



**FRIEDRICH NAUMANN  
STIFTUNG** Für die Freiheit.

# MEHR FREIHEIT UND SICHERHEIT IM NETZ

Gutachten zum Entwurf des Digital Services Act  
im Auftrag der Friedrich-Naumann-Stiftung Für die Freiheit

Prof. Dr. Henrike Weiden, LL.M.  
Hochschule München University of Applied Sciences

# Impressum

## Herausgeberin

Friedrich-Naumann-Stiftung für die Freiheit  
Truman-Haus  
Karl-Marx-Straße 2  
14482 Potsdam-Babelsberg

🌐/freiheit.org

📘/FriedrichNaumannStiftungFreiheit

📺/FNFreiheit

📷/stiftungfuerdiefreiheit

## Autorin

Prof. Dr. Henrike Weiden, LL.M.  
Hochschule München University of Applied Sciences

## Redaktion

Ann Cathrin Riedel, Themenmanagerin Digitalisierung & Innovation,  
Referat Globale Themen im Fachbereich Internationales

Teresa Widlok, Referentin für Bürgerrechte & Rechtsstaatlichkeit,  
Liberales Institut der Friedrich-Naumann-Stiftung für die Freiheit

## Kontakt

Telefon +49 30 220126-34  
Telefax +49 30 690881-02  
E-Mail [service@freiheit.org](mailto:service@freiheit.org)

## Mit freundlicher Unterstützung von

„Europäischer Dialog“ der  
Friedrich-Naumann-Stiftung für die Freiheit,  
Büro Brüssel

## Stand

Januar 2022

## Hinweis zur Nutzung dieser Publikation

Diese Publikation ist ein Informationsangebot der Friedrich-Naumann-Stiftung für die Freiheit. Die Publikation ist kostenlos erhältlich und nicht zum Verkauf bestimmt. Sie darf nicht von Parteien oder von Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden (Bundestags-, Landtags- und Kommunalwahlen sowie Wahlen zum Europäischen Parlament).

## Lizenz

Creative Commons (CC BY-NC-ND 4.0)

## ISBN

978-3-948950-31-6

# Inhaltsverzeichnis

<b>EXECUTIVE SUMMARY</b> .....	<b>5</b>
<b>AUF EINEN BLICK</b> .....	<b>6</b>
<b>RECHTSGUTACHTEN</b> .....	<b>7</b>
Vorbemerkung.....	7
Regelungsziele des Digital Services Act.....	7
<b>Frage 1: Inwieweit gelingt es mit den vorgeschlagenen Regelungen, einen einheitlichen europäischen Regulierungsrahmen zu setzen und so die wirtschaftliche Macht des europäischen Binnenmarkts zum Setzen von globalen Standards zu nutzen? Inwieweit bleiben daneben nationale Regelungskompetenzen etwa für das deutsche NetzDG bestehen? .....</b>	<b>8</b>
Zusammenfassende Antwort.....	8
1.1 Verordnung als Regelungsinstrument.....	9
1.2 Herkunftsland- und Marktortprinzip .....	10
1.3 Der Digital Services Act und benachbarte Regulierung .....	10
1.4 Harmonisierung durch vereinheitlichte Durchsetzung.....	16
1.5 Harmonisierung durch teilweise vereinheitlichten Sanktionsrahmen .....	17
<b>Frage 2: Sind die vorgeschlagenen Änderungen zu Verpflichtungen und Haftungsregeln für Hosting-Diensteanbieter (insb. Melde- und Abhilfeverfahren nach Artikel 14), Online-Plattformen (insb. Meldung des Verdachts von Straftaten nach Artikel 21) und sehr große Online-Plattformen (insb. Risikobewertungen nach Artikel 26) insbesondere vor dem Hintergrund folgender Erwägungen problematisch? .....</b>	<b>17</b>
<b>Frage 2a: Könnten die geplanten Haftungsregelungen ein Overblocking begünstigen und dadurch die Informations- und Meinungsfreiheit über Gebühr einschränken? Inwieweit werden die Erfahrungen mit vergleichbaren Regelungen wie dem NetzDG im DSA-Entwurf bereits berücksichtigt, wo sind Anpassungen angezeigt? .....</b>	<b>17</b>
Zusammenfassende Antwort.....	17
1. NetzDG und Besorgnis des Overblockings .....	18
2. Overblocking und der Digital Services Act.....	19
<b>Frage 2b: Kann das geplante Haftungsregime zu einer (weiteren) Privatisierung der Auslegung und Sanktionierung von Content über die Grenzen der Meinungsfreiheit hinaus beitragen? Welche rechtliche Bedeutung würde und sollte Community Standards/Nutzungsbedingungen der Anbieter zukommen?.....</b>	<b>21</b>
Zusammenfassende Antwort.....	21
1. Risikobewertung und -minderung.....	22
2. Haftung von Plattformbetreiber und Nutzerinnen und Nutzern.....	22
3. Voraussetzungen für Notice and Action.....	23
4. AGB und Gemeinschaftsstandards .....	23
5. Meldepflichten nach Art. 21 DSA-E .....	24

<b>Frage 2c: Wird mit den geplanten Haftungsregelungen ein „Überwachungsgebot“ für Plattformen konstituiert, das beispielsweise Uploadfilter für die Plattformbetreiber erforderlich macht? .....</b>	<b>25</b>
Zusammenfassende Antwort.....	25
<b>Frage 2d: Könnten sich die geplanten Vorgaben wachstumsfeindlich im Hinblick auf kleinere Anbieter, innovative Geschäftsmodelle und neue Marktteilnehmer auswirken? ....</b>	<b>26</b>
Zusammenfassende Antwort.....	26
<b>Frage 3: Gelingt es dem Entwurf, den Themenkomplex der Verbreitung von Falsch- und Desinformationen über Online-Plattformen zu adressieren und sachgerechte Lösungen aufzuzeigen? .....</b>	<b>27</b>
Zusammenfassende Antwort.....	27
1. Kommunikationsfreiheit und ihre Schranken.....	27
2. Der Digital Services Act und freiwillige Verhaltenskodizes.....	27
3. Verpflichtende Maßnahmen im Digital Services Act.....	28
4. Europäischer Aktionsplan für Demokratie .....	29
<b>ERGÄNZUNGEN DER REDAKTION.....</b>	<b>31</b>
1. Abkürzungsverzeichnis.....	31
2. Glossar .....	32
<b>ÜBER DIE AUTORIN.....</b>	<b>33</b>

# Executive Summary

Mit dem Paket aus dem Digital Services Act (DSA) und dem Digital Markets Act (DMA) wird die Europäische Union das wohl größte Projekt zur internationalen, rechtlichen Standardsetzung nach der Datenschutzgrundverordnung (DSGVO) verabschiedet. Es ist zu erwarten, dass der DSA weitreichende Auswirkungen über die EU hinaus haben wird. Das vorliegende Rechtsgutachten behandelt konkrete Fragestellungen zur Wirksamkeit des DSA, auch im Spannungsfeld zur Kommunikationsfreiheit und in Bezug auf die Verbreitung von Desinformation. Dem Gutachten liegt der im Dezember 2020 von der Europäischen Kommission veröffentlichte Entwurf zugrunde.

Die bearbeiteten **Fragestellungen beziehen sich auf die folgenden Aspekte:**

- Die **Vereinheitlichung** des Rechtsrahmens in Bezug auf die Verantwortlichkeit von Plattformanbietern durch den DSA;
- Die Risiken für die Grundrechte der Nutzerinnen und Nutzer durch neue **Verpflichtungen und Haftungsregelungen** im DSA, insbesondere das sog. Overblocking oder die (weitere) Privatisierung der Rechtsauslegung und mögliche Gegenmaßnahmen;
- Die Behandlung des Themenkomplexes der Verbreitung von **Falsch- und Desinformationen** durch den DSA.

Der DSA soll nach 20 Jahren die europäische E-Commerce-Richtlinie an die aktuellen Gegebenheiten anpassen. Sie wird dabei grundsätzlich aufrechterhalten, insbesondere das abgestufte Haftungsprivileg für unterschiedliche Diensteanbieter und das Herkunftslandprinzip bleiben bestehen. Als neue Anbieterkategorie mit besonderen Pflichten kommen die „sehr großen Online-Plattformen“ hinzu.

## Führt der DSA zu einer Vereinheitlichung des Rechtsrahmens?

Durch das Regelungsinstrument der Verordnung harmonisiert der DSA den europäischen Binnenmarkt in den Bereichen, auf die sich die Verordnung bezieht. Allerdings wird er nicht zu einer kompletten Vereinheitlichung der Regeln zur Plattformverantwortlichkeit führen. Der Flickenteppich weiterer bereichsspezifischer Regeln bleibt erhalten. Ein eigener Regelungsbereich verbleibt in Deutschland durch das UrhDaG, den MStV und teilweise das NetzDG. Löschrufen, Meldepflichten für Videosharing-Dienste in anderen EU-Mitgliedsstaaten und andere Regelungen, die über die Festlegungen des DSA hinausgehen, werden auf nationaler Ebene jedoch unzulässig sein. Das betrifft auch die deutschen Regelungen zur proaktiven Ausleitungspflicht der Diensteanbieter an das BKA, die viel kritisiert wurden.

Der DSA schreibt vor, dass die Mitgliedstaaten nationale Koordinatoren für digitale Dienste als Aufsichtsbehörden für die Einhaltung der Verpflichtungen des DSA benennen. Das verpflichtet Deutschland nicht zwingend eine neue Behörde zu errichten. Für die Übernahme dieser Aufgabe kommen beispielsweise die BNetzA, das Bundesamt für Justiz oder die Medienanstalten der Länder in Betracht. Andere Mitgliedstaaten verfügen über Verbraucherschutzbehörden mit entsprechender Zuständigkeit. Das bedeutet, dass in Fällen wie in Deutschland sehr unterschiedliche Zuständigkeiten und Kompetenzen zentral abgestimmt werden müssen. Zusätzlich erhält die Europäische Kommission eigene Eingriffsbefugnisse gegenüber sehr großen Online-Plattformen, die den Umsetzungsdruck erhöhen werden.

## Gefährden die neuen Pflichten für Diensteanbieter die Grundrechte?

Die geplanten Verpflichtungen im Rahmen der Haftungsprivilegien für Diensteanbieter stellen keine größere Gefahr des Overblockings dar als bisherige Regelungen. Inwieweit Maßnahmen wie Begründungs- und Transparenzanforderungen, *trusted flagger*, Bußgeldandrohungen und Maßnahmen gegen missbräuchliche Meldungen dem Overblocking entgegenwirken, wird im Rahmen der Evaluation des DSA zu untersuchen sein. Der Begriff „illegaler Inhalt“ wird im DSA nicht näher bestimmt, er ist jedoch weitgehender als der bisher im NetzDG verwendete Begriff rechtswidriger Inhalte im Sinne einzelner Strafnormen. Zu Hinweisen auf illegale oder gegen die Gemeinschaftsstandards verstoßende Inhalte ist jeder berechtigt. Der DSA normiert keine Anforderungen an eine subjektive Berechtigung, sieht aber Maßnahmen gegen eine extensive Hinweispraxis vor. Allerdings fehlen im Entwurf der Kommission zivilrechtliche Durchsetzungsbefugnisse für nicht gerechtfertigte Sperrungen.

Der DSA löst nicht den Grundkonflikt, dass private Anbieter die Rechtmäßigkeit von Inhalten bewerten müssen. Sehr großen Online-Plattformen wird zusätzlich eine Pflicht zur Risikobewertung und -minimierung in Bezug auf die betroffenen Kommunikationsrechte auferlegt. Inhaltliche Anforderung zur Erfüllung dieser Risikobewertungspflicht und zur Auswahl von Gegenmaßnahmen werden im Entwurf allerdings nicht aufgestellt. Die Nutzungsbedingungen des Diensteanbieters gewinnen an Bedeutung. Sie unterliegen der Grundrechtsbindung und der AGB-Kontrolle des jeweiligen Mitgliedsstaats. Filtertechniken werden von der Kommission als probates Mittel für die „Erkennung von Inhalten“ erachtet, solange diese datenschutzkonform betrieben werden. Compliance im Zusammenhang mit der neu eingeführten *Notice and Stay Down*-Verpflichtung wird ohne eine gewisse Inhalteüberwachung und -filterung nicht möglich sein.

### Welche Regelungen trifft der DSA zu Falsch- und Desinformation?

Der DSA erkennt den großen Handlungsbedarf zur Eindämmung von Falsch- und Desinformationen. Er skizziert erstmals Maßnahmen, um auf Online-Plattformen ein Umfeld zu schaffen, mit dem Falsch- und Desinformationen eingedämmt werden können: *trusted flagger*, Datenzugang für die

Forschung, Transparenz in Bezug auf Werbung und freiwillige Verhaltenskodizes. Sehr große Online-Plattformen können bei der Erkennung systemischer Risiken zur Mitarbeit an der Ausarbeitung eines Verhaltenskodex aufgefordert werden. Ergänzt wird der DSA durch den „Verhaltenskodex zur Bekämpfung von Desinformation“ der Kommission und dem „Europäischen Aktionsplan für Demokratie“ der Kommission.

# Auf einen Blick

### Die Harmonisierungswirkung des DSA wird gestärkt durch...

- das Regelungsinstrument **Verordnung**. Denn das bedeutet, dass keine nationale Regelungskompetenz im koordinierten Bereich besteht.
- die Regulierung auch von Diensten mit **Sitz außerhalb der EU**.
- die weiterhin einheitliche Anwendung der **Haftungsprivilegierung**.
- die vereinheitlichte **Durchsetzung** des DSA in Form von Kontaktstellen/Inlandsvertretern, die Zusammenarbeit nationaler Koordinatoren für digitale Dienste, das europäische Gremium für digitale Dienste, die regulierten Befugnisse der EU-Kommission und durch einen (teilweise) harmonisierten **Sanktionsrahmen**.

### Die Harmonisierungswirkung des DSA wird geschwächt durch...

- den **Anwendungsvorrang** europäischer Verordnungen und Richtlinien. Denn der erfasst auch nationales Recht, durch das europäische Richtlinien umgesetzt sind. Das gilt insbesondere für die jeweils nationale Umsetzung des Art. 17 DSM (Uploadfilter zur Wahrung des Urheberrechts im **UrhDaG**). Auch die Anwendung der **DSGVO** durch die Mitgliedstaaten wird zu Unterschieden im durch den DSA koordinierten Bereich führen. In Bezug auf die Umsetzung der **AVMD-RL** führt der Anwendungsvorrang dazu, dass Videosharing-Plattformen anderen (national umgesetzten) Regeln zu folgen haben als soziale Medien, die den DSA anzuwenden haben.
- die Aufrechterhaltung des **Herkunftslandprinzips** für die Anwendung der Haftungsprivilegierung. Dadurch gelten für die Feststellung eines illegalen Inhalts neben der EU-Gesetzgebung die jeweils nationalen Regelungen der Mitgliedstaaten.
- den unbestimmten Rechtsbegriff **„illegaler Inhalt“**. Denn der ist im DSA lediglich durch Verweis auf Unionsrecht und auf nationale Vorschriften beschrieben. Die Ausfüllung des unbestimmten Rechtsbegriffs wird in jedem Mitgliedstaat anders vorgenommen werden.
- das Fehlen **zivilrechtlicher Durchsetzungsbefugnisse**, etwa in Gestalt von Schadenersatzansprüchen bei nicht gerechtfertigter Sperrung eines Inhalts.

### Zur Zulässigkeit nationaler Regelungen, sobald der DSA in der Fassung des Kommissionsentwurfs anzuwenden ist:

- Die Mitgliedstaaten dürfen im **nicht-koordinierten Bereich** Recht setzen, also zum Beispiel Vorschriften betreffend nicht-kommerzielle Dienste erlassen.
- Grundsätzlich verbleibt ein eigener Regelungsbereich für die Mitgliedstaaten, wie er in Deutschland durch UrhDaG, MStV und NetzDG ausgefüllt ist. Doch es bestehen Einschränkungen.
- Eine „Konkretisierung“ des durch den DSA koordinierten Bereichs etwa durch **Löschfristen im NetzDG** wird unzulässig sein. Auf Art. 14 Abs. 3 ECRL/Art. 5 Abs. 4 DSA-E können sich nationale Gesetzgeber nicht berufen.
- Videosharing-Dienste mit Sitz in einem anderen Mitgliedstaat der EU kann der deutsche Gesetzgeber künftig nicht im **NetzDG** regulieren. Melde- und Übermittlungspflichten von Videosharing-Diensten wie bisher im NetzDG können nicht auf Art. 15 ECRL gestützt werden und sind unter dem DSA unzulässig.
- Soweit der **Medienstaatsvertrag** Dienste regelt, die eine Verbreitung nutzergenerierter Inhalte als Nebenfunktion anbieten, werden diese Dienste künftig (nur) die Vorschriften des DSA über Hosting-Dienste anzuwenden haben, also insbesondere Transparenzanforderungen.

# Rechtsgutachten

## Vorbemerkung

Dieses Gutachten behandelt konkrete Fragestellungen in Bezug auf die Vereinbarkeit mit und Wirksamkeit des Digitale Dienste Gesetzes (Digital Services Act, DSA) im Sinne einer liberalen Netzpolitik. Die Fragen wurden von der Friedrich-Naumann-Stiftung für die Freiheit vorgegeben, die Antworten auf Grund einer wissenschaftlichen Untersuchung und persönlichen Bewertung von der Verfasserin entwickelt.

Beim Entwurf des Digital Services Act (DSA-E) in der im Dezember 2020 von der EU-Kommission, Generaldirektion Kommunikationsnetze, Inhalte und Technologien (GD Connect), vorgelegten Fassung<sup>1</sup> handelt es sich um den ersten Entwurf einer Verordnung des Digitale Dienste Gesetzes. Dieser Entwurf liegt der Begutachtung zugrunde.

## Regelungsziele des Digital Services Act

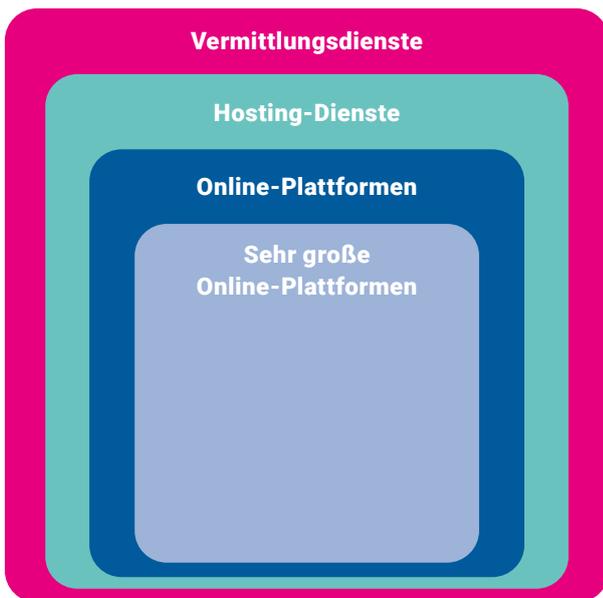
Die EU-Kommission hat eine Reihe von Missständen in Bezug auf das Geschäftsgebaren der Betreiber digitaler Dienste, die wirksame Ausübung von Grundrechten durch ihre Nutzerinnen und Nutzer und die rechtlichen Rahmenbedingungen für digitale Geschäftsmodelle im Binnenmarkt aufgegriffen. Einheitliche, horizontal anwendbare rechtliche Grundlage für digitale Dienste, die in der Union angeboten werden, ist vor allem die E-Commerce Richtlinie (ECRL) von vor über 20 Jahren.<sup>2</sup> Diese Richtlinie gilt es derzeit zu überprüfen und an die aktuellen und zu erwartenden Gegebenheiten anzupassen, die sich seit In-Kraft-Treten der ECRL mannigfaltig weiterentwickelt

haben. Dabei wird die ECRL grundsätzlich aufrechterhalten. Die zentralen Vorschriften über die Befreiung der Diensteanbieter von der Verantwortlichkeit für die Inhalte Dritter werden herausgelöst und in den DSA-E übernommen.

Ebenso haben sich die Reichweite von Plattformen und das Nutzerverhalten innerhalb der letzten zwei Dekaden spürbar verändert. Plattformen werden nicht von allen Usern in der vorgesehenen Form genutzt, sondern auch für Straftaten, für gezielte Desinformationskampagnen oder jedenfalls in ungebührlicher Weise eingesetzt. Zugleich ergeben sich auch Schwierigkeiten gerade europäischer Anbieter, neben den übermächtigen Tech-Konzernen aus den USA und aus China zu bestehen, mit denen sie im globalisierten Wirtschaftsgefüge im unmittelbaren Wettbewerb stehen.

**Der Digital Services Act soll für die Digitalwirtschaft einen zeitgemäßen Rahmen schaffen. Ausweislich ihres Folgenabschätzungsberichts<sup>3</sup> hat sich die Kommission dabei Folgendes zum Ziel gesetzt:**

- die Aufrechterhaltung eines sicheren Online-Umfelds,
- die Verbesserung der Bedingungen für innovative grenzüberschreitende digitale Dienste,
- die Stärkung der Position der Nutzerinnen und Nutzer und der Schutz ihrer Grundrechte im Internet sowie
- die Einführung einer wirksamen Beaufsichtigung digitaler Dienste und die Zusammenarbeit zwischen den Behörden.



- **Vermittlungsdienste**, die über ein Infrastruktur-Netz verfügen: Internetanbieter, Domänennamen-Registrierstellen, darunter:
- **Hosting-Dienste** wie Cloud- und Webhosting-Dienste, darunter:
- **Online-Plattformen**, die Verkäufer und Verbraucher zusammenbringen, wie Online-Marktplätze, App-Stores, Plattformen der kollaborativen Wirtschaft und Social-Media-Plattformen.
- **Sehr große Online-Plattformen** bergen besondere Risiken für die Verbreitung illegaler Inhalte und für Schäden in der Gesellschaft. Für Plattformen, die mehr als 10 % der 450 Millionen Verbraucher/innen in Europa erreichen, sind besondere Vorschriften vorgesehen.

Quelle: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment\\_de#worauf-zielt-das-gesetz-ber-digitale-dienste-zentral-ab](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de#worauf-zielt-das-gesetz-ber-digitale-dienste-zentral-ab)

<sup>1</sup> Abrufbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>, alle Links zuletzt aufgerufen am 13.12.2021.

<sup>2</sup> Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“).

<sup>3</sup> COM(2020) 825 final, Arbeitsunterlage der Kommissionsdienststellen, Bericht über die Folgenabschätzung (Zusammenfassung), Begleitunterlage zum Gesetz über digitale Dienste, S.1, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020SC0349&from=EN>.

Die Kommission hat hierfür einen Regulierungsrahmen entworfen, der, abgestuft je nach Größe und Reichweite eines Dienstes, bestimmte Verhaltensregeln vorsieht:

Die Basis bilden die Vorschriften des Kapitel I (Allgemeine Vorschriften), Kapitel II (Haftung der Anbieter von Vermittlungsdiensten) und Kapitel III (Sorgfaltspflichten für ein transparentes und sicheres Online-Umfeld). Sie sind auf sämtliche Vermittlungsdienste anwendbar, d.h. auf Access-, Cache- und Hosting-Diensteanbieter gem. Art. 2 lit. f DSA-E.

Auf der zweiten Stufe stehen ergänzende Vorschriften, die von Hosting-Diensteanbietern zu beachten sind (Kapitel III Abschnitt 2). Hierzu gehören nach dem DSA-E auch Online-Plattformen. Das sind beispielsweise Online-Marktplätze, soziale Netzwerke, Cloud- und Webhosting-Services.

Hierauf baut die dritte Anwendungsstufe auf, die (nur) von den Betreibern von Online-Plattformen anzuwenden sind. Nur wenn es sich dabei um „sehr kleine Anbieter“ handelt, sind diese vom Anwendungsbereich ausgenommen. Wer Kleinst- oder Kleinunternehmen im Sinne des DSA ist, richtet sich nach der Definition der Empfehlung 2003/361/EG. Darunter fasst die EU-Kommission Unternehmen mit weniger als 50 Mitarbeiterinnen und Mitarbeitern und höchstens 10 Mio. Euro Jahresumsatz.

