27.3.2014 - C-314/12, ECLI:EU:C:2014:192 Rn. 54, 57 = GRUR 2014, 468, 471 – UPC Telekabel/Constantin Film; zum rechtlichen Gehör auch *Spindler*, GRUR 2014, 826, 833.

¹²⁶ S. dazu bereits in diese Richtung *Spindler*, Gutachten zum 69. DJT 2012 F S. 56 ff; ebenso jetzt *Wagner*, GRUR 2020, 447, 455.

stehen, doch steht es nach wie vor im Ermessen des Providers, mit welcher Streitschlichtungsstelle er kooperieren will. Denkbar ist aber auch ein Schadensersatzanspruch durch den Nutzer, der von einer ungerechtfertigten Sperre betroffen ist und erst durch ein gerichtliches Verfahren Rechtsschutz erhält, was schneller durch ein außergerichtliches Verfahren hätte realisiert werden können. In der Praxis wird daher wohl eher die öffentlich-rechtliche Durchsetzung der Normalfall sein.

Hinsichtlich der Anforderungen an die Zertifizierung solcher außergerichtlichen Streitschlichtungsstellen durch den Digitale Dienste Koordinator verlangt Art. 18 Abs. 2 DSA, dass diese unparteiisch und unabhängig vom Plattformbetreiber und von den Nutzern sein müssen, ferner, dass sie über die nötige Expertise in einer oder mehrerer der betroffenen Fragen der rechtswidrigen Inhalte oder der Verletzung der Vertragsbedingungen des Providers verfügen, sowie dass sie einfach elektronisch erreichbar sind, schnell und kosteneffizient in einer der Sprachen der EU-Mitgliedstaaten handeln können und über klare und faire Verfahrensregeln verfügen – ohne dass diese näher von Art. 18 Abs. 2 DSA spezifiziert würden. Der Charakter des nur zugunsten des Nutzers installierten außergerichtlichen Streitschlichtungsverfahrens, das nicht dem Provider selbst offensteht,¹²⁷ zeigt sich nicht zuletzt anhand der aus zivilprozessualer Sicht eigenartig anmutenden Kostentragungsregelung des Art. 18 Abs. 3 DSA: So muss der Provider zwar im Falle, dass er unterliegt, die Kosten des Nutzers tragen, aber nicht umgekehrt, wenn der Nutzer unterliegt. Hinsichtlich der Kosten der Streitschlichtungsstelle selbst präzisiert Art. 18 Abs. 3 UAbs. 2 DSA diese nicht weiter, sondern begnügt sich damit, dass diese „vernünftig“ sein müssen und nicht die Kosten des Verfahrens selbst übersteigen dürfen. Die zertifizierten Streitschlichtungsstellen müssen vom Digitale Dienste Koordinator an die Kommission übermittelt werden, die eine Liste der verfügbaren Stellen veröffentlicht. Unberührt von diesen Verfahren bleiben die von der Richtlinie 2013/11/EU¹²⁸ vorgesehenen alternativen Streitschlichtungsmechanismen für Verbraucher; Art. 18 DSA ist vielmehr für alle Nutzer einer Online-Plattform anwendbar, damit auch für kommerzielle Nutzer, wie z.B. Händler.

3. Trustedflaggers

Abweichend von den Regelungen für alle Host-Provider sieht Art. 19 DSA die Einführung eines „trustedflagger“-Verfahrens für Beschwerdeführer vor, die Beschwerden über rechtswidrige Inhalte einreichen und sich in der Vergangenheit als vertrauenswürdig erwiesen haben. Nachrichten bzw. Beschwerden, die von diesen

¹²⁷ *Rössel*, ITRB 2021, 35, 40.

¹²⁸ Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten), ABl. L 165 vom 18.6.2013, S. 63.

Personen kommen, sollen von den Providern der Online-Plattformen mit Priorität und ohne Verzögerung behandelt werden – allerdings sieht schon Art. 14 DSA vor, dass Nachrichten bzw. Beschwerden ohne Verzögerung bearbeitet werden sollen, so dass sich hieraus eine gewisse zeitliche Hierarchie ergibt. Wer als „trustedflagger“ gelten kann, wird wiederum vom Digitale Dienste Koordinator festgelegt, wobei nach Art. 19 Abs. 2 DSA nur diejenigen Unternehmen („entities“) in Betracht kommen,¹²⁹ die über besondere Erfahrung in der Entdeckung, Identifizierung und Benachrichtigung von rechtswidrigen Inhalte verfügen und diese auch zeitnah und objektiv ausführen, ferner die kollektive Interessen vertreten und unabhängig von jeder Online-Plattform sind. ErwGr 46 S. 3 DSA führt als Beispiele Europol oder nicht-Regierungsorganisationen wie das Netzwerk INHOPE an, das sich um Kindesmissbrauch kümmert. Aber auch im Urheberrecht sollen Verbände oder Organisationen der Industrie und der Rechteinhaber den „trustedflagger“-Status erhalten – was einmal mehr zeigt, dass der DSA hier durchaus Art. 17 DSM-RL flankieren will, obwohl prima vista Art. 1 Abs. 5c DSA das Urheberrecht nicht tangieren will.¹³⁰

4. Maßnahmen gegen Missbrauch von Plattformen

Eng verwandt mit der Behandlung von „trustedflaggers“ bzw. quasi die Kehrseite sind die Pflichten der Provider, um gegen Missbrauch sowohl seitens der Nutzer als auch von Beschwerdeführern vorzugehen. Art. 20 Abs. 1 DSA hält fest, dass Betreiber von Online-Plattformen für eine angemessene Zeit und nach vorheriger Warnung ihre Dienste für Nutzer sperren sollen, die zuvor in erheblicher Weise rechtswidrige Inhalte eingestellt haben. Gleiches gilt nach Art. 20 Abs. 2 DSA für die Behandlung von Beschwerden von Unternehmen bzw. Organisationen („entities“) und Einzelpersonen, die öfters Nachrichten oder Beschwerden eingereicht haben, die offensichtlich unbegründet waren. Art. 20 Abs. 3 DSA verpflichtet die Provider dazu, jeweils im Einzelfall zeitnah und objektiv zu überprüfen, ob Nutzer oder Beschwerdeführer missbräuchlich gehandelt haben, wobei der Provider insbesondere die absolute Zahl von ersichtlich rechtswidrigen Inhalten oder unbegründeten Beschwerden im vergangenen Jahr ins Verhältnis zu setzen hat, ebenso die relative Zahl im Verhältnis zu allen Informationen und Nachrichten im letzten Jahr, ferner das Ausmaß bzw. die qualitative Bedeutung des Missbrauchs bis hin zur Absicht des Nutzers bzw. des Unternehmens.

