DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschüsse Geistiges Eigentum und Informationsrecht

zum Verordnungsvorschlag der Europäischen Kommission für ein Gesetz über digitale Dienste (Digital Services Act) COM(2020) 825 final

Stellungnahme Nr.: 34/2021 Berlin, im Mai 2021

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Köln
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski

Mitglieder des Ausschusses Geistiges Eigentum

- Rechtsanwalt Prof. Dr. Jochen Bühling, Düsseldorf (Vorsitzender)
- Rechtsanwalt Prof. Dr. Johannes Kreile, München
- Rechtsanwältin Jana Bogatz, München
- Rechtsanwalt Dr. Dirk Bruhn, Hamburg (Berichterstatter)
- Rechtsanwalt Klaus Haft, Dipl.-Phys., Düsseldorf

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

- Rechtsanwältin Dr. Verena Hoene, Köln
- Rechtsanwalt Prof. Dr. Reinhard Ingerl, LL.M., München
- Rechtsanwältin Dr. Andrea Jaeger-Lenz, Hamburg
- Rechtsanwalt beim Bundesgerichtshof Dr. Matthias Koch LL.M., Karlsruhe
- Rechtsanwalt Dr. Henrik Lehment, Düsseldorf
- Rechtsanwältin Dr. Birte Lorenzen, Hamburg

Zuständig in der DAV-Geschäftsstelle und Ansprechpartner in Brüssel

- Rechtsanwältin Eva Schriever, LL.M
- Hannah Adzakpa, LL.M
- Anja Wyrobek

Verteiler

Europa

Europäische Kommission
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien
- Generaldirektion Justiz und Verbraucher
- Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU

Europäisches Parlament
- Rechtsausschuss
- Ausschuss für Binnenmarkt und Verbraucherschutz
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen bei der EU
Rat der Europäischen Anwaltschaften (CCBE)
Bundesverband der Freien Berufe (BFB) – Büro Brüssel
Deutscher Industrie- und Handelskammertag (DIHK) – Büro Brüssel
Bundesverband der deutschen Industrie e.V. (BDI) – Büro Brüssel

Deutschland

Bundesministerium des Innern, für Bau und Heimat
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundeskanzleramt
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Ausschuss für Angelegenheiten der Europäischen Union
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Justizministerien und Justizverwaltungen der Bundesländer der Bundesrepublik Deutschland
Die Datenschutzbeauftragten der Bundesländer
Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer (BRAK)
Bundesnotarkammer
Bundesverband der Freien Berufe (BFB)
Deutscher Richterbund (DRB)
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband (DStV)
Bundesverband der Deutschen Industrie (BDI)
Deutscher Industrie- und Handelskammertag (DIHK)
Max-Planck-Institut für Innovation und Wettbewerb
Bundesverband Musikindustrie e.V. (BVMI)
Deutscher Journalisten-Verband e.V. (DJV)
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
Ver.di, Abteilung Richterinnen und Richter

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Arbeitsgemeinschaften
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Die Welt
NJW
Juve-Verlag
Verlag C.H. Beck
Anwaltsblatt
Juris
MultiMedia und Recht (MMR)
Zeitschrift für Datenschutz ZD
heise online
Monatsschrift für Deutsches Recht (MDR)
Zeitschrift für die anwaltliche Praxis (ZAP)
Juristenzeitung (JZ)
Bundesrechtsanwaltskammer-Mitteilungen / BRAK-Mitteilungen
Legal Tribune Online
Zeitschrift Gewerblicher Rechtsschutz und Urheberrecht (GRUR)
Zeitschrift „Mitteilungen der deutschen Patentanwälte“
Zeitschrift „ZEuP“
Netzpolitik.org

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 62.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 252 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Brief summary

The German Bar Association supports that the structure of the E-Commerce Directive 2000/31/EC shall be maintained in the current proposal for the DSA-Regulation. The fact that the liability privileges of intermediaries are to be retained in essence is to be welcomed. This enables European companies to develop and expand services in competition with American and Asian service providers without having to take on overwhelming liability risks.

The DAV would like to underline that the CJEU’s case law on an "active role" of the providers (giving rise to liability) is not included in the enacting terms of the proposed Regulation. For reasons of legal certainty, however, a clear provision should be added, in particular with regard to Art. 6 DSA.