Auf der vierten Regelungsstufe stehen die so genannten sehr großen Online-Plattformen mit den strengsten Anforderungen. Als sehr große Online-Plattform gilt ein Dienst, der mindestens 45 Mio. „aktive Nutzer“ verzeichnet. Dieser Wert entspricht zurzeit etwa 10 % der Bevölkerung in der Union. Diesen Schwellenwert dürften die alleseits bekannten Dienste wie Twitter, Facebook, Amazon, AirBnB, Booking.com, TikTok usw. erfüllen. Sie nimmt die Kommission deshalb besonders in die Pflicht, weil sie auf Grund ihrer Reichweite eine „systemische Rolle“ in der öffentlichen Meinungsbildung oder in der Digitalwirtschaft übernehmen.

Herzstück des DSA bleibt, wie schon in der Regulierung durch die ECRL, die **Haftungsprivilegierung für Vermittlungsdienste**, die in die neue Verordnung übernommen werden soll. Dieses Haftungsregime regelt, vereinfacht gesagt, dass Access-, Cache- und Hosting-Diensteanbieter für die Inhalte ihrer Nutzer nicht verantwortlich sind, sofern die Dienste bestimmte technische Voraussetzungen erfüllen. Für Hosting-Diensteanbieter gilt das jedenfalls, solange sie keine Kenntnis von der Rechtswidrigkeit des Inhalts haben bzw. ab Kenntnis den rechtswidrigen Inhalt entfernen oder den Zugang dazu sperren.

Im Folgenden wird untersucht, inwieweit die von der Kommission in ihrem ersten Entwurf vorgeschlagenen Vorschriften geeignet sind, die angestrebten Regelungsziele zu erreichen und zugleich einen harmonisierten liberalen, innovationsfreundlichen Rahmen für Angebot und Nutzung von Vermittlungsdiensten zu gewährleisten.

**Frage 1: Inwieweit gelingt es mit den vorgeschlagenen Regelungen, einen einheitlichen europäischen Regulierungsrahmen zu setzen und so die wirtschaftliche Macht des europäischen Binnenmarkts zum Setzen von globalen Standards zu nutzen? Inwieweit bleiben daneben nationale Regelungskompetenzen etwa für das deutsche NetzDG bestehen?**

### Zusammenfassende Antwort

Die Mitgliedstaaten haben im Anwendungsbereich des Digital Services Act (DSA) keine eigene Regelungskompetenz. Wie weit dieser reicht, ist anhand des Art. 1 Abs. 5 DSA-E festzustellen, der bestimmten europarechtlichen Vorschriften einen Anwendungsvorrang einräumt. Wo kein EU-Recht dem DSA vorgeht, wird die Verordnung den höchsten Harmonisierungsgrad erzielen.

Da die E-Commerce-Richtlinie nach Erlass des DSA grundsätzlich fortgilt, bleibt nur noch sehr eingeschränkter Raum für das deutsche Netzwerkdurchsetzungsgesetz. Jedoch wird der DSA nicht zur Klärung beitragen, wie weit nationale Gesetzgebung bei einer „Konkretisierung“ der dem DSA vorgehenden EU-Vorschriften gehen kann. Auch tragen bisher bei der Umsetzung der Richtlinie über audiovisuelle Mediendienste im Netzwerkdurchsetzungsgesetz herangezogene Ermächtigungen unter dem DSA nicht oder nicht mehr. Die vorgesehenen Durchsetzungsvorschriften taugen mit Ausnahme des Sanktionsrahmens für eine EU-weite Harmonisierung.

In ihrem Folgenabschätzungsbericht führt die Kommission aus: *„Die Bereitstellung und Nutzung von Inhalten und Diensten über das Internet erfolgt in der Regel länderübergreifend. Parallele, voneinander abweichende Regelungen der einzelnen Mitgliedstaaten behindern die Erbringung von Vermittlungsdiensten in der Union und sind wirkungslos, wenn es darum geht, die Sicherheit und den Schutz aller europäischen Bürger zu gewährleisten.“* Deshalb seien durch harmonisierte Regelungen auf Unionsebene die Fragmentierung der gesetzlichen Regelungen zu überwinden und dadurch die Kosten der Rechtsbefolgung zu verringern und die Rechtssicherheit zu erhöhen.<sup>4</sup> Zugleich sei für einen gleichberechtigten Schutz der Bürgerinnen und Bürger und gleiche Wettbewerbsbedingungen für Unternehmen zu sorgen. Die Integrität des Binnenmarkts sei dafür zu stärken und eine wirksame grenzüberschreitende Beaufsichtigung zu ermöglichen.<sup>5</sup> Eine für den Binnenmarkt vereinheitlichte Regulierung der digitalen Angebote für die Nutzer in der EU ist aus Sicht der Kommission demnach aus ganz unterschiedlichen Gründen erstrebenswert. Sie liegt im Interesse aller Akteure - Gesellschaft, individuelle Nutzer, Diensteanbieter und deren Wettbewerber.

<sup>4</sup> Combined Evaluation Roadmap/Inception Impact Assessment: Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services, Ref. Ares(2020)2877686 - 04/06/2020, S. 3, abrufbar unter [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Legislativpaket-uber-digitale-Dienste-Vertiefung-des-Binnenmarkts-und-Klarung-der-Zustandigkeiten-fur-digitale-Dienste\\_de](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Legislativpaket-uber-digitale-Dienste-Vertiefung-des-Binnenmarkts-und-Klarung-der-Zustandigkeiten-fur-digitale-Dienste_de).

<sup>5</sup> COM(2020) 825 final, Arbeitsunterlage der Kommissionsdienststellen, Bericht über die Folgenabschätzung (Zusammenfassung), Begleitunterlage zum Gesetz über digitale Dienste, S. 1.

## 1.1 Verordnung als Regelungsinstrument

Den rechtlichen Rahmen für digitale Dienste bildet bisher vor allem die europäische Regulierung durch die ECRL. Deren Umsetzung in nationales Recht und die jeweils dazu entwickelte Rechtsprechung weisen zwischen den Mitgliedstaaten nach Untersuchungen des Europäischen Parlaments teils sehr unterschiedliche Züge auf, die den Betreibern wie auch den Nutzern rechtskonformes Verhalten im Zusammenhang mit digitalen Angeboten im Binnenmarkt maßgeblich erschweren, wenn sie die Dienste grenzüberschreitend anbieten oder nutzen.<sup>6</sup>

Im Zusammenhang mit dem DSA-Vorhaben hatte die Kommission schon früh einen „Act“ oder ein „Gesetz“ angekündigt. Warum sie diese Bezeichnung gewählt hat, ist unklar. Denn europäische „Gesetze“ sind nach dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) nicht vorgesehen. In Art. 288 AEUV sind als typische Akte des Sekundärrechts Verordnungen, Richtlinien und Beschlüsse aufgeführt. Atypische, nicht in Art. 288 AEUV genannte Rechtsakte umfassen v.a. Mitteilungen, Entschlüsse, Weißbücher oder Grünbücher.

Letztlich kann die Frage aber dahinstehen, weil der Begriff „Act“ (oder in der nachträglich veröffentlichten deutschen Sprachfassung des Entwurfs „Gesetz“) nur in der unverbindlichen Kurzbezeichnung des Rechtsakts genannt ist. Im Übrigen ergibt sich aber aus dem Titel des Regelungsvorschlags und aus den weiteren Ausführungen des Entwurfs, dass es sich um eine Verordnung im herkömmlichen Sinn handeln soll.

Die Regulierung in Gestalt einer europäischen Verordnung verspricht qua Regelungsinstrument einen höheren Harmonisierungsgrad als die bisherige ECRL. Denn anders als die (bisherige) Richtlinie ist die (künftige) Verordnung in den Mitgliedstaaten unmittelbar anwendbares Recht, ohne dass es dafür einer Umsetzung durch die jeweiligen nationalen Gesetzgeber bedarf. Die Mitgliedstaaten werden in allen vom DSA erfassten Bereichen grundsätzlich **keine Regelungskompetenz** haben; sie dürfen keine nationalen Vorschriften für Sachverhalte erlassen, die durch die Verordnung geregelt sind.<sup>7</sup>

Aufschlussreich, wenngleich fragwürdig hinsichtlich der beabsichtigten Wirkung, ist insoweit aber der Blick auf den Entwurf des mit dem DSA in engem Zusammenhang stehenden und zeitgleich veröffentlichten Digital Markets Act (DMA<sup>8</sup>). Während in dessen Art. 1 Abs. 5 S. 1 ausdrücklich spezifiziert ist, dass die Mitgliedstaaten den im DMA regulierten „Torwächtern“ keine weiteren Verpflichtungen durch Rechts- und Verwaltungsvorschriften auferlegen, also keine weitergehenden nationalen Regelungen erlassen dürfen, um bestreitbare und faire Märkte zu gewährleisten, fehlt eine Entsprechung dazu im DSA-E.

<sup>6</sup> Wissenschaftlicher Dienst des Europäischen Parlaments (Tambiana Mediega), PE 649.404 – Mai 2020, Reform der EU-Haftungsregelung für Online-Vermittler, S. 5, abrufbar unter [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS\\_IDA\(2020\)649404\\_DE.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_DE.pdf).

<sup>7</sup> Diese Sperrwirkung der europäischen Verordnung gegenüber nationalem Recht ist nicht in den Verträgen festgelegt, wurde aber vom EuGH anerkannt, Rechtssache 6/64, Costa/E.N.E.L., Urt. v. 15.7.1964.

<sup>8</sup> COM(2020) 842 final, Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte).

Obwohl DMA und DSA – anders als die ECRL – auf eine ausdrückliche Normierung des jeweiligen Regelungsziels verzichten, könnte man auf den Gedanken kommen, dass neben dem DSA (analog zum DMA) nationale Vorschriften zulässig sein sollen, sofern sie nur anderen als den geregelten **legitimen öffentlichen Interessen** im Einklang mit dem Unionsrecht<sup>9</sup> dienen. Denkbar wären hier etwa Regelungen zur Wahrung der Medienvielfalt wie durch den Medienstaatsvertrag (MStV<sup>10</sup>).<sup>11</sup> Angesichts des betont parallelen Verfahrens bei der Vorhaben ist jedoch davon auszugehen, dass eine solche Klausel **bewusst nicht** in den Entwurf des DSA aufgenommen worden ist. Die Kommission beabsichtigt eine möglichst flächige Harmonisierung mit geringem Spielraum für flankierende mitgliedstaatliche Regelungen.

Etwas anderes gilt freilich für den durch den DSA **nicht koordinierten Bereich**. So sind vor allem nicht-kommerzielle digitale Dienste vom DSA in seiner bisher geplanten Gestalt nicht erfasst. Denn hierbei handelt es sich nicht um eine „in der Regel gegen Entgelt elektronisch im Fernabsatz und im individuellen Auftrag eines Nutzers erbrachte Dienstleistung“.<sup>12</sup> „In der Regel gegen Entgelt erbracht“ sind nicht nur unmittelbar von Nutzerinnen und Nutzern bezahlte, sondern auch werbefinanzierte Dienste. Rein spendenfinanzierte Dienste wie Wikipedia sollen wohl nicht von den Regelungen des DSA erfasst sein<sup>13</sup>, obwohl dem Dienst ein umfängliches Moderationssystem für die von Dritten hochgeladenen Inhalte zugrunde liegt. Das systemische Risiko dürfte hier also jedenfalls theoretisch kaum geringer sein als bei vom DSA regulierten Diensteanbietern.

Es steht den Mitgliedstaaten also frei, insoweit eigene Haftungsprivilegierungen, Sorgfaltspflichten oder Durchsetzungsmechanismen vorzusehen. Denn es sind keine Anhaltspunkte dafür ersichtlich, dass der EU-Verordnungsgeber mit der geplanten Verordnung eine abschließende Harmonisierung anstrebt, die solchen gesonderten Regelungen außerhalb des Anwendungsbereichs des DSA entgegensteht.<sup>14</sup>

Die Kommission hat für die Verordnung wie bei der ECRL einen horizontalen Ansatz gewählt. Der DSA soll demnach grundsätzlich für alle Vermittlungsdienste gelten, und zwar ergänzend zur ECRL. Sie wird durch sektorspezifische Vorschriften verdrängt, soweit diese anwendbar sind.<sup>15</sup> Das sind auf europäischer Ebene insbesondere die Urheberrechtsrichtlinie (DSM-RL<sup>16</sup>), die Richtlinie über audiovisuelle Medien-

<sup>9</sup> Vgl. Art. 1 Abs. 5 S. 2 DMA-E.

<sup>10</sup> vom 14./18.4.2020, in Kraft seit 7.11.2020.

<sup>11</sup> Jörg Ukrow, Die Vorschläge der EU-Kommission für einen Digital Services Act und einen Digital Markets Act, abrufbar unter [https://emr-sb.de/wp-content/uploads/2021/01/Impulse-aus-dem-EMR\\_DMA-und-DSA.pdf](https://emr-sb.de/wp-content/uploads/2021/01/Impulse-aus-dem-EMR_DMA-und-DSA.pdf), S. 50.

<sup>12</sup> ErwGrd. 5 DSA-E.

<sup>13</sup> Anders offenbar Prabhat Agrawal, Referatsleiter GD CNECT der EU-Kommission, Interview vom 14.9.2021, abrufbar unter [https://www.stiftung-nv.de/en/publication/transcript-background-talk-new-eu-rules-big-tech-how-improve-digital-services-act#collapse-newsletter\\_banner\\_bottom](https://www.stiftung-nv.de/en/publication/transcript-background-talk-new-eu-rules-big-tech-how-improve-digital-services-act#collapse-newsletter_banner_bottom); wie Agrawal auch Reda/Selinger, Digital Services Act: Europaparlament diskutiert Netzsperrungen gegen Plattformen, abrufbar unter <https://verfassungsblog.de/dsa-netzsperrungen/>.

<sup>14</sup> Gerald Spindler, Der Vorschlag für ein neues Haftungsregime für Internetprovider - der EU-Digital Services Act (Teil 1), GRUR 2021, 545 (547), der dem Unionsgesetzgeber insoweit auch eine Regelungskompetenz abspricht.

<sup>15</sup> Art. 1 Abs. 5 DSA-E.

<sup>16</sup> Digital Single Market, Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17.4.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG.

dienste (AVMD-RL<sup>17</sup>), die *Platform to Business*-Verordnung (P2B-VO<sup>18</sup>), die Richtlinie zur Terrorismusbekämpfung<sup>19</sup> und die Datenschutz-Grundverordnung (DSGVO<sup>20</sup>). Die Sperrwirkung der Verordnung entfaltet also dort keine Wirkung, wo die genannten europäischen Verordnungen anzuwenden und Richtlinien in nationales Recht umgesetzt sind.

Aus den zuvor in der Roadmap diskutierten Regulierungsoptionen<sup>21</sup> hat sich die Kommission letztlich für diejenige entschieden, die digitale Geschäftsmodelle von besonderer Reichweite mit strengeren Pflichten belegt als kleinere digitale Angebote. Dieser asymmetrische Ansatz sei allgemein von den Stakeholdern gegenüber der Option der Vollharmonisierung bevorzugt worden.<sup>22</sup> Das bedeutet auch, dass der koordinierte Bereich, in dem die Verordnung ihre Sperrwirkung entfaltet, jeweils für die einzelnen Typen von Normadressaten gesondert festzustellen ist.

### 1.2 Herkunftsland- und Marktortprinzip

Art. 3 Abs. 2 ECRL regelt für die Sicherstellung des freien, das heißt grenzüberschreitenden Verkehrs digitaler Dienste im Binnenmarkt das **Herkunftslandprinzip**: *Innerhalb des koordinierten Bereichs dürfen die Mitgliedstaaten den freien Verkehr von Diensten aus einem anderen Mitgliedstaat nicht einschränken*. Das bedeutet, dass der Dienst eines Anbieters mit Sitz im EU-Ausland keinen von der Richtlinie abweichenden nationalen Vorschriften eines anderen EU-Mitgliedstaats unterworfen werden darf. Das Herkunftslandprinzip setzt also dem nationalen Gesetzgeber Grenzen in Bezug auf ausländische Anbieter, sofern diese einen Sitz in der EU, aber nicht im Inland haben. Stattdessen sind die Diensteanbieter grundsätzlich dem Rechtssystem desjenigen Mitgliedstaates unterworfen, in dem sie niedergelassen sind<sup>23</sup>.

Nach dem DSA als unmittelbar in allen Mitgliedstaaten einheitlich geltender Verordnung jedoch soll grundsätzlich das **Marktortprinzip** gelten. Ähnlich wie bei der DSGVO<sup>24</sup> bedeutet dies, dass sich die Betreiber von Vermittlungsdiensten an die Vorgaben der Union nach dem DSA zu halten haben, wenn sie in den territorialen Anwendungsbereich der Verordnung fallen. Dieser ist in Art. 1 Abs. 3 DSA-E festgelegt: *Die Verordnung gilt für Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Wohnsitz in der Union erbracht werden, ungeachtet des Orts der Niederlassung des Anbieters dieser Dienste*.

Ob ein Dienst für Nutzerinnen und Nutzer in der Union erbracht wird, soll daran festgemacht werden, ob eine „wesentliche Verbindung zur Union“ vorliegt<sup>25</sup>. Diese ist nach Erwägungsgrund 8 DSA-E ohne eine Niederlassung in der EU

anzunehmen, wenn der Dienst von einer erheblichen Zahl von Usern in der Union genutzt wird oder Sprache, Währung, Bestellmöglichkeiten, geografische Top Level Domain etc. eine solche Verbindung nahelegen.

Gleichzeitig hält die Kommission am **Herkunftslandprinzip für die Haftungsprivilegierung** der Vermittlungsdienste, wie wir sie aus der ECRL kennen, weiter fest. Die Feststellung eines illegalen Inhalts bestimmt sich im Rahmen des Haftungsprivilegs von Access-, Cache- und Hosting-Diensteanbietern nach EU-Recht und auch nach dem nationalen Recht desjenigen Mitgliedstaates, in dem der jeweilige Dienst seinen Sitz hat.

Das **Herkunftslandprinzip** der ECRL ist außerdem in Art. 40 DSA-E aufrechterhalten, also etwa in Bezug auf die Sorgfaltspflichten für ein transparentes und sicheres Online-Umfeld und in Bezug auf die nationalen Koordinatoren für Digitale Dienste (vgl. Abschnitt 1.4.2 Grenzüberschreitende Kompetenzen nationaler Behörden).

### 1.3 Der Digital Services Act und benachbarte Regulierung

Der Digital Services Act soll als Verordnung mit horizontalem, also bereichsübergreifendem Anwendungsbereich ergehen. Deren Vorschriften treten als *lex generalis*-Regelungen hinter sektorspezifischen *lex specialis*-Normen zurück<sup>26</sup>, die in Art. 1 Abs. 5 DSA-E aufgeführt sind. Das entspricht grundsätzlich demselben Regelungsprinzip, nach dem das Verhältnis zwischen der ECRL und angrenzenden bereichsspezifischen Regelungen gestaltet ist<sup>27</sup>.

#### 1.3.1 Der Digital Services Act und das Urheberrecht

Im Folgenden soll am Beispiel der Verletzung einer urheberrechtlichen Vorschrift gezeigt werden, wo die Schwachstellen der Harmonisierungsbemühungen durch den Digital Services Act sind, die sich aus Art. 1 Abs. 5 DSA-E ergeben.

Zunächst kann sich die Rechtswidrigkeit von Inhalten aus der Verletzung einer nationalen urheberrechtlichen Vorschrift ergeben, die **nicht auf einer Unionsvorschrift** fußt. Für diesen Fall regelt der DSA-E keinen Anwendungsvorrang des Urheberrechts, das Haftungsregime des DSA ist dann also einschlägig. In der praktischen Umsetzung bedeutet dies: Wenn ein Nutzer beispielsweise auf einem Online-Marktplatz durch Hochladen eines Inhalts eine Urheberrechtsverletzung begeht, ist eine Verantwortlichkeit des Marktplatz-Anbieters dafür nicht von der Urheberrechts-Richtlinie (Directive on Copyright in the Digital Single Market, DSM-RL<sup>28</sup>) und nicht vom Urheberrechts-Diensteanbieter-Gesetz erfasst (§ 3 Ziff. 5 UrhDaG). Sondern die Betreiber-Haftung bestimmt sich nach den Vorschriften des DSA. **Insoweit** erreicht der Digital Services Act das Ziel der **Harmonisierung**.

Am Beispiel der in Art. 1 Abs. 5 DSA-E genannten Unionsvorschriften auf dem Gebiet des Urheberrechts lässt sich jedoch

<sup>17</sup> (EU) 2018/1808.

<sup>18</sup> (EU) 2019/1150.

<sup>19</sup> (EU) 2017, 541.

<sup>20</sup> (EU) 2016/679.

<sup>21</sup> Combined Evaluation Roadmap/Inception Impact Assessment: Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services, Ref. Ares(2020)2877686 - 04/06/2020, S. 4 ff.

<sup>22</sup> COM(2020) 825 final, Arbeitsunterlage der Kommissionsdienststellen, Bericht über die Folgenabschätzung (Zusammenfassung), Begleitunterlage zum Gesetz über digitale Dienste, S. 2.

<sup>23</sup> ErwGrd. 22 ECRL, Art. 3 Abs. 1 ECRL.

<sup>24</sup> Art. 3 Abs. 2 der Verordnung (EU) 2016/679, Datenschutz-Grundverordnung.

<sup>25</sup> ErwGrd. 7 DSA-E.

<sup>26</sup> ErwG 9 f DSA-E.

<sup>27</sup> Art. 1 Abs. 5 ECRL.

<sup>28</sup> Richtlinie (EU) 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG.

erkennen, dass die Harmonisierung durch den DSA besonders dort geschwächt wird, wo er durch Spezialregelungen verdrängt wird, die ihrerseits nur als Richtlinie erlassen worden sind. Die DSM-RL hätte bis zum 7. Juni 2021 von allen Mitgliedstaaten in nationales Recht umgesetzt werden müssen. Das ist nicht überall passiert. Die meisten Mitgliedstaaten haben die DSM-RL überhaupt nicht fristgerecht umgesetzt.<sup>29</sup> Doch auch dort, wo die Umsetzung fristgerecht erfolgt ist, haben die Mitgliedstaaten unterschiedliche Lösungen für die Implementierung etwa des umstrittenen Art. 17 DSM-RL, den Uploadfiltern, gefunden.

So hat zum Beispiel der deutsche Gesetzgeber mit der „mutmaßlich erlaubten Nutzung“ (§ 9 Abs. 2 UrhDaG) eine sehr eigene Systematik der gesetzlichen Vermutung mit Benachrichtigung und Beschwerdemöglichkeit entwickelt. Dazu gehört auch der vertrauenswürdige Hinweisgeber, der in § 14 Abs. 4 UrhDaG über das interne Beschwerdeverfahren mit besonderen Befugnissen ausgestattet wird. Erklärt dieser *trusted flagger*, dass die Vermutung der erlaubten Nutzung zu widerlegen ist und die fortdauernde öffentliche Wiedergabe eines geschützten Werkes dessen wirtschaftliche Verwertung erheblich beeinträchtigt, dann ist der Diensteanbieter zum sofortigen Blockieren der Wiedergabe bis zum Abschluss des Beschwerdeverfahrens verpflichtet („Roter Knopf“).

Die Regelung des § 14 Abs. 4 UrhDaG fußt auf Unionsrecht und verdrängt deshalb das Haftungsregime des DSA. Doch ist nach bisherigem Stand nicht davon auszugehen, dass sich diese Form der Umsetzung der DSM-RL als einheitlicher Standard in allen Mitgliedstaaten durchsetzen wird. Das bedeutet für den Diensteanbieter, der vom UrhDaG erfasst ist, dass er nicht von der Haftungsprivilegierung des DSA profitiert. Wegen des Anwendungsvorrangs nach Art. 1 Abs. 5 DSA-E richtet sich seine Haftung stattdessen allein nach den Vorschriften des UrhDaG, ohne dass in anderen Mitgliedstaaten unbedingt eine Entsprechung dazu gilt. Anhaltspunkte dafür, dass die Vorschriften über vertrauenswürdige Hinweisgeber nicht mit der DSM-RL vereinbar wären, sind nicht ersichtlich.