¹²⁹ Nach ErwGr 46 S. 2 DSA soll der Status als „trustedflagger“ nicht individuellen Personen zukommen.

¹³⁰ Zu trustedflaggern unter Art. 17 DSM-RL schon Erklärung der Bundesregierung bei der Abstimmung im Ministerrat vom 15.04.2019, Pkt 8, Interinstitutional File: 2016/0280 (COD), 7986/19 ADD 1 REV 2; dazu *Spindler*, CR 2020, 50, 55 Rn. 36 f.; *Spindler*, CR 2019, 277, 286 Rn. 55; *Hofmann*, GRUR 2019, 1219, 1228; *Raue/Steinebach*, ZUM 2020, 355, 363; mit einem eigenen Entwurfsvorschlag *Leistner*, ZUM 2020, 505, 512 ff.

Wie Provider mit dem Problem des Missbrauchs umgehen, müssen sie in ihren Vertragsbedingungen bekanntgeben, einschließlich der Tatsachen und Umstände, die sie hierzu heranziehen, und der Dauer der Sperre der Dienste, Art. 20 Abs. 4 DSA. Dazu hält ErwGr 47 S. 4 DSA fest, dass Art. 20 nicht den Provider daran hindert, schärfere Bedingungen für den Ausschluss wegen Missbrauchs vorzusehen. Ebenso will ErwGr 47 S. 8 DSA die Regelungen zum Missbrauch nicht als abschließend ansehen, so dass andere europäische oder nationale Vorschriften nach wie vor anwendbar sind, mithin aus deutscher Sicht § 826 BGB oder § 823 Abs. 2 BGB im Zusammenhang mit den Möglichkeiten, gegen missbräuchliche Abmahnungen vorzugehen.¹³¹ Aber auch (neben-)vertragliche Ansprüche der Nutzer aus dem Teilnahmevertrag mit der Online-Plattform können durch Art. 20 DSA konkretisiert werden, wobei diese aufgrund ihres zwingenden (öffentlich-rechtlichen) Charakters auch nicht abbedungen werden dürften, erst recht nicht in AGB (§ 307 BGB).

5. Mitteilungs- und Publizitätspflichten

Für die Pflichten nach Art. 21 Abs. 1 DSA hat offenbar das deutsche NetzDG Pate gestanden: Denn Art. 21 DSA verpflichtet die Online-Plattform Betreiber zur Mitteilung von Informationen an die Aufsichts- bzw. Strafverfolgungsbehörden,¹³² die den Verdacht auf eine erhebliche Straftat mit Gefahr für Leib und Leben nahelegen, insbesondere Straftaten wie sie in der Kinderpornografie-Bekämpfung-RL¹³³ aufgeführt werden, ErwGr 48 DSA, wozu vor allem Kinderpornographie und sexueller Mißbrauch von Kindern gehören.¹³⁴

Auch die Publizitätspflichten, die für alle Provider bereits nach Art. 13 gelten, werden für Online-Plattformen nochmals durch Art. 23 Abs. 1 DSA ausgeweitet, indem die Berichte die Zahl, Dauer und Ergebnisse von außergerichtlichen Streit-schlichtungen umfassen müssen, die Zahl von Sperrungen von Nutzer-Konten und von Beschwerdeführern unter getrennter Angabe der verschiedenen Kategorien (ob wegen rechtswidriger Inhalte oder unbegründeter Beschwerden), sowie die Angabe, ob automatisierte Verfahren zur „contentmoderation“ eingesetzt wurden, einschließlich der damit verfolgten Ziele und von Indikatoren zur Einhaltung

¹³¹ BGH, GRUR 2016, 630, 631 f.Rn. 14 f.; BGH, GRUR 2015, 578, 579 Rn. 16; BGH, GRUR 2006, 433, 434 Rn. 16 f.; BGH, NJW 2005, 3141, 3142; OLG Frankfurt/M, GRUR-RS 2015, 10631 Rn. 40 f.

¹³² Zur Zuständigkeit des jeweiligen Mitgliedstaates s. Art. 21 Abs. 2 DSA.

¹³³ Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 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. L 335 vom 17.12.2011, S. 1–14.

¹³⁴ Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 über die Umweltverträglichkeitsprüfung bei bestimmten öffentlichen und privaten Projekten, ABl. L 26 vom 28.1.2012, S. 1–21.

dieser Ziele. Damit erhöht Art. 13 DSA den Druck auf die Online-Plattformen, gerade auch über die Parameter und den Einsatz automatisierter Verfahren jenseits der eher individuell gehaltenen Pflichten wie nach Art. 13 Abs. 2 f DSGVO Bericht zu erstatten. Für den Anwendungsbereich des DSA insbesondere der Feststellung, ob es sich um sehr große Online-Plattformen handelt, ist ferner die halbjährliche Berichterstattung der Online-Plattform Betreiber über die Zahl der aktiven Nutzer der Plattform in jedem Mitgliedstaat in diesem Zeitraum von Relevanz, Art. 23 Abs. 2 DSA, auf der Grundlage der mit einem Durchführungsrechtakt nach Art. 25 Abs. 2 DSA festgelegten Berechnungsmethode, wobei keine personenbezogenen Daten zu übermitteln sind, Art. 25 Abs. 3 DSA.