Furthermore, the complicated national case law and practical application of due diligence obligations which cause liability under the so called "Störerhaftung" under German law remain unresolved. The position paper comments on certain provisions and offers possible solutions in order to create legal certainty for all parties involved. In particular, the DAV takes a critical look at the additional compliance burden that companies will have to face. The relationship between data protection and other areas of law, such as intellectual property, is also examined.

Kurzzusammenfassung

Art. 3 bis 9 DSA bauen auf den Bestimmungen der Art. 12 bis 15 E-Commerce Richtlinie 2000/31/EG (in weiterer Folge ECRL) auf. Die Regelungsstruktur entspricht

weitgehend den Haftungsprivilegien der Art. 12 bis 15 ECRL, die nicht grundlegend neugestaltet werden sollen.

Dass die Haftungsprivilegien der Intermediäre im Kern beibehalten werden sollen, ist zu begrüßen. Dies ermöglicht europäischen Unternehmen, im Wettbewerb mit amerikanischen und asiatischen Diensteanbietern, Dienste neu zu entwickeln und auszubauen, ohne erdrückende Haftungsrisiken eingehen zu müssen. Das „Notice and Take Down“-Prinzip hat sich in den letzten 20 Jahren bewährt.

Durchbrochen wurde das „Notice and Take Down“-Prinzip von Handlungs- und Unterlassungspflichten nach dem jeweiligen Recht der EU-Mitgliedsstaaten. So entschied der BGH in Deutschland sehr früh, dass die Art. 12 bis 15 ECRL nicht auf Beseitigungs- und Unterlassungsansprüche anwendbar seien (erstmals BGH vom 11.3.2004, CR 2004, 763 ff. mit Anm. Volkmann = MMR 2004, 668 ff. = K&R 2004, 486 ff. – Internet-Versteigerung; seitdem ständige Rechtsprechung). Dies führte dazu, dass die Bestimmungen der Art. 12 bis 15 ECRL nach und nach überlagert wurden durch eine äußerst komplizierte Rechtsprechung zur Störerhaftung im Netz. Selbst Experten fällt es schwer, den Überblick über diese Rechtsprechung zu behalten. Die Rechtssicherheit, die die Art. 12 bis 15 ECRL schaffen sollten, wurde dadurch nur partiell erreicht.

Parallel begann der EuGH, den Begriff des Intermediärs und damit die Reichweite der Haftungsprivilegien einzuengen, indem er zwischen „reinen Intermediären“ und Intermediären mit einer „aktiven Rolle“ unterschied. Auf letztere sind die Art. 12 bis 15 ECRL daher nicht anwendbar (vgl. EuGH vom 12.7.2011, C-324/09, Rdnr. 113).

Die EuGH-Rechtsprechung zu einer (haftungsbegründenden) „aktiven Rolle“ der Provider wird in dem DSA-Entwurf nicht in den verfügenden Teil aufgenommen. Aus Gründen der Rechtssicherheit sollte hierzu jedoch eine klare Regelung getroffen werden, insbesondere im Hinblick auf Art. 6 DSA.

Im Ergebnis folgt daraus ein Nebeneinander von zwei nur schwer gegeneinander abgrenzbaren Haftungsregimen – der deutschen Störerhaftung und den Haftungsprivilegien der E-Commerce-RL –, das in der Praxis mit viel

Rechtsunsicherheit verbunden ist. Der DAV schlägt deshalb vor, klarzustellen, dass der DSA eine Vollharmonisierungswirkung anstrebt, und zwar ausdrücklich auch für die Haftung von Providern auf Beseitigung und Unterlassung.

Art. 5 Abs. 3 DSA

Nach Art. 5 Abs. 3 DSA soll die Privilegierung für die verbraucherschutzrechtliche Haftung des Host Providers nicht gelten, wenn der Provider den Eindruck vermittelt, dass er dem Nutzer selbst als Vertragspartner gegenübertritt.

Dies ist ein verbraucherschutzrechtlicher Fremdkörper in dem Entwurf. Art. 5 Abs. 3 DSA beschreibt einen Tatbestand, der als Irreführung verstanden werden kann und daher verbraucherschutz- und wettbewerbsrechtliche, nicht jedoch haftungsrechtliche Fragen aufwirft. Art. 5 Abs. 3 DSA erscheint entbehrlich.