Inwieweit das UrhDaG in diesem Punkt mit höherrangigem europäischem Recht, dem DSA, vereinbar ist und ob das UrhDaG insoweit wirksam den DSA verdrängt, wird zu überprüfen sein, falls der DSA in der geplanten Fassung in Kraft tritt.<sup>30</sup> Zwar ist der *trusted flagger* auch im DSA-E vorgesehen, aber die konkrete Ausgestaltung entspricht nicht der des UrhDaG. So wird etwa nach Art. 19 DSA-E der Status eines vertrauenswürdigen Hinweisgebers auf Antrag einer Stelle vom Koordinator für digitale Dienste des Mitgliedstaats, in dem der Antragsteller niedergelassen ist, zuerkannt, nachdem der Antragsteller nachgewiesen hat, dass er alle Bedingungen dafür erfüllt. Dagegen entscheidet nach dem UrhDaG der Diensteanbieter freihändig, ob er einen bestimmten Hinweisgeber als *trusted flagger* anerkennt oder nicht. Auch der Entzug des Status' als vertrauenswürdiger Hinweisgeber ist in Art. 19 Abs. 6 DSA-E geregelt, im UrhDaG dagegen nicht.

In der praktischen Umsetzung werden solche Abweichungen für die Rechtsanwender im Binnenmarkt einen Unterschied machen. Denn das deutsche UrhDaG einerseits und der DSA andererseits knüpfen jeweils haftungsrelevante Folgen an das Einschreiten eines vertrauenswürdigen Hinweisgebers.

Sollte sich erweisen, dass die Vorschriften über den vertrauenswürdigen Hinweisgeber im UrhDaG mit den Regelungen des DSA vereinbar und deshalb wirksam sind, wäre die **Harmonisierungswirkung** des DSA im Binnenmarkt jedenfalls **geschwächt**.

### 1.3.2 Der Digital Services Act und die Datenschutz-Grundverordnung

**Das Beispiel der Datenschutz-Grundverordnung (DSGVO) zeigt, dass die Harmonisierung dieser sektorspezifischen Regulierung besonders davon abhängt, wie die Vorschriften über den Anwendungsbereich der Verordnung ausgelegt werden, soweit es noch nicht**

- durch die Rechtsprechung des EuGH oder
- auf Grund des Kohärenzverfahrens (Art. 63 ff DSGVO) oder
- mittels Einschreitens des Europäischen Datenschutzausschusses im Rahmen seiner Aufgaben

zu einer gleichartigen Anwendungspraxis gekommen ist.

Wenn die Aufsichtsbehörden mehrerer Mitgliedstaaten beispielsweise den Begriff des Personenbezugs verschieden weit auslegen, dann wird im einen Fall die DSGVO angewendet, im anderen vielleicht nicht. Das bedeutet, dass im ersten Fall die Vorschriften des DSA hinter den Vorschriften der DSGVO zurücktreten, im zweiten aber nicht. Ein gehöriger Unterschied. Denn nur im zweiten Fall, wenn die DSGVO auf Grund einer engeren Auslegung des Begriffs des Personenbezugs nicht angewendet wird, kommt eine Haftungsprivilegierung nach dem Digital Services Act in Betracht. Eine **durchgreifende Harmonisierung** im Binnenmarkt findet insoweit durch den DSA nicht **statt**.

### 1.3.3 Der Digital Services Act und das Netzwerkdurchsetzungsgesetz

Anders als in den in Art. 1 Abs. 5 DSA-E genannten Fällen sieht die geplante Verordnung für **nationale Gesetze**, wie das deutsche Netzwerkdurchsetzungsgesetz (NetzDG), nicht per se einen Anwendungsvorrang vor. Fraglich ist aber, inwieweit die Mitgliedstaaten **neben** dem koordinierten Bereich des DSA eigene Vorschriften erlassen können. Grundsätzlich haben die EU-Mitglieder das Recht, Sachverhalte außerhalb des Anwendungsbereichs einer Verordnung selbst zu regeln oder mit einer Verordnung deckungsgleiche Vorschriften zu erlassen. Lediglich mit dem Unionsrecht unvereinbare nationale Vorschriften werden verdrängt.

Ursprünglich wurde das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken 2017 erlassen, um Hassrede und andere strafbare Handlungen im Internet ein-

<sup>29</sup> <https://www.lto.de/recht/nachrichten/n/eu-kommission-vertragsverletzungsverfahren-umsetzung-richtlinie-urheberrecht/>.

<sup>30</sup> Spindler, GRUR 2021, 653 (655).

zudämmen. Nach dem Gesetz sind soziale Netzwerke ab einer Reichweite von zwei Millionen Nutzerinnen und Nutzern zu einem bestimmten Umgang mit Beschwerden über strafrechtswidrige Inhalte verpflichtet. Sie haben Beschwerden in einem wirksamen, transparenten Verfahren entgegenzunehmen, zu prüfen und entsprechende Maßnahmen zu ergreifen. Anbieter sozialer Netzwerke haben unabhängig von ihrem Sitz und ihrer Größe einen Zustellungsbevollmächtigten im Inland zu benennen.

Durch die jüngste Reform durch das Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes (NetzDGÄndG) mit Wirkung zum 28. Juni 2021 wurden die Nutzerrechte namentlich durch die Einführung eines Gegenvorstellungsverfahrens und durch die Klärung der Zuständigkeit des Zustellungsbevollmächtigten auch für Wiederherstellungsklagen gestärkt. Ferner wurden Vorschriften über die Einrichtung von Schlichtungsstellen und über die Durchsetzung von Auskunftsansprüchen eingefügt.

Im DSA-E finden sich nun Anklänge an dieses reformierte NetzDG.<sup>31</sup> Online-Plattformen werden zu internen Beschwerdemanagementsystemen, außergerichtlicher Streitbeilegung und Publizität über diese Schutzmaßnahmen verpflichtet, ähnlich wie das NetzDG Berichtspflichten für Betreiber vorsieht und klare Vorgaben zum Umgang mit Beschwerden macht. Doch es gibt auch Unterschiede, die im Folgenden beleuchtet werden.

### 1.3.3.1 Regelung konkreter Löschvorgaben (-fristen)

Die für digitale Geschäftsmodelle grundlegende ECRL legt ein seit zwei Dekaden unverändertes Haftungsregime fest („Safe Harbor Regelung“<sup>32</sup>, s.o. Regelungsziele des DSA). Bisher gilt das sogenannte *Notice and Take Down*-Verfahren, das die Haftungsprivilegierung des Hosting-Diensteanbieters an seine Verpflichtung knüpft, ab Kenntnis der Rechtswidrigkeit eines Inhalts diesen unzugänglich zu machen. An dieser Systematik hat der europäische Gesetzgeber seitdem festgehalten. Sie soll grundsätzlich auch durch den DSA fortgeführt werden; die entsprechenden Art. 12, 13 und 14 ECRL sind in den DSA-E übertragen (§§ 3, 4 und 5 DSA-E). Sie werden etwas modifiziert, vor allem aber ergänzt durch weitere mit der Haftungsbefreiung verbundene Sorgfalts- und Transparenzverpflichtungen (*Notice and Action*).

Beim *Notice and Action*-Konzept bleibt es dabei, dass der Hosting-Diensteanbieter ab Kenntnisnahme von der Rechtswidrigkeit eines Inhalts Maßnahmen zu ergreifen verpflichtet ist, um in den Genuss der Haftungsprivilegierung zu kommen. Doch es geht über das bisherige *Notice and Take down* hinaus. Abhilfe („*action*“) auf eine Meldung hin („*notice*“) ist nicht auf die Löschung oder die Sperrung des Zugangs zum rechtswidrigen Inhalt („*take down*“) beschränkt. Vielmehr ist der Meldung erstattenden Person oder Einrichtung die Entscheidung über das Abhilfeersuchen nebst Rechtsbehelfen mitzuteilen.

Es ist offenzulegen, inwieweit sich der Diensteanbieter zur Bearbeitung automatisierter Mittel bedient. Außerdem hat der Anbieter die Entscheidung gegenüber der Nutzerin oder dem Nutzer zu begründen, die oder der von einer Entfernung oder Sperrung eines Inhalts betroffen ist. Für diese Begründung gelten spezifische Anforderungen. Sie muss zudem in einer öffentlich zugänglichen Datenbank veröffentlicht werden.

Unter der aktuellen Rechtslage ist umstritten<sup>33</sup>, inwieweit konkrete Vorgaben für die Löschverpflichtung der vom NetzDG erfassten Diensteanbieter und Tatbestände neben der ECRL zulässig sind. So geht insbesondere der deutsche Gesetzgeber in seiner Gesetzesbegründung zum NetzDG<sup>34</sup> davon aus, dass ein Ausfüllen nationaler Spielräume im Sinne der ECRL dergestalt möglich ist, dass das NetzDG abstrakt-generell konkrete Vorgaben zur „unverzöglichen“ Löschung oder Sperrung macht. So sind offensichtlich rechtswidrige, strafbare Inhalte nach dem NetzDG binnen 24 Stunden nach Eingang eines Hinweises zu entfernen oder zu sperren (§ 3 Abs. 2 Ziff. 2 NetzDG). Für andere rechtswidrige Inhalte im Sinne des NetzDG hat der Anbieter des sozialen Netzwerks in der Regel sieben Tage Zeit für die Prüfung und um entsprechend zu reagieren (§ 3 Abs. 2 Ziff. 3 NetzDG). Diese Konkretisierung der Reaktionszeiten haben auch Anbieter sozialer Netzwerke aus anderen EU-Mitgliedstaaten zu beachten, weil in § 5 NetzDG das **Marktortprinzip** verankert ist.

Ein solches „Konkretisieren“ der ECRL widerspricht jedoch dem Wortlaut der Richtlinie. Denn diese lässt lediglich Ausnahmen von Art. 3 Abs. 4 ECRL in Gestalt von Einzelfallregelungen zu bestimmten Zwecken („Maßnahmen“) zu. Das sind also gerade keine abstrakt-generellen Gesetze. Hier geht es demnach nicht bloß um das Wie, um die im NetzDG vorgesehenen Verpflichtungen zu den Löschvorgaben. Sondern die Regulierung in Form von abstrakt-generellen Gesetzen ist insgesamt unzulässig, soweit sie den **koordinierten Bereich** der ECRL betrifft (hier Art. 14 Abs. 3 ECRL).

Etwas anderes gilt nur, wo spezifische Anforderungen vor der Entfernung oder Sperrung des Zugangs zu bestimmten Inhalten normiert werden sollen.<sup>35</sup> Doch darauf kann sich der nationale Gesetzgeber nicht berufen, wenn er durch seine Vorschriften den koordinierten Bereich der Richtlinie antastet. Wenn also Art. 14 Abs. 1 ECRL festlegt, ein rechtswidriger Inhalt sei „unverzöglich“ unzugänglich zu machen, dann berührt die Auslegung dieses unbestimmten Rechtsbegriffs den **Kernbereich dieser Norm**. Eine nationale Regulierung zur Festlegung der Begrifflichkeit in Form von Fristen würde die von der Richtlinie angestrebte Harmonisierung ad absurdum führen.

Der hier geschilderte **noch offene Meinungsstreit** zur Zulässigkeit nationaler Vorschriften zur „Konkretisierung“ des durch die ECRL regulierten Bereichs wird wohl auch nach Inkrafttreten des DSA noch weiter ausgetragen werden. Denn

<sup>31</sup> Gerald Spindler, <https://rsw.beck.de/aktuell/daily/magazin/detail/digitaler-wumms-aus-bruessel>: „Ein Hauch von NetzDG durchweht die nächste Stufe für Online-Plattformen [...]“.

<sup>32</sup> Gerald Spindler, Digitaler Wumms aus Brüssel, abrufbar unter <https://rsw.beck.de/aktuell/daily/magazin/detail/digitaler-wumms-aus-bruessel>.

<sup>33</sup> zum Meinungsstand in der Literatur vgl. Sachstandsbericht des Wiss. Dienst des Bundestages, Marktortprinzip und Herkunftslandprinzip im Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, WD 10 – 3000 – 023/20 v. 15.6.2020, abrufbar unter <https://www.bundestag.de/resource/blob/691846/cb11c99d9a39b6e-73151549e22d76b73/WD-10-023-20-pdf-data.pdf>.

<sup>34</sup> Gesetzentwurf der Bundesregierung, Begründung, Teil A. V.1.

<sup>35</sup> ErwGrd. 46 und 48 ECRL.

auch im DSA-E sind keine konkreten Fristen vorgesehen (vgl. Frage 2a, Abschnitt 2.3 „zügiges“ Handeln nach Kenntnisnahme). Allerdings wird im Vergleich zur geltenden Rechtslage der Spielraum für Konkretisierungen des Verfahrens durch die Mitgliedstaaten angesichts der Vorgaben in einer unmittelbar anwendbaren Verordnung kleiner. Das gilt insbesondere, solange und soweit das Marktortprinzip im NetzDG verankert bleibt.<sup>36</sup>

### 1.3.3.2 Regulierung von Videosharing-Plattformen im NetzDG

Außerdem wurde im Zuge des NetzDGÄndG die Richtlinie 2018/1808 über audiovisuelle Mediendienste (AVMD-RL) in deutsches Recht umgesetzt. §§ 3 d bis f NetzDG enthalten nun gesonderte Sorgfaltspflichten für die von der AVMD-RL regulierten Videosharing-Dienste, die, anders als zuvor, auch Plattformen geringerer Reichweite und themenspezifische Angebote erfassen.

Einer besonderen Würdigung bedarf ein grundlegender Unterschied in den Regelungen für soziale Netzwerke und Video-sharing-Diensten: Während erstere nach dem NetzDG weiterhin dem **Marktortprinzip** unterworfen sind, unterliegen Videosharing-Plattformen seit der letzten Reform des Gesetzes jedenfalls in weiten Teilen dem **Herkunftslandprinzip**.

#### 1.3.3.2 a) Mindestharmonisierung der AVMD-RL

Zunächst geht entsprechend den Vorgaben der AVMD-RL der deutsche Gesetzgeber davon aus, dass das Schutzniveau hinsichtlich bestimmter Inhalte grundsätzlich in allen Mitgliedstaaten der Union gewährleistet ist (Mindestharmonisierung des Art. 28 b AVMD-RL). Nach der Gesetzesbegründung trägt der Regelungsgehalt der AVMD-RL die Differenzierung zwischen koordiniertem und nicht koordiniertem Bereich auch in der Umsetzung. So sei die Anwendung des Marktortprinzips für soziale Medien einerseits und des Herkunftslandprinzips für in einem anderen EU-Mitgliedstaat ansässige Videosharing-Dienste in Bezug auf das vorgeschriebene Beschwerde- und Gegenvorstellungsverfahren gerechtfertigt.

Bei Anbietern von **Videosharing-Diensten** mit Sitz in einem **anderen EU-Mitgliedstaat** (zum Beispiel YouTube in Irland) kann jedoch auf Grund des NetzDG<sup>37</sup> das deutsche Bundesamt für Justiz **im Einzelfall** für die Durchsetzung von Verhaltensmaßstäben entsprechend dem NetzDG zuständig sein, soweit der Dienst auch in Deutschland genutzt werden kann. Was wie ein Zugeständnis an das Herkunftslandprinzip und an die Zuständigkeit des Niederlassungsstaates<sup>38</sup> wirkt, heißt letztlich nur: Wo die Verhaltenspflichten für ausländische Anbieter audiovisueller Mediendienste ohnehin mit denen des NetzDG übereinstimmen, genügt den deutschen Durchsetzungsbehörden eine Einzelfallzuständigkeit für die Durchsetzung der harmonisierten Verhaltensregeln. Die Behörden sollen sich also auf § 3 e Abs. 3 S. 2 NetzDG berufen können, um beispielsweise gegen eine nicht gerechtfertigte Gewaltdarstellung i.S.d. § 131 StGB auf YouTube vorzugehen.

Voraussetzung für die Ausübung dieser Zuständigkeit ist, dass die **Durchsetzungsanordnung** durch das Bundesamt für Justiz einem der Zwecke des § 3 Abs. 5 TMG<sup>39</sup> dient und auch die verfahrensmäßigen Voraussetzungen der Norm erfüllt sind. Insbesondere ist die inländische Behörde dabei zur vorherigen Konsultation der zuständigen Behörde im Sitzland des Anbieters verpflichtet, auf dessen Plattform der fragliche Inhalt hochgeladen wurde. Angesichts dieser Rechtsgrundverweisung auf § 3 Abs. 5 TMG erscheint die praktische Relevanz solcher Einzelfallanordnungen jedoch gering.

Auch hier zeigt sich aber, dass im Anwendungsvorrang des Unionsrechts, den der Digital Services Act auch für die AVMD-RL festlegen soll, mehrere Einfallstore für nationale Besonderheiten angelegt sind. Denn die Implementierung des koordinierten Bereichs der AVMD-RL obliegt den Mitgliedstaaten und birgt schon deshalb das Potenzial für Unterschiede in der Umsetzung. Diese werden **Einfluss** auf die Wirksamkeit der **Harmonisierung** durch den DSA haben.

Fraglich ist im Übrigen, ob wegen § 3 e Abs. 3 S. 2 NetzDG ein Anbieter wie YouTube ohne Sitz in Deutschland künftig nichts zu befürchten hat, wenn er einen strafbaren Inhalt nicht nach den Vorgaben des DSA sperrt oder löscht. Die positive **Regulierung der Verantwortlichkeit**, also die Voraussetzungen für eine Haftung, obliegt den Mitgliedstaaten.<sup>40</sup> Der DSA selbst kann und soll eine Haftung nicht begründen, er harmonisiert lediglich, wie zuvor die ECRL, Haftungsausschlüsse.<sup>41</sup> In Deutschland normiert das Netzwerkdurchsetzungsgesetz Sorgfalts-, Berichts- und Transparenzpflichten für einige Plattformen, begründet aber seinerseits keine Haftung für rechtswidrige Inhalte. Der MStV ordnet Transparenzvorgaben für Empfehlungssysteme und für Onlinewerbung an. Auch das UrhDaG<sup>42</sup> kodifiziert lediglich bestimmte Sorgfalts- und Verfahrensvorschriften zum Schutz der Interessen von Rechteinhabern und Plattformnutzern, verbunden mit einer Haftungsbefreiung für den Plattformbetreiber bei Einhaltung der Vorgaben. Dem § 10 TMG, der lediglich die Haftungsprivilegierung der ECRL für Hosting-Anbieter umsetzt, wird neben der DSA-Verordnung ohnehin kein eigener Regelungsgehalt zukommen.

Wenn eine Verpflichtung zur Sperrung oder Löschung durch einen Videosharing-Dienst aus einem anderen EU-Mitgliedstaat also nicht im Einzelfall auf Grundlage des NetzDG in Verbindung mit dem TMG **angeordnet** wird, fehlt jedenfalls dann eine Grundlage, um ein Nichtentfernen des Inhalts durch den Plattformbetreiber zu sanktionieren, wenn dem Plattformbetreiber keine **zentrale, aktive Rolle** nachzuweisen ist. (Vgl. dazu Frage 2b, Abschnitt 1)

<sup>36</sup> Vgl. auch die näheren Ausführungen in Frage 1, Abschnitt 1.3.3.2 b.

<sup>37</sup> § 3 e Abs. 3 S. 2 NetzDG in Verbindung mit § 3 Abs. 5 TMG, Art. 3 Abs. 4 b ECRL.

<sup>38</sup> Abs. 5 AVMD-RL.

<sup>39</sup> z.B. ernsthafte und schwerwiegende Gefahr für öffentliche Sicherheit und Ordnung oder für öffentliche Gesundheit.

<sup>40</sup> Begründung des DSA-E, Abschnitt Kohärenz mit der Politik der Union in anderen Bereichen.

<sup>41</sup> ErwGrd. 17 DSA-E.

<sup>42</sup> Urheberrechts-Diensteanbieter-Gesetz vom 31.5.2021 (BGBl. I S. 1204, 1215).

Auf einem anderen Blatt steht, inwieweit auf Grund von Community Standards und Compliance-Praxis von Betreibern wie YouTube de facto bereits jetzt Verantwortung übernommen wird und nach untergesetzlichen Regeln Inhalte der Nutzerinnen und Nutzer gelöscht werden.<sup>43</sup> (Vgl. dazu Frage 2 b, Abschnitt 3)

### 1.3.3.2 b) Die Öffnungsklauseln in der ECRL und die Umsetzung der AVMD-RL im NetzDG

Im Folgenden wird untersucht, ob die Öffnungsklauseln Art. 14 Abs. 3 ECRL (künftig Art. 5 Abs. 4 DSA-E), Art. 3 Abs. 4 lit. a i ECRL oder Art. 15 Abs. 2 ECRL herangezogen werden können, um im NetzDG Regelungen zu Videosharing-Plattformen mit Sitz im europäischen Ausland zu treffen, wenn der Digital Services Act in seiner bisher vorgeschlagenen Gestalt in Kraft tritt.

Bei der Umsetzung der AVMD-RL in ihrer Fassung der RL 2018/1808 hat der deutsche Gesetzgeber ausweislich der Gesetzesbegründung<sup>44</sup> zum NetzDGÄndG erneut vom Gestaltungsspielraum für die Mitgliedstaaten Gebrauch gemacht, der in **Art. 14 Abs. 3 ECRL** angelegt ist. Schon unter bisherigem Recht wollte sich, so jedenfalls die Begründung zum NetzDGÄndG, der Gesetzgeber für eine Regelungskompetenz auf Art. 14 Abs. 3 ECRL in Verbindung mit deren Erwägungsgründen 45 und 46 stützen.<sup>45</sup> Art. 14 Abs. 3 ECRL findet seine Entsprechung teilweise in Art. 5 Abs. 4 DSA-E. Jedoch fehlt ein gewichtiger Teil der Öffnungsklausel: „*[Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern,] oder dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.*“

Dieser Passus des Art. 14 Abs. 3 ECRL gilt auch nicht gemäß Art. 1 Abs. 5 DSA-E fort; denn Art. 71 Abs. 1 DSA-E ordnet die Streichung der Art. 12 bis 15 ECRL an. Sie sind also nur insoweit nach Inkrafttreten des DSA anwendbar, als sie in die neue Verordnung übernommen sind. Das bedeutet, dass nationale Vorschriften zur Konkretisierung von Verfahren für das Löschen oder Sperren von Informationen nicht mehr auf Grundlage des Art. 14 Abs. 3 ECRL erlassen werden dürfen, weil sie abschließend im DSA geregelt sind.

Bei den Regelungen des NetzDG zu den Voraussetzungen und der Durchsetzbarkeit der Verpflichtung, Inhalte Dritter in sozialen Netzwerken oder auf Videosharing-Plattformen zu sperren oder zu entfernen, handelt es sich aber um eben solche Festlegungen im Sinne des aktuellen Art. 14 Abs. 3 ECRL, der im DSA in seiner bisher vorgesehenen Gestalt offenbar bewusst nicht fortgeführt wird. Denn die Kommission will gerade die nationalen Auswüchse im koordinierten Bereich eindämmen. Deshalb würde bei Inkrafttreten des DSA

in seiner derzeitigen Fassung die **bisherige Begründung** des deutschen Gesetzgebers für eine nationale Regelung im koordinierten Bereich **nicht mehr tragen**.

Der deutsche Gesetzgeber hat sich beim Erlass des NetzDGÄndG unter geltendem Recht „hilfsweise“ **auf Art. 3 Abs. 4 lit. a i) ECRL** berufen. Nach dieser Vorschrift dürfen die Mitgliedstaaten den freien Verkehr von Diensten der Informationsgesellschaften aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die in den koordinierten Bereich fallen. Dieser ist in Art. 2 h ECRL definiert und umfasst auch die vom Diensteanbieter zu erfüllenden Anforderungen in Bezug auf die Ausübung der Tätigkeit, insbesondere Sorgfaltspflichten und Anforderungen an die Verantwortlichkeit des Diensteanbieters. Diese sind auch im NetzDG geregelt.

Es ist nicht ersichtlich, dass Teile des Art. 3 ECRL vom Anwendungsvorrang und der Fortgeltung der Richtlinie gemäß Art. 1 Abs. 5 DSA-E nach Inkrafttreten des Digital Services Act ausgenommen werden sollten.

Fraglich ist daher, ob die Ausweitung des Anwendungsbereichs des NetzDG auf Diensteanbieter, die ihren Sitz in einem anderen Mitgliedstaat der EU haben, nach den geltenden und voraussichtlich auch künftig anwendbaren europäischen Regelungen zulässig ist und sein wird. Dies wird von der Europäischen Kommission wie auch in der Literatur verneint. Denn Art. 3 Abs. 4 lit. a i) ECRL gestattet mitgliedstaatliche „Maßnahmen“, die im Hinblick auf einen „bestimmten“ Dienst der Informationsgesellschaft entgegen dem Herkunftslandprinzip des Art. 3 Abs. 2 ECRL nach nationalem Recht des Marktortes ergriffen werden dürfen.