C. Vierte Stufe: Pflichten für besonders große Online-Plattformen

Neben den wesentlich erweiterten Pflichten für Online-Plattformen treten als weiteres Herzstück des DSA die Anforderungen an besonders große Online-Plattformen, für die der DSA an den Begriff der systemischen Risiken anknüpft, wie sie aus der Finanzmarkt-Regulierung bekannt sind (Art. 2c) Europäischer Ausschuss für Systemrisiken-VO¹³⁵). Denn die besonders großen Online-Plattformen werden als potentielle Verursacher von gesellschaftlichen Risiken und Gatekeeper (ErwGr 56 DSA), insbesondere für die demokratische Meinungsbildung angesehen.¹³⁶ Neben den Regelungen zu systemischen Risiken in Art. 25 – 28 DSA, zu denen auch die Pflicht zur Einführung eines Compliance-Beauftragten (Art. 32 DSA) gehört, führt der DSA auch spezielle Anforderungen für Systeme zu Empfehlungen oder zur online Werbung ein; ferner werden die Transparenz- und Publizitätspflichten nochmals verschärft, Art. 33 DSA.

Speziell für die auf systemische Risiken ausgerichteten Pflichten des DSA kommt in erster Linie nur die Qualifizierung als öffentlich-rechtliche Pflichten in Betracht, was sich nicht zuletzt in den zahlreichen Ermächtigungsbefugnissen der EU-Kommission sowie der Digitale Dienste Koordinatoren in Art. 23 Abs. 4, 25, 31, 33 Abs. 2, 34 ff DSA äußert. Es handelt sich im Wesentlichen – vergleichbar den finanzmarktrechtlichen Pflichten – um Corporate Governance-Vorschriften, die im Wege der Aufsicht durch Behörden, hier dem Digitale Dienste Koordinator, durchgesetzt werden müssen, und nur in Ausnahmefällen zivilrechtliche Pflichten auslösen.

¹³⁵ Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken, ABL. L 331 vom 15.12.2010, S. 1–11.

¹³⁶ Umfassend *Bauer*, WRP 2020, 171; *Stark*, MMR 2017, 721; schon *Holznapel*, NordÖR 2011, 205.

1. Anwendungsbereich

Art. 25 DSA definiert den Anwendungsbereich besonders großer Online-Plattformen als solche, bei denen monatlich durchschnittlich mindestens 45 Millionen Teilnehmer in der EU aktiv sind, was wiederum auf der Grundlage der in einem Durchführungsrechtsakt der EU-Kommission (Art. 25 Abs. 3 DSA) festgelegten Berechnungsmethode ermittelt werden soll. Demgemäß soll es nicht auf die registrierten Nutzer ankommen, sondern nur auf die „aktiven“; vergleichbare Probleme der Berechnung der Nutzerzahl sind auch aus dem NetzDG bekannt.¹³⁷ Die Liste der betroffenen besonders großen Online-Plattformen soll nach Art. 25 Abs. 4 DSA von der Kommission im Amtsblatt der EU veröffentlicht werden, mitsamt einer Übergangsfrist für die betroffenen Provider zur Anwendung der Pflichten von 4 Monaten.

2. Systemische Risiken

Vergleichbar den Ansätzen aus der Regulierung des Finanzmarktsektors verpflichtet Art. 26 Abs. 1 DSA die Plattformbetreiber zunächst mindestens einmal jährlich zur Analyse, ob systemische Risiken durch ihre Plattformen entstehen, worunter Art. 26 Abs. 1 S. 2 DSA die Verbreitung rechtswidriger Inhalte versteht, einschließlich des Vertriebs von Piraterie-Produkten (ErwGr 57 S. 1 DSA). Denn die Möglichkeit der weitreichenden Verbreitung illegaler Inhalte sieht die Kommission infolge der Netzwerkeffekte als besonders kritisch, mithin systemisch an (ErwGr 57 S. 2 DSA). Ferner fallen unter die systemischen Risiken negative Auswirkungen auf die Ausübung von Grundrechten hinsichtlich der Meinungs- und Informationsfreiheit, dem Schutz der Privat- und Familiensphäre, der Rechte von Kindern sowie der Verhinderung von Diskriminierung, wobei die Kommission hier vor allem an den Einsatz von Algorithmen durch die Plattformbetreiber oder Dritte denkt, die etwa die Meinungsfreiheit gefährden können (ErwGr 57 S. 5 DSA). Schließlich umfassen die systemischen Risiken Manipulationen der Dienste, einschließlich der automatischen Nutzung der Dienste, die negative Effekte auf den Schutz der öffentlichen Gesundheit, Minderjährige, aber auch auf Wahlen sowie die öffentliche Sicherheit haben können. Damit zielt Art. 26 Abs. 1 DSA neben der Verhinderung von Desinformationskampagnen auch auf Phänomene wie „hate speech“ oder die Beeinflussung von Wahlen ab, wie etwa durch falsche Nutzerkonten, den Einsatz von social bots etc. (ErwGr 57 S. 7 DSA).

Im Rahmen dieser Risikoanalyse müssen die Plattformbetreiber nach Art. 26 Abs. 2 DSA die Auswirkungen ihrer Systeme zur Moderation und zur Empfehlung von Inhalten, einschließlich der Werbung, auf die Verbreitung von rechtswidrigen Inhalten oder solchen, die nicht mit den Vertragsbedingungen der Platt-

¹³⁷ *Liesching*, in: Spindler/Schmitz, TMG, § 1 NetzDGRn. 70; ähnlich schon *Guggenberger*, ZRP 2017, 98; *Spindler*, K&R 2017, 533, 543; dagegen *Hoven/Gersdorf*, in: BeckOK Info MedienR, 33. Edition 1.5.2021, § 1 NetzDGRn. 30.

formbetreiber vereinbar sind, berücksichtigen. Aufbauend auf dieser Risikoanalyse müssen die Plattformen Risikomanagementsysteme einrichten, die unter anderem nach Art. 27 Abs. 1 DSA Anpassungen in den Systemen zur Moderation und zur Empfehlung von Inhalten enthalten, ferner Maßnahmen zur Begrenzung von Werbung in Verbindung mit den angebotenen Diensten, die Stärkung der internen Überwachung der Plattformen im Hinblick auf die systemischen Risiken, die Initiierung einer Zusammenarbeit mit „trustedflaggers“ nach Art. 19 DSA, bis hin zur Zusammenarbeit mit anderen Online-Plattformen (ohne Beschränkung auf besonders große Online-Plattformen) hinsichtlich der Codes of Conduct (Art. 35 DSA) und Krisenprotokollen nach Art. 37 DSA.

