

19.01.24**Empfehlungen**
der Ausschüsse

Vk - FJ - In - K - R - U - Wi

zu **Punkt ...** der 1041. Sitzung des Bundesrates am 2. Februar 2024

Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze

A

Der **federführende Verkehrsausschuss (Vk)**,der **Ausschuss für Innere Angelegenheiten (In)**,der **Ausschuss für Kulturfragen (K)**,der **Rechtsausschuss (R)**,der **Ausschuss für Umwelt, Naturschutz und nukleare Sicherheit (U)** undder **Wirtschaftsausschuss (Wi)**

empfehlen dem Bundesrat, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

In 1. Zu Artikel 1 (§ 12 Absatz 3 DDG)

(bei
Annahme
entfällt
Ziffer 2)

In Artikel 1 § 12 Absatz 3 sind die Wörter „Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständige Behörde“ durch die Wörter „Die Aufsichtsbehörden der Länder im Sinne des § 40 des Bundesdatenschutzgesetzes sind zuständige Behörden“ zu ersetzen.

Folgeänderung:

In Artikel 1 § 33 Absatz 8 Nummer 4 sind die Wörter „der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit“ durch die Wörter „die jeweilige Aufsichtsbehörde der Länder im Sinne des § 40 des Bundesdatenschutzgesetzes“ zu ersetzen.

Begründung:

Die in § 12 Absatz 3 DDG enthaltene Zuständigkeitsübertragung an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) begegnet erheblichen Einwänden und überzeugt auch aus verfahrenswirtschaftlichen Gesichtspunkten nicht. Vielmehr sollte aus den nachfolgenden Gründen eine Zuständigkeit der Datenschutzaufsichtsbehörden der Länder vorgesehen werden.

Adressaten der Verpflichtungen nach Artikel 26 und 28 DSA sind ausschließlich nicht öffentliche Stellen (Unternehmen als Anbieter von Online-Plattformen), deren Datenverarbeitung nach § 40 BDSG der Datenschutzkontrolle durch die Datenschutzaufsichtsbehörden der Länder unterliegt. Entgegen der Einzelbegründung zu § 12 Absatz 3 DDG, welche auf eine einschlägige Erfahrung und Expertise des BfDI verweist, muss nach Ansicht des Bundesrates festgestellt werden, dass diesem bislang nicht mehr als eine eingeschränkte sektorale Aufsicht über Telekommunikationsanbieter obliegt. Demgegenüber besteht im vorliegend relevanten Bereich auf Seiten der Landesdatenschutzaufsichtsbehörden eine umfassende Vollzugserfahrung.

Auch wenn Artikel 53 DSA ein eigenständiges Beschwerdeverfahren regelt, sind Berührungspunkte einer solchen Beschwerdeprüfung zu allgemeindatenschutzrechtlichen Fragen, die der Vollzugsverantwortung der Datenschutzaufsichtsbehörden der Länder vorbehalten sind, regelmäßig vorbestimmt. Ob ein Verantwortlicher einer Online-Plattform besonders geschützte Daten nach Artikel 9 DSGVO zu Werbezwecken und Profiling nutzt, berührt von vornherein nicht nur Artikel 26 Absatz 3 DSA, sondern genauso etwa allgemeine Erhebungsbefugnisse im Sinne von Artikel 9 DSGVO oder Sicherheitsanforderungen im Sinne von Artikel 32 DSGVO. Die Datenschutzaufsichtsbehörden der Länder sind im Rahmen ihrer Überwachungsaufgaben gegenüber Werbetreibenden, Online-Shops, Finanzinstituten oder Auskunftsteilen regelmä-

Big mit vergleichbaren Fragestellungen befasst und verfügen insofern über die bereits genannte umfassende einschlägige Vollzugserfahrung und Expertise.

Eine Zuständigkeitszuweisung an den BfDI führt darüber hinaus absehbar zur Aufspaltung von datenschutzrechtlichen Beschwerdeverfahren, was den Zielen der Effektivität und Rechtssicherheit widerspricht: Beschwerden werden regelmäßig die Datenverarbeitung eines Internet-Angebots oder einer Online-Plattform als solche thematisieren, nicht allein die Ausrichtung des Werbeangebots. Dies würde stets die Frage nach Abgaben und Verfahrensabtrennungen zwischen dem BfDI und den Landesdatenschutzaufsichtsbehörden aufwerfen. Diese Spaltung, etwa des Beschwerdeverfahrens in eine Beschwerde im Anwendungsbereich des DDG und – gesondert – eine solche nach Artikel 77 DSGVO, würde vermieden, wenn § 12 Absatz 3 DDG von vornherein nicht anders als das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG – vergleiche § 1 Absatz 1 Nummer 8 Halbsatz 2 TTDSG) eine Zuständigkeit der nach § 40 BDSG zuständigen Behörden der Länder vorsehen würde (vergleiche BR-Drucksache 163/21 (Beschluss), Ziffer 8, in deren Rahmen eine entsprechende Zuständigkeitszuweisung an den BfDI abgelehnt wurde).

Auch wenn verschiedene Bestimmungen, wie beispielsweise § 17 DDG zur Unterstützung bei der Erstellung des Tätigkeitsberichts, die Verpflichtungen zum Informationsaustausch nach § 18 DDG oder die Koordinierungserfordernisse im Rahmen zentraler Beschwerdebearbeitung nach § 20 DDG Schnittstellen zwischen einer auf Bundesebene angesiedelten Koordinierungsstelle und Vollzugsbehörden der Länder schaffen würden, würde eine Artikel 83 des Grundgesetzes folgende Zuständigkeitsverteilung weder die effektive Anwendung noch die praktische Durchsetzung des DSA unterlaufen, zumal Kooperationen und ein Informationsaustausch nach den Prinzipien der loyalen Zusammenarbeit (EuGH, Urteil vom 4. Juli 2023, C-252/21) über den Wortlaut des § 18 hinaus ohnehin erforderlich bleiben.