Art. 6 DSA

Zu begrüßen ist die in Art. 6 DSA getroffene Regelung, die es verhindert, dass Bemühungen eines Providers zur Vermeidung von Rechtsverstößen als das „Zu-eigen-Machen“ von Inhalten mit der Folge eines Verlusts von Haftungsprivilegien verstanden wird (vgl. Zur jetzigen Rechtslage BGH vom 12.11.2009, CR 2010, 468, 470 mit Anm. Hoeren/Plattner = WRP 2010, 922, 925 – marions-kochbuch.de).

Art. 8 und 9 DSA

Art. 8 und 9 DSA verstärken die Verpflichtungen der Intermediäre, „orders“ (also Anordnungen) zu befolgen. Dies soll sowohl für behördliche als auch für gerichtliche Anordnungen gelten. Somit würde – mehr noch als bisher – den Mitgliedsstaaten die Möglichkeit gegeben, Handlungs- und Unterlassungspflichten der Provider im nationalen Recht zu verankern, die die Haftungsprivilegien der DSA überlagern. In Deutschland würde es mit an Sicherheit grenzender Wahrscheinlichkeit bei der Rechtsprechung des BGH zur Störerhaftung bleiben, die sich nur sehr lose an das europäische Recht (derzeit Art. 12 bis 15 ECRL) anlehnt. Im Interesse einer

Vereinheitlichung der Haftungsregeln erscheint es wünschenswert, den Rahmen, der in den Art. 8 und 9 DSA vorgeschlagen wird, deutlich einzuengen.

Insbesondere ist dabei wichtig, klarzustellen, was unter solchen „Orders“ zu verstehen ist. Wenn das Grundprinzip der „Haftung erst ab Kenntnis“ (und damit die spezielle Funktion der Provider) nicht unterlaufen werden soll, so kann unter einer „Order“ nur eine konkret-individuelle Anordnung zu verstehen sein, d.h. eine Anordnung für den konkreten Einzelfall.

Art. 9 DSA dürfte zudem eine datenschutzrechtliche Dimension haben, da diese Vorschrift die Intermediäre unter näher bestimmten Voraussetzungen verpflichtet, Anordnungen zur Preisgabe von Nutzerinformationen zu befolgen. An dieser und zahlreichen anderen Stellen des Entwurfs fällt auf, dass Datenschutzfragen vollständig ausgeblendet werden. Konkret sollte die durch Art. 9 DSA angeordnete Preisgabe von Nutzerinformationen die datenschutzrechtlichen Interessen der Betroffenen berücksichtigen.

Dem DAV ist bekannt, dass solche Fragen in der Praxis eine wichtige Rolle spielen. Insbesondere betrifft das die folgenden Fragen:

- Wie verhalten sich die Betroffenenrechte nach der DSGVO zum „Notice and Take Down“-Prinzip? Durchbrechen diese das Prinzip, oder umgekehrt? (Beispiel: Ein Betroffener macht ein Löschbegehren nach Art. 17 DSGVO gelten. Unter welchen Voraussetzungen gilt das Löschbegehren auch in Bezug auf Inhalte, die der Anbieter bislang nicht zur Kenntnis genommen hat?)

- Wie verhalten sich „Takedown“-Pflichten, die nach dem DSA oder anderen Rechtsgebieten bestehen, zur DSGVO und/oder der Richtlinie 2002/58/EG (ePrivacy-RL)? Muss der Anbieter zur Umsetzung solcher Takedown-Pflichten auch in Datenschutzrechte Dritter eingreifen (indem er deren personenbezogene Daten verarbeitet oder sogar löscht)? Muss der Anbieter zur Umsetzung solcher Takedown-Pflichten auch auf Inhalte zugreifen (bzw. löschen), die dem Fernmeldegeheimnis unterfallen? Dies insbesondere vor dem Hintergrund der Ausweitung des Anwendungsbereichs des Begriffs „Elektronischer

Kommunikationsdienst“ durch den EU-Kodex zur elektronischen Kommunikation (EKEK), was indirekt auch den Anwendungsbereich der EU-Regelung zur Vertraulichkeit der elektronischen Kommunikation (Art. 5 Abs. 1 ePrivacy-RL) ausdehnt.