Bei der Erfassung der systemischen Risiken und der Maßnahmen sollen nach ErwGr 59 DSA Repräsentanten von Nutzern und von etwaig betroffenen Gruppen sowie unabhängige Experten und Organisationen der Zivilgesellschaft beteiligt werden – ohne dass der DSA hierfür ein besonderes Format oder gar einen Anspruch dieser genannten Gruppen vorsähe.

Die rechtliche Qualifikation dieser Pflichten fällt eher zugunsten einer öffentlich-rechtlichen Pflicht aus, da es primär um interne Governance-Aspekte der Provider von besonders großen Plattformen geht, die sich zivilrechtlich kaum in vertragsrechtliche Pflichten der Provider „übersetzen“ lassen – mit Ausnahme der Zusammenarbeit etwa mit „trustedflaggers“, für die sich ein Anspruch auf Kooperation ergeben könnte, auch wenn Art. 17 DSM-RL dementsprechende Pflichten nicht enthält. Allerdings zählt Art. 27 DSA die Pflichten nur beispielhaft auf, so dass sich nur in Ausnahmekonstellationen ein Anspruch darauf stützen lässt.

Der öffentlich-rechtliche, an die Finanzmarktregulierung angelehnte Charakter wird auch in der weiteren Struktur des Umgangs mit systemischen Risiken deutlich, indem nach Art. 27 Abs. 2 DSA das Europäische Gremium für digitale Dienste jährliche Berichte publizieren soll, die die wichtigsten und wiederkehrenden systemischen Risiken, über die die Plattformen berichtet haben, zusammenfassen und bewerten soll. Auch soll das Europäische Gremium für digitale Dienste „best practices“ identifizieren, um mit systemischen Risiken umzugehen. Auch die Kommission wird in Art. 27 Abs. 3 DSA ermächtigt, unter Anhörung der Öffentlichkeit generelle Richtlinien zu erlassen, die Maßnahmen zur Bekämpfung der systemischen Risiken enthalten – wobei Art. 27 Abs. 3 DSA die Wahrung der Grundrechte aller Beteiligten anmahnt.

Deutlich wird aber das Anliegen der EU-Kommission, einen möglichst umfassenden Ansatz für sehr große Online Plattformen vorzusehen, der eben auch die Gefahren für die demokratisch verfassten Ordnungen der EU und der Meinungsfreiheit umfasst – wobei die Balance zwischen den verschiedenen Grundrechten und erfassten Zielen offen bleibt, was wiederum Kritik hinsichtlich der Verlagerung von staatlichen Pflichten auf Private hervorruft.

3. Audits

Ebenfalls aus der Regulierung systemischer Risiken von Finanzmärkten (vgl. Art. 69 Abs. 2 i MIFID II) ist die Verkoppelung der Pflichten mit regelmäßigen Auditierungen bekannt: So müssen auf Kosten der Provider von besonders großen Plattformen diese mindestens einmal jährlich unabhängige Audits durchführen, um die Erfüllung der Pflichten des gesamten Kapitels III des DSA zu überprüfen, mithin der Pflichten der Provider über diejenigen der Host-Provider und der Online-Plattformen bis hin zu den intensivsten Pflichten nach Art. 26 ff. DSA zum Riskmanagement. Aber auch die Einhaltung von Pflichten auf der Grundlage der Codes of Conduct oder von Krisenprotokollen nach Art. 37 DSA werden vom Audit umfasst.

Die Audits dürfen nach Art. 28 Abs. 2 DSA nur von solchen Organisationen durchgeführt werden, die unabhängig von den Betreibern der besonders großen Plattformen sind und die über genügend Fachkompetenz auf diesen Gebieten verfügen, insbesondere in der Auditierung von Algorithmen (ErwGr 60 S. 4 DSA), ferner, die sich bestimmten Standards hinsichtlich Objektivität und des Berufsethos unterworfen haben. Der DSA geht aber nicht so weit wie in den jüngsten Richtlinien zu Wirtschaftsprüfungen, die ein Rotationsprinzip vorsehen (vgl. Art. 42 Abs. 2 Abschlussprüfer-RL¹³⁸ und Art. 17 Abs. 7 Abschlussprüfer-VO¹³⁹). Auch bietet das Kriterium der „Unabhängigkeit“ wieder Anlass zur Diskussion wie mit Konstellationen verfahren werden soll, in denen eine Schwestergesellschaft der auditierenden Gesellschaft den Provider berät.¹⁴⁰

Art. 28 Abs. 3 DSA konkretisiert die Anforderungen an die Audit-Reports, die neben selbstverständlichen Angaben zu den Auditoren und der auditierten Plattform eine Beschreibung der angewandten Methode sowie der wesentlichen Ergebnisse des Audits und eine Erklärung des Auditors verlangen, ob der Plattformprovider die Pflichten nach Art. 28 Abs. 1 erfüllt hat, gegebenenfalls mit Angaben, welche Verbesserungen der Provider durchzuführen hat. Ob diese Erklärung ihrerseits Haftungswirkungen gegenüber Dritten seitens des Auditors auslöst, wird nicht durch den DSA geklärt.

Indes sind die Provider nicht an die Empfehlungen des Audit-Berichts gebunden, indem sie zwar innerhalb eines Monats nach Erhalt des Berichts nach Art. 28

¹³⁸ Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates, ABl. L 157 vom 09.06.2006, S. 87.