Schließlich ist auch die Beteiligung des BfDI an den Durchsetzungsaufgaben der Koordinierungsstelle für digitale Dienste nicht zu unterstützen, da die vorgesehene Mitwirkung der Gewährleistung einer unabhängigen Datenschutzkontrolle widerspricht. Dies beruht darauf, dass der BfDI zugleich zuständige Datenschutzaufsichtsbehörde gegenüber der Bundesnetzagentur und der Koordinierungsstelle für digitale Dienste wäre. Konflikte bei der Verarbeitung personenbezogener Daten sind nicht zuletzt aufgrund der weitreichenden Verfahrensregelungen der §§ 24 ff. DDG indessen vorgezeichnet. Eine Kontrollstelle, die zugleich in die Vollzugsaufgaben nach dem DDG zuarbeitend gegenüber der Koordinierungsstelle für digitale Dienste eingebunden wäre, gefährdet insoweit die geforderte Unabhängigkeit oder steht jedenfalls in einem Rollenkonflikt.

Die Folgeänderung passt die Zuständigkeit im Bußgeldverfahren entsprechend an.

Vk
Wi
2. Zu Artikel 1 (§ 12 Absatz 3 DDG)

(entfällt
bei
Annahme
von
Ziffer 1)

In Artikel 1 ist § 12 Absatz 3 wie folgt zu fassen:

„(3) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die nach Landesrecht für den Datenschutz zuständigen Behörden sind zuständige Behörden für die Durchsetzung des Artikels 26 Absatz 3 und des Artikels 28 Absatz 2 und 3 der Verordnung (EU) 2022/2065.“

Begründung:

§ 12 Absatz 3 DDG weist die Zuständigkeit für die Durchsetzung von Artikel 26 Absatz 3 und Artikel 28 Absatz 2 des Digital Services Act (DSA) dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu. Dabei geht es um die Zuständigkeit für das Verbot der Anzeige von Werbung, die auf Profiling gemäß Artikel 4 Nummer 4 Datenschutzgrundverordnung (DSGVO) beruht unter Verwendung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO beziehungsweise unter Verwendung von Daten minderjähriger Nutzer.

Wie der Begründung zu § 12 Absatz 3 DDG zu entnehmen ist, verfolgt die Regelung das Ziel, Abstimmungs- und Koordinierungsbedarfe zu verringern. Hier droht allerdings das Gegenteil einzutreten: Mit § 12 Absatz 3 DDG würde eine Aufsichtsstruktur eingeführt, die eine nicht gebotene nationale Zuständigkeitszersplitterung und weitere Abstimmungsbedarfe in der Praxis nach sich zöge und einheitliche Lebens- und Prüfungsvorgänge aufspalten würde.

Der Vorgang der Anzeige von Werbung auf einer Online-Plattform ist im Regelfall eng mit Prozessen verknüpft, die in den Anwendungsbereich von § 25 TTDSG (künftig § 25 TDDDG) fallen, und mit der Verarbeitung personenbezogener Daten insbesondere zum Zwecke des Profiling. Für deren Kontrolle sind (und bleiben auch künftig) die Landesdatenschutzbehörden zuständig.

Mit der Einführung der Zuständigkeit des BfDI für die Überprüfung von Webseiten bezüglich Profiling entstünde in der Folge zusätzlicher Abstimmungsbedarf zwischen dem BfDI und den Landesdatenschutzbehörden. Dies kann vermieden werden, wenn die Landesdatenschutzbehörden für die Webseiten, für die sie ohnehin zuständig sind, auch bezüglich Profiling im Sinne von Artikel 26 Absatz 3 und Artikel 28 Absatz 2 des DSA zuständig werden.

In
R

3. Zu Artikel 1 (§ 13 DDG)

- a) Der Bundesrat weist darauf hin, dass es im Vergleich zur aktuellen Rechtslage zu regulatorischen Rückschritten bei der Meldung strafbarer Inhalte durch die Plattformbetreiber an die Strafverfolgungsbehörden kommen wird. Anders als das Netzwerkdurchsetzungsgesetz, das in seinem § 3a Absatz 2 einen Katalog meldepflichtiger Straftatbestände definiert, sieht Artikel 18 des Digital Services Act eine Meldepflicht nur bei Straftaten vor, die eine Gefahr für das Leben oder die Sicherheit von Personen darstellen. Insbesondere Straftaten gegen die öffentliche Ordnung werden hiervon nicht rechtssicher erfasst. § 13 DDG beschränkt sich insofern auf eine bloße Zuständigkeitsregelung und verzichtet auf eine nationalrechtliche Erstreckung der Meldepflicht auf weitere Straftaten.
- b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob im nationalen Recht eine Ausdehnung der Meldepflicht auf Straftaten gegen die öffentliche Ordnung unionsrechtskonform möglich ist. Sollte dies zu verneinen sein, wird gebeten zu prüfen, ob zumindest eine über Artikel 18 Digital Services Act hinausgehende Meldepflicht für Plattformbetreiber mit Sitz in Deutschland sowie außerhalb der EU normiert werden kann.
- c) Der Bundesrat fordert die Bundesregierung auf, ungeachtet gesetzlicher Regelungen auch darauf hinzuwirken, dass sich die zuständigen Bundesbehörden zur Schaffung einer sachgerechten und einheitlichen Meldepraxis sozialer Netzwerke auf europäischer Ebene in einem geeigneten Rahmen, wie zum Beispiel dem durch den Digital Services Act vorgesehenen „Europäischen Gremium für digitale Dienste“, für eine Ergänzung des Verhaltenskodex zur Bekämpfung illegaler Hassrede im Netz und für die Schaffung von entsprechenden Leitlinien einsetzen.