Unstimmig ist die Rolle des jeweiligen Digital Services-Koordinators, der sämtliche Anordnungen (auch der Zivilgerichte) zur Kenntnis erlangen und an alle Kollegen in den anderen EU-Mitgliedsstaaten weiterleiten soll (Art. 8 Abs. 3 und Art. 9 Abs. 3 DSA). Welche Konsequenzen die Benachrichtigung und Weiterleitung haben soll, bleibt unklar. Dies sollte geregelt werden.

Illegale Inhalte

Soweit es europäische Regulierung (wie im Urheberrecht und im Markenrecht) gibt, mag sich eine Harmonisierung mit dem DSA noch halbwegs erreichen lassen. Auf Schwierigkeiten wird eine Harmonisierung indes im Äußerungsrecht stoßen, da jeder EU-Mitgliedsstaat die Grenzen zwischen „legalen“ und „illegalen“ Äußerungen anders gestaltet. Der DSA-Entwurf sieht von jedem Versuch ab, Regelungen für den Fall zu treffen, dass Inhalte nach dem Äußerungsrecht verschiedener Mitgliedsländer unterschiedlich zu beurteilen sind. Es bedarf hier jedenfalls einer Klarstellung, dass Äußerungen, die von Art. 11 GRCh (Meinungsfreiheit) gedeckt sind, nicht zugleich „illegal“ sein können

Pflichten für Host Provider

Art. 14 und 15 DSA gelten für alle Host Provider– unabhängig von deren Größe. Host Provider sind Provider, die Informationen der Nutzer speichern (Art. 5 Abs. 1 DSA – ebenso bereits Art. 14 Abs. 1 ECRL). Art. 14 DSA verpflichtet alle Host Provider zur Einrichtung eines Systems zur Meldung von Rechtsverstößen. Spiegelbildlich dazu sollen die Host Provider durch Art. 15 DSA gegenüber den Nutzern verpflichtet werden, Entscheidungen über die Entfernung oder Sperrung von Inhalten zu begründen.

Die Bestimmungen der Art. 14 und 15 DSA folgen dem „Notice and Action“-Prinzip, könnten allerdings für Start-Ups und Newcomer zu einer Marktzutrittshürde werden, da sie mit nicht unbeträchtlichen Implementierungskosten verbunden sind.

Insbesondere die Pflicht, Löschungen ausführlich zu begründen (Art. 15 Abs. 2 DSA), ist kritisch zu betrachten, da diese Verpflichtung in die Vertragsfreiheit des Diensteanbieters eingreift und ihre Umsetzung mit erheblichem Aufwand verbunden ist. Weshalb es zudem einer Begründung selbst dann bedürfen soll, wenn die Gründe der Löschung (etwa bei gravierenden Rechtsverstößen oder erheblichen Verstößen gegen die Nutzungsbedingungen) evident sind, ist nicht ersichtlich. Es sollte jedenfalls ausreichen, den Diensteanbieter zu einer Begründung zu verpflichten, wenn der betroffene Nutzer eine solche Begründung verlangt.

Datenschutzrechtlich heikel und daher abzulehnen ist die grundsätzlich geplante Verpflichtung, Meldesysteme so einzurichten, dass sie die Angabe des Namens und der Mailadresse des Meldenden obligatorisch voraussetzen (Art. 14 Abs. 2 lit. c DSA). Hiermit würden unnötige Hürden für Meldungen errichtet, und (datenschutzrechtlich) kann von einer „Erforderlichkeit“ der Angaben nicht die Rede sein.

Pflichten für Online-Plattformen

Art. 17 bis 24 DSA gelten – wie Art. 13 DSA – nicht für Provider, die zu den kleinen und mittelständischen Unternehmen zählen (Art. 16 DSA), dies allerdings mit einer zusätzlichen Einschränkung: Es muss sich um „Online-Plattformen“ handeln. Hierbei sind nach Art. 2 lit. h DSA Host Provider gemeint, die auf Veranlassung ihrer Nutzer nicht nur Informationen speichern, sondern diese Informationen auch öffentlich verbreiten. Die „öffentliche Verbreitung“ von Informationen unterscheidet den Betreiber einer „Online-Plattform“ somit von Cloud-Anbietern und anderen Host Providern, deren Dienst sich in einer Speicherung von Informationen für den Nutzer erschöpft. Derartig verschachtelte Unterscheidungen zwischen unterschiedlichen Kategorien verschiedener Provider gehen zu Lasten der Übersichtlichkeit des Entwurfs.