¹³⁹ Verordnung (EU) Nr. 537/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über spezifische Anforderungen an die Abschlussprüfung bei Unternehmen von öffentlichem Interesse und zur Aufhebung des Beschlusses 2005/909/EG der Kommission, ABl. L 158 vom 27.05.2014, S. 77-112.

¹⁴⁰ Vgl. BGH, NZG 2004, 770; zum Streit Müller, NZG 2004, 1037; Paal, DStR 2007, 1210; Bormann, BB 2002, 190, 192.

Abs. 4 S. 2 DSA Stellung dazu beziehen müssen, ihnen aber Art. 28 Abs. 4 S. 3 DSA erlaubt, die Vorschläge nicht umzusetzen, was die Provider allerdings begründen und alternative Maßnahmen erläutern müssen – ähnlich dem aus dem Aktienrecht bekannten Mechanismus des *Comply-or-Explain* (§ 161 AktG).

4. Zugang zu Daten

Ein heißes Eisen – auch im Zusammenhang mit dem parallel verabschiedeten Vorschlag eines *Digital Markets Act*¹⁴¹ – dürfte auch Art. 31 DSA sein, der die Betreiber besonders großer Online-Plattformen dazu verpflichtet, sowohl dem Digitale Dienste Koordinator als auch der Kommission auf deren Verlangen hin den Zugang zu Daten zu ermöglichen, um die Einhaltung der Verpflichtungen nach dem DSA zu überprüfen. Dieser Zugang soll aber nach Art. 31 Abs. 2 DSA auch Forschern zur Verfügung stehen, um die systemischen Risiken solcher Plattformen gem. Art. 26 Abs. 1 DSA zu erforschen. Forscher, die für diesen Zugang in Betracht kommen, werden durch Art. 26 Abs. 4 DSA definiert als solche, die mit akademischen Institutionen in Verbindung stehen und unabhängig sind von kommerziellen Interessen, die aber auch die Datensicherheit und Vertraulichkeit gewährleisten können. Der Sensibilität der Daten trägt das Verfahren von Art. 31 Abs. 6 DSA Rechnung, indem der Provider bei dem Digitale Dienste Koordinator oder der Kommission beantragen kann, dass der Antrag auf den Zugang zu den Daten die Geheimhaltungspflicht, insbesondere von Geschäftsgeheimnissen tangiert. Der DSA enthält indes keine Kriterien, wie in diesem Fall zu entscheiden ist.

5. Compliance-Officer

Wiederum in Analogie zu den Finanzmarktregulierungen (§ 87 Abs. 5 WpHG, Art. 22 Abs. 2 VO (EU) 2017/565¹⁴² in Ergänzung zu Art. 16 Abs. 2 MiFID II-RL) sieht auch Art. 32 DSA vor, dass die Betreiber von besonders großen Online-Plattformen Compliance Officer einsetzen müssen, seien sie intern oder extern, was Art. 32 Abs. 2 DSA zulässt. Diese Personen müssen die erforderlichen Erfahrungen und Kompetenzen besitzen, um neben der Zusammenarbeit mit dem Digitale Dienste Koordinator auch den Audit nach Art. 28 DSA begleiten zu können, vor allem aber die Erfüllung der Verpflichtungen nach dem DSA zu überwachen (Art. 32 Abs. 3 DSA). Der Compliance Officer muss seine Aufgaben

¹⁴¹ Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (*Digital Markets Act*), COM/2020/842 final.

¹⁴² Delegierte Verordnung (EU) 2017/565 der Kommission vom 25. April 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie, ABl. L 87 vom 31.03.2017, S. 1–83.

unabhängig wahrnehmen können – was aber der DSA nicht weiter spezifiziert, z.B. ob er einen Kündigungsschutz genießt etc. Demgegenüber sieht Art. 32 Abs. 6 DSA die üblichen Pflichten wie die Ausstattung mit den nötigen Ressourcen vor, ebenso die direkte Berichterstattung gegenüber der Geschäftsführung.

6. Transparenz- und Publizitätspflichten

Last but not least verschärft auch Art. 33 DSA die schon für Online-Plattformen geltenden Transparenz- und Publizitätspflichten, indem die Berichte nach Art. 13 DSA alle halben Jahre veröffentlicht werden müssen. Zusätzlich muss nach Art. 33 Abs. 2 DSA mindestens jährlich und 30 Tage nach der Annahme des Audit-Berichts der Betreiber einer besonders großen Plattform nach Art. 33 Abs. 2 DSA berichten über die Ergebnisse der Risikoanalysen nach Art. 26 DSA, die ergriffenen Maßnahmen zur Risikobewältigung, den Audit-Bericht sowie über die Maßnahmen hinsichtlich der Umsetzung der Empfehlungen im Audit-Bericht, Art. 33 Abs. 2 DSA.

D. Neue Durchsetzungsmechanismen

Die neuen Pflichten für Plattformen, insbesondere besonders große Plattformen, werden von verschiedenen neuen Durchsetzungsmechanismen flankiert, die hier nur kurz skizziert werden können, und die von Selbstregulierungsmechanismen wie technische Standards und Codes of Conduct über detaillierte Regelungen zu einem Digitale Dienste Koordinator bis zu einem neuen Europäischen Gremium für digitale Dienste reichen, das die Kommission bei der Einschätzung systemischer Risiken etc. beraten soll.

Hervorzuheben ist allerdings zunächst, dass der DSA anders als etwa die DSGVO in Art. 82 keinerlei Aussagen über Schadensersatzansprüche oder vertragliche Ansprüche von Nutzern – jedenfalls nicht explizit – enthält, so dass es hier bei den nationalen Ansprüchen und Sanktionen in zivil- und wettbewerbsrechtlicher Hinsicht bleibt.