Begründung:

§ 3a NetzDG verpflichtet große soziale Netzwerke, bestimmte katalogartig aufgelistete strafbare Inhalte, die der Betreiber infolge einer Beschwerde entfernt oder gesperrt hat, zusammen mit bestimmten Nutzerdaten an die Strafverfolgungsbehörden zu übermitteln. Diese Vorschrift soll im Zuge des vorliegenden Gesetzgebungsverfahrens vollständig aufgehoben werden. Künftig richtet sich die Meldepflicht von Plattformbetreibern allein nach Artikel 18 DSA. Dieser verpflichtet die Betreiber, Informationen, die den Verdacht begründen, dass eine Straftat, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, begangen wurde, begangen wird oder began-

gen werden könnte, unverzüglich den Strafverfolgungs- oder Justizbehörden des betreffenden Mitgliedstaats oder der betreffenden Mitgliedstaaten zu übermitteln.

Diese Mitteilungspflicht bleibt hinter der Konzeption des § 3a NetzDG deutlich zurück. Die Grenzen der Mitteilungspflicht sind sehr unklar ausgestaltet, was die Gefahr birgt, dass die Betreiber die Pflicht sehr restriktiv handhaben werden. Das betrifft insbesondere die Frage, ob die Meldepflicht auch Straftaten gegen die öffentliche Ordnung wie zum Beispiel Volksverhetzung nach § 130 StGB oder das Verwenden von Kennzeichen verfassungswidriger und terroristischer Organisationen nach § 86a StGB erfasst. Auch in Bezug auf diese Straftaten ist es zur wirksamen Bekämpfung von strafbarem Hass im Netz unerlässlich, dass die Strafverfolgungsbehörden zuverlässig Kenntnis erlangen und die nötigen Daten zur Verfügung gestellt bekommen, um Ermittlungen gegen die Täter einleiten zu können.

Die Bundesregierung wurde aus dem Kreis der Länder mehrfach gebeten zu prüfen, ob im nationalen Recht noch Spielräume für eine erweiterte Meldepflicht – idealerweise im Umfang des § 3a NetzDG – bestehen. Im vorliegenden Gesetzentwurf findet sich zwar eine auf Artikel 18 DSA Bezug nehmende Vorschrift (§ 13 DDG), diese erschöpft sich aber in einer bloßen Zuständigkeitsregelung zugunsten des Bundeskriminalamts als derjenigen Stelle, die Meldungen der Plattformbetreiber über Straftaten entgegenzunehmen und dann an die zuständigen Strafverfolgungsbehörden weiterzugeben hat. Weder Gesetzestext noch Begründung lassen erkennen, ob sich die Bundesregierung mit dem Anliegen der Länder auseinandergesetzt hat, mögliche Spielräume im nationalen Recht für erweiterte Meldepflichten zu identifizieren.

Das Unionsrecht, insbesondere der als Verordnung unmittelbar geltende DSA, setzt nationalen Regelungen zwar unzweifelhaft Grenzen, in der juristischen Literatur wird mit beachtlichen Argumenten aber durchaus vertreten, dass noch Spielräume im nationalen Recht für eine erweiterte Meldepflicht bestehen (vergleiche Raue/Heesen: Der Digital Services Act, NJW 2022, 3537, 3541; Dregelies: Digital Services Act MMR 2022, 1033, 1036). Mit diesen Meinungen muss im weiteren Gesetzgebungsverfahren eine ausführliche Auseinandersetzung erfolgen. Sollte diese Prüfung dazu führen, dass jedenfalls für im EU-Ausland sitzende Plattformbetreiber keine über Artikel 18 DSA hinausgehenden Meldepflichten geregelt werden können, muss erwogen werden, ob die Pflicht, vor allem auch Straftaten gegen die öffentliche Ordnung zu melden, zumindest für Plattformbetreiber mit Sitz in Deutschland sowie im Nicht-EU-Ausland etabliert werden sollte. Hier erscheinen die unionsrechtlich verbleibenden Spielräume jedenfalls deutlich größer.

Unabhängig von der Möglichkeit, die Meldepflicht nach Artikel 18 DSA im nationalen Recht zu konkretisieren, können auf Freiwilligkeit beruhende Regelungen in Leitlinien und Verhaltenskodizes ein wirksames Mittel darstellen, um auf eine EU-weit einheitliche Meldepraxis für strafbaren Hass und Hetze in sozialen Netzwerken hinzuwirken. Als Beispiel nach bisheriger Rechtslage kann der durch die Kommission gemeinsam mit verschiedenen Plattformanbietern 2016 erstellte „Verhaltenskodex zur Bekämpfung illegaler Hetze im Internet“ genannt werden, der jedoch in seiner bisherigen Fassung keine Ausführungen zur Meldung strafbarer Inhalte an die Strafverfolgungsbehörden enthält.