Art. 17 bis 20 DSA knüpfen an Art. 15 DSA an und regeln zusätzliche Verpflichtungen der Betreiber größerer Online-Plattformen beim Umgang mit Beschwerden ihrer Nutzer. Ergänzend werden die Betreiber zudem durch Art. 21 DSA verpflichtet, bei Verdacht schwerer Straftaten staatliche Ermittlungsbehörden zu verständigen. Es ist zu

begrüßen, dass sich diese Meldepflicht auf schwere Straftaten beschränkt, die sich gegen Leib und Leben richten.

Art. 15 DSA sowie Art. 17 bis 20 DSA schränken die Freiheit der Betreiber von Online-Plattformen ein, Inhalte von seiner Plattform wegen des Verdachts eines Rechtsverstoßes zu entfernen. Dies ist ebenso ein Eingriff in die Vertragsfreiheit wie beispielsweise Identifikationspflichten (Art. 22 DSA) und Vorgaben für die Ausgestaltung der Nutzungsbedingungen (Art. 12 DSA). Diese Eingriffe in die Vertragsfreiheit sollen nicht nur für die „Riesen“ gelten und können dementsprechend auch nicht durch deren Marktmacht legitimiert werden. Was aber rechtfertigt es, den Betreiber einer kleineren Verkaufsplattform zu verpflichten, mit seinen Kunden zu streiten, wenn er nach Erhalt einer wettbewerbsrechtlichen Abmahnung Werbung des Kunden von der Plattform entfernt (vgl. Art. 15 DSA)? Hier bedarf es zumindest einer Klarstellung, dass es den Providern aufgrund ihrer Unternehmens- und ggf. Medienfreiheit freigestellt sein muss, Kommunikationsinhalte auch innerhalb der Grenzen der Meinungsfreiheit zu sperren. Anderes kann allenfalls für die „Riesen“ gelten.

Art. 18 DSA

Das Schiedsgerichtssystem in Art. 18 des Entwurfs hat ein Kostenproblem: Viele private Beteiligte werden sich die Kosten eines solchen Schiedsgerichts nicht leisten können, selbst wenn die Schiedseinrichtung nur die tatsächlich entstandenen Kosten in Rechnung stellt, wie es in Art. 18 Abs. 3 vorgesehen ist. Zumindest in Deutschland könnten Gerichtskosten - jedenfalls in den meisten veröffentlichten Fällen - deutlich geringer sein. Die Kostenfrage bleibt im Ergebnis offen. In jedem Falle darf der Verbraucher nicht deutlich belastet werden.

Art. 19 DSA

Gemäß Art. 19 Abs. 2 DSA kann der Digital Services-Koordinator eines Mitgliedsstaats einen bestimmten Hinweisgeber aufgrund dessen Bewerbung als „trusted flagger“ anerkennen, wenn er ein „Vertreter gemeinschaftlicher Interessen“ ist und folgende weitere Voraussetzungen erfüllt:

- besondere Fachkenntnisse;
- Unabhängigkeit von jeder Online-Plattform;
- zügige, sorgfältige und objektive Tätigkeit.

Die Europäische Kommission möchte die Daten aller europäischen „trusted flaggers“ sammeln und in einer öffentlich zugänglichen Datenbank verwalten (Art. 19 Abs. 3 und Abs. 4 DSA). Die Anlegung umfangreicher Datenbanken durch die Kommission ist datenschutzrechtlich problematisch und zudem rechtsstaatlich heikel. Dies sollte allenfalls durch den Rat aller Digital Service Koordinatoren (vgl. Art. 47 DSA) erfolgen, da eine umfassende Kontrolle von Netzaktivitäten durch die Europäische Kommission abzulehnen ist.