1. Standards und Codes of Conduct

Hervorzuheben ist zunächst die aktive Rolle, die Art. 34 Abs. 1 DSA der Kommission bei der Entwicklung von industriellen Standards zuweist, etwa für elektronische Nachrichten nach Art. 14 DSA (z.B. zur Interoperabilität) oder von trustedflaggern nach Art. 19 DSA, ebenso wie für das Auditing nach Art. 28 DSA. Aber auch Codes of Conduct sollen von der Kommission nach Art. 35 DSA gefördert werden, die die Pflichten des DSA spezifizieren sollen, etwa im Hinblick auf Desinformation oder den Gebrauch von Bots (ErwGr 68 S. 3 DSA) – ohne dass Art. 35 DSA allerdings im Gegensatz etwa zu Art. 40 Abs. 9 DSGVO die rechtlichen Wirkungen der Codes of Conduct angeben würde. Insbesondere für systemische Risiken soll die Kommission besonders große Plattformen, aber auch

andere Beteiligte zur Verabschiedung von Codes of Conduct für die Bewältigung dieser Risiken einladen, Art. 35 Abs. 2 DSA. Die Codes of Conduct sollen die übrigen Bemühungen auf der EU-Ebene zur Selbstregulierung flankieren, etwa den Code of practice on disinformation, ErwGr 69 DSA.

Ein weiteres, neues Instrument stellen die sog. „Krisenprotokolle“ bzw. Krisenpläne nach Art. 37 Abs. 1 DSA dar, die das Europäische Gremium für digitale Dienste der Kommission empfehlen kann, die außerordentliche Umstände hinsichtlich von Risiken für die öffentliche Sicherheit oder Gesundheit betreffen. Diese „Krisenprotokolle“, die von der Kommission für besonders große Plattformen angeregt werden, sollen nach Art. 37 Abs. 2 DSA einen Maßnahmenkatalog umfassen, der die Einhaltung der Pflichten aus Art. 14, 17, 19, 20 und 27 DSA sicherstellen soll. Art. 37 Abs. 4 DSA verlangt insbesondere die genaue Angabe der Umstände, die zur Annahme einer Krise führen, das Prozedere, um das Eintreten der Krise festzustellen, die Aufgaben jedes Beteiligten und die durchzuführenden Maßnahmen, die Dauer der Krisenmaßnahmen und die entsprechende Berichterstattung hierüber. In die Erstellung solcher Krisenprotokolle können aber auch andere Organisationen eingebunden werden, etwa der Zivilgesellschaft.

2. Digitale Dienste Koordinator

Aber auch hinsichtlich der Aufsichtsstruktur schlägt der DSA neue Wege ein und dürfte der deutschen Diskussion um die Einführung einer Digitalbehörde neue Nahrung geben, indem nämlich Art. 38 Abs. 2 DSA vorsieht, dass die Mitgliedstaaten einen Digitalen Dienste Koordinator einrichten sollen, der für alle Angelegenheiten nach dem DSA zuständig und verantwortlich sein soll, einschließlich von Beschwerden von Nutzern (Art. 43 DSA) – wobei die Mitgliedstaaten immer noch die Möglichkeit haben, bestimmte spezifische Sektoren oder Aufgaben anderen Behörden zuzuordnen. Art. 39 Abs. 2 DSA verlangt aber neben den üblichen Anforderungen an angemessene Ausstattung mit Ressourcen die vollständige Unabhängigkeit der Digitale Dienste Koordinatoren, frei vom Einfluss anderer privater Unternehmen oder öffentlicher Behörden, wobei ErwGr 74 S. 2 DSA klarstellt, dass das Haushaltsrecht der Parlamente natürlich unberührt bleibt – vergleichbar den Datenschutzaufsichtsbehörden nach Art. 52 DSGVO.¹⁴³

Art. 41 DSA verleiht den Digital Dienste Koordinatoren umfangreiche Befugnisse zur Durchführung von Ermittlungen sowie zu Anordnungen gegenüber Providern, um die Pflichten des DSA durchzusetzen, einschließlich der Verhängung von Geldbußen nach Art. 42 DSA. Unter bestimmten, sehr detaillierten Bedingungen wie der wiederholten Nichterfüllung der Pflichten des DSA und der Gefährdung des Lebens und der Sicherheit von Personen, kann der Digitale Dienste

¹⁴³ Siehe dazu auch schon EuGH, 9.3.2010 – C-518/07, ECLI:EU:C:2010:125 = NJW 2010, 1265, der für die damaligen deutschen Datenschutzbehörden mehr Unabhängigkeit verlangte; ähnlich EuGH, 16.10.2012 - C-614/10, ECLI:EU:C:2012:631 = ZD 2012, 563 für die Datenschutzkommission in Österreich.

Koordinator auch bei Gerichten die zeitweise Sperrung der Nutzer, die für die Verletzungen verantwortlich sind, beantragen, Art. 41 Abs. 3 b DSA, die aber im Prinzip auf 4 Wochen beschränkt ist. Die sehr ausführliche Bestimmung des Art. 41 Abs. 3 DSA reflektiert einmal mehr den Spagat, den der DSA zwischen den verschiedenen Grundrechtspositionen versucht einzuschlagen.

Entsprechend dem Vorbild der DSGVO (vgl. Art. 83 Abs. 4, 5 DSGVO) fallen auch die von Art. 42 DSA vorgesehenen Bußgelder aus, die bis zu 6% des jährlichen Umsatzes des betroffenen Providers betragen können, Art. 42 Abs. 3 S. 1 DSA, wobei bei wiederkehrenden Bußgeldern eine Deckelung auf 5% des jährlichen Umsatzes des Providers eingreift, Art. 42 Abs. 4 DSA. Eine Erstreckung auf die Unternehmensgruppe, wie in ErwGr 150 S. 2 DSGVO vorgesehen, fehlt indes.