Die Kommission lehnt zu Recht ein abstrakt-generelles Gesetz wie das NetzDG als eine „Maßnahme“ im Sinne des Art. 3 Abs. 4a i) ECRL ab. Sie nennt als Anwendungsbeispiele für diese Vorschrift eine Mahnung oder ein Zwangsgeld gegenüber einem Anbieter, der einen **nicht harmonisierten Dienst** im jeweiligen Mitgliedstaat zugänglich macht und dabei zum Beispiel Verbraucherschutzregeln des Bestimmungslandes missachtet.<sup>46</sup> Ausweislich des Wortlauts eröffnet die Norm lediglich einen mitgliedstaatlichen Gestaltungsspielraum im Sinne spezifischer Einzelanordnungen, die sich auf einen bestimmten Dienst beziehen, also nicht in einem förmlichen Gesetz wie dem NetzDG.<sup>47</sup> Zudem ist die Liste der Ausnahmen von Art. 3 im Anhang der ECRL im Sinne zulässiger nationaler Gesetzgebung innerhalb des koordinierten Bereichs abschließend.<sup>48</sup>

Vor diesem Hintergrund wird für die Regulierung von Diensteanbietern mit Sitz in einem anderen EU-Mitgliedstaat auch nach Inkrafttreten **kein Raum für nationale Gesetzgebung** auf Grund des **Art. 3 Abs. 4 lit. a i) ECRL** verbleiben.

<sup>43</sup> Marc Liesching, Gilt das NetzDG für Facebook, Youtube und Twitter? <https://community.beck.de/2020/02/11/gilt-das-netzdg-fuer-facebook-youtube-und-twitter?destination=node/69296>, veröffentlicht am 11.2.2020.

<sup>44</sup> ausdrücklich auch in der Notifizierung gegenüber der EU-Kommission, abrufbar unter <https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2020&num=174>.

<sup>45</sup> Vgl. Abschnitt 1.3.3.1.

<sup>46</sup> Mitteilung KOM(2003) 0259 endg., Ziff. 2.1.2., abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52003DC0259>.

<sup>47</sup> Marc Liesching, Gilt das NetzDG für Facebook, Youtube und Twitter?, abrufbar unter <https://community.beck.de/2020/02/11/gilt-das-netzdg-fuer-facebook-youtube-und-twitter?destination=node/69296>, veröffentlicht am 11.2.2020, m.w.N.

<sup>48</sup> Hain/Ferreau/Brings-Wiesen, Regulierung sozialer Netzwerke revisited, K&R 2017, 433 (434).

Im Ergebnis bedeutet das, dass die Regelung im NetzDG zu Videosharing-Diensten mit Sitz in einem anderen EU-Mitgliedstaat als Deutschland gegen europäisches Recht verstößt, falls Art. 5 Abs. 4 DSA-E wie von der Kommission vorgeschlagen in Kraft gesetzt wird.

In einer Stellungnahme zur Klage von Google Ireland Ltd. gegen die Berichtspflicht gegenüber dem Bundeskriminalamt gemäß § 3 a NetzDG (s.u. Abschnitt 1.3.3.2 c) hat sich das Bundesjustizministerium dem Vernehmen nach<sup>49</sup> zudem auf **Art. 15 ECRL** als eine Ausnahme vom Herkunftslandprinzip berufen. Nach dieser Vorschrift können die Mitgliedstaaten den Anbietern von Diensten der Informationsgesellschaft Melde- und Übermittlungspflichten im Hinblick auf mutmaßlich rechtswidrige Tätigkeiten oder Informationen auferlegen.

Art. 15 Abs. 2 ECRL gestattet, dass „die Mitgliedstaaten [...] Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.“

Unabhängig davon, ob dieser Gestaltungsspielraum durch das NetzDG in zulässiger Weise ausgefüllt worden ist, wird sich ein mitgliedstaatlicher Gesetzgeber auf diese Ermächtigungsnorm mit Inkrafttreten des DSA voraussichtlich nicht mehr berufen können; denn sie soll ausweislich des bisherigen Verordnungsentwurfs ersatzlos gestrichen werden, Art. 71 DSA-E. Sie findet sich auch nicht in Art. 8 oder 9 DSA-E wieder. Diese betreffen lediglich Auskünfte auf Grund behördlicher Anordnungen in Gestalt von Einzelfallregelungen, keine abstrakt-generellen Verpflichtungen.

### 1.3.3.2 c) Überprüfung durch das Verwaltungsgericht Köln

Google Ireland Ltd. hat nach Berichten der FAZ vom 27. Juli 2021<sup>50</sup> auf Grund der Vorschriften zur Umsetzung der AVMD-RL im NetzDG in seiner ab 1. Februar 2022 geltenden Fassung Feststellungsklage vor dem Verwaltungsgericht Köln erhoben und Eilbedürftigkeit geltend gemacht.<sup>51</sup> Das Unternehmen beruft sich dabei auf die Unvereinbarkeit der künftigen Verpflichtung, Nutzerdaten beim Verdacht bestimmter Straftaten (zum Beispiel Androhung von Mord oder Vergewaltigung) ohne eine Information an die entsprechenden User an das Bundeskriminalamt weiterzuleiten, mit höherrangigem Recht. Sie verletze die Datenschutz-Rechte der Betroffenen.

Die Aktivlegitimation von Google Ireland ergibt sich aus der Anwendung des § 3 e Abs. 3 S. 1 NetzDG. Danach werden die Anbieter von Videosharingplattform-Diensten mit Sitz im EU-Ausland nicht von der Anwendung des künftig geltenden

§ 3 a NetzDG über die Benachrichtigung des BKA befreit sein; die Vorschrift ist ab Februar 2022 anzuwenden.

Das Verwaltungsgericht wird also unter anderem die Vereinbarkeit der Vorschrift mit dem Herkunftslandprinzip der ECRL zu überprüfen haben. Die Erwägungen des Verwaltungsgerichts in diesem Verfahren werden übertragbar sein auf die Frage, inwieweit das NetzDG mit dem künftigen DSA vereinbar sein wird. Denn wie die Kommission festgestellt hat, setzt die Vereinbarkeit voraus, dass eine Einzelfallanordnung für einen nicht harmonisierten Dienst, also außerhalb des koordinierten Bereichs ergeht. Das wäre nicht der Fall, wenn der DSA in der bisher vorgeschlagenen Fassung in Kraft träte.

### 1.3.4 Der Digital Services Act und der Medienstaatsvertrag

Der Medienstaatsvertrag (MStV) stand bei seiner Verabschiedung aus ähnlichen Gründen auf der Kippe, wie heute die Vereinbarkeit des NetzDG mit der ECRL infrage gestellt wird. Die EU-Kommission hatte während der Verhandlungen der Länder ihre Bedenken hinsichtlich der Vereinbarkeit des Staatsvertrages mit EU-Recht geltend gemacht. Auch sei geplant, mit Erlass des DSA medienpolitische Aspekte der Plattformregulierung einheitlich für den Binnenmarkt zu erlassen.<sup>52</sup> Hintergrund war wohl auch, dass die ECRL eine gesellschaftspolitische Würdigung der systemischen Bedeutung digitaler Dienste nicht kennt.<sup>53</sup> Stattdessen stellt die Richtlinie wettbewerbs- und lauterkeitsrechtliche Rahmenbedingungen für digitale Angebote auf.

Im DSA-E findet sich nun jedenfalls **keine Öffnungsklausel** zum Erhalt der Medienvielfalt im Binnenmarkt, wie Art. 85 Abs. 2 DSGVO eine vorsieht. Dort ist den Mitgliedstaaten ausdrücklich ein eigener Regelungsspielraum für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken eingeräumt, wenn nationale Regelungen erforderlich sind, um das Recht auf Schutz der personenbezogenen Daten mit der Meinungs- und Informationsfreiheit in Einklang zu bringen.

Stattdessen nimmt der DSA-E in Erwägungsgrund 13 solche Hosting-Dienste von den Sondervorschriften für Online-Plattformen ausdrücklich aus, die eine Verbreitung nutzergenerierter Inhalte als bloße **Nebenfunktion** des Hauptdienstes integrieren. Wenn etwa eine Online-Zeitung einen Kommentarbereich anbiete, liege die Hauptfunktion in der Veröffentlichung von Nachrichten unter der redaktionellen Verantwortung des Verlegers; nach dem Verständnis des DSA handele es sich mithin um einen Hosting-Dienst, nicht aber um eine Online-Plattform.

Doch die Dienste, die von den Vorschriften der Art. 16 ff. DSA-E für Online-Plattformen erfasst sind, sollen wie diejenigen, die vom MStV reguliert werden, erhöhte **Transparenz-anforderungen** im Bereich der Online-Werbung erfüllen, Art. 24 DSA-E. Dazu gehört neben dem Echtzeit-Hinweis auf die

<sup>49</sup> <https://www.faz.net/aktuell/feuilleton/medien/youtube-klagt-gegen-netzwerkdurchsetzungsgesetz-17456916.html>.

<sup>50</sup> <https://www.faz.net/aktuell/feuilleton/medien/youtube-klagt-gegen-netzwerkdurchsetzungsgesetz-17456916.html>.

<sup>51</sup> Az. 6 K 3769/21 und 6 L 1277/21 vom 16.7.2021.

<sup>52</sup> [https://ec.europa.eu/germany/news/20200428-mediensstaatsvertrag\\_de](https://ec.europa.eu/germany/news/20200428-mediensstaatsvertrag_de).

<sup>53</sup> Michael Hanfeld, Im digitalen Sandkasten, FAZ.net v. 29.4.2020, abrufbar unter <https://www.faz.net/aktuell/feuilleton/medien/eu-kommission-billigt-den-deutschen-mediensstaatsvertrag-16745740.html>.

Qualität der Anzeige als Werbebotschaft auch, die wichtigsten Parameter zur Bestimmung der Nutzerinnen und Nutzer, denen die Werbung angezeigt wird, aussagekräftig offenzulegen. Insofern wird **nach Inkrafttreten des DSA** der MStV mit Blick auf die neuen Vorschriften der DSA-Verordnung ausdünnen sein.

### 1.4 Harmonisierung durch vereinheitlichte Durchsetzung

In der Begründung des DSA-E fasst die Kommission die Ergebnisse der öffentlichen Konsultation dahingehend zusammen, dass unter den Interessenträgern Einvernehmen herrsche, dass die Zusammenarbeit zwischen den Behörden sowohl grenzüberschreitend als auch innerhalb der Mitgliedstaaten verbessert werden solle. Die Beaufsichtigung durch die EU werde als wesentlich angesehen, und die Mehrheit der Befragten scheine eine zentrale Aufsichtsstelle zu befürworten.

#### 1.4.1 Kontaktstelle oder Inlandsvertreter

Eine gewisse Vereinheitlichung der Durchsetzung der Plattformregulierung soll der Digital Services Act durch die Verpflichtung der Vermittler erreichen, eine „zentrale Kontaktstelle“ für die zuständigen Behörden, für die Kommission und für das Europäische Gremium für digitale Dienste zu benennen (Art. 10 DSA-E). Für Anbieter aus Nicht-EU-Staaten bedeutet das, dass sie einen Rechtsvertreter in der Union benennen müssen, der unmittelbar für die Einhaltung der Verordnung haftet (Art. 11 DSA-E).

#### 1.4.2 Koordinator für digitale Dienste

Der DSA-E setzt grundsätzlich auf die bestehenden behördlichen Strukturen der Mitgliedstaaten auf. Er verpflichtet die Mitgliedstaaten nicht zwingend, neue Behörden einzurichten, schreibt aber die Einführung verpflichtender nationaler Koordinatoren für mehr Einheitlichkeit in der Durchsetzung der Verordnung vor (Art. 38 DSA-E). Diese Koordinatoren für digitale Dienste sollen jeweils die wichtigste zentrale Stelle für die Anwendung der Verordnung sein. Sie genießen besondere Befugnisse (Art. 41 DSA-E).

Möglicherweise problematisch, mindestens aber herausfordernd ist dabei, dass der nationale Koordinator in Mitgliedstaaten mit mehreren zuständigen Behörden nur eine von mehreren Stellen ist, die mit der Anwendung der Verordnung betraut sind und nach dem DSA-E auch bleiben können<sup>54</sup>. In Deutschland etwa kommen Wettbewerbsbehörden, BNetzA, Bundesamt für Justiz oder auch Medienanstalten in Betracht. Andere Mitgliedstaaten verfügen über eine eigene Verbraucherschutzbehörde. Das bedeutet, dass in Fällen wie in Deutschland **sehr unterschiedliche Zuständigkeiten** und Kompetenzen zentral abgestimmt werden müssen. Ob die damit verbundenen unvermeidlichen Berichte und Abstimmungen tatsächlich zu einer verbesserten Kohärenz allein im Inland beitragen, müsste sich noch erweisen.

Die Verpflichtung der Koordinatoren zur Zusammenarbeit untereinander mag jedenfalls die Vereinheitlichung der Anwen-

dung und Durchsetzung der Verordnung im Binnenmarkt unterstützen, mindestens aber die Transparenz bezüglich jeder ergangenen Anordnung im Sinne des Art. 8 DSA-E. So würde sich zumindest das **Herkunftslandprinzip** als (weitere<sup>55</sup>) Ausnahme vom Marktortprinzip des DSA begründen lassen. Das ist in Art. 40 DSA-E für die Durchsetzung bestimmt. Zuständig ist der Koordinator des Mitgliedstaates, in dem der Anbieter seine Hauptniederlassung hat oder gemäß Art. 11 DSA-E seinen Inlandsvertreter benannt hat. Wer keinen solchen Vertreter bestimmt hat, begründet damit die Zuständigkeit jedes Mitgliedstaates.

#### 1.4.3 Europäisches Gremium für digitale Dienste

Die Einrichtung einer unabhängigen Beratergruppe der Koordinatoren (**Europäisches Gremium für digitale Dienste**, Art. 47 DSA-E) erinnert an den Europäischen Datenschutzausschuss. Auch diesem kommt nur eine koordinierende und beratende Funktion im Verhältnis zu den unabhängigen nationalen Behörden zu. Die Stellungnahmen des Gremiums für digitale Dienste, seine Empfehlungen und Ratschläge für die Koordinatoren (Art. 49 Abs. 1c DSA-E<sup>56</sup>), welche gemäß Art. 48 Abs. 1 DSA-E sämtlich dem Gremium selbst angehören, sind für diese nicht verbindlich.<sup>57</sup> Ein Nichtbefolgen durch die Koordinatoren ist lediglich zu begründen. Das entspricht der in Art. 39 Abs. 2 DSA-E vorgesehenen Stellung der Koordinatoren als unabhängige, weisungsfrei arbeitende Behörden.

#### 1.4.4 Grenzüberschreitende Kompetenzen nationaler Behörden

Von einem anderen in den Erwägungsgründen des DSA benannten Vorschlag ist zwar eine gewisse Harmonisierung zu erwarten. Ob dieser sich aber rechtspolitisch durchsetzen lässt, darf noch bezweifelt werden: Nach Erwägungsgrund 31 DSA-E soll die zuständige Behörde bei einer Anordnung wegen einer spezifischen Information auch bewerten, „*ob diese Informationen auch in anderen betroffenen Mitgliedstaaten illegale Inhalte darstellen könnten und gegebenenfalls sowohl die einschlägigen Vorschriften des Unionsrechts und Völkerrechts als auch die Interessen diplomatischer Gepflogenheiten berücksichtigen.*“

Das kann zum Beispiel bedeuten, dass eine nach Art. 40 DSA-E örtlich zuständige ungarische Behörde in ihrer Durchsetzungsentscheidung bewertet, dass ein Post einer deutschen Nutzerin auf einer Plattform mit Rechtsvertreter in Ungarn auch in Deutschland illegal sein könnte. Dann hat diese Behörde jedenfalls zu erwägen, auch im Hinblick auf die Abrufbarkeit des Inhalts in Deutschland Maßnahmen zu ergreifen. Hier würde also das **Herkunftslandprinzip**, das hinsichtlich der Haftungsbefreiung gilt, durch die rechtliche Einschätzung einer ausländischen Behörde **ausgehebelt**. Das mag ein Stück weit der technisch kaum umsetzbaren Inhaltessperrung innerhalb nationaler Grenzen geschuldet und der Harmonisierung im Binnenmarkt zuträglich sein, verspricht aber nicht eben befriedigende Behördenentscheidungen aus Sicht der

<sup>55</sup> Vgl. Abschnitt 1.3.3.2 Regulierung von Video-Sharing-Plattformen im NetzDG.

<sup>56</sup> In Art. 49 Abs. 2 DSA-E sind Stellungnahmen, Aufforderungen und Empfehlungen als Handlungsinstrumente des Gremiums genannt.

<sup>57</sup> ErwGrd. 90 DSA-E.

<sup>54</sup> Art. 38 Abs. 2 DSA-E.

Nutzerinnen und Nutzer. Denn sie wären der Durchsetzung des Digital Services Act unmittelbar durch eine ausländische Behörde ausgesetzt. Welche Besonderheiten hinsichtlich der Rechtsschutzmöglichkeiten gegen solche ausländische Einmischung und mit Blick auf die gerichtliche Zuständigkeit zu ihrer Überprüfung gelten sollen, lässt der Verordnungsentwurf offen.

#### 1.4.5 Befugnisse der EU-Kommission

Anders als in der DSGVO soll die EU-Kommission nach dem Entwurf des Digital Services Act mit eigenen Eingriffsbefugnissen ausgestattet werden, um unionsweit auftretende systemische Risiken für den gesamten Binnenmarkt einzudämmen. Insbesondere soll ihr nach Art. 51 DSA-E ein Eintritts- und Sanktionsrecht zukommen, wenn eine Verfehlung einer sehr großen Online-Plattform im Raum steht. Sie kann dann von Amts wegen tätig werden, Auskunftsverlangen gegenüber den Plattformbetreibern aussprechen, Ermittlungen vor Ort anstellen und schließlich selbst Bußgelder verhängen oder Zwangsgelder festsetzen (Artt. 59 f. DSA-E).

Wo die Kommission also solche umfassenden Kompetenzen eingeräumt bekommt, hält sie ein Instrument in Händen, das eine einheitliche Durchsetzung des Digital Services Act im Anwendungsbereich der Artt. 50 ff. DSA-E gegenüber sehr großen Plattformen ermöglicht. Hier könnten also ähnlich aufsehenerregende Entscheidungen der Kommission wie in den Fällen ergehen, in denen sie von ihren Befugnissen als Wettbewerbshüterin Gebrauch macht. Ob sich diese umfassenden Kompetenzen für die Kommission allerdings im Laufe des **Verordnungsgebungsverfahrens** halten lassen, wird abzuwarten sein.

Ein anderes Problem ergibt sich daraus, dass die Kommission selbst keine unabhängige, unparteiische Behörde ist, wie es für die nationalen Koordinatoren vorgeschrieben ist (Art. 39 DSA-E). Sie ist das **politisch** gewählte Exekutivorgan der Union.

#### 1.5 Harmonisierung durch teilweise vereinheitlichten Sanktionsrahmen

Ähnlich wie nach der DSGVO obliegt es auch nach dem DSA-E den Mitgliedstaaten, konkrete Sanktionen vorzusehen (Art. 42 DSA-E). Die Verordnung soll lediglich **Obergrenzen** festlegen. Die Erfahrungen mit der DSGVO seit deren Anwendbarkeit (05/2018) zeigen, dass die Bußgeldpraxis der nationalen Aufsichtsbehörden ausgesprochen unterschiedlich streng ist. Sowohl in Bezug auf die Anwendung der Verordnung als auch in der Bereitschaft oder Fachkompetenz, bei Nichtbefolgen der DSGVO einzuschreiten, sowie im Hinblick auf die Höhe der verhängten Bußgelder gibt es nicht nur zum Beispiel innerhalb Deutschlands, sondern vor allem auch innerhalb des Binnenmarktes eine enorme Bandbreite.<sup>58</sup> Ob für den DSA eine gewisse Harmonisierung der Sanktionen durch die vorgesehenen Maßnahmen zur Vereinheitlichung der Durchsetzung (s.o. 1.4) erzielt werden kann, muss sich erst erweisen.

Die Verordnung ist ihrer Rechtsnatur nach hybrid angelegt. Das bedeutet, dass öffentlich-rechtliche, zivilrechtliche und strafrechtliche Elemente oder Maßstäbe enthalten sind. Das spiegelt sich allerdings nicht in einem gemeinsamen Sanktionsrahmen wider. Es fehlt ein gemeinsamer **zivilrechtlicher** Sanktionsrahmen. Es gibt keine konkrete Festlegung, wie beispielsweise Verstöße gegen die eigenen Community Standards gegenüber den Betroffenen auszugleichen sind oder ob und welcher Art zivilrechtlicher Schadenersatz zu leisten ist, wenn ein User zu Unrecht von der Nutzung einer Plattform ausgeschlossen wurde. Die DSGVO geht insoweit weiter (Art. 82 DSGVO). Dort ist für den Verstoß gegen die Verordnung ein Ersatzanspruch für materielle und sogar für immaterielle Schäden auch in Bezug auf die Zuordnung der Verantwortlichkeit geregelt. Wie für die Fälle des Overblockings ausgeführt (Frage 2a, Abschnitt 2.6), sollte der Kommissionsvorschlag den zivilrechtlichen Bereich durch entsprechende zivilrechtliche Verstoßfolgen schlüssig zu Ende regulieren und einen Rahmen für die private Rechtsdurchsetzung vorsehen. Für einen einheitlichen Rahmen der **strafrechtlichen** Sanktionen fehlt der Union dagegen die Regelungskompetenz.

**Frage 2: Sind die vorgeschlagenen Änderungen zu **Verpflichtungen und Haftungsregeln** für Hosting Diensteanbieter (insb. Melde- und Abhilfeverfahren nach Artikel 14), Online-Plattformen (insb. Meldung des Verdachts von Straftaten nach Artikel 21) und sehr große Online-Plattformen (insb. Risikobewertungen nach Artikel 26) insbesondere vor dem Hintergrund folgender Erwägungen problematisch?**

**Frage 2a: Könnten die geplanten Haftungsregelungen ein **Overblocking** begünstigen und dadurch die Informations- und Meinungsfreiheit über Gebühr einschränken? Inwieweit werden die Erfahrungen mit vergleichbaren Regelungen wie dem NetzDG im DSA-Entwurf bereits berücksichtigt, wo sind Anpassungen angezeigt?**

#### Zusammenfassende Antwort

Für die Wirkungen des NetzDG im Sinne von Overblocking fehlt es bisher an belastbaren Daten. Daher ist umstritten, ob das Gesetz Overblocking und die damit verbundenen Grundrechtsverletzungen begünstigt. Vor diesem Hintergrund ist schwer abzusehen, ob die geplanten Vorschriften die Gefahr des Overblocking erhöhen oder ob vor allem das vorgeschlagene verpflichtende Beschwerdemanagement der Diensteanbieter umgekehrt Overblocking eindämmen wird.

Zwar soll der DSA eine Legaldefinition der „illegalen Inhalte“ vorhalten, für die der Hosting-Anbieter rechtlich einstehen muss, wenn er sie nicht rechtzeitig entfernt. Doch allein mit diesem Verweis auf einschlägiges Unionsrecht und auf mitgliedstaatliche Vorschriften bleibt die Definition vage. Das Gleiche gilt für die Anforderung, für eine Haftungsbefreiung „zügig“ tätig zu werden. Eine größere Gefahr des Overblockings als bisher ist mit den beiden unbestimmten Rechtsbegriffen jedoch nicht verbunden.

<sup>58</sup> Ständig aktualisierter Überblick abrufbar unter <https://www.enforcementtracker.com>.

Der DSA normiert keine Anforderungen an eine subjektive Berechtigung zur Meldung eines illegalen Inhalts oder eines Verstoßes gegen Gemeinschaftsstandards (Nutzungsbedingungen). Stattdessen gelten qualitative Anforderungen an die Meldung.

Inwieweit die geplanten Maßnahmen gegen Overblocking (Begründungs- und Transparenzanforderungen, *trusted flaggers*, Bußgeldandrohung, Maßnahmen gegen missbräuchliche Meldungen) zusammengenommen die gewünschte Wirkung entfalten, wird im Rahmen der Evaluation zu untersuchen sein.