Artikel 45 DSA sieht vor, dass die Kommission und das gemäß Artikel 61 DSA aus zuständigen Behörden der Mitgliedstaaten zu bildende „Europäische Gremium für digitale Dienste“ die Erstellung von Verhaltenskodizes fördern. Als Ziel der Verhaltenskodizes wird dabei unter anderem ausdrücklich die Bekämpfung rechtswidriger Inhalte und systemischer Risiken benannt. Nach Erwägungsgrund 80 DSA stellt die Verbreitung rechtswidriger Hassrede ein systemisches Risiko dar. Die Kommission hat mitgeteilt, dass bereits seit März 2023 an einem neuen Verhaltenskodex gearbeitet wird, der nach den Regeln des DSA formalisiert werden soll (vergleiche Gemeinsame Mitteilung der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik mit dem Titel „Kein Platz für Hass: Ein geeintes Europa gegen Hass“ vom 6. Dezember 2023 (JOIN(2023) 51 final), Seite 8). Es bietet sich daher an, über die im Europäischen Gremium für digitale Dienste vertretene Bundesbehörde darauf hinzuwirken, dass zur Kompensation der Rückschritte von Artikel 18 DSA gegenüber § 3a NetzDG ein von möglichst vielen sozialen Netzwerken anerkannter neuer Verhaltenskodex geschaffen oder der bestehende Verhaltenskodex entsprechend um Regelungen zur Meldung von strafbaren Formen von Hass und Hetze ergänzt wird. Eine hierdurch etablierte sachgerechte und einheitliche Meldepraxis könnte gewährleisten, dass den Strafverfolgungsbehörden der Mitgliedstaaten durch die sozialen Netzwerke bei strafbarer Hate Speech die für die Strafverfolgung erforderlichen Daten zur Verfügung gestellt werden.

Zur Erhöhung der Transparenz und zur Gewährleistung der Wirksamkeit der Selbstverpflichtung sollte zudem vorgesehen werden, dass die Plattformen über die entsprechenden Transparenzverpflichtungen der Artikel 15, 24 und 42 DSA hinaus auch regelmäßig Informationen dazu veröffentlichen, inwieweit sie strafbare Inhalte an die zuständigen Strafverfolgungsbehörden gemeldet haben.

K 4. Zu Artikel 1 (§ 14 Absatz 3 Satz 2 – neu – DDG)

Dem Artikel 1 § 14 Absatz 3 ist folgender Satz anzufügen:

„Die Koordinierungsstelle kooperiert in ihrer Forschungstätigkeit soweit möglich mit externen Forschenden.“

Begründung:

Die Datenökonomie insbesondere der großen Plattformen ist ein ebenso dynamisches wie strukturell aufwendiges Forschungsfeld, innerhalb dessen es in vielen Fragen noch keinen grundlegenden Konsens gibt. Eine Kooperation und Vernetzung in der Forschung ist damit dringend geboten. Da die in der Begründung des Gesetzentwurfes in Aussicht genommene Höhe des Forschungsetats mit 300 000 Euro auch nicht groß ist, würde der Etat durch Kooperation mit anderen Einrichtungen und Forschungsverbänden zudem eine Hebelwirkung erfahren und dadurch die Forschungstätigkeit der Koordinierungsstelle stärken.

R 5. Zu Artikel 1 (§ 18 Absatz 3,
§ 19 Absatz 2 und 3 DDG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Aufnahme einer Regelung zu Lösungsfristen und gegebenenfalls Aussonderungsüberprüfungsfristen hinsichtlich der der Koordinierungsstelle übermittelten personenbezogenen Daten geboten ist.

Begründung:

Die in §§ 18 Absatz 3, 19 Absatz 2 und 3 DDG vorgesehenen Regelungen erlauben die Übermittlung personenbezogener Daten an die Koordinierungsstelle durch andere Behörden, ohne eine Regelung zur höchsten zulässigen Dauer der Speicherung der Daten vorzusehen.

Unionsrechtlich nicht vollständig determiniertes innerstaatliches Recht ist primär am Maßstab der Grundrechte des Grundgesetzes zu messen, auch wenn das innerstaatliche Recht der Durchführung des Unionsrechts dient (vergleiche BVerfG, Beschluss vom 6. November 2019 – 1 BvR 16/13 –, BVerfGE 152, 152-215, Rn. 42 f.). So liegt es hier, da der Datenaustausch zwischen den Behörden in den umzusetzenden Verordnungen nicht geregelt beziehungsweise vorgegeben ist. Die Übermittlung personenbezogener Daten, mit der eine Behörde die von ihr erhobenen Daten einer anderen Stelle zugänglich macht, begründet einen eigenen Grundrechtseingriff, welcher an dem Grundrecht zu messen ist, in das bei der ursprünglichen Datenerhebung eingegriffen wurde (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, BVerfGE 162, 1-178, Rn. 230). Danach ist der Eingriff an dem Recht auf informationelle Selbstbestimmung aus Artikel 1 Absatz 1 in Verbindung mit Artikel 2 Absatz 1 GG zu messen. Die Nutzung personenbezogener Daten für die behördliche Aufgabenwahrnehmung muss den Verhältnismäßigkeitsanforderungen genügen. Um sicherzustellen, dass die Datenübermittlung und -verwertung auf das erforderliche Maß beschränkt ist, erscheint die Normierung von Lösungsfristen als notwendig. Der Regelung einer Lösungsfrist dürfte veranlasst sein, um zu

gewährleisten, dass die personenbezogenen Daten nicht dauerhaft, sondern zeitlich begrenzt gespeichert und nach der bestimmten Zeit gelöscht werden. Die Löschungspflicht konkretisiert auch den datenschutzrechtlichen Grundsatz, dass nur notwendige Datenverarbeitungen erlaubt sind.