3. Spezielle Ermächtigungen der Kommission gegenüber sehr großen Online-Plattformen

Ein spezieller Abschnitt mit zahlreichen Ermächtigungen für die Kommission, das Europäische Gremium für digitale Dienste und die Digitale Dienste Koordinatoren befasst sich nur mit den Befugnissen gegenüber besonders großen Plattformen für den Fall, dass diese gegen Pflichten des DSA verstoßen. Der Kommission selbst werden nach Art. 51 DSA Befugnisse eingeräumt, wenn die Verstöße dauerhafter Natur sind, die über Untersuchungsbefugnisse einschließlich der Anforderung von Daten und Informationen (Art. 52 DSA), vor Ort Untersuchungen (Art. 54 DSA) bis hin zu Bußgeldverhängung von bis zu 6% des jährlichen Umsatzes (Art. 59 DSA) und zur Veröffentlichung der Entscheidung im Sinne von naming-and-shaming (Art. 64 DSA) reichen und hier nicht en detail nachgezeichnet werden können.

IV. Fazit

Lässt man bar jeder Komplexität der geschilderten Regelungen das NetzDG und den Vorschlag eines DSA Revue passieren, so zeigt sich, dass die nationalen und europäischen Gesetzgeber bestrebt sind, dem Phänomen der fake news und des hate speech Einhalt zu gebieten. Vor allem aber der DSA weist immer wieder auf die Balance zwischen den jeweiligen Grundrechtsfreiheiten und Grundrechtsgarantien hin, gibt aber en detail wenig Hinweise darauf, wie man den grundlegenden Problemen der automatisierten Rechtsdurchsetzung und den Notwendigkeiten einer schnellen und effizienten Rechtsfindung umzugehen ist – auch die an sich befürwortenswerten Regelungen des Art. 18 DSA zur Heranziehung zertifizierter außergerichtlicher Streitbelegung vermögen hier nicht weiter zu helfen, da sie nach wie vor mit etlichen Defiziten konfrontiert sind, wie bereits erwähnt. Daher sind beide Rechtssetzungsakte zwar geeignet, aber noch wesentlich verbesserungsbedürftig, um der Balance zwischen fake news und hate speech auf der

einen Seite und dem effizienten Rechtsschutz der Betroffenen auf der anderen Seite gerecht werden zu können. Die alles entscheidende „Eierlegende Wollmilchsau“¹⁴⁴ wird sich dabei nicht finden lassen.

Literaturverzeichnis

Abkürzungsverzeichnis der Zeitschriften

- AfP** – Zeitschrift für das gesamte Medienrecht (Verlag Otto Schmidt, Köln)
BB – Betriebs Berater (Beck)
CR – Computer und Recht (de Gruyter Verlag)
DStR – Deutsches Steuerrecht (Beck)
DuD – Datenschutz und Datensicherheit (Springer Verlag)
ECLR – European Competition Law Review (Sweet & Maxwell)
GRUR – Gewerblicher Rechtsschutz und Urheberrecht (Beck)
GRUR-Prax: Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht
ITRB – Informationsdienst für IT-Recht und Datenschutz (Verlag Otto Schmidt)
K&R – Kommunikation & Recht (dfv Mediengruppe)
MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung (Beck)
NJW – Neue Juristische Wochenschrift
NordÖR – Zeitschrift für Öffentliches Recht in Norddeutschland (Beck)
NVwZ – Neue Zeitschrift für Verwaltungsrecht (Beck)
NZG – Neue Zeitschrift für Gesellschaftsrecht (Beck)
WRP – Wettbewerb in Recht und Praxis (Juris)
ZRP – Zeitschrift für Rechtspolitik (Beck)
ZUM – Zeitschrift für Urheber- und Medienrecht (Beck)

Gesetzesausgaben und Kommentare

BeckOK GG, Hrsg. Epping/Hillgruber: <https://s.gwdg.de/Uu9Ebo>

BeckOK InfoMedienR: <https://s.gwdg.de/CAJGbq>

Bornemann/Erdemir: Jugendmedienschutz-Staatsvertrag, 2. Aufl. 2021; Nomos- Kommentar

H. Dreier. Grundgesetz Kommentar: GG Bd. I-III, 4. Aufl. 2013, Mohr Siebeck

V. Erb/J. Schäfer (Hrsg.). Münchner Kommentar zum StGB (MüKo), Verlag C.H. Beck München

Eifert/Gostomyk (Hrsg.). Netzwerkecht - Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, Nomos-Verlag, 2018

¹⁴⁴ S. dazu https://de.wikipedia.org/wiki/Eierlegende_Wollmilchsau, zuletzt abgerufen am 09.10.2021.

Gersdorf/Paal (Hrsg.). Medienrecht, 2. Aufl. 2021, Beck-Verlag

Hahn/Vesting (Hrsg.). Rundfunkrecht, 3. Aufl. 2012, Beck Verlag

Dirk Heckmann (Hrsg.), juris PraxisKommentar Internetrecht, Saarbrücken (juris), 5. Aufl. 2015, juris GmbH Saarbrücken

Liesching. Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Auswirkungen auf die aktuelle Mediengesetzgebung in Deutschland, 2020, Band 1 in der Schriftenreihe Medienrecht & Medientheorie, Verlag Carl Grossmann

Sachs. Grundgesetz: GG – Kommentar, 9. Aufl. 2021, C.H. Beck

Spindler/Schmitz (Hrsg.). TMG Telemediengesetz mit Netzwerkdurchsetzungsgesetz (NetzDG). 2. Aufl. 2018, C.H. Beck München

Spindler/Schuster (Hrsg.). Recht der elektronischen Medien, 4. Aufl. 2019, Beck München

Einzelne Aufsätze in Zeitschriften

M. Bauer. Kartellrecht 4.0? – Herausforderungen der Plattformökonomie für die Regulierung des Meinungsbildungsprozesses. WRP 2020, 171–176

J. Bizer. Was sind Telemedien? DuD 2007, 40

Bormann. Unabhängigkeit des Abschlussprüfers: Aufgabe und Chance für den Berufsstand, BB 2002, 190–196

M. Beurskens. „Hate-Speech“ zwischen Lösungsrecht und Veröffentlichungspflicht, NJW 2018, 3418–3420

M. Cole. Die Bewertung von Rundfunkprogrammen durch Einrichtungen der Freiwilligen Selbstkontrolle und ihre Folgen. ZUM 2005, 452–461