Ein zivilrechtlicher Schadenersatzanspruch im Fall von Overblocking ist nach bisherigem Stand nicht vorgesehen.

Das System der Haftungsbefreiung nach dem *Notice and Action*-Verfahren<sup>59</sup>, das das bisherige *Notice and Take Down*-Verfahren modifiziert, legt nahe, dass Betreiber von Vermittlungsdiensten nach Auffassung der Kommission dazu neigen, zur Vermeidung einer rechtlichen Verantwortlichkeit eher zu großzügig als zu sparsam Inhalte ihrer Nutzerinnen und Nutzer zu sperren oder zu entfernen. Die Gefahr, dass rechtlich nicht zu beanstandende Inhalte gelöscht werden, etwa weil ein rein technisches Filtern den Kontext nicht erkennt (zum Beispiel zulässige Parodie, Zitat), wird in der rechtspolitischen Debatte auf europäischer Ebene ebenso diskutiert wie seinerzeit bei Erlass des NetzDG. Ausführlich wurden die Bedenken im Zusammenhang mit der Urheberrechtsreform in Brüssel und bei ihrer Umsetzung in Deutschland behandelt.

### 1. NetzDG und Besorgnis des Overblockings

Bereits in der ursprünglichen Fassung des NetzDG hatte der deutsche Gesetzgeber die Gefahr des Overblockings adressiert. Eine der Maßnahmen, um ihr entgegenzuwirken, ist die Festsetzung einer **Frist** von in der Regel sieben Tagen für eine sorgfältige Prüfung von gemeldeten nicht offensichtlich rechtswidrigen Inhalten. Auf diese Weise wollte der Gesetzgeber strukturellen Fehlbewertungen vorbeugen.<sup>60</sup> Nur offensichtlich rechtswidrige Inhalte sind binnen 24 Stunden zu löschen oder zu sperren.

Bei der umfassenden Reform des NetzDG wurde außerdem ein **Gegenvorstellungsverfahren** eingeführt, das helfen soll, vor zu Unrecht gelöschten oder gesperrten Inhalten zu schützen. Es verpflichtet soziale Netzwerke, ihre eigenen Entscheidungen über die Löschung oder die Beibehaltung eines Inhalts auf Antrag zu überprüfen. Allerdings ist der Anwendungsbereich auf die Fälle von Löschungen oder Sperrungen auf Grund der Normen des Strafrechts beschränkt, die im NetzDG genannt sind. Löschungen auf Grund der Community Standards der Plattformen brauchen von den Betreibern nicht im Gegenvorstellungs- oder im Schlichtungsverfahren behandelt zu werden.

Im Zuge der Reform des NetzDG waren die verfassungsrechtlichen Bedenken mit Blick auf Anreize des Gesetzes zum Overblocking wiederholt worden. Teils wurde geltend gemacht, sowohl die überwiegend nicht nach StGB, sondern nach AGB der Anbieter erfolgenden Löschungen („Flucht in die AGB-Löschung“) sowie eine Bearbeitungsdauer von unter 24 Stunden bei fast 90 % der gelöschten Beschwerdefälle seien nicht unerhebliche Indizien für das Vorliegen von Overblocking.<sup>61</sup> Andere Stimmen brachten vor, für die Gefahr eines Overblockings gebe es keine empirischen Indizien.<sup>62</sup>

Die später entsprechend der Gesetzesbegründung des NetzDG durchgeführte **Evaluation** des Gesetzes<sup>63</sup> legt nahe, dass sich die Befürchtungen des Overblockings innerhalb der ersten Jahre der Anwendung des Gesetzes nicht bestätigt haben; ein Overblocking lasse sich empirisch nicht belegen. Vielmehr gebe es (nicht belegbare) Indizien für ein Underblocking, das auch durch die Praxis der Meldeverfahren mit hohen inhaltlichen und/oder formalen Anforderungen begünstigt werde.<sup>64</sup> Eine eigene quantitative Auswertung lag der Evaluation allerdings nicht zugrunde. Der Autor des Berichts fasst seine Erkenntnisse folgendermaßen zusammen: *„Die ursprünglich weit verbreitete Annahme, das NetzDG führe zu systematischem Overblocking, bleibt damit ohne umfassende inhaltliche Evaluation bloße Spekulation und erscheint angesichts mangelnder Hinweise aus den sensibilisierten Kreisen der Betroffenen oder der beobachtenden Medien unplausibel.“*<sup>65</sup>

Im NetzDG ist, wie auch im DSA-E, das Overblocking nicht ausdrücklich normiert. Es wird auch nach den **Bußgeldvorschriften** des NetzDG nicht explizit sanktioniert. In den **Bußgeldleitlinien** des Bundesjustizministeriums zum NetzDG wird das Problem des Underblocking, das letztlich zum Verlust der Haftungserleichterung führt, ausdrücklich behandelt; das Overblocking wird dort aber durch die „gebotene systemische Betrachtungsweise“ von Fehlentscheidungen bei ungerechtfertigten Sperrungen oder Löschungen im Einzelfall von der Bußgeldandrohung ausgeklammert.<sup>66</sup>

<sup>61</sup> Marc Liesching, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes v. 15.6.2020, S. 10, abrufbar unter <https://www.bundestag.de/resource/blob/700788/83b06f596a5e729ef69348849777b045/liesching-data.pdf>; Liesching bezieht sich u.a. auf einen Bericht von YouTube, aus dem das Verhältnis zwischen NetzDG- und Community Standard-Löschungen im 2. HJ/2019 abzulesen ist.

<sup>62</sup> SPD-Bundestagsabgeordneter Jens Zimmermann; ähnlich HateAid-Mitarbeiterin Josephine Ballon, die die Gefahr des Underblocking für „weiterhin gängige Praxis“ hält, beide in: <https://www.euractiv.de/section/innovation/news/deutschland-fordert-nach-schaerfungen-beim-digital-services-act/>.

<sup>63</sup> Martin Eifert u.a., Evaluation des NetzDG Im Auftrag des BMJV, S. 53.

<sup>64</sup> Eifert, a.a.O.

<sup>65</sup> Eifert, S. 54.

<sup>66</sup> NetzDG-Bußgeldleitlinien - Leitlinien zur Festsetzung von Geldbußen im Bereich des Netzwerkdurchsetzungsgesetzes (NetzDG) vom 22.3.2018 (S. 7 f.).

<sup>59</sup> s.o. Frage 1, Abschnitt 1.3.3.1.

<sup>60</sup> BT-Drucks. 18/12356 v. 16.5.2017, S. 23; die Vereinbarkeit der Fristen mit der ECRL ist nicht unumstritten.

## 2. Overblocking und der Digital Services Act

### 2.1 Anforderungen an Hinweise auf illegale Inhalte

**Anders als der Begriff der „rechtswidrigen Tätigkeit oder Information“ in der ECRL sind in Art. 2 lit. g DSA-E „illegale Inhalte“ definiert:**

*„alle Informationen, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit, einschließlich des Verkaufs von Produkten oder der Erbringung von Dienstleistungen, nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften“.*

In Art. 14 Abs. 2 DSA-E verwendet die Kommission davon abweichend den Begriff der „Rechtswidrigkeit der fraglichen Inhalte“. Was eine „rechtswidrige Tätigkeit“ (Art. 5 Abs. 1 lit. a DSA-E) ist, ist im Verordnungsentwurf nicht näher bezeichnet.

Gegenüber der bisherigen Rechtslage – keine Legaldefinition der rechtswidrigen Information in der ECRL – gewinnt der Rechtsanwender mit dem Digital Services Act – Legaldefinition des illegalen Inhalts – jedenfalls ein Stück weit an Rechtssicherheit. Dass der unbestimmte Rechtsbegriff dabei vage bleibt, ist vor allem dem Umstand geschuldet, dass neben der Verletzung europäischer Vorschriften eben auch solche des nationalen Rechts erfasst sein sollen. Und die können im Rahmen einer Verordnung, die nicht in nationales Recht umzusetzen ist, freilich nur abstrakt umschrieben werden.

Der unbestimmte Rechtsbegriff des illegalen Inhalts ist bei der Rechtsanwendung auszufüllen. Dafür hätten sich manche mehr Anleitung im DSA gewünscht, um einerseits die Rechtssicherheit für die Diensteanbieter zu erhöhen und andererseits der Gefahr eines Overblockings entgegenzuwirken.<sup>67</sup>

Dass die Ausfüllung des unbestimmten Rechtsbegriffs neben den EU-rechtlichen Vorgaben anhand der unterschiedlichen nationalen Gesetzgebung erfolgen wird, liegt auf der Hand. So werden Nutzerinnen und Nutzer wie auch die zuständigen Behörden die jeweils in ihrem Mitgliedstaat anwendbaren Maßstäbe zugrunde legen. Für die Diensteanbieter bedeutet das aber, dass sie die im Binnenmarkt verfügbaren Inhalte an den Maßstäben des EU Rechts sowie am nationalen Recht sämtlicher Mitgliedstaaten messen müssen. Welches nationale Recht im Einzelfall für sie anwendbar ist, wird sich nach dem Sitzland oder dem Wohnort derjenigen richten, die eine Meldung nach Art. 14 DSA-E erstatten. Oder sie haben das Recht des Mitgliedstaates derjenigen Justiz- oder Verwaltungsbehörde zu beachten, die eine Anordnung nach Art. 8 DSA-E erlassen hat.

In Erwägungsgrund 12 DSA-E stellt die Kommission klar, dass sie ihrem Verordnungsvorschlag einen weit gefassten Begriff der illegalen Inhalte zugrunde legt. Er umfasse auch Informationen im Zusammenhang mit illegalen Inhalten, Produkten,

Dienstleistungen oder Tätigkeiten. Insbesondere solle er so ausgelegt werden, dass er sich auf Informationen unabhängig von ihrer Form beziehe. Das schließe neben den an sich rechtswidrigen Inhalten (zum Beispiel terroristische Inhalte) auch mit rechtswidrigen Handlungen zusammenhängende Inhalte (zum Beispiel Darstellung von Kindesmissbrauch, Verkauf gefälschter Produkte, Verstoß gegen das Verbraucherschutzrecht) mit ein. Anhaltspunkte dafür, dass insoweit eine Änderung gegenüber der „rechtswidrigen Tätigkeit oder Information“ der ECRL angestrebt ist, sind nicht ersichtlich.

Der Begriff des illegalen Inhalts im Digital Services Act ist damit deutlich weiter als die Definition eines rechtswidrigen Inhalts in § 1 Abs. 3 NetzDG. Das bedeutet, dass (nur) bei Vorliegen der im NetzDG aufgeführten Straftatbestände die Verpflichtungen nach dem NetzDG neben denen nach dem DSA zu erfüllen sind.

Zu Hinweisen auf illegale oder auch gegen Gemeinschaftsstandards verstoßende Inhalte ist **jeder berechtigt**, der DSA-E enthält insoweit keine Einschränkung.<sup>68</sup> Wie im Urheberrecht könnte das dazu führen, dass Dritte, die zum Beispiel keine Kenntnis von einer Lizenzvereinbarung zwischen dem Rechteinhaber und dem betroffenen User haben oder fälschlich von der persönlichkeitsverletzenden Veröffentlichung eines Fotos ausgehen, einen überflüssigen, lästigen und rechtlich nicht haltbaren Hinweis platzieren. Dieser kann zu einer ungerechtfertigten Sperrung oder Löschung, also zum **Overblocking** führen.

Andererseits haben Hinweisgeber gemäß Art. 14 Abs. 2 lit. a DSA-E konkret zu **begründen**, weshalb sie den beanstandeten Inhalt für rechtswidrig halten. Ein solcher Begründungszwang, verbunden mit den übrigen Anforderungen des Art. 14 DSA-E, soll nicht nur den Diensteanbietern die Arbeit erleichtern. Er soll auch eine ernsthafte Auseinandersetzung der Hinweisgeberinnen und Hinweisgeber mit den Inhalten erforderlich machen, für die sie eine Löschung oder Sperrung erwirken wollen, mithin eine **extensive Hinweispraxis vermeiden**. Dieser Begründungszwang darf jedoch durch die Diensteanbieter nicht so weit ausgedehnt werden, dass sie von ihren Hinweisgebern fordern, konkrete Straftatbestände oder andere verletzte Rechtsnormen zu benennen. Denn wie bei einer Anzeige bei einer Polizeibehörde von den Bürgerinnen und Bürgern nicht erwartet wird, dass sie benennen können, gegen welche Strafvorschrift ein angezeigter Täter ihrer Auffassung nach verstoßen hat, so kann das auch bei einer Meldung gegenüber einem privaten Diensteanbieter nicht verlangt werden.

So wie das europäische Verbraucherrecht durch eine verpflichtend verfügbar zu machende Musterklärung den einzelnen davor schützen will, von seinem Recht auf Widerruf mangels einschlägiger Rechtskenntnis keinen Gebrauch zu machen<sup>69</sup>, so sollte auch niemand vor einem Hinweis an einen Diensteanbieter zurückschrecken müssen, weil die eigene Sachkenntnis zur rechtlichen Einordnung illegaler Inhalte

<sup>67</sup> Z. B. Stellungnahme des Bundesverbands Digitale Wirtschaft zum DSA-E vom 30.3.2021, [https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitalpolitik/BVDWStellungnahmeDigitalServicesAct30032021\\_final.pdf](https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitalpolitik/BVDWStellungnahmeDigitalServicesAct30032021_final.pdf).

<sup>68</sup> Die Meldewege haben vorzugeben, dass die Hinweisgeber unter ihrem Klarnamen auftreten; lediglich für kinderpornographische Delikte ist keine Identifikation erforderlich, Art. 14 Abs. 2 lit. c DSA-E.

<sup>69</sup> Art. 6 Abs. 1 lit. h Richtlinie 2011/83/EU.

fehlt. Schließlich ist es eine Sache, den Diensteanbietern eine Mitwirkung an der Beseitigung rechtswidriger Zustände aufzuerlegen, die sie durch ihr Angebot erst ermöglichen oder befördern. Aber eine Mitwirkung im Sinne juristischer Einschätzungen von denjenigen zu verlangen, die durch ihre Meldung den Diensteanbieter lediglich zum Handeln veranlassen, würde über das Ziel hinausschießen. Das gilt insbesondere deshalb, weil erst die qualifizierte, also eine im Sinne des DSA hinreichend genaue und angemessen begründete Meldung, die Kenntnisnahmefiktion des Art. 14 Abs. 3 DSA-E auslöst (siehe unten 2.2).

Zugleich gibt Art. 14 DSA-E einen Rahmen vor, um ausufernde Informationsanforderungen (zum Beispiel Arbeitgeber oder Beruf des Hinweisgebers) der Diensteanbieter einzudämmen. Dass die Meldewege leicht zugänglich und benutzerfreundlich zu sein haben, ähnelt den Vorgaben des § 3 NetzDG. Die praktische Umsetzung dieser Voraussetzungen ist noch verbesserungswürdig.<sup>70</sup>

### 2.2 Kenntnisnahmefiktion des Art. 14 Abs. 3 DSA-E

Art. 14 Abs. 3 DSA-E regelt für die Hosting-Dienste, dass eine qualifizierte Meldung, die den inhaltlichen Anforderungen des Art. 14 Abs. 2 DSA-E genügt, bewirkt, dass die Kenntnis des Diensteanbieters fingiert wird. Anhaltspunkte dafür, dass diese Vermutung widerlegbar ist, sind nicht ersichtlich. Problematisch könnte sein, dass auch bei einem großen Aufkommen von Meldungen die Kenntnisnahmefiktion die Pflicht zum Handeln nach Art. 5 Abs. 1 DSA-E auslöst. Allein der Eingang qualifizierter Meldungen könnte demnach Betreiber digitaler Dienste zwar unter Zugzwang setzen und **Overblocking begünstigen**. Aber insoweit ist die Rechtslage nicht anders als unter der ECRL.

### 2.3 „Zügiges“ Handeln nach Kenntnisnahme

Im DSA-E ist wie nach der ECRL eine konkrete **Frist** für das Entfernen oder Sperren illegaler Inhalte nicht vorgesehen. Stattdessen muss der Anbieter, um in den Genuss der Haftungsbefreiung zu kommen, nicht mehr „unverzüglich“ nach Kenntnisnahme vom rechtswidrigen Inhalt (Wortlaut des Art. 14 Abs. 1 ECRL), sondern **„zügig“** danach tätig werden (Wortlaut des Art. 5 Abs. 1 lit b DSA-E). „Unverzüglich“ ist künftig noch der zuständigen Justiz- oder Verwaltungsbehörde mitzuteilen, welche Maßnahme wann auf die Anordnung zum Vorgehen gegen einen bestimmten illegalen Content ergriffen wurde. „Unverzüglich“ ist der meldenden Person oder Einrichtung außerdem eine Empfangsbestätigung zu senden und eine Begründung der Entscheidung über die Meldung mitzuteilen. „Zeitnah“ ist nach Art. 14 Abs. 6 DSA-E der Vorgang zu bearbeiten. Was mit der sprachlichen Änderung von „unverzüglich“ in der ECRL hin zu „zügig“ im DSA für die Haftungsbefreiung beabsichtigt wurde, ist **unklar**. Das gilt insbesondere deshalb, weil in Erwägungsgrund 22 DSA-E wieder beschrieben ist, dass Hosting-Dienste für den Haftungsausschluss „unverzüglich“ tätig werden sollten.

Die Ausfüllung dieser inkonsistent im Verordnungsentwurf verwendeten unbestimmten Rechtsbegriffe im Sinne einer Festlegung bestimmter Fristen im nationalen Recht würde, wie oben<sup>71</sup> ausgeführt, nach hiesiger Auffassung **gegen europäisches Recht verstoßen**. Doch sei an dieser Stelle erneut darauf hingewiesen, dass diese Frage umstritten ist.

Dass eine konkrete Reaktionsfrist im Rahmen des *Notice and Action*-Verfahrens im DSA nicht vorgesehen ist, könnte ein vorschnelles Reagieren aus Gründen der Übervorsicht bei den digitalen Diensten begünstigen – jedoch wohl nicht mehr als nach bisheriger Rechtslage unter der ECRL. Denn wo „zügig“ ähnlich wie „unverzüglich“ verstanden werden soll, weiß ein Rechtsanwender zumindest in Deutschland, dass er „ohne schuldhaftes Zögern“ zu agieren hat (§ 121 BGB). Das muss nicht, kann aber zu (rechts-)sicherheitsorientiertem Overblocking führen, das schließlich anders als das Underblocking, also Untätigkeit nach Kenntnisnahme, nicht sanktioniert wird. Zu eng gesetzte konkrete Fristen, namentlich solche ohne Differenzierung nach Komplexität und Bedeutung der gemeldeten Angelegenheiten, könnten freilich ebenfalls zu Inhaltssperrungen ohne vorherige sorgfältige Abwägungen führen. Andererseits fehlen nach der Auswertung der bisherigen Anwendungspraxis des NetzDG belastbare Erkenntnisse dazu, dass die Festsetzung bestimmter Reaktionsfristen zu einer Vermeidung von Overblocking führen und auch wie lang angemessene Fristen zu diesem Zweck sein müssten.

### 2.4 Begründungszwang bei Löschung oder Sperrung

Art. 15 DSA-E verpflichtet alle Hosting-Dienste, Entscheidungen über das Löschen oder Sperren von nutzergeneriertem Content dem jeweiligen User mitzuteilen. Die Mitteilung ist mit einer Begründung der Entscheidung zu versehen, deren Inhalt in Art. 15 Abs. 2 DSA-E näher spezifiziert ist.

Dass die Anbieter gemäß Art. 15 Abs. 4 DSA-E verpflichtet werden, ihre Lösch- und Sperrentscheidungen nebst Begründung (um personenbezogene Daten bereinigt) in einer öffentlich zugänglichen **Datenbank** zu publizieren, kann insofern ein Beitrag gegen ein Overblocking sein, als auch Dritte, sogar Nicht-Nutzerinnen und -Nutzer des Dienstes diese Entscheidungen und Begründungen einsehen können.

Eine **Begründung für Untätigkeit** ist dagegen auf die Meldung eines Hinweisgebers hin nach dem DSA-E **nicht** einmal dann erforderlich, wenn es sich um einen *trusted flagger* handelt.<sup>72</sup> Jedoch verliert bekanntlich der Hosting-Diensteanbieter, der auf eine Meldung hin, also nach mindestens fiktiver Kenntnisnahme eines illegalen Inhalts, untätig bleibt, seine Haftungsbefreiung.

### 2.5 Internes Beschwerdemanagement

Das interne **Beschwerdemanagement**-System, das (nur) Online-Plattformen vorzuhalten haben (Art. 17 DSA-E), soll die Überprüfung von Entscheidungen über die Sperrung oder Lö-

<sup>71</sup> Frage 1, Abschnitt 1.3.3.1.

<sup>72</sup> Das Beschwerdeverfahren nach dem NetzDG enthält dagegen in jedem Fall einen Begründungszwang gegenüber dem Beschwerdeführer sowie dem Nutzer, § 3 Abs. 2 Ziff. 5 NetzDG.

schung von Inhalten und Nutzerkonten wegen Rechtswidrigkeit oder wegen Verstoßes gegen Community Standards gewährleisten. Wenn Art. 17 Abs. 3 DSA-E auf die Verpflichtung der Plattform verweist, ihre Entscheidung über Sperrung oder Löschung von Inhalten oder über das Aussperren einer Nutzerin „unverzögerlich rückgängig“ zu machen, kann damit nur die **Wiederherstellung** des Inhalts oder die Wiederaufnahme des Leistungsangebotes an die Nutzerinnen und Nutzer gemeint sein. Anderenfalls wäre das Beschwerdeverfahren für die Nutzerin sinnlos.

Soweit der Beschwerde entsprochen wird, genügt im Umkehrschluss aus Art. 17 Abs. 5 DSA-E eine automatisierte Entscheidung. Die Ablehnung des Gesuchs muss mindestens auch durch eine Person entschieden werden; Nutzerinnen und Nutzer sind auf die Möglichkeit der außergerichtlichen Streitbeilegung (Art. 18 DSA-E) hinzuweisen.

Dieses Verfahren soll dazu beitragen, dass jedenfalls zu Unrecht erfolgte Maßnahmen der Inthementation geheilt werden. Es kann zugleich einem extensiven Löschen oder Sperren von Inhalten und Accounts präventiv entgegenwirken. Ob und in welchem Umfang diese Maßnahme wirksam ist, lässt sich schwerlich feststellen, ohne dass auf empirische Erkenntnisse insbesondere über die Anwendung des § 3 b NetzDG zurückgegriffen werden kann.

## 2.6 Bußgeldandrohung

Auch die Bußgeldandrohung, insbesondere die Androhung der Geldbußen, die die EU-Kommission gegen sehr große Online-Plattformen verhängen kann, ist Teil der Maßnahmen gegen Overblocking. Nach Art. 59 DSA-E soll die Kommission vorsätzliche und fahrlässige Verstöße „gegen die einschlägigen Bestimmungen dieser Verordnung“ mit empfindlichen Geldbußen belegen können. Dazu gehört auch Art. 12 Abs. 2 DSA-E, nach dem die Anbieter von Vermittlungsdiensten bei der Anwendung und Durchsetzung ihrer AGB und Community Standards ausdrücklich die **Grundrechte** der Nutzerinnen und Nutzer zu wahren haben.

Selbst wenn man der Auffassung folgt, das Overblocking erfordere eine systemische Betrachtungsweise und sei per definitionem keine einzelfallbezogene Erscheinung, so wäre doch ein ergänzender **zivilrechtlicher Schadenersatzanspruch** für Fälle des ungerechtfertigten Löschens, Sperrens oder Aussperrens empfehlenswert und dem Grundrechtsschutz zuträglich.<sup>73</sup> Er könnte die Anbieter digitaler Dienste zu weiterer Sorgfalt veranlassen, ein Overblocking zu vermeiden. Der Anspruch sollte unabhängig von Androhung und Verhängung von Bußgeldern geltend gemacht werden können und für Fälle besonders gravierender Fehlentscheidungen in der Anwendung der eigenen Gemeinschaftsstandards oder in Folge einer Meldung zur Verfügung stehen. Er sollte (wie die DSGVO) materielle und immaterielle Schäden erfassen.