Art. 22 DSA

Art. 22 DSA verpflichtet den Betreiber einer Online-Plattform zur Erhebung zahlreicher (personenbezogener) Daten von Händlern, die Waren und Dienstleistungen auf der Plattform anbieten. Dies mag im Sinne des Verbraucherschutzes zu begrüßen sein, sollte jedoch ausdifferenzierter gestaltet sein und unter Berücksichtigung der unterschiedlichen Größe und Kategorien von Plattformen und ihren technischen und wirtschaftlichen Möglichkeiten formuliert werden. Dabei müssten auch Regelungen getroffen werden, die der datenschutzrechtlichen Dimension der Datensammlung Rechnung tragen.

Art. 24 DSA

In Art. 24 DSA geht es um „Transparenz“ durch Informationspflichten für Online-Werbung. Hier stellt sich die Frage, ob es nicht wünschenswert ist, für Online-Werbung ein eigenes Rechtsinstrument zu schaffen und den Anbietern ein Dickicht verschiedener Vorschriften in verschiedenen Verordnungen (DSGVO, ePrivacy, DSA) zu ersparen. „Transparenz“ können zudem allenfalls die großen Werbenetzwerke schaffen - mit den Google-Diensten an der Spitze. Plattformen steuern die Werbung selten selbst, sondern arbeiten mit spezialisierten Dienstleistern zusammen. Nur die Dienstleister verfügen über Informationen, die „Transparenz“ schaffen können.

Richtigerweise müsste die Norm diejenigen verpflichten, die über diese Informationen verfügen. Gegebenenfalls müsste diese Information über einen Link auf der Werbeplattform zu den Werbedienstleistern zur Verfügung gestellt werden.

Undifferenzierte Offenlegungspflichten – also die „Daumenschraube auf der Personalisierung“ – bergen das Risiko, dass das Angebot nicht auf Gewinnerzielung gerichteter Plattformen zunehmend weniger lohnenswert wird. Solche Plattformen sollten von der Regelung ausgenommen werden.

Umgang mit systemischen Risiken, Art. 26, 27 DSA

Sehr große Plattformen sollen nach Art. 26 DSA jährlich systemische Risiken bestimmter Art identifizieren, analysieren und einschätzen. Sie sollen dann nach Art. 27 DSA angemessene, verhältnismäßige und effektive Mittel einsetzten, um solche Gefahren abzumildern. Zu diesen Gefahren gehören:

- die Verbreitung illegaler Inhalte (Art. 26 Nr. 1 lit. a DSA)
- negative Auswirkungen für den Schutz vor privatem und familiärem Leben, für die Meinungs- und Informationsfreiheit, das Verbot der Ungleichbehandlung und die Kinderrechte (Art. 26 Nr. 1 lit. b DSA)
- absichtliche Manipulationen ihrer Dienste mit Auswirkungen auf die öffentliche Gesundheit, Minderjährige, bürgerlichen Diskurs, oder aktuelle oder vorhersehbare Auswirkungen auf Wahlen und öffentliche Sicherheit (Art. 26 Nr. 1 lit. c DSA)

Sehr große Plattformen als quasi-staatliche Akteure?

Es liegt sicher im öffentlichen Interesse, die Verbreitung illegaler Inhalte zu verhindern. Es liegt ebenso im öffentlichen Interesse, absichtliche Manipulationen besonders großer Intermediäre wie der sehr großen Plattformen zu verhindern. Letzteres liegt sicher auch im Interesse der Plattformen selbst. Insoweit begegnen die angesprochenen Vorschriften keinen großen Bedenken, auch wenn es im Einzelfall schwer sein dürfte, festzustellen, welche Manipulationen wann Auswirkungen auf den

bürgerlichen Diskurs vorliegen. Die Regelungen zum ersten und zum letzten Spiegelstrich begegnen daher keinen grundsätzlichen Bedenken.