M. Cornils. Präzisierung, Vervollständigung und Erweiterung: Die Änderungen des Netzwerkdurchsetzungsgesetzes 2021. NJW 2021, 2465–2471

Feldmann. Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung. K&R 2017, 292–296

M. Friehe. Löschen und Sperren in sozialen Netzwerken. NJW 2020, 1697–1701

H. Gersdorf. Hate Speech in den sozialen Netzwerken. MMR 2017, 439–446

Grimm. Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts. NJW 1995, 1687–1704

N. Guggenberger. Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht. ZRP 2017, 99–100

T. Handel. Hate Speech – Gilt deutsches Strafrecht gegenüber ausländischen Anbietern sozialer Netzwerke? MMR 2017, 227–230

Hain/Ferreau/Brings-Wiesen. Regulierung sozialer Netzwerke revisited. K&R 2017, 433–438

- D. Heckmann/J. Wimmers. Internet und E-Commerce. Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG). CR 2017, 310–333
- M. Höferlein/T. Widlok. Die Tragödie des NetzDG. MMR 2021, 277
- Hofmann. Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL. GRUR 2019, 1219–1228
- B. Holzngel. Meinungsbildung im Internet. NordÖR 2011, 205–211
- K. Hopf/B. Braml: Eingeschränkte gerichtliche Überprüfbarkeit des Beurteilungsspielraums der Kommission für Jugendmedienschutz (KJM). MMR 2009, 153–157
- J.C. Kalbhenn/M. Hemmert-Halswick. Der Regierungsentwurf zur Änderung des NetzDG. MMR 2021, 518–522
- A. Koreng. Entwurf eines Netzwerkdurchsetzungsgesetzes: Neue Wege im Kampf gegen „Hate Speech“? GRUR-Prax 2017, 203
- K.-H. Ladeur/T. Gostomzyk. Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit. K&R 2017, 390–393
- M. Leistner. Filtertechnologien und das Urheberrecht – Acht Thesen zur Umsetzung des Art. 17 DSM-RL mit einem Vorschlag für ein komplementär menschlich-algorithmisches Durchsetzungssystem für OCSP-Plattformen. ZUM 2020, 505–513
- S. Leitgeb. Virales Marketing – Rechtliches Umfeld für Werbefilme auf Internetportalen wie YouTube. ZUM 2009, 39–48
- M. Liesching. Die Durchsetzung von Verfassungs- und Europarecht gegen das Netz DG. MMR 2018, 26–30
- J. Lüdemann. Grundrechtliche Vorgaben für die Löschung von Beiträgen in sozialen Netzwerken. MMR 2019, 279–284
- S. Müller-Franken. Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrechtliche Fragen. AFP 2018, 1–14
- W. Müller. Der befangene Abschlussprüfer im Unternehmensverbund. NZG 2004, 1037–1039
- S. Niggemann. Die NetzDG-Novelle – Eine Kritik mit Blick auf die Rechte der Nutzerinnen und Nutzer. CR 2020, 326–331
- P. Nölscher. Das Netzwerkdurchsetzungsgesetz und seine Vereinbarkeit mit dem Unionsrecht. ZUM 2020, 301–311
- G. Nolte. Hate-Speech, Fake-News, das ‚Netzwerkdurchsetzungsgesetz‘ und Vielfaltssicherung durch Suchmaschinen. ZUM 2017, 552–564
- B. P. Paal. Suchmaschinen, Marktmacht und Rechtsbehelfe bei Inhabilität des Abschlussprüfers. DStR 2007, 1210–1216

- H. J. Papier. Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft. NJW 2017, 3025–3030
- A. Peukert. Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken. MMR 2018, 572–577
- J. Prütting. Das Prinzip der regulierten Selbstregulierung im Jugendmedienschutz. K&R 2013, 775–780
- B. Raue/M. Steinebach. Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung. ZUM 2020, 355–364
- A. Roßnagel. Das Telemediengesetz – Neuordnung für Kommunikations- und Informationsdienste. NVwZ 2007, 743–748
- M. Rössel. Digital Services Act. ITRB-IT 2021, S. 35–43
- R. Schwartmann/R. L. Mühlenbeck: NetzDG und das virtuelle Hausrecht sozialer Netzwerke. ZRP 2020, 170–172
- S. Schwiddessen. Medienbezogenes Straf- und Ordnungswidrigkeitenrecht bei Sachverhalten mit Auslandsbezug – Teil 1. CR 2017, 443–454
- G. Spindler. Das Netzwerkdurchsetzungsgesetz. K&R 2017, 533–543
- G. Spindler. Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig? ZUM 2017, 473–506
- G. Spindler. Löschung und Sperrung von Inhalten aufgrund von Teilnahmebedingungen sozialer Netzwerke – Eine Untersuchung der zivil- und verfassungsrechtlichen Grundlagen. CR 2019, 238 ff.
- G. Spindler. Die neue Urheberrechts-Richtlinie der EU, insbesondere „Upload-Filter“ – Bittersweet? Analyse der Änderungen beim Text- und Datamining, Leistungsschutz für Presseerzeugnisse und Pflichtenkreis für Hostprovider. CR 2019, 277–291
- G. Spindler. Upload-Filter: Umsetzungsoptionen zu Art. 17 DSM-RL. Vorschläge zur „Quadratur des Kreises“ in nationalen Recht. CR 2020, 50–59
- G. Spindler. Haftung für Urheberrechtsverstöße auf Online-Plattformen – YouTube Reloaded. NJW 2021, 2554
- B. Stark. Meinungsbildung im Netz – Die Macht der Algorithmen. MMR 2017, S. 721–722
- C. Weiner/C. Schmelz: Die elektronische Presse und andere neue Kommunikationsformen im neuen rechtlichen Regulierungsrahmen. K&R 2006, 453–459
- J. Wimmers/B. Heymann. Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG) – eine kritische Stellungnahme. AfP 2017, 93–102