## 2.7 Trusted Flaggers

Art. 19 DSA-E sieht eine besondere Stellung von **vertrauenswürdigen Hinweisgebern, sogenannten *trusted flaggers***, vor.<sup>74</sup> Deren Hinweise auf rechtsverletzende Inhalte sind bevorzugt zu behandeln. Der Status als vertrauenswürdiger Hinweisgeber wird vom nationalen Koordinator für digitale Dienste wieder aberkannt, wenn sich die betreffende Stelle als unzuverlässig erweist. Das soll nach Art. 19 Abs. 5 f. DSA-E gelten, wenn ein *trusted flagger* eine erhebliche Anzahl nicht hinreichend präziser oder unzureichend begründeter Meldungen übermittelt hat. Dass der Koordinator insoweit auch auf Grund entsprechender Hinweise **Dritter**, insbesondere betroffener Nutzerinnen und Nutzer, tätig werden und gegebenenfalls den Status widerrufen muss, gibt den Usern ein neues, möglicherweise sehr wirksames Schwert gegen ungerechtfertigtes Sperren und Löschen in die Hand.

## 2.8 Maßnahmen gegen missbräuchliche Hinweise

Nach Art. 20 Abs. 2 DSA-E sind die Betreiber von Online-Plattformen verpflichtet, die Bearbeitung von Meldungen und Beschwerden eine Zeitlang auszusetzen, die von Personen oder Stellen stammen, die „häufig offensichtlich unbegründete Meldungen oder Beschwerden einreichen“. Sie haben die Betroffenen vorher darauf hinzuweisen.

Auf diese Weise werden die Betreiber zunächst veranlasst, überhaupt zu identifizieren, welche Quellen durch häufige offensichtlich unbegründete Hinweise oder Beschwerden auffallen. Und die Vorschrift kann jedenfalls einen Beitrag zum **Schutz redlicher Nutzerinnen und Nutzer** leisten, Opfer gezielter Attacken aus einem bestimmten Meinungsspektrum zu werden.

**Frage 2b: Kann das geplante Haftungsregime zu einer (weiteren) **Privatisierung der Auslegung** und Sanktionierung von Content über die Grenzen der Meinungsfreiheit hinaus beitragen? Welche rechtliche Bedeutung würde und sollte Community Standards/Nutzungsbedingungen der Anbieter zukommen?**

### Zusammenfassende Antwort

Sehr große Online-Plattformen soll die Pflicht zur Risikobewertung und -minimierung auferlegt werden. Inhalt und Maßstäbe für die Erfüllung dieser Pflicht bleiben im Verordnungsentwurf zu vage. Darüber hinaus sind im Entwurf Verpflichtungen zur rechtlichen Bewertung der Inhalte vorgesehen, die von Nutzerinnen und Nutzern hochgeladen werden. Dabei soll der Anbieter betroffene Grundrechte gegeneinander abwägen und Datenschutzbestimmungen einhalten. (Möglicherweise) illegale Inhalte werden dem Anbieter von privaten Nutzerinnen und Nutzern oder Einrichtungen zur Kenntnis gebracht. Diese lösen eine verpflichtende Rechtsprüfung durch den privaten Anbieter auf Grund ihrer eigenen rechtlichen Expertise aus. Die eigenen Nutzungsbedingun-

<sup>73</sup> Vgl. Frage 1, 1.5 Harmonisierung durch teilweise vereinheitlichten Sanktionsrahmen.

<sup>74</sup> Vgl. Frage 3, 3. Verpflichtende Maßnahmen im DSA-E.

gen des Diensteanbieters gewinnen durch den Regulierungsrahmen im DSA an Bedeutung. Sie unterliegen nicht nur der Grundrechtsbindung, sondern auch der AGB-Kontrolle des jeweiligen Mitgliedstaates. Wo bestimmte Straftaten einer Meldepflicht durch den Anbieter unterliegen, sind anspruchsvolle rechtliche Einschätzungen von einem privaten Unternehmer vorzunehmen.

### 1. Risikobewertung und -minderung

In Art. 26 DSA-E ist für sehr große Online-Plattformen vorgesehen, dass sie mindestens jährlich eine **Bewertung** aller „erheblichen systemischen Risiken“ vornehmen, die sich aus dem Betrieb und der Nutzung ihrer Dienste ergeben. Dazu gehört auch der Blick auf die Wahrung der Grundrechte einschließlich der Kommunikationsfreiheit. Auf der Grundlage dieser Einschätzung haben die Betreiber Einzelmaßnahmen zur Risikominderung vorzunehmen, Art. 27 DSA-E.

Problematisch an dieser Verpflichtung zur Risikobewertung ist jedoch, dass sie **keine klaren Anforderungen** enthält. „Alle erheblichen systemischen Risiken, die sich aus dem Betrieb und der Nutzung ihrer Dienste ergeben“ legt einen denkbar unbestimmten Bewertungsumfang fest, der auch durch die genannten Kategorien

- Verbreitung illegaler Inhalte
- nachteilige Auswirkungen auf die Grundrechtsausübung
- vorsätzliche Manipulationen des Dienstes

kaum zu fassen ist. Das gilt insbesondere deshalb, weil diese drei Risikobereiche in einem **Spannungsfeld** zueinander stehen. Die Verbreitung illegaler Inhalte einerseits und die Ausübung der Kommunikationsfreiheit andererseits ist der Kern des Konflikts, den es durch den DSA zu lösen gilt. Diese hochkomplexe Aufgabe den Diensteanbietern ohne weitere Anleitung zu übertragen, muss diese **zwangsläufig überfordern**. Leitlinien für die Risikominderung „können“ nach Art. 27 Abs. 3 DSA-E lediglich erstellt werden. Der Entwurfstext legt nahe, dass die Ausarbeitung von Leitlinien in Zusammenarbeit mit den nationalen Koordinatoren für digitale Dienste und nach öffentlicher Konsultation im Sinne einer beispielhaften Auflistung von *best practices* beabsichtigt ist. Eine solche würde jedenfalls einen Beitrag zur einheitlichen Anwendung des Digital Services Act in Bezug auf die zentrale Verpflichtung zur Risikominderung leisten. Eine Rechtspflicht zur Erarbeitung von Leitlinien, ähnlich wie in Art. 17 Abs. 10 DSM-RL, ist zu erwägen.

In Bezug auf die Erfüllung der Verpflichtungen zur Risikoeinschätzung und -minimierung hilft der Blick in das europäische Datenschutzrecht nicht. Denn die Pflicht zur Risikoevaluierung und Folgenabschätzung des Verantwortlichen nach Art. 35 DSGVO, zu der übrigens der fachliche Rat des Datenschutzbeauftragten obligatorisch einzuholen ist<sup>75</sup>, knüpft an konkrete Verarbeitungsvorgänge an. Sind diese tatbestandlich erfüllt, ist das Risiko, das der Verantwortliche durch sein Tun selbst setzt, mit den Interessen der betroffenen Person(en)

abzuwägen. Für die Vornahme und Dokumentation der datenschutzrechtlichen Risikobewertung gibt die DSGVO ein Verfahren unter Einbezug der zuständigen Aufsichtsbehörde vor. Außerdem ist in Art. 36 DSGVO die Rechtsfolge der Feststellung eines hohen Risikos für die Rechte und Freiheiten der Betroffenen geregelt: Der Verantwortliche hilft selbst ab (ähnlich Art. 27 Abs. 1 DSA-E) oder konsultiert die Aufsichtsbehörde. Diese empfiehlt Verbesserungen und macht gegebenenfalls von ihren Eingriffsbefugnissen Gebrauch.

Demgegenüber eröffnet die an die eigene allgemeine, nicht konkret funktionsbezogene Risikobewertung (und deren Publikation, Art. 33 DSA-E) geknüpfte Pflicht zur Risikominderung gemäß Art. 27 DSA-E einen weiten Ermessensspielraum sowohl für die Anbieter als auch für die Koordinatoren oder die Kommission. Greifbare Konsequenzen aus festgestellten Risiken fehlen, spezifische Sanktionen bei Missachtung oder unzureichender Erfüllung der Risikobewertung und -minderung sind nicht festgeschrieben.

### 2. Haftung von Plattformbetreiber und Nutzerinnen und Nutzern

Grundsätzlich nimmt die EU-Kommission ausweislich der Erwägungsgründe die Perspektive ein, dass das Problem illegaler Inhalte und Tätigkeiten im Netz nicht allein durch eine Regulierung der Haftung der Intermediäre bewältigt werden solle. Stattdessen sollten von rechtsverletzenden Inhalten betroffene Dritte versuchen, **Konflikte untereinander** und gegebenenfalls offline beizulegen. Das impliziert auch eine Haftung vor allem derjenigen, die rechtswidrige Inhalte generieren: der Nutzerinnen und Nutzer selbst.<sup>76</sup> Doch eine konkrete Verankerung dieses Grundverständnisses einer Subsidiarität der Haftung der Vermittler fehlt im Verordnungstext.

So bleibt es dem Grunde nach bei dem Haftungsregime der ECRL, nach dem für Rechtsverletzungen Dritter Vermittlungsdienste haften, soweit ihnen **eigenes Fehlverhalten** vorgeworfen werden kann. Das besteht, soweit es um die Haftung für rechtswidrige Inhalte geht, entweder in einer aktiven Beteiligung an der Verbreitung illegalen Contents<sup>77</sup> oder in einem Verstoß gegen die Verhaltensregeln zur Befreiung von der Haftung (*Notice and Action*-Verfahren). Daneben kommen nach der Rechtsprechung des EuGH und des BGH zur ECRL beziehungsweise zum TMG in Bezug auf Unterlassungsansprüche auch die Grundsätze der Störerhaftung in Betracht.<sup>78</sup> Das soll sich ausweislich der Erwägungsgründe auch unter dem DSA nicht ändern.<sup>79</sup>

Dieses Haftungsregime wird ergänzt durch die ausdrückliche Klarstellung, dass freiwillige Untersuchungen **auf eigene Initiative** der Vermittlungsdienste **nicht zu einer Verschärfung** des Haftungsmaßstabs führen (Art. 6 DSA-E). Der EuGH hat jüngst seine Rechtsprechung zu Art. 14 ECRL in diesem Sinne

<sup>76</sup> ErwGrd. 26 DSA-E.

<sup>77</sup> ErwGrd. 18 DSA-E.

<sup>78</sup> EuGH C-484/14 v. 15.9.2016 McFadden/Sony, BGH I ZR 304/01 v. 11.3.2004 Internet-Versteigerung I, BGH I ZR 35/04 v. 19.4.2007 Internet-Versteigerung II.

<sup>79</sup> ErwGrd. 24 DSA-E; Gerald Spindler, Der Vorschlag für ein neues Haftungsregime für Internetprovider - der EU-Digital Services Act, Teil 1, GRUR 2021, 545 (550).

<sup>75</sup> Für sehr große Online-Plattformen ist die Einbeziehung von unabhängigen Sachverständigen nur als Empfehlung in ErwGrd. 59 formuliert.

im urheberrechtlichen Kontext bestätigt. In den verbundenen Verfahren *Petersen/Google* und *Elsevier/Cyando* hat das Gericht ausgeführt, dass wenn der Betreiber einer Videosharing-Plattform [Anm.: rein] technische Maßnahmen anwendet, um urheberrechtsverletzende Inhalte zu erkennen, dies nicht bedeutet, dass er damit eine aktive Rolle übernimmt, die ihm im Rechtssinne Kenntnis vom Inhalt dieses Contents oder Kontrolle darüber verschafft.<sup>80</sup> Etwas anderes gilt bloß, wenn der Betreiber die Inhalte inhaltlich-redaktionell überprüft.<sup>81</sup>

Das deutsche Recht regelt eine haftungsbegründende Beteiligung des Betreibers einer Videosharing-Plattform bisher nur für **Urheberrechtsverletzungen** und nur für bestimmte Plattformen in § 1 Abs. 1 UrhDaG. Denn dort ist die öffentliche Wiedergabe nutzergenerierter Inhalte durch den Plattformbetreiber normiert und auf diesem Wege eine eigene Verantwortlichkeit des Plattformbetreibers begründet.

Die bisherige Haftungserleichterung für Hosting-Diensteanbieter einschränkend, hat die Kommission in Art. 5 Abs. 3 DSA-E eine Ausnahme für den Fall eingefügt, dass der Verbraucher bei einem Marktplatz-Angebot davon ausgehen kann, das **Angebot stamme vom Plattformbetreiber** selbst. Auch hier geht es darum, nicht allein darauf zu schauen, wer etwas konkret hochgeladen hat. Sondern auch der Betreiber, dem ein Inhalt auf Grund des Anscheins vom durchschnittlichen Nutzer zugeordnet wird, soll sich nicht auf die Haftungsfreistellung des DSA berufen können.

### 3. Voraussetzungen für Notice and Action

Wie bisher unter der ECRL wird auch im DSA-E für die Haftungsbefreiung des Hosting-Diensteanbieters auf dessen **tatsächliche Kenntnis** von einer rechtsverletzenden Tätigkeit oder einem illegalen Inhalt sowie auf die **Offensichtlichkeit** der Rechtswidrigkeit von durch sie vermittelten Tätigkeiten oder Inhalten abgestellt, Art. 5 Abs. 1 lit. a DSA-E. Dass im DSA nicht zwischen offensichtlich rechtswidrigen Inhalten und anderen differenziert wird, zeigt, dass die Kommission insoweit keine allzu hohen Anforderungen an die rechtliche Sachkenntnis der privaten Anbieter stellen will. Sie brauchen nur zu unterscheiden, was nach ihrer positiven Kenntnis oder nach ihrem Verständnis „offensichtlich“ rechtmäßig und was rechtswidrig ist.

Das ist letztlich Folge der Vermengung von Durchgriffsbefugnissen. Wenn Private in die Verfolgung und Durchsetzung allgemeiner Rechtsvorschriften (aus guten Gründen) eingebunden werden, dann sind dabei an sie angemessene Anforderungen zu stellen (und besondere Rechtsschutzverfahren vorzusehen). Positive Kenntnis einer rechtswidrigen Tätigkeit oder eines illegalen Inhalts ist nicht leicht zu erlangen. Die Offensichtlichkeit als Merkmal im Befugnistatbestand zieht aber eine Grenze, die Beliebigkeit in der rechtlichen Beurtei-

lung wirksam eindämmt. Sie hat sich als Kriterium für eine rechtlich relevante Einschätzung durch die Allgemeinheit in anderen rechtlichen Zusammenhängen bewährt.<sup>82</sup>

Nach Art. 15 Abs. 1 ECRL, der in Art. 7 DSA-E fortgeführt wird, dürfen die Mitgliedstaaten Anbietern von Vermittlungsdiensten ausdrücklich **keine allgemeinen Verpflichtungen zur Überwachung** oder zu aktiven Nachforschungen hinsichtlich möglicherweise rechtswidriger Inhalte auferlegen. Ohne eine solche verpflichtende Inhaltskontrolle beschränkt sich die Vorwerfbarkeit gegenüber Diensteanbietern auf ein Nichthandeln trotz Hinweises von außen – also durch die eigenen Nutzerinnen und Nutzer oder durch Dritte. Ein eigenes Bemühen um die Vermeidung rechtswidriger Inhalte auf der eigenen Plattform befördert das Merkmal der tatsächlichen Kenntnis dagegen nicht.<sup>83</sup>

Das NetzDG soll das bisher dadurch auffangen, dass auf Grundlage des Art. 15 Abs. 2 ECRL eine bestimmte Behandlung von Beschwerden vorgeschrieben ist. Aber dieser Spielraum für die Konkretisierung des Digital Services Act ist in dem Entwurf bislang nicht vorgesehen (vgl. Frage 1, 1.3.3.2 b).

## 4. AGB und Gemeinschaftsstandards

### 4.1 AGB und Gemeinschaftsstandards im Lichte der Grundrechte

Fraglich ist, welche Bedeutung neben der regulierten Sanktionierung von Rechtsverstößen durch die Vermittler deren Allgemeinen Geschäftsbedingungen und Gemeinschaftsstandards (Community Standards) zukommt.<sup>84</sup> Das hängt maßgeblich davon ab, wie das Gefüge zwischen den Grundrechten der Nutzerinnen und Nutzer einerseits, die wegen ihrer mittelbaren Drittwirkung auch vom Plattformbetreiber zu beachten sind, und den Grundrechten der Diensteanbieter<sup>85</sup> andererseits verstanden wird.

Die Unternehmen, die Plattformen betreiben, dürfen nach verbreiteter Auffassung in Deutschland auf Grund ihres virtuellen Hausrechts auch solche Inhalte ihrer User sperren oder löschen, die nicht rechtswidrig sind, sondern lediglich gegen die eigenen Community Standards verstoßen.<sup>86</sup> Die Grenze wird gemeinhin dort gezogen, wo für die Löschung kein sachlicher Grund besteht oder wo eine bestimmte Meinung sanktioniert wird. Auch ist der Verhältnismäßigkeitsgrundsatz insbesondere dort zu beachten, wo es um die Abwägung der Mittel (nur) Inhaltslöschung oder (gar) Account-Sperrung geht.<sup>87</sup>

<sup>80</sup> EuGH Rechtssache C-682/ und C-683/18, Rz. 109.

<sup>81</sup> EuGH, Rechtssache C-682/ und C-683/18, Rz. 115; vergleichbar BGH GRUR 2015, 1129 (1132) Hotelbewertungsportal, wo das Gericht ein Zu-Eigen-Machen von Inhalten Dritter i.S.d. § 4 Nr. 8 UWG als Tatsachenbehauptung durch den Portalbetreiber ablehnt, wenn dieser die Äußerungen nicht inhaltlich-redaktionell aufbereitet oder ihren Wahrheitsgehalt überprüft.

<sup>82</sup> Z.B. „offensichtlich rechtswidrig hergestellte Vorlage“ in § 53 Abs. 1 S. 1 UrhG zur Eindämmung des rechtswidrigen Filesharings.

<sup>83</sup> Thomas Hoeren, Innovationsverantwortung und Haftung im Internet, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, S. 123 (128).

<sup>84</sup> AGB und Gemeinschaftsstandards stehen bei einigen Anbietern nebeneinander, teils sind sie miteinander verbunden; Gemeinschaftsstandards werden in jedem Fall auch an den §§ 305 BGB AGB gemessen. Sie enthalten i.d.R. inhaltliche Rahmenbedingungen, wie z.B. dass Spam, gewalttätige Inhalte, Hate Speech nicht hochgeladen werden dürfen und ggf. gelöscht werden. Teils wird für anstößige Inhalte schlicht ein Tagging vorgeschrieben, um andere Nutzer vor unpassenden Inhalten z.B. am Arbeitsplatz zu schützen.

<sup>85</sup> Namentlich Eigentumsfreiheit, Art. 14 GG, Berufsfreiheit, Art. 12 GG, Privatautonomie (Vertragsinhaltsfreiheit), Art. 2 Abs. 1 GG.

<sup>86</sup> Z.B. OLG Stuttgart, 4 W 63/18, Beschl. v. 6.9.2018; OLG Karlsruhe, 6 W 81/18, Beschl. v. 28.2.2019.

<sup>87</sup> OLG Dresden, 4 W 577/18, Beschl. v. 8.8.2018.

#### 4.2 AGB und Gemeinschaftsstandards im Digital Services Act

Für sämtliche Anbieter von Vermittlungsdiensten unabhängig von ihrer Reichweite ist vorgeschrieben, dass sie in ihren **Nutzungsbedingungen** offenlegen müssen, ob und unter welchen Voraussetzungen nutzergenerierte Inhalte vom Upload ausgeschlossen sind oder gesperrt beziehungsweise gelöscht werden, Art. 12 DSA-E. Das ist neu und anders als im NetzDG, das allein auf die Verletzung bestimmter Straftatbestände abstellt und keine Vorgaben bezüglich der eigenen Gemeinschaftsstandards der Anbieter macht. Die nach dem DSA-E verfügbar zu machenden Informationen umfassen auch Verfahren, Maßnahmen und Werkzeuge zur Moderation von Inhalten einschließlich algorithmischer Entscheidungsfindung und deren Überprüfung durch eine Person.

Ausdrücklich schreibt der DSA-E in diesem Zusammenhang die Verpflichtung zur Wahrung der **Grundrechte** der Nutzerinnen und Nutzer durch die Diensteanbieter vor. Diese Verpflichtung entspricht dem in Deutschland allgemeinen Verständnis der mittelbaren Drittwirkung der Grundrechte, wie das Bundesverfassungsgericht es 1958 im Lüth-Urteil<sup>88</sup> mit Verweis auf das Wertesystem des Grundgesetzes begründet und später im Hinblick auf Plattformen bestätigt<sup>89</sup> hat. Diese Verpflichtung dürfte vor allem dann beachtlich sein, wenn Anbieter aus **autoritären Regimen** oder mit fragwürdigem Moderationsverhalten auf Grund ihrer eigenen Gemeinschaftsstandards aus europäischer Sicht grundrechtswidriges Zensurverhalten in die EU zu übertragen versuchen. Beispielhaft sei hier nur die Unterdrückung regimekritischer Beiträge auf TikTok vor allem im Zusammenhang mit den Protesten in Hongkong 2019/20 oder mit dem Tian'anmen Massaker von 1989 genannt.<sup>90</sup>

Zum bisherigen Recht hat der BGH jüngst die deutsche Rechtsprechung bestätigt, dass Voraussetzung für die Rechtmäßigkeit einer Löschung oder Sperrung auf Grund eines Verstoßes gegen die eigenen Nutzungsbedingungen eines sozialen Netzwerks ist, dass die Nutzungsbedingungen ihrerseits als **allgemeine Geschäftsbedingungen rechtmäßig** sind, §§ 305 ff. BGB. Sie dürfen insbesondere die Nutzerinnen und Nutzer nicht unangemessen benachteiligen (§ 307 BGB).<sup>91</sup> Diese Rechtsprechung wird auch mit Inkrafttreten des DSA **weiterhin haltbar** sein.

In formeller Hinsicht ist im Verordnungsentwurf außerdem festgelegt, dass Maßnahmen, die auf Grund der AGB des digitalen Dienstes ergriffen werden, im Rahmen des nach Art. 13 DSA-E vorgeschriebenen **Transparenzberichts** gesondert aufzuführen sind. Auch auf Initiative des Anbieters durchgeführte Maßnahmen zur Moderation von Inhalten müssen Gegenstand des Berichts sein, Art. 13 Abs. 1 lit. c DSA-E. Die Dienste haben also separat zu berichten über

- die Entfernung und Sperrung von Informationen wegen deren Rechtswidrigkeit nach nationalem Recht oder Gemeinschaftsrecht und
- die Entfernung und Sperrung von Informationen wegen Verstoßes gegen die Community Standards.

Bei Online-Plattformen sind Entscheidungen auf Grund eines Verstoßes gegen die AGB Gegenstand des verpflichtenden internen **Beschwerdemanagement**-Systems. Private und gewerbliche Nutzerinnen und Nutzer können Beschwerden auf dieser Grundlage niedrigschwellig in einem kostenfreien Verfahren einreichen und gemäß Art. 17 Abs. 3 DSA-E erwirken, dass Entscheidungen über die Entfernung oder Sperrung eines Uploads oder über die Schließung eines Accounts rückgängig gemacht werden.

Aber die Betroffenen werden deshalb nicht von der Inanspruchnahme behördlicher und gerichtlicher Hilfe ausgeschlossen. Vielmehr werden die Plattformen als *cheapest cost avoider* in Anspruch genommen, um möglichst nachvollziehbar, effektiv und effizient Rechtsverletzungen abzustellen. Zur Entlastung staatlicher Durchsetzungsbehörden und Gerichte, die angesichts knapper Ressourcen und zunehmender Rechtsverletzungen auf Plattformen auf die Unterstützung durch diejenigen angewiesen sind, die selbst Teil des Problems sind, ist dieses Vorgehen verständlich. Im Sinne der Fragestellung bedeutet es eine weitere Privatisierung bei der Bewertung von Inhalten.

#### 5. Meldepflichten nach Art. 21 DSA-E

Mit der in § 3 a NetzDG vorgeschriebenen Verpflichtung sozialer Netzwerke vergleichbar, sieht Art. 21 DSA-E für alle Online-Plattformen eine Meldepflicht gegenüber den zuständigen Strafverfolgungs- oder Justizbehörden vor, wenn der Verdacht auf eine realisierte oder drohende strafrechtlich relevante Gefahr für Leben oder Sicherheit von Personen<sup>92</sup> besteht. Anders als das NetzDG mit seinen detaillierten Vorgaben etwa zum Inhalt der Meldung regelt Art. 21 DSA-E nur eine **allgemeine Mitwirkungspflicht** der Plattformbetreiber im Sinne der Zurverfügungstellung „*aller vorliegenden einschlägigen Informationen*“. Dazu gehören nach Erwägungsgrund 48 „*gegebenenfalls auch die jeweiligen Inhalte und eine Erläuterung ihres Verdachts*“.