K 6. Zu Artikel 1 (§ 21 Absatz 11 Satz 2 – neu – DDG)

Dem Artikel 1 § 21 Absatz 11 ist folgender Satz anzufügen:

„Die schriftlichen Dokumente des Beirats wie Berichte, Empfehlungen, Gutachten und Positionspapiere sind entsprechend der Vorgaben für die Koordinierungsstelle in § 17 Absatz 3 frei zugänglich auf deren Webseite zu veröffentlichen.“

Begründung:

In Präzisierung von Artikel 55 Absatz 1 DSA legt § 17 Absatz 3 DDG der Koordinierungsstelle Transparenzpflichten in der Weise auf, dass der Tätigkeitsbericht nicht nur an die gesetzgebenden Körperschaften zu adressieren ist, sondern zeitgleich in elektronischer Form und in einem für Menschen mit Behinderungen barrierefreien Format auf der Internetseite der Koordinierungsstelle zu veröffentlichen ist. Hinzu treten weitere Informationspflichten gegenüber der Öffentlichkeit (vergleiche § 28 DDG). Da der Beirat die Koordinierungsstelle in grundsätzlichen Fragen berät, Empfehlungen ausspricht und wissenschaftliche Fragestellungen an die Koordinierungsstelle heranträgt (vergleiche § 21 DDG), ist diese Transparenz auch auf den Beirat auszudehnen, um Entscheidungen der Koordinierungsstelle für die Öffentlichkeit verständlich und nachvollziehbar zu halten und insbesondere die Regeln guter wissenschaftlicher Praxis für die durch DSA und DDG ermöglichte Forschung sicherzustellen.

R 7. Zu Artikel 1 (§ 25 Absatz 3 DDG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob hinsichtlich des Artikel 1 § 25 Absatz 3 (Durchsuchung von Büro- und Geschäftsräumen) das verfassungsrechtliche Zitiergebot (Einschränkung des Artikel 13 des Grundgesetzes) gewahrt ist und gegebenenfalls eine entsprechende Bestimmung in das Gesetz aufzunehmen sein könnte.

Begründung:

In § 25 Absatz 3 DDG sind Ermächtigungen zur Durchsuchung von Büro- und Geschäftsräumen enthalten. Hierin dürfte eine Einschränkung des Artikel 13 des Grundgesetzes liegen, denn neben Privatwohnungen fallen auch Betriebs- und Geschäftsräume in dessen Schutzbereich (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 192). Für Grundrechtseingriffe verlangt Artikel 19 Absatz 1 Satz 2 des Grundgesetzes, dass das einschränkende Gesetz das Grundrecht unter Angabe des Artikels nennt. Das Zitiergebot dient – nach der engen Auslegung des BVerfG – der Sicherung derjenigen Grundrechte, die aufgrund eines spezifischen, vom Grundgesetz vorgesehenen Gesetzesvorbehalts über die im Grundrecht selbst angelegten Grenzen hinaus eingeschränkt werden können (BVerfG, Beschluss vom 21. Juli 2022 – 1 BvR 469/20 – Rn. 92), also Grundrechte, die auf Grund einer ausdrücklichen Ermächtigung vom Gesetzgeber eingeschränkt werden dürfen. Hierunter fällt das Recht auf Unverletzlichkeit der Wohnung (vergleiche Artikel 13 Absatz 2 bis 5, Absatz 7 des Grundgesetzes). Es ist nicht ersichtlich, dass das Gesetz feststellt, dass Artikel 13 des Grundgesetzes eingeschränkt wird.

In
R8. Zu Artikel 1 (§ 33 Absatz 4 DDG)

- a) Der Bundesrat weist darauf hin, dass digitale Plattformen zu einer Basisinfrastruktur unserer Gesellschaft geworden sind, über die Menschen miteinander kommunizieren und interagieren. Sie haben daher eine herausragende gesellschaftliche Relevanz erlangt. Zugleich ergeben sich Gefährdungslagen daraus, dass Plattformbetreiber Kommunikationsräume schaffen und kontrollieren, aus denen heraus strafbare Handlungen ihrer Nutzer hervorgehen. Zur Wahrung der berechtigten Interessen Dritter und der Gesellschaft bedarf es einer Regulierung. Eine wirksame Regulierung setzt insbesondere eine Verpflichtung zum angemessenen Umgang der Hostingprovider mit eingehenden Beschwerden über rechtswidrige Inhalte voraus. Angesichts einer fehlenden Pflicht zur fortlaufenden Nutzerbeobachtung kann nur auf diese Weise ausreichend gewährleistet werden, dass strafbare Inhalte umgehend entdeckt und entfernt oder gesperrt werden. Pflichtverletzungen müssen mit effektiven Sanktionen bedroht sein. Die Sanktionsvorschrift in § 33 Absatz 4 DDG trägt diesen Anforderungen nicht ausreichend Rechnung, indem sie eine Geldbuße nur für den Fall androht, dass Hostingprovider ihre Entscheidungen über eine Nutzerbeschwerde nicht frei von Willkür oder nicht objektiv treffen und eine solche Handlung beharrlich wiederholen.

- b) Der Bundesrat bittet daher, die Sanktionsvorschrift in § 33 Absatz 4 DDG im weiteren Gesetzgebungsverfahren dahingehend zu ändern, dass nicht zeitnahe, nicht sorgfältige, nicht willkürfreie und nicht objektive Entscheidungen der Hostingprovider über Nutzerbeschwerden über rechtswidrige Inhalte mit effektiven Sanktionen bedroht werden. Bei qualifizierten Verstößen, insbesondere bei offenkundig strafbaren Inhalten, sollten auch strafrechtliche Sanktionen erwogen werden.

Begründung:

Bei der Kontrolle von Inhalten setzt der DSA auf ein reaktives System zum angemessenen Umgang mit eingehenden Beschwerden über rechtswidrige Inhalte. Kernelement ist dabei das in Artikel 16 DSA geregelte Melde- und Abhilfeverfahren. Die Regelung verpflichtet die Netzbetreiber zur Implementierung von Beschwerdemanagementsystemen, die dafür sorgen sollen, dass soziale Netzwerke und andere digitale Plattformen häufiger als bislang strafbare Inhalte von den Plattformen entfernen und damit ihrer Perpetuierung und Verbreitung entgegenwirken. Für den Umgang mit – nach Ansicht der meldenden Person – rechtswidrigen Inhalten zentral ist die Regelung in Artikel 16 Absatz 6 DSA. Nach dessen Satz 1 bearbeiten die Hostingdiensteanbieter alle Meldungen, die sie im Rahmen der in Absatz 1 genannten Verfahren erhalten und entscheiden zeitnah, sorgfältig, frei von Willkür und objektiv über die gemeldeten Informationen. Verstöße hiergegen müssen nach Artikel 52 DSA von den Mitgliedstaaten sanktioniert werden (können). Die Sanktionsdrohung ist ein unentbehrliches Druckmittel, um die Hostingprovider zu einem angemessenen Umgang mit eingehenden Beschwerden zu bewegen.