Besonderheit des Art. 26 Nr. lit. b DSA

Schwieriger ist dies bei den Gefahren, denen die Plattformbetreiber nach Art. 26 Nr. 1 lit. b DSA begegnen sollen. Grundsätzlich ist es zwar richtig, dass es sinnvoll und evtl. auch nötig ist, gegen solche Gefahren vorzugehen. Dennoch bestehen hier erhebliche Bedenken:

Wann das private und familiäre Leben schutzbedürftig ist, wird von Einzelnen sehr unterschiedlich gesehen – auch verschiedene Gesellschaften sehen das oft verschieden. Noch stärker zeigt sich das, wenn es um Meinungs- und Informationsfreiheit geht. Morddrohungen gegen Andersdenkende stellen sicher Gefahren dar. Sie sind aber ebenso klar illegale Inhalte und fallen daher schon unter die in Art. 26 Nr. 1 lit. a DSA genannten Gefahren. Ist aber z.B. die – nicht seltene – Aufforderung, einem Andersdenkenden einen Lehrstuhl zu entziehen – wahlweise, weil er z.B. nach Meinung der Fordernden ungläubig, Rassist oder homosexuell sei, schon eine Gefahr für die Meinungsfreiheit? Gilt das nur, wenn derjenige, der die Gefahren bekämpfen soll – also die Verantwortlichen der großen Plattformen – der Ansicht sind, dass ein von einer solchen Aufforderung Betroffener kein Ungläubiger, Rassist oder Homosexueller ist? Oder gilt das immer – also auch für Aufforderungen, offenen und bekennenden Rassisten einen Lehrstuhl zu entziehen? Hängt es davon ab, wie viele solche Aufforderungen unterstützen? Oder gilt dies nur, wenn dadurch die Gefahr entsteht, dass der Lehrstuhl tatsächlich entzogen wird? Kommt es darauf an, wie oft solche Aufforderungen als Kampfmittel eingesetzt werden? Ähnliches wird für Gefahren für das Verbot der Ungleichbehandlung gelten.

Unklare Grenzen der Befugnisse von großen Plattformen

Das Problem besteht hier darin, dass jede denkbare Maßnahme zur Bekämpfung solcher Gefahren gleichzeitig dazu führt, dass in Freiheitsrechte derjenigen eingegriffen wird, die diese Gefahren auslösen. Diesen werden z.B. Äußerungen erschwert oder gar unmöglich gemacht. Das ist grundrechtlich sogar zulässig: „Keine Freiheit für die

Feinde der Freiheit.“ ist jedenfalls in Deutschland nach den Erfahrungen der Weimarer Republik Teil der Grundrechtsordnung. Aber: Es kann sich nur um seltene, für Extremfälle vorbehaltene Ausnahmen handeln. Beschränkt man das Vorgehen gegen die Freiheit einzelner nicht auf einen so engen Rahmen, droht die Gefahr, dass diejenigen, die die Eingriffe vornehmen, nur noch ihnen persönlich genehme Meinungen zulassen. Freiheit ist nun mal in erster Linie die Meinung des Andersdenkenden.

Für solche Einschränkungen muss es daher in den entsprechenden Gesetzen klare Vorgaben geben. Diese Vorgaben fehlen hier fast ganz. Es wird weder vorgegeben, nach welchen Kriterien hier Gefahren definiert werden noch werden die entgegenstehenden Grundrechte und Grundfreiheiten benannt. Es wird im Gesetzestext noch nicht einmal von erheblichen Gefahren gesprochen. Dass es nur um systemische Gefahren geht, verhindert nur Maßnahmen im Einzelfall, nicht jedoch ein Vorgehen gegen eine Vielzahl gleichgelagerter - nach Ansicht der Verantwortlichen - gefährlicher Handlungen.

Darüber hinaus sind nach dieser Norm in erster Linie die Plattformbetreiber in der Pflicht, festzustellen, wann hier Gefahren drohen. Sie treffen dann auch die Entscheidung, gegen wen wie vorgegangen wird. Dies ist aber im Prinzip eine staatliche Aufgabe demokratisch legitimierter Behörden, die ggf. richterlich überprüft werden kann. Sie kann nicht einfach den Betreibern großer Plattformen übertragen werden.

Die Regelungen zur Bekämpfung systemischer Risiken sind daher grundsätzlich sehr bedenklich, soweit sie die in Art. 26 Nr. 1 lit. b DSA genannten Gefahren betreffe.

Art. 35 und 36 DSA

Eine zentrale Stellung behält sich die Europäische Kommission bei der Entwicklung von "Codes of Conduct" in Art. 35 und 36 des Entwurfs vor. Die Bestimmungen wirken unübersichtlich und geben der Kommission die rechtsstaatlich problematische Befugnis, an der weiteren Entwicklung von Regeln für Diensteanbieter im Netz in bestimmender Position mitzuwirken.