Eingehegt wird die Verpflichtung durch den **Anwendungsvorhang der DSGVO** gemäß Art. 1 Abs. 5 DSA-E. Die Kommission stellt in den Erwägungsgründen klar, Art. 21 DSA-E sei kein Freibrief für die Erstellung von Nutzerprofilen für eine mögliche Feststellung von Straftaten. Denn die Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten von Nutzerinnen und Nutzern muss sich unverändert an den Vorgaben der DSGVO messen lassen, ohne dass sich der Diensteanbieter auf Art. 21 DSA-E im Sinne eines Erlaubnistatbestands berufen könnte.

Für die Anbieter bedeutet das in der praktischen Umsetzung eine hohe Anforderung an ihre juristische Expertise. Denn sie

<sup>88</sup> BVerfGE 7, 198.

<sup>89</sup> BVerfG 1 BvQ 42/19 Beschluss v. 22.5.2019.

<sup>90</sup> Vgl. <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>.

<sup>91</sup> III ZR 179/20 und III ZR 192/20 v. 29.7.2021 zu den Gemeinschaftsstandards von Meta in der inzwischen überholten Fassung v. 19.4.2019: Unwirksamkeit wegen fehlender Selbstverpflichtung, den Nutzer über die Entfernung seines Beitrags zumindest nachträglich und über eine beabsichtigte Sperrung seines Nutzerkontos vorab zu informieren, ihm den Grund dafür mitzuteilen und eine Möglichkeit zur Gegenäußerung mit anschließender Neubewertung einzuräumen und damit wegen unangemessener Benachteiligung der Nutzer.

<sup>92</sup> V.a. Kinderpornographie und sexueller Missbrauch von Kindern, ErwGrd. 48 DSA-E.

müssen einerseits ihren Meldepflichten nachkommen. Dabei werden sie zwangsläufig eine Vielzahl juristisch nicht haltbarer Anschuldigungen melden. Denn die Prüfung der möglicherweise einschlägigen Straftatbestände ist nicht eben trivial. Andererseits sind sie an die Vorgaben der DSGVO gebunden, dürfen also gerade keine personenbezogenen Daten ohne Erlaubnistatbestand erheben, verarbeiten oder gar an Strafverfolgungsbehörden weitergeben. Ein DSGVO-Verstoß ist nicht nur bußgeldbewehrt, sondern er kann auch zivilrechtliche Ersatzansprüche nach sich ziehen.

Auch darüber hinaus sind die **Anforderungen** an die Betreiber von Online-Plattformen sehr hoch geschraubt, wenn ihnen nur allgemein vorgegeben wird, sie mögen „auch andere anwendbare Vorschriften des Unionsrechts oder des nationalen Rechts zum Schutz der Rechte und Freiheiten von Einzelpersonen beachten, wenn sie die Strafverfolgungsbehörden informieren.“<sup>93</sup> Das gilt insbesondere vor dem Hintergrund, dass hierfür nicht nur die Rechte und Freiheiten des jeweiligen Users in Betracht kommen, dessen Upload gemeldet werden soll, sondern auch desjenigen, der von einer Rechtsverletzung betroffen sein könnte.

**Frage 2c: Wird mit den geplanten Haftungsregelungen ein „Überwachungsgebot“ für Plattformen konstituiert, das beispielsweise Uploadfilter für die Plattformbetreiber erforderlich macht?**

#### Zusammenfassende Antwort

Soweit es um urheberrechtlich geschützte Inhalte geht, werden die nationalen Regelungen zur Umsetzung der DSM-RL Anwendungsvorrang gegenüber dem DSA genießen. Hier sind bisher keine Vorschläge für eine rechtssichere Umsetzung ohne eine faktische Verpflichtung zur Überwachung von nutzergenerierten Uploads mittels Filtertechnik ersichtlich.

Im Übrigen werden Filtertechniken von der Kommission durchaus als probates Mittel für die „Erkennung von Inhalten“ erachtet, solange sie datenschutzkonform betrieben werden. Die Verpflichtung der Diensteanbieter, einer *Notice and Stay Down*-Anordnung Folge zu leisten, wird ohne eine gewisse Inhalteüberwachung nicht auskommen. Die Kommission will mit ihrem Verordnungsvorschlag ausdrücklich eine „geeignete Grundlage für die Entwicklung solider Techniken zur Verhinderung des erneuten Auftretens illegaler Informationen“ bieten.<sup>94</sup> Unter ähnlichen Erwägungen war auch schon die ECRL in Kraft getreten.<sup>95</sup>

Zwar ist außerhalb nutzergenerierter Inhalte, die auf Grund bereichsspezifischer Vorschriften zu kontrollieren sind (vor allem Urheberrechtsverletzungen, Darstellungen von Kindesmissbrauch, terroristische Inhalte), eine **allgemeine Überwachungspflicht** für übermittelte oder gespeicherte Informationen im DSA-E **ausdrücklich ausgeschlossen**, Art. 7 DSA-E. Aber diese Vorschrift ist insbesondere im Zusammenhang

mit **Art. 17 DSM-RL** zu sehen, der ebenfalls nicht ausdrücklich die Installation von Uploadfiltern zur Vermeidung von Urheberrechtsverletzungen vorschreibt, de facto in der praktischen Umsetzung aber kaum ohne einen solchen auskommt.

Auch die vergangene Bundesregierung hatte in ihrer Koalitionsvereinbarung festgehalten, keine verpflichtenden Uploadfilter im Urheberrecht verankern zu wollen.<sup>96</sup> Letztlich erfordert aber die Umsetzung der Richtlinie im UrhDaG eine technische Unterstützung, um sicherzustellen, dass von Rechteinhabern gemeldete geschützte Inhalte gar nicht erst auf die jeweilige Plattform hochgeladen werden. Denn der Plattformbetreiber ist dafür verantwortlich, ein Sperrverlangen (in der Regel wohl eine Referenzdatei) mit dem hochzuladenden Inhalt einzelner Nutzerinnen und Nutzer abzugleichen. Auch ob für den hochzuladenden Inhalt eine Lizenz mit dem Rechteinhaber zugunsten der Plattform oder des privaten Users vorliegt, wird nur durch automatisierte Verfahren feststellbar sein.

Da das UrhDaG ohnehin nur Plattformen mit einem gewissen Volumen nutzergenerierter Inhalte reguliert, ist kaum vorstellbar, wie die Vorgaben des Gesetzes ohne eine Filtertechnik umgesetzt werden könnten. Soweit es um rechtswidrige nutzergenerierte Inhalte im Sinne des Urheberrechts geht, stellt sich die Frage nach einem Überwachungsgebot in Deutschland im Zusammenhang mit dem DSA also nicht mehr. Dass die anderen Mitgliedstaaten bei der überwiegend noch ausstehenden Umsetzung der DSM-RL ohne jeden Uploadfilter auskommen, ist nicht anzunehmen. Die Umsetzung genießt **Anwendungsvorrang** gegenüber dem DSA, Art. 1 Abs. 5 DSA-E.

Noch liegen kaum **Erfahrungen** mit der praktischen Umsetzung des UrhDaG vor. Wegweisend für das weitere Verfahren zum Erlass des DSA dürfte aber sein, die Erkenntnisse insbesondere solcher Anbieter zu berücksichtigen, die nicht als kleine Diensteanbieter im Sinne des § 2 Abs. 3 UrhDaG oder Startup-Diensteanbieter im Sinne des § 2 Abs. 2 UrhDaG vom Anwendungsbereich des Urheberrechts-Diensteanbieter-Gesetzes ausgenommen sind, aber dennoch nicht zu den Marktführern unter den Plattformen gehören. Plattformen wie YouTube haben längst spezielle Filtersysteme für die Durchsetzung ihrer Community Standards und ihrer gesetzlichen Verpflichtungen. Diese Systeme werden die Betreiberkonzerne nun an die Anforderungen des UrhDaG anpassen können. Aber kleinere Anbieter werden entweder bestehende Tools lizenzieren oder eigene entwickeln müssen. Beides ist kostspielig und in der Implementierung aufwendig. Auch solche Erfahrungen sollten im weiteren Verordnungsgebungsverfahren berücksichtigt werden.

Der Verordnungsentwurf lässt automatisierte Verfahren nur in der Begründung anklingen, wenn er auf Anordnungen im Einzelfall verweist, durch die Anbieter zum Vorgehen gegen oder gar zum Verhindern spezifischer Inhalte verpflichtet werden. „Die in dieser Verordnung niedergelegten Haftungsbestimmungen sollten die verschiedenen Beteiligten nicht daran hindern, innerhalb der von der Verordnung (EU) 2016/679 ge-

<sup>93</sup> ErwGrd. 48 DSA-E

<sup>94</sup> Begründung des DSA-E, Abschnitt 1, Unterabschnitt „Kohärenz mit den bestehenden Vorschriften in diesem Bereich“.

<sup>95</sup> ErwGrd. 40 ECRL.

<sup>96</sup> Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Rz. 2212, abrufbar unter <https://www.bundesregierung.de/resource/blob/974430/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1>.

zogenen Grenzen technische Schutz- und Erkennungssysteme und eine durch Digitaltechnik ermöglichte, automatisierte Erkennung von Inhalten zu entwickeln und wirksam anzuwenden.“<sup>97</sup>

Hier will die Kommission aber ausdrücklich die Rechtsprechung des EuGH<sup>98</sup> unberührt lassen. Das bedeutet auch, dass eine Anordnung zum **Notice and Stay Down** auf Grund des europäischen oder mitgliedstaatlichen Rechts mit Inkrafttreten des DSA beachtlich bleibt. Zusammen mit den auf Grund bereichsspezifischer Normen aufzuspürenden Inhalten läuft das gerade bei den sehr großen Online-Plattformen wegen des schieren Volumens wohl **faktisch** auf einen Aufgabenkanon hinaus, der verdächtig nah an einer allgemeinen Verpflichtung zur **automatisierten Inhalteüberprüfung** liegt.

#### Frage 2d: Könnten sich die geplanten Vorgaben **wachstumsfeindlich** im Hinblick auf kleinere Anbieter, innovative Geschäftsmodelle und neue Marktteilnehmer auswirken?

##### Zusammenfassende Antwort

Kleine Anbieter profitieren im Digital Services Act von der abgestuften Regulierung: Je kleiner Umsatz und Reichweite eines Dienstes, desto weniger streng sind die Verhaltensmaßstäbe. Denkbar ist, dass Anbieter gezielt unterhalb der Schwellenwerte für Kleinunternehmen oder für sehr große Online-Plattform bleiben. Um der Anwendung des DSA insgesamt zu entgehen, könnten Anbieter einzelne Funktionalitäten wie etwa eine Kommentarfunktion gerade nicht aktivieren.

Es ist eines der Regelungsziele des DSA, den Wettbewerb digitaler Dienste im Binnenmarkt zu befeuern, wenngleich neben dem parallel vorgeschlagenen Digital Markets Act nur als ein untergeordnetes Ziel. Mit dem DSA will die Kommission die zunehmende **Zerfaserung** der von den Anbietern zu beachtenden nationalen Vorschriften eindämmen. Denn sie treibt die Rechtsbefolgungskosten für grenzüberschreitend tätige Unternehmen in die Höhe und überfordert mitunter kleinere Anbieter. Typischerweise sollen von der Vereinheitlichung Startup- und Scaleup-Unternehmen profitieren. **Vertrauenswürdige Plattformen** sollen außerdem solchen Anbietern zugutekommen, die ihre Produkte und Leistungen auf digitalen Plattformen anbieten, auch grenzüberschreitend.

Ähnlich wie in der DSGVO geht es beim DSA darum, über die EU hinausreichende **Standards** zu setzen und so ein *level playing field* für die Anbieter aus dem Binnenmarkt und darüber hinaus zu gewährleisten. Das bedeutet allerdings auch für kleinere Anbieter aus dem EU-Ausland, die in den Anwendungsbereich fallen, dass sie die Vereinbarkeit ihrer Dienste mit den Vorgaben des DSA sicherzustellen haben.

Auf die besonderen Belange von Kleinunternehmen, von kleineren Anbietern und von neuen Marktteilnehmern soll der DSA durch die **abgestufte Regulierung** von Vermittlungs-

diensten, Hosting-Diensteanbietern, Online-Plattformen und sehr großen Plattformen Rücksicht nehmen. Klein- und Kleinunternehmen erhalten Welpenschutz, indem sie von den Vorschriften über Transparenzberichtspflichten (Art. 13 DSA-E) und solchen für Online- und für sehr große Online-Plattformen ausgenommen sind, Art. 16 DSA-E. Das betrifft insbesondere die Vorschriften über ein internes Beschwerdemanagementsystem, vertrauenswürdige Hinweisgeber, Meldung des Verdachts auf Straftaten gegenüber Strafverfolgungsbehörden, *Know your business customer*-Sorgfaltspflichten und besondere Transparenzanforderungen. Das erleichtert zugleich den Marktzutritt für Anbieter geringer Größe und innovativer Geschäftsmodelle, weil sie in die Anforderungen des **DSA hineinwachsen** können.

**Kosten** für die Einhaltung gewisser Sorgfalts- und Transparenzpflichten des DSA treffen dagegen alle Vermittler, auch Kleinunternehmen. Dazu gehören neben den formalen Anforderungen wie der Einrichtung einer Kontaktstelle und der Benennung eines Rechtsvertreters im Inland auch Compliance-Kosten zum Beispiel für ein verlässliches, haftungsbefreiendes *Notice and Take Down*-Verfahren oder für den Umgang mit Anordnungen zum Vorgehen gegen illegale Inhalte.

Anhaltspunkte für **wettbewerbschädliche** Auswirkungen sind darüber hinaus insoweit festzustellen, als Anbieter zur Vermeidung bestimmter Verpflichtungen gezielt Funktionalitäten ihrer digitalen Dienste möglicherweise abschalten oder gar nicht erst entwickeln. Sie könnten etwa Kommentarfunktionen<sup>99</sup>, das Teilen von Inhalten oder auch Vertriebsmöglichkeiten für andere Gewerbetreibende in ihrem digitalen Dienst ausschließen, um Anforderungen des DSA auszuweichen. Aus ähnlichen Gründen könnten Unternehmen auf eine Verbesserung ihrer Angebote durch die Weiterentwicklung von Algorithmen verzichten, weil die erhöhten Transparenzanforderungen die Offenlegung der Berechnungsmethoden grundsätzlich einschließen. Das könnte insgesamt zu weniger gezielten Empfehlungen und weniger individualisierbaren Angeboten, mithin zu weniger innovativen Geschäftsmodellen führen.

Kleinere Anbieter, die von den gleichen Haftungsregeln betroffen sind wie größere, könnten erwägen, Uploads ihrer Nutzerinnen und Nutzer nur verzögert anzuzeigen, um längere Bearbeitungszeiten für vorgeschriebene oder selbst initiierte inhaltliche Überprüfungen zu gewinnen. Oder sie könnten nutzergenerierte Inhalte hinsichtlich der Quellen (zum Beispiel nur registrierte User) oder bezüglich der Inhalte (zum Beispiel keine Fotos oder Videos) zur Vermeidung von Haftungsrisiken beschränken.<sup>100</sup>

**Wachstumsschädlich** kann sich freilich die abgestufte Regulierung insofern auswirken, als im Wachstum begriffene Plattformen gezielt innerhalb der Schwellenwerte für Klein- und Kleinunternehmen gemäß der Empfehlung 2003/361/EG

<sup>97</sup> Begründung DSA-E, Ziff. 1, Kohärenz mit den bestehenden Vorschriften in diesem Bereich.

<sup>98</sup> C-18/18 v. 10.1.2018, Glawischning-Pleszczyk.

<sup>99</sup> ErwGrd. 13 nimmt zB den Kommentarbereich einer Online-Funktion nur vom Anwendungsbereich der Vorschriften für Online-Plattformen aus, nicht aber von denen für Vermittler und für Hosting-Dienste, vgl. Frage 1, 1.3.4 DSA und der Medienstaatsvertrag.

<sup>100</sup> Oxera Consulting, The impact of the Digital Services Act on business users, 20.10.2020, S. 47, abrufbar unter <https://www.oxera.com/wp-content/uploads/2020/10/The-impact-of-the-Digital-Services-Act-on-business-users-Methodology-report-2020-10-26.pdf>.

oder unterhalb der Kriterien für sehr große Online-Plattformen gehalten werden. Doch diese Gefahr darf als überschaubares Risiko für die Wettbewerbsfähigkeit europäischer Diensteanbieter betrachtet werden.

### Frage 3: Gelingt es dem Entwurf, den Themenkomplex der Verbreitung von Falsch- und Desinformationen über Online-Plattformen zu adressieren und sachgerechte Lösungen aufzuzeigen?

#### Zusammenfassende Antwort

Die grundrechtlich verbürgte Kommunikationsfreiheit schützt nur im Ausnahmefall erwiesenermaßen falsche oder bewusst unwahre Tatsachenbehauptungen. Wichtigstes Instrument des DSA, um Falsch- und Desinformation zu vermeiden, ist die Förderung freiwilliger Selbstverpflichtungen. Der einer Selbstregulierung inhärente Effekt, in seiner Wirksamkeit hinter einer Regulierung durch den Gesetzgeber zurückzubleiben, zeigt sich auch im aktuellen Beispiel der Selbstverpflichtung mehrerer Diensteanbieter im Zusammenhang mit COVID 19. Der DSA-E verzichtet auf die Normierung einer rechtlichen Bindungswirkung, die über die Überprüfbarkeit der Einhaltung hinausgeht. Das ist angesichts der Freiwilligkeit von Selbstverpflichtungen im Gegensatz zu verbindlicher Normierung sachgerecht.

Für Werbung in Form von kommerzieller Kommunikation und auch Wahlwerbung sollen Transparenzverpflichtungen gelten, die jedenfalls die Erkennbarkeit als und Nachvollziehbarkeit von Werbung erleichtern. Die Offenlegung relevanter Daten für Prüfung, Forschung und Archivierung sowie Steuerungsmöglichkeiten der Anzeige von Werbung für die Nutzerinnen und Nutzer selbst tragen sämtlich dazu bei, Desinformation aufzudecken und so letztlich einzudämmen. Die Europäische Kommission will das Kuratieren von Inhalten insgesamt von der Entscheidung der Nutzerinnen und Nutzer abhängig machen.

Online wie offline kommt es vor, dass Inhalte verbreitet werden, die rechtswidrig oder jedenfalls schädlich sind. In digitalen Diensten, die technisch ermöglichen, dass Nutzerinnen und Nutzer Informationen

- weltweit,
- dauerhaft abrufbar und
- kommentierbar machen,

entwickeln unwahre Behauptungen mitunter eine Dynamik, wie eine flüchtige Äußerung in der analogen Welt sie nie erreichen könnte. Dabei erreichen die in großen sozialen Medien wie Facebook und TikTok geteilten Inhalte ein breites Publikum, das häufig nicht in der Lage ist, dort veröffentlichte Beiträge einzuordnen und zwischen Informations-, Meinungs- und Werbe-Postings zu unterscheiden.<sup>101</sup>

Zuletzt hat die **Corona**-Pandemie verdeutlicht, welchen Schaden Falsch- und Desinformationen anrichten können. Allerdings haben auch gerade im Zusammenhang mit dieser Krise die Marktführer unter den Online-Plattformen einen freiwilligen Beitrag geleistet, um die Verbreitung von Unwahrheiten einzudämmen. Was in diesem Kontext wahr und was falsch ist, lässt sich überwiegend anhand wissenschaftlicher Erkenntnisse feststellen. Gerade in der politischen Werbung ist das allerdings schwieriger. So stellte sich im Zusammenhang mit der Bundestagswahl 2021 und wird sich auch mit der nächsten Europawahl die Frage stellen, inwieweit Desinformationskampagnen vor allem in Form von Verschwörungserzählungen und verschleierte Quellen gezielt entgegengewirkt werden kann und sollte.

#### 1. Kommunikationsfreiheit und ihre Schranken

Die Äußerung von Meinungen und der Austausch darüber sowie das Einholen von Informationen – privat wie durch die Presse – sind **verfassungsrechtlich** auf deutscher und auf europäischer Ebene geschützt.<sup>102</sup> Diesen Kommunikationsgrundrechten kommt in einer freiheitlich-demokratischen Grundordnung besondere Bedeutung zu: Sie ermöglichen Freiheit und Demokratie. Art. 5 Abs. 2 GG gestattet Beschränkungen der Kommunikationsfreiheit durch allgemeine Gesetze. Nach allgemeiner Auffassung ist dafür im Einzelfall darauf abzustellen, ob das jeweilige Gesetz nicht speziell eine bestimmte Meinung ausschließt (Sonderrechtslehre) und ob es dem Schutz eines gegenüber der Meinungsfreiheit höherrangigen Rechts dient (Abwägungslehre).<sup>103</sup> Nach der Wechselwirkungslehre ist das Gesetz seinerseits im Lichte der Meinungsfreiheit auszulegen und anzuwenden.<sup>104</sup> Nach der Rechtsprechung des BVerfG sind erwiesen oder bewusst unwahre Tatsachenbehauptungen vom Schutzbereich des Art. 5 GG nicht umfasst.<sup>105</sup> Dagegen kann der Schutzbereich der Meinungsfreiheit eröffnet sein, wenn die Äußerung mit Elementen der Stellungnahme und des Dafürhaltens verbunden ist.<sup>106</sup>

#### 2. Der Digital Services Act und freiwillige Verhaltenskodizes

Durch den DSA will die Kommission sicherstellen, dass sich systemische Risiken im Online-Bereich nicht realisieren. Der wichtigste Beitrag des Digital Services Act zur Eindämmung von Desinformation wird daher sein, sehr große Online-Plattformen dazu zu bewegen, sich effektiven Maßnahmen der freiwilligen Selbstverpflichtung anzuschließen und diese einzuhalten.

Es ist das Wesen freiwilliger Verhaltenskodizes, dass sich die Akteure einer solchen Kooperationslösung aus eigenem Antrieb eigenverantwortlich Ziele auferlegen, in der Regel um eine Regulierung durch den Gesetzgeber zu vermeiden. Dass eine ordnungsrechtliche Lösung unterbleibt, setzt eine

<sup>101</sup> <https://www.spiegel.de/kultur/digitale-medienkompetenz-in-deutschland-studie-liefert-beunruhigende-ergebnisse-a-13624abd-cd41-4541-9cf1-7f4ff822d0e0>.

<sup>102</sup> Art. 5 GG; Art. 11 Charta der Grundrechte der Europäischen Union.

<sup>103</sup> BVerfGE 95, 220.

<sup>104</sup> BVerfGE 7, 198 (Schranken-Schranken).

<sup>105</sup> BVerfGE 99, 185.

<sup>106</sup> BVerfGE 61, 1.

gewisse Verbindlichkeit der Selbstregulierung voraus. In Bezug auf den Schutz vor Desinformation im Online-Bereich soll das dergestalt erfolgen, dass die Kommission bei erheblichen systemischen Risiken, die mehrere sehr große Online-Plattformen betreffen, diese, allerdings auch andere Online-Plattformen und Vermittlungsdienste, **auffordern** kann, sich (lediglich) an der Ausarbeitung von Verhaltenskodizes zu beteiligen, Art. 35 Abs. 2 DSA-E. Dies gilt jedoch nicht für Kodizes für **Online-Werbung**. Diese ist gesondert in Art. 36 DSA-E geregelt. Der Verordnungsentwurf enthält außerdem Vorschriften allgemein für die Ausarbeitung und Transparenz von Verhaltenskodizes (Artt. 34 ff. DSA-E).

Die Verordnung wird ergänzt durch den Verhaltenskodex der Kommission zur Eindämmung erwiesenermaßen falscher oder irreführender Informationen<sup>107</sup>, den Vermittlungsdienste freiwillig unterzeichnen können. Dieser Verhaltenskodex soll auch künftig ko-regulierend neben dem DSA fortgeführt werden.