Für die Umsetzung in nationales Recht sieht § 33 Absatz 4 DDG insoweit eine Bußgeldvorschrift dergestalt vor, dass ordnungswidrig handelt, wer (vorsätzlich) entgegen Artikel 16 Absatz 6 Satz 1 DSA eine Entscheidung nicht frei von Willkür oder nicht objektiv trifft und eine solche Handlung beharrlich wiederholt.

Die Ausgestaltung dieser Regelung wird der Verantwortlichkeit der Hostingprovider nicht gerecht. Sie steht auch nicht im Einklang mit den Vorgaben des DSA und bleibt damit hinter dem nach Europarecht Geforderten zurück. Insbesondere sind Sanktionen für eine nicht zeitnahe Entscheidung über die gemeldeten Informationen nicht vorgesehen. Damit fehlt jeglicher Druck, strafbare Inhalte möglichst rasch zu entfernen oder zu sperren. Aber auch in den gesetzlich erfassten Fällen, also den Fällen willkürlicher oder nicht objektiver Entscheidung, wird eine Sanktionierung weitgehend verhindert, da – erstens – nur vorsätzliches Handeln bußgeldbewehrt sein soll und – zweitens – der Täter beharrlich wiederholt handeln muss. Beharrlichkeit ist – nach der üblichen Auslegung im Strafrecht – nicht bereits bei bloßer Wiederholung gegeben. Vielmehr bezeichnet der Begriff eine in der Tatbegehung zum Ausdruck kommende besondere Hartnäckigkeit und eine gesteigerte Gleichgültigkeit des Täters gegenüber dem gesetzlichen Verbot, die zugleich die Gefahr weiterer Be-

gehung indiziert. Angesichts dieser hohen Anforderungen wird der Nachweis beharrlich wiederholten Handelns gegenüber einer identifizierbaren Person beim Hostingprovider kaum jemals gelingen. Für die Bearbeitung von Beschwerden werden gerade bei größeren Providern typischerweise eine Vielzahl von Personen befasst sein.

Die Sanktionsregelung in § 33 Absatz 4 DDG sollte daher in ihrer tatbestandlichen Ausgestaltung „geschärft“ werden. Da ein Hostingprovider für seinen Organisationsbereich verantwortlich ist, ist es gerechtfertigt, ihn gegen Strafe zu verpflichten, für einen angemessenen Umgang mit eingehenden Beschwerden über – in seinem Organisationsbereich zutage getretene – rechtswidrige Inhalte Sorge zu tragen. Dazu gehören auch und gerade die in Artikel 16 Absatz 6 Satz 1 DSA statuierten Pflichten.

Für eine effektive und europarechtskonforme Ausgestaltung der Bußgeldvorschrift kommt beispielsweise eine Rückkehr zur noch im Referentenentwurf vorgesehenen Fassung in Betracht. Danach sollte ordnungswidrig handeln, wer vorsätzlich oder fahrlässig entgegen Artikel 16 Absatz 1 Satz 1 DSA eine Entscheidung nicht zeitnah, nicht sorgfältig, nicht frei von Willkür oder nicht objektiv trifft. Aber selbst wenn man davon ausgehen sollte, dass eine solche Regelung sehr weitgehend ist und die Gefahr eines „Overblockings“ und übermäßiger Sanktionen unangemessen erhöht, sind tatbestandliche Einschränkungen denkbar, die der Sanktionsvorschrift (anders als § 33 Absatz 4 DDG) nicht ihre Wirksamkeit nehmen. In Betracht käme beispielsweise eine Einschränkung in Gestalt einer objektiven Bedingung der Ahndbarkeit, wonach die Tat Bestandteil wiederholter Verstöße vergleichbarer Art sein muss.

Neben der Statuierung einer wirksamen Bußgeldvorschrift ist auch zu erwägen, für qualifizierte Verstöße eine strafrechtliche Sanktion vorzusehen. In Betracht kommt dies etwa für den Fall der nicht zeitnahen oder nicht willkürfreien Entscheidung über eine Information, die ein offenkundig strafbares Verhalten eines Nutzers zum Gegenstand hat.

In
R

9. Zu Artikel 1 allgemein

- a) Der Bundesrat weist darauf hin, dass es im Vergleich zur aktuellen Rechtslage zu regulatorischen Rückschritten beim Löschen strafbarer Inhalte auf Online-Plattformen kommen wird. Anders als das Netzwerkdurchsetzungsgesetz sieht das System Digital Services Act / Digitale-Dienste-Gesetz insbesondere keine klare sanktionsbewehrte fristgebundene gesetzliche Löschpflicht für Plattformbetreiber bei gemeldeten rechtswidrigen Inhalten mehr vor. Der schlichte Verweis auf die medienrechtlichen Bestimmungen der Länder in § 1 Absatz 2 Satz 1 und § 12 Absatz 5 DDG stellt keine ausreichende Kompensation hierfür dar.