Compliance-Aufwand

Wenn die DSA-Vorstellungen der Europäischen Kommission Wirklichkeit werden, kommt auf die Unternehmen erheblicher zusätzlicher Compliance-Aufwand zu. Dies gilt natürlich ganz besonders für die Betreiber der sehr großen Online-Plattformen, die vor allem folgende (jeweils detaillierte) Vorgaben zu erfüllen haben:

- Bestellung von Compliance-Beauftragten (Art. 32 DSA);
- regelmäßige Vornahme von „Risikobewertungen“ (Art. 26 DSA);
- Maßnahmen der „Risikominimierung“ geben (Art. 27 DSA);
- jährliche Audits (Art. 28 DSA);
- halbjährliche Berichtspflichten (Art. 33 und 13 DSA);
- Hinweismanagementsystem (Art. 14 DSA);
- Beschwerdemanagementsystem (Art. 15 sowie 17 bis 20 DSA);
- Transparenzpflichten (Art. 12, 24, 29 und 30 DSA);
- Identifikationspflichten bei Online-Händlern (Art. 22 DSA).

Die „Riesen“, für die diese Compliance-Vorschriften gelten, haben die personellen und finanziellen Ressourcen, um den neuen Anforderungen gerecht zu werden. Dies zeigt die Erfahrung mit der Umsetzung der DSGVO, die kleinere Unternehmen meist vor deutlich größere Herausforderungen stellte, als dies bei den großen Anbietern der Fall war.

Rechtsdurchsetzung

Compliance bedeutet in der Praxis unternehmerische Bürokratie. Und von der Liebe zur Bürokratie sind auch die Bestimmungen zur Rechtsdurchsetzung durch Digital Services-Koordinatoren, durch den Europäischen Ausschuss für Digital Service und die Europäische Kommission durchzogen. Diese Bestimmungen machen – nach dem Vorbild der DSGVO – mit Art. 38 bis 66 DSA fast die Hälfte des DSA-Entwurfs aus. Auffällig ist, dass die Bestimmungen zur Rechtsdurchsetzung bei den sehr großen Online-Plattformen durch die Europäische Kommission (Art. 50 bis 66 DSA) primär auf Bußgelder setzen, während die Bußgelder in dem Abschnitt zur Rechtsdurchsetzung

bei den übrigen Providern (Art. 38 bis 49 DSA) in Art. 42 DSA nur rudimentär und eher stiefmütterlich behandelt werden. Weshalb man bei der Rechtsdurchsetzung – je nach der Größe der Provider – völlig unterschiedliche Wege geht, erschließt sich nicht.

Nach den Vorstellungen der Europäischen Kommission sollen alle Provider – unabhängig von ihrer Größe – demnächst von zwei ganz unterschiedlichen Behörden beaufsichtigt werden – einer Datenschutzbehörde für Fragen des Datenschutzes und einem Digital Services-Koordinatoren für Fragen des DSA. Ein Zusammenwirken der Behörden ist im DSA-Entwurf nicht vorgesehen, obwohl ein solches Zusammenwirken alles andere als fernliegt. Denn bei der Erfüllung der Verpflichtungen zum Hinweis- und Beschwerdemanagement wird es notwendig sein, eine Vielzahl personenbezogener Daten zu verarbeiten. Konflikte mit dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) werden nicht ausbleiben. Und was unternimmt dann ein Provider, wenn der Digital Services-Koordinator von ihm die Verarbeitung von Personendaten verlangt, obwohl die Erforderlichkeit einer solchen Verarbeitung - datenschutzrechtlich – alles andere als evident ist?

„Unabhängigkeit“ der Digital Services-Koordinatoren

Dass es jetzt neben den Datenschutzbehörden weitere „unabhängige“ Behörden zur Netzaufsicht geben soll, ist problematisch, da es an einer hinreichenden parlamentarischen Kontrolle fehlt. Es bedarf einer parlamentarischen Verantwortlichkeit der Behörden. „Unabhängigkeit“ brauchen Behörden nur dann, wenn es ihre Aufgabe – wie beim Datenschutz – ist, (auch) staatliche Behörden und Einrichtungen zu kontrollieren. Dies ist bei den Digital Service-Koordinatoren nicht der Fall.