Im Zusammenhang mit diesem Verhaltenskodex haben die bekanntesten sehr großen Online-Plattformen Facebook, Instagram, Google, YouTube, Bing, Twitter und TikTok bereits mehrfach in Bezug auf das „Überwachungs- und Berichterstattungsprogramm COVID19“ ihre Berichte über die Umsetzung der vereinbarten Maßnahmen vorgelegt.<sup>108</sup> Die Zahlen der wegen Falschinformation gelöschten nutzergenerierten Uploads mögen als Indikator für die Wirksamkeit der freiwilligen Maßnahmen der Online-Plattformen gelten. Andererseits überarbeitet die Kommission zurzeit den Kodex wegen seiner verbesserungswürdigen Durchschlagkraft.<sup>109</sup>

Dabei geht es neben einer weiteren Transparenzoffensive auch um die mitunter gegenläufigen Anliegen von Diensteanbietern, einerseits als seriöse Online-Plattformen wahrgenommen zu werden, andererseits aber auf Werbeeinnahmen aus wirtschaftlich potenten Quellen angewiesen zu sein. Das kann leicht zu Interessenkonflikten führen. In ihrem Werben um weitere Unterzeichner nennt die Kommission die Verankerung von Verhaltenskodizes im DSA-E einen zusätzlichen Anreiz, sich ihnen anzuschließen.<sup>110</sup> Worin dieser Anreiz bestehen soll, ist jedoch unklar; insbesondere befreien freiwillige Selbstverpflichtungen die Unterzeichner nicht von bestehenden normierten Verpflichtungen.

Durch diese Kodifizierung freiwilliger Selbstverpflichtungen im Verordnungsentwurf sind diese zwar im Vergleich zur bestehenden Rechtslage<sup>111</sup> einer Kontrolle leichter zugänglich. Die Kommission und das Gremium für digitale Dienste sollen gemäß Art. 35 DSA-E Verhaltenskodizes ausdrücklich fördern und erleichtern. Und der Verordnungsentwurf sieht eine **Überprüfbarkeit** der Einhaltung von Selbstverpflichtungen durch einen unabhängigen externen Prüfer vor (Art. 28 Abs. 1b DSA-E). Das Gremium für digitale Dienste soll außerdem regelmäßig überwachen und bewerten, inwieweit die Ziele der Kodizes erreicht werden (Art. 35 Abs. 5 DSA-E).

<sup>107</sup> EU Code of Practice on Disinformation.

<sup>108</sup> <https://digital-strategy.ec.europa.eu/en/library/reports-june-actions-fighting-covid-19-disinformation-monitoring-programme>.

<sup>109</sup> <https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement>.

<sup>110</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2585](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585).

<sup>111</sup> Art. 16 ECR.

Aber welche **rechtliche Wirkung** Verhaltenskodizes zukommen soll, ist nicht normiert.<sup>112</sup> Nur in den Erwägungsgründen findet sich der Hinweis, dass „die Beteiligung einer sehr großen Online-Plattform an einem Verhaltenskodex und dessen Einhaltung als geeignete **Risikominderungsmaßnahme** angesehen werden“ kann; verweigere eine Online-Plattform ohne angemessene Begründung auf Aufforderung der Kommission die Beteiligung, könne das „hinsichtlich möglicher Zuwiderhandlungen im Rahmen der Verordnung berücksichtigt“ werden.<sup>113</sup>

Der Natur der freiwilligen Selbstregulierung entsprechend werden die Maßnahmen dadurch geschwächt, dass keine klaren **Konsequenzen** an die Nichteinhaltung oder die Weigerung der Beteiligung auf Aufforderung geknüpft werden. Auch müssen sehr große Online-Plattformen bei einem negativen Prüfbericht gemäß Art. 28 Abs. 4 DSA-E bloß begründen, warum sie operative Empfehlungen zur Abstellung festgestellter Verstöße nicht umsetzen. Sie schlagen dann eigene Lösungen vor, ohne dass dies ein darauf aufbauendes verbindliches Verfahren auslösen würde.

Letztlich kommt es bei Verhaltenskodizes also weiterhin auf die Freiwilligkeit und auf das Streben nach einem guten Ruf durch die privaten Unternehmen an. Eine von der Kommission im Einzelfall gewünschte Steuerungswirkung kann nur von der Berücksichtigung der Beteiligung an und der Einhaltung von Selbstverpflichtungen als (dem Grunde nach verpflichtende, in der konkreten Ausgestaltung aber freie) Risikominderungsmaßnahme ausgehen. Das entspricht der rechtlichen Qualität von Selbstverpflichtungen, die gerade nicht im Sinne unmittelbarer Durchsetzbarkeit wie ein Gesetz oder eine Verordnung wirken. Diese Unverbindlichkeit ist gerade im Fall der Löschung oder Sperrung nutzergenerierter Inhalte allerdings auch im Spannungsfeld mit den eigenen Nutzungsbedingungen der Online-Plattformen zu sehen. Diese können die Vertragsparteien immerhin im Zivilrechtsweg durchsetzen.

### 3. Verpflichtende Maßnahmen im Digital Services Act

Art. 24 DSA-E schreibt für den Bereich der **Werbung** für alle Online-Plattformen vor, offenzulegen, dass es sich bei einer Botschaft um Werbung handelt, in wessen Namen sie angezeigt wird und welche Parameter verwendet wurden, um die Nutzerinnen und Nutzer zu bestimmen, denen die Werbung angezeigt wird. Art. 30 DSA-E ergänzt diese Transparenzpflichten für sehr große Online-Plattformen. Das ist aus Nutzersicht wichtig, damit beispielsweise Wahlwerbung als solche überhaupt erkennbar ist und damit die Quelle und damit die Integrität angezeigter Botschaften eingeschätzt werden kann.

Ferner sollen die Betreiber sehr großer Plattformen die Aufsicht über und die Erforschung von Informationsblasen erleichtern, indem sie ihre Werbe- und Empfehlungssysteme nachvollziehbar machen. Unabhängige externe **Prüfer**, die sehr große Online-Plattformen einmal jährlich einzusetzen haben, erhalten nach Art. 28 DSA-E Zugang zu Informationen,

<sup>112</sup> Anders etwa Art. 40 Abs. 9 DSGVO, nach dem die Kommission genehmigte Verhaltensregeln für allgemeingültig in der Union erklären kann.

<sup>113</sup> ErwGrd. 68 DSA-E.

deren Vertraulichkeit, Sicherheit und Integrität sie selbst sicherzustellen haben.<sup>114</sup> Durch solche Audits soll die Wirksamkeit der Vorkehrungen gegen Desinformation überprüfbar gemacht werden; sie umfassen sowohl die auf Online-Werbung bezogenen Verpflichtungen als auch die Einhaltung von Selbstverpflichtungen.

Der Zugang des national zuständigen **Koordinators** für digitale Dienste zu Daten für die Überwachung und Bewertung der Compliance mit der Verordnung soll die systemischen Risiken einer Plattform weiter überprüfbar machen und die Genauigkeit, Funktionsweise und Prüfung von Berechnungsmethoden für die Moderation von Inhalten, Empfehlungs- und Werbesystemen zu ermöglichen. Untersuchungen von **Forscherinnen und Forschern** auf Grundlage eben solcher Informationen sollen insbesondere Informationsasymmetrien beseitigen, um die systemischen Risiken zu mindern.<sup>115</sup>

Die **Archivierung** von Werbung durch sehr große Online-Plattformen gemäß Art. 30 DSA-E dient dem Zweck, neu entstehende Risiken im Zusammenhang mit der Verbreitung von Werbung zu verstehen. Solche Risiken sieht die Kommission etwa in illegaler Werbung oder manipulativen Techniken und Desinformation.<sup>116</sup> Gesonderte **Krisenprotokolle** sind vorgesehen, wenn sehr große Online-Plattformen zur Bewältigung von Krisensituationen herangezogen werden sollen, Art. 37 DSA-E.

Außerdem müssen sehr große Online-Plattformen gemäß Art. 29 DSA-E den **Nutzerinnen und Nutzern** ermöglichen, selbst Einfluss auf die Anzeige von Informationen zu nehmen, indem sie selbst die empfohlenen Inhalte vom Nutzerprofil entkoppeln oder die Reihenfolge von Informationen individualisieren können, zum Beispiel je nach Quelle oder Aktualität. Auf diese Weise haben Nutzerinnen und Nutzer die Möglichkeit, selbst dazu beizutragen, die Grundlagen für ihre Informationsbeschaffung zu objektivieren. Die Hoffnung ist, dass sich die angezeigten Inhalte damit weniger nach den kommerziellen Interessen der Intermediäre richten (denn diese wollen die User durch gezielte, zunehmend fesselnde Ansprache möglichst lange auf der Plattform halten) als nach den individuellen Interessen ihrer Nutzerinnen und Nutzer. Die weitergehende Forderung des Rechtsausschusses des Europäischen Parlaments, das Kuratieren von Inhalten zum Beispiel über die Browsereinstellungen durch die Nutzerin ganz abschalten zu können<sup>117</sup>, findet sich nicht im Entwurf wieder. Das würde freilich ganze Geschäftsmodelle auf den Prüfstand stellen. Inwieweit die rechtspolitische Diskussion diesen Vorschlag im Trilog aufnimmt, bleibt abzuwarten.

<sup>114</sup> ErwGrd. 60 DSA-E.

<sup>115</sup> Art. 31 Abs. 2 DSA-E, ErwGrd. 64. Vgl. § 5 a NetzDG (ab 1.2.2022), der allerdings eine Aufwandsentschädigung der Plattformbetreiber vorsieht und auch die Möglichkeit zur Ablehnung eines Zugangs für Forscher, wenn die Plattformbetreiber geltend machen, dass ihre schutzwürdigen Interessen das öffentliche Interesse an der Forschung erheblich überwiegen; das NetzDG bleibt insoweit und auch im Hinblick auf detaillierte Anforderungen an ein Schutzkonzept des Forschers für die Informationen über die Plattform hinter dem DSA zurück und wäre deshalb mit Inkrafttreten des DSA erneut zu überprüfen.

<sup>116</sup> ErwGrd. 63 DSA-E.

<sup>117</sup> <https://www.europarl.europa.eu/news/de/agenda/briefing/2020-10-19/1/prioritaeten-des-parlaments-zum-kunftigen-gesetz-uber-digitale-dienste>.

Stellen mit besonderer Sachkenntnis und Kompetenz als **vertrauenswürdige Hinweisgeber** (*trusted flagger*) sind eine weitere Maßnahme, um Desinformationen aufzuspüren und Plattformen mit dem Ziel der Haftungsbefreiung zur Entfernung oder Sperrung der Inhalte zu veranlassen. Erweist sich ein Hinweisgeber als nicht (mehr) vertrauenswürdig, weil er eine erhebliche Zahl unzureichend begründeter Meldungen übermittelt hat, kann ihm der Sonderstatus wieder genommen werden. Dafür ist ebenfalls der nationale Koordinator zuständig, so dass hier eine gewisse öffentliche Kontrolle stattfindet. Das unterscheidet den vertrauenswürdigen Hinweisgeber im DSA von dem im Urheberrechts-Diensteanbieter-Gesetz (DSM), das mit Inkrafttreten des DSA auf seine Vereinbarkeit mit der Verordnung zu überprüfen wäre.<sup>118</sup>

In der Summe tragen diese Maßnahmen dazu bei, Desinformationen aufzudecken. Diese Transparenz ist notwendige Voraussetzung, um dem Phänomen wirksam entgegenzuwirken. Der Digital Services Act schafft also jedenfalls ein Umfeld, das dafür geeignet sein wird, Desinformation einzudämmen.

#### 4. Europäischer Aktionsplan für Demokratie

Nur wenige Tage vor der Veröffentlichung des DSA-E hat die Kommission ihre Mitteilung „Europäischer Aktionsplan für Demokratie“ veröffentlicht.<sup>119</sup> Darin beschreibt sie die Bedeutung eines von Meinungsfreiheit geprägten Klimas, das Voraussetzung für das Gedeihen der Demokratie sei. Die Resilienz der Demokratien in der EU sei auf der Ebene der EU wie auch der Mitgliedstaaten unter Wahrung der Grundrechte und Grundfreiheiten zu stärken. Es geht, wie unter anderem durch ausdrückliche Bezugnahmen auf die Europawahl im Mai 2024 deutlich wird, vorrangig um die Ausübung der demokratischen Grundrechte durch die Bevölkerung in der Union insgesamt. Aber die Vorschriften sollen auch auf solche politische Werbung anwendbar sein, die sich an Einzelpersonen in nur einem Mitgliedstaat richtet.

Die rasche Zunahme und Zentrierung von Kampagnen auf Online-Plattformen identifiziert die Kommission im Aktionsplan als besondere Einfallstore für die Gefährdung der Integrität von Wahlen, für Desinformation und Manipulation und für die Schwächung von Medienvielfalt und Pressefreiheit. Denn Plattformen können Funktionen wie Nachrichtenmedien erfüllen und als Torwächter Informationsgehalte steuern, ohne dabei denselben nationalen Vorschriften und berufsständischen Standards wie die Presse zu unterliegen.

Wie im DSA legt die Kommission auch im Aktionsplan nicht fest, was **politische Werbung** im Einzelnen ist. Sie spricht stattdessen von bezahltem politischem Material, das es von anderen politischen Inhalten zu unterscheiden gelte. Am 25. November 2021 hat sie einen Verordnungsvorschlag zur Verbesserung der Transparenz gesponserter politischer Inhalte

<sup>118</sup> Gerald Spindler, Der Vorschlag für ein neues Haftungsregime für Internetprovider - der EU-Digital Services Act, Teil 2, GRUR 2021, 653 (655); vgl. Frage 1, 1.3.1 DSA und das Urheberrecht, und Frage 2a, 2.7 Trusted Flaggers.

<sup>119</sup> COM(2020) 790 final v. 3.12.2020.

vorgelegt,<sup>120</sup> der die Vorschriften des DSA über Online-Werbung ergänzen soll; dem DSA ist ausdrücklich ein Anwendungsvorrang im Entwurf dieses Verordnungsvorschlags über transparente politische Werbung eingeräumt. In den Begriffsbestimmungen ist demnach zum Beispiel eine (unentgeltliche) nutzergenerierte Werbung für eine politische Partei oder Botschaft in einem sozialen Netzwerk konsequent aus dem Begriff der politischen Werbedienstleistung ausgenommen.

Wie im DSA geht es im Verordnungsvorschlag für transparentere politische Werbung nicht um konkrete Inhalte, sondern um Mechanismen zur Überwachung und Durchsetzung der einschlägigen Vorschriften. Wichtigste Regelungsinstrumente sind auch hier Transparenzverpflichtungen von Diensteanbietern und bei Anbietern aus EU-Drittstaaten die Pflicht, durch einen bevollmächtigten Vertreter in der EU die Durchsetzung sicherzustellen. Es bleibt damit aus ähnlichen Erwägungen wie zum DSA abzuwarten, ob das angekündigte Regelungsinstrument geeignet ist, um jedenfalls für den Bereich der politischen Desinformation im Zusammenspiel mit dem DSA effektiv eine Irreführung der Nutzerinnen und Nutzer zu vermeiden.

---

<sup>120</sup> Vorschlag über eine Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung, COM(2021) 731 final v. 25.11.2021.

# Ergänzungen der Redaktion

## 1. Abkürzungsverzeichnis

**AEUV:** Vertrag über die Arbeitsweise der Europäischen Union

**AGB:** Allgemeine Geschäftsbedingungen

**AVMD-RL:** Richtlinie über audiovisuelle Mediendienste

**BGB:** Bürgerliches Gesetzbuch

**BGH:** Bundesgerichtshof

**BKA:** Bundeskriminalamt

**BNetzA:** Bundesnetzagentur

**DSA(-E):** Digital Services Act(-Entwurf).

Dt.: Digitale Dienste Gesetz

**DSGVO:** Europäische Datenschutz-Grundverordnung

**DSM-RL:** Digital Single Market-Richtlinie, Richtlinie über das Urheberrecht im europäischen Binnenmarkt

**ECRL:** E-Commerce Richtlinie 2000

**EU:** Europäische Union

**EuGH:** Europäischer Gerichtshof

**MStV:** Medienstaatsvertrag

**NetzDG:** Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz)

**NetzDGÄndG:** Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes

**P2B-VO:** Platform to Business-Verordnung

**StGB:** Strafgesetzbuch

**TMG:** Telemediengesetz

**UrhDaG:** Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten (Urheberrechts-Diensteanbieter-Gesetz)

## 2. Glossar

**Audiovisueller Mediendienst:** Dienst, für den gem. Art. 1 Abs. 1 lit. a i) AVMD-RL ein Medienanbieter die redaktionelle Verantwortung trägt und dessen Hauptzweck die Bereitstellung von Sendungen zur Information, Unterhaltung oder Bildung der breiten Öffentlichkeit über elektronische Kommunikationsnetze ist.

**Community Standards:** s. Gemeinschaftsstandards.

**Diensteanbieter:** Anbieter einer Dienstleistung der Informationsgesellschaft im Sinne der Richtlinie (EU) 2015/1535, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Im Sinne dieser Definition bezeichnet der Ausdruck:

1. „im Fernabsatz erbrachte Dienstleistung“ eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
2. „elektronisch erbrachte Dienstleistung“ eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und

Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;

3. „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

**Einzelfallanordnung:** Gerichtliche oder behördliche Anordnung, die nicht abstrakt-generell, sondern im Einzelfall ausgesprochen wird.

**Gemeinschaftsstandards:** „Spielregeln“ einer (Social Media) Plattform, auch „Community Standards“, zu deren Einhaltung sich Nutzerinnen und Nutzer verpflichten.

**Haftungsprivileg/Haftungsbefreiung:** Befreiung von bestimmten Haftungstatbeständen für Diensteanbieter, die Informationen ihrer Nutzerinnen und Nutzer lediglich durchleiten, übermitteln oder bereitstellen; Hosting-Anbieter (s. Vermittlungsdienst) haften beispielsweise grundsätzlich

nicht für rechtswidrige Inhalte Dritter, solange die Anbieter die Informationen nicht im Auftrag der User speichern und von der Rechtswidrigkeit keine Kenntnis haben (s. Notice and Take Down). Mit Kenntniswerb der Diensteanbieter endet deren Haftungsprivileg. Geregelt ist dies bisher in der ECRL, in den DSA soll die Privilegierung übernommen werden.

**Harmonisierter Dienst:** Durch EU-weit harmonisierte Vorschriften regulierter Dienst.

**Herkunftslandprinzip:** Diensteanbieter sind den Regelungen des Landes unterworfen, in dem sie ihren europäischen Hauptsitz (also ihre Niederlassung) haben. So wird in der EU nur eine Regelungszuständigkeit am Niederlassungsort begründet, andere Mitgliedstaaten dürfen keine Regelungen erlassen.

**Hosting-Dienste:** Dienste, bei denen Inhalte gespeichert und bereitgestellt werden, die von Nutzerinnen und Nutzern hochgeladen werden; darunter fallen auch Online-Plattformen.

**Intermediär:** Vermittlungsdienst, der digitale Inhalte seiner Nutzerinnen und Nutzer zugänglich macht, z.B. soziale Netzwerke, Suchmaschinen, Videoportale, Verkaufsplattformen.

**Kenntnisnahmefiktion:** Es wird fingiert (angenommen), dass der Anbieter tatsächliche Kenntnis von einer Tatsache hat. Im Falle des DSA bezieht sich die Kenntnis auf die Tatsache, dass eine Meldung über einen mutmaßlich illegalen Inhalt vorliegt.

**Marktortprinzip:** Anders als beim Herkunftslandprinzip sind Diensteanbieter den Regelungen der Länder unterworfen, in denen sie ihre Dienste den Nutzerinnen und Nutzern anbieten (also wo sie mit ihren Diensten auf dem Markt sind).

**Notice and Action:** Notice and Take Down wird bei Notice and Action modifiziert, z.B. durch die Ergänzung weiterer Sorgfalts- und Transparenzverpflichtungen, die eingehalten werden müssen, um in den Genuss der Haftungsprivilegierung zu kommen.

**Notice and Take Down:** Verfahren, bei dem der Hosting-Anbieter für die Inanspruchnahme des Haftungsprivilegs nach Kenntnisnahme (notice) den rechtswidrigen Inhalt einer Nutzerin oder eines Nutzers löscht oder sperrt (take down).

**Öffnungsklausel:** Sie ermöglicht, dass die Mitgliedstaaten im durch europäische Regulierung koordinierten Bereich bestimmte Sachverhalte individuell normieren.

**Online-Plattform/sehr große Online-Plattform:** Hosting-Diensteanbieter (gem. Art. 2 lit. h DSA-E), der im Auftrag von Nutzerinnen und Nutzern Informationen speichert und verbreitet; beispielsweise Marktplätze, die zwischen Akteuren der Digitalwirtschaft vermitteln. Als sehr große Online-Plattform gilt (gem. Art. 25 Abs. 1 DSA-E) ein Dienst, der mindestens 45 Mio. „aktive Nutzer“ verzeichnet. Dieser Wert entspricht zurzeit etwa 10 % der Bevölkerung in der EU. Diesen Schwellenwert dürften allseits bekannte Dienste wie Twitter, Facebook, Amazon, AirBnB, Booking.com, TikTok usw. erfüllen.

**Overblocking:** Die vor allem durch fehlende Einzelfallüberprüfung von Inhalten vorgenommene übermäßige Löschung oder Sperrung nutzergenerierter Inhalte, bei der auch rechtmäßige Inhalte unzugänglich gemacht werden, insbesondere durch technische Filtermethoden.

**Top Level Domain:** Bezeichnet den letzten Abschnitt einer Domain im Internet (z.B. „.de“ oder „.com“).

**Trusted Flagger/vertrauenswürdiger Hinweisgeber:** Stelle mit besonderem Vertrauensstatus im Sinne des DSA, der ein nationaler Koordinator für digitale Dienste diesen Status auf Grund ihrer besonderen Sachkenntnis und Kompetenz im Umgang mit illegalen Inhalten und ihrer Überprüfung zuerkannt hat. (Social Media Plattformen oder Foren arbeiten teilweise mit Nutzerinnen und Nutzern zusammen, die besondere Befugnisse zur Moderation von Inhalten haben. Diese sind hier nicht gemeint.)

**Vermittlungsdienst:** Eine der drei folgenden Dienstleistungen (gem. Art. 2 lit. f DSA-E):

- Durchleitung fremder Inhalte innerhalb eines Kommunikationsnetzes oder Vermittlung des Zugangs zu einem solchen (Access Provider, z.B. Telekom).
- automatische, vorübergehende Zwischenspeicherung fremder Informationen zur Übermittlung innerhalb eines Kommunikationsnetzes (Caching-Dienst, z.B. Speicherung von E-Mails auf dem Server des E-Mail-Anbieters).
- Speicherung von Informationen, die Nutzerinnen oder Nutzer bereitstellen (Hosting, z.B. YouTube, Facebook, Amazon).

**Videosharing-Dienst:** Ein Dienst, für den gem. Art. 1 Abs. 1 lit. aa AVMD-RL (neu) der Video-Sharing-Plattform-Anbieter keine redaktionelle Verantwortung trägt und dessen wesentliche Funktion darin besteht, Sendungen oder nutzergenerierte Videos der Allgemeinheit über elektronische Kommunikationsnetze zur Information, Unterhaltung oder Bildung bereitzustellen, und deren Organisation vom Video-Sharing-Plattform-Anbieter bestimmt wird, auch mit automatischen Mitteln oder Algorithmen, insbesondere durch Anzeigen, Tagging und Festlegung der Abfolge.

# Über die Autorin



## **Prof. Dr. Henrike Weiden, LL.M.**

Prof. Dr. Henrike Weiden, LL.M. hat Rechtswissenschaften in Erlangen, Leipzig und Fukuoka (Japan) studiert. 1999 begann sie ihre berufliche Laufbahn als Rechtsanwältin in der Andersen Luther Rechtsanwaltsgesellschaft. Ab 2001 verantwortete sie im Bundesverband der Deutschen Industrie die Interessenvertretung im Gewerblichen Rechtsschutz und im Datenschutz. Nach einem mehrjährigen Aufenthalt in Brasilien und den USA wechselte Henrike Weiden 2012 zu Telefónica Deutschland. Nachdem sie 2015 bis 2017 in Tokio v.a. als Hochschuldozentin freiberuflich tätig war, arbeitete sie bei Sky Deutschland, bis sie eine Professur an der Hochschule München University of Applied Sciences übernahm. Hier vertritt sie heute das Wirtschaftsprivatrecht und das Recht in der Digitalisierung.