- b) Der Bundesrat bittet daher, im weiteren Gesetzgebungsverfahren zu prüfen, wie diese regulatorischen Rückschritte auch auf der Ebene des Bundesrechts effektiv und unionsrechtskonform kompensiert und wirksame Sanktionsmöglichkeiten geschaffen werden können.
- c) Für Verstöße gegen Löschanordnungen, die strafrechtliche Inhalte betreffen, sollten auch strafrechtliche Sanktionen vorgesehen werden.

Begründung:

§ 3 NetzDG verpflichtet große soziale Netzwerke zur Einrichtung eines wirksamen und transparenten Verfahrens über den Umgang mit Beschwerden über rechtswidrige Inhalte. Die betroffenen Betreiber werden nicht nur verpflichtet, ein leicht erkennbares, unmittelbar erreichbares, leicht bedienbares und ständig verfügbares Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte vorzuhalten, sondern sie müssen über dieses Verfahren gemeldete Inhalte auch unverzüglich prüfen und im Falle der Rechtswidrigkeit binnen festgelegter Fristen (24 Stunden bei Offensichtlichkeit, sonst grundsätzlich binnen sieben Tagen) löschen oder sperren. Verstöße gegen diese Pflichten – einschließlich der Löschpflicht – sind bußgeldbewehrt.

Der zum 17. Februar 2024 umfassend und EU-weit Geltung erlangende DSA sieht in Artikel 16 zwar die Pflicht von Plattformbetreibern zur Einrichtung eines leicht zugänglichen und benutzerfreundlichen Meldekanals für rechtswidrige Inhalte vor, er verzichtet jedoch auf eine klare gesetzliche Löschpflicht bei Feststellung der Rechtswidrigkeit und sieht insbesondere – anders als das NetzDG – keine klaren Bearbeitungsfristen vor. Entsprechend gibt es auch keine klare Grundlage für eine Bußgeldsanktionierung bei Nichtlöschen trotz Rechtswidrigkeit. In seinem Artikel 9 stellt der DSA allerdings klar, dass das nationale Recht Grundlagen für behördliche Einzelfallanordnungen zum Vorgehen gegen einen oder mehrere bestimmte rechtswidrige Inhalte vorsehen kann.

Das DDG verzichtet allerdings darauf, die insofern bestehenden nationalen Regelungsspielräume auszufüllen. Für terroristische Inhalte bestehen bereits die Anordnungsbefugnisse des Bundeskriminalamts nach dem TerrOIBG. Im Übrigen verweist Artikel 1 §§ 1 Absatz 2 Satz 1, 12 Absatz 5 DDG schlicht auf die medienrechtlichen Bestimmungen der Länder. Es ist zwar zutreffend, dass die §§ 4, 20 JMStV Löschanordnungen der Landesmedienanstalten gegenüber Plattformbetreibern (auch solchen mit Sitz außerhalb Deutschlands) bei bestimmten strafbaren Inhalten ermöglichen. Der Katalog des § 4 JMStV bleibt aber deutlich hinter dem Katalog rechtswidriger Inhalte nach § 1 Absatz 3 NetzDG zurück. Insbesondere fehlen die auch für die Bekämpfung von Hass im Netz relevanten Straftatbestände § 111 StGB (Öffentliche Aufforderung zu Straftaten), § 140 StGB (Belohnung und Billigung von Straftaten), § 166 StGB (Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen), §§ 185 bis 187 StGB (Beleidigung, üble

Nachrede, Verleumdung), § 189 StGB (Verunglimpfung des Andenkens Verstorbener), § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen) und § 241 StGB (Bedrohung). Eine über die Regelungen des TerrOIBG sowie des JMStV hinausgehende klare und rechtssichere spezialgesetzliche Befugnis zur Anordnung der Sperrung und Löschung eines rechtswidrigen Online-Inhalts besteht nicht.

Im weiteren Gesetzgebungsverfahren müssen daher Überlegungen angestellt werden, wie diese Rückschritte auch auf der Ebene des Bundesrechts effektiv und unionsrechtskonform (insbesondere in Übereinstimmung mit dem DSA) kompensiert und wirksame Sanktionsmöglichkeiten geschaffen werden können.

Dabei sollte auch die Rechtsfolgenseite in den Blick genommen werden. Zu erwägen sind neben Löschanordnungen bezüglich konkreter Inhalte beispielsweise auch Stay-down-Anordnungen, Löschanordnungen bezüglich identischer und sinngemäß gleichartiger Posts sowie Anordnungen von (zumindest zeitweiligen) Accountsperrern im Fall wiederholter oder schwerer Verstöße.

Darüber hinaus ist an eine „Nachschärfung“ der in Betracht kommenden Sanktionen zu denken. Als Sanktion für die Zuwiderhandlung gegen die nach nationalem Recht (JMStV, TerrOIBG) möglichen Löschanordnungen ist aktuell jeweils nur Geldbuße vorgesehen. Es liegt nahe, entsprechende Verstöße zumindest dann als Straftat einzuordnen, wenn sich die Löschanordnungen auf strafbare Inhalte beziehen. Hierfür spricht, dass das vorsätzliche Belassen, also das Nicht-Löschen, des staatlicherseits als strafbar eingeordneten Inhalts strukturell dem einer Beihilfehandlung zu der jeweiligen Straftat entspricht.

U 10. Zu Artikel 21 Nummer 4 – neu – (§ 20 Absatz 1 Nummer 01 – neu –, Absatz 3 UWG)

Dem Artikel 21 ist folgende Nummer 4 anzufügen:

,4. § 20 wird wie folgt geändert:

a) In Absatz 1 wird der Nummer 1 folgende Nummer 01 vorangestellt:

„01. entgegen § 3 Absatz 1 eine unlautere geschäftliche Handlung begeht, indem er im Anwendungsbereich der Verordnung (EU) 2022/2065 als Anbieter einer Online-Plattform eine Online-Schnittstelle so konzipiert, organisiert oder betreibt, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden,“

- b) In Absatz 3 werden die Wörter „des Absatzes 1 Nummer 1 und 2“ durch die Wörter „des Absatzes 1 Nummer 01, 1 und 2“ ersetzt.

Begründung:

Zu Buchstabe a:

Es stellt einen Wertungswiderspruch dar, wenn ein Verstoß gegen Artikel 25 der Verordnung (EU) 2022/2065 nach § 33 Absatz 5 Nummer 19 Digitale-Dienste-Gesetz eine Ordnungswidrigkeit begründet, dieselbe irreführende Handlung jedoch, sobald sie die Schwelle einer unlauteren Geschäftspraktik im Sinne der Richtlinie 2005/29/EG erreicht, ohne Bußgeldsanktion bleibt. Daher ist im Sinne einer effektiven Um- und Durchsetzung sowohl der Verordnung (EU) 2022/2065 als auch der Richtlinie 2005/29/EG ein entsprechender Bußgeldtatbestand für sogenannte „Dark Patterns“ in § 20 des Gesetzes gegen den unlauteren Wettbewerb (UWG) aufzunehmen.

Zu Buchstabe b:

Als Folge der Änderung unter Buchstabe a sollte – entsprechend der aufsichtlichen Zuständigkeit für den Vollzug von Artikel 25 der Verordnung (EU) 2022/2065 – die Zuständigkeit der Bundesnetzagentur in § 20 Absatz 3 UWG angepasst werden.

R 11. Zu Artikel 29 Nummer 4 Buchstabe a Doppelbuchstabe bb (§ 5 Absatz 1 Satz 1 NetzDG)

- a) Der Bundesrat weist darauf hin, dass es im Vergleich zur aktuellen Rechtslage zu regulatorischen Rückschritten bei gerichtlichen Zustellungen an Plattformbetreiber mit Sitz im EU-Ausland kommen wird. Anders als der bisherige § 5 des Netzwerkdurchsetzungsgesetzes soll künftig die Pflicht zur Bestellung eines inländischen Bevollmächtigten für Zustellungen in Gerichtsverfahren vor deutschen Gerichten auf Plattformbetreiber beschränkt werden, bei denen kein anderer EU-Mitgliedstaat Sitzland ist oder als Sitzland gilt. Dies wird in der gerichtlichen Praxis voraussichtlich zu deutlichen Erschwernissen bei der Zustellung von Klagen und damit auch zu längeren Verfahrensdauern führen.
- b) Der Bundesrat bittet daher, im weiteren Gesetzgebungsverfahren zu prüfen, ob nicht doch unionsrechtliche Spielräume für eine nationalrechtliche Pflicht zur Benennung eines inländischen Zustellungsbevollmächtigten bei Plattformbetreibern mit Sitz im EU-Ausland bestehen. Sollte dies zu ver-

neinen sein, wird gebeten zu prüfen, ob hilfsweise unionsrechtskonform eine Rechtsgrundlage im nationalen Recht geschaffen werden kann, die einer deutschen Behörde per Einzelentscheidung ermöglicht, einen Plattformbetreiber mit Sitz im EU-Ausland zur Benennung eines inländischen Zustellungsbevollmächtigten zu verpflichten.

- c) Der Bundesrat fordert die Bundesregierung auf, sich auf EU-Ebene für klare Regelungen im Unionsrecht einzusetzen, die die Verpflichtung von Plattformbetreibern zur Benennung eines inländischen Zustellungsbevollmächtigten direkt im Unionsrecht vorsehen oder im nationalen Recht ermöglichen.

Begründung:

§ 5 NetzDG verpflichtet derzeit große soziale Netzwerke mit Sitz im Ausland dazu, im Inland einen Bevollmächtigten für Zustellungen in Bußgeldverfahren, aufsichtsrechtlichen Verfahren sowie in Gerichtsverfahren vor deutschen Gerichten zu bestellen. Diese Vorschrift stellt vor allem für zivilgerichtliche Verfahren, die auf Beseitigung eines vorhandenen Inhalts oder auch die Wiederherstellung eines gelöschten Inhalts gerichtet sind, eine wesentliche Verfahrensvereinfachung dar. Insbesondere in nicht selten angestregten Verfahren des vorläufigen Rechtsschutzes kann über den inländischen Zustellungsbevollmächtigten ein beklagter Plattformbetreiber schnell erreicht werden. Die Vorschrift dient damit in Verfahren auf schnelle Beseitigung eines vom Betroffenen für rechtswidrig erachteten Inhaltes auch der effektiven Durchsetzung privater Rechte im Kontext von Hate-Speech.

Dieses Ziel teilt auch die Bundesregierung. Nach den Anfang 2023 vom Bundesministerium der Justiz vorgestellten Eckpunkten für ein Gesetz gegen digitale Gewalt sollte § 5 NetzDG inhaltlich aufrechterhalten und sogar auf vorgerichtliche Korrespondenz ausgeweitet werden.

Im vorliegenden Gesetzentwurf soll hiervon allerdings Abstand genommen werden. Nach Artikel 29 Nummer 4 der Vorlage soll die Pflicht zur Benennung eines inländischen Zustellungsbevollmächtigten künftig nur noch Plattformbetreiber mit Sitz außerhalb der EU treffen. Dies stellt einen erheblichen regulatorischen Rückschritt dar, weil die relevantesten Betreiber wie Meta, Google, X oder TikTok einen Sitz innerhalb der EU haben. An diese kann – abgesehen von der Möglichkeit, freiwillig einen Bevollmächtigten zu bestellen oder den bisherigen zu belassen – künftig nur noch über die unionsrechtlichen Regelungen zur Zustellung im Binnenmarkt zugestellt werden (insbesondere die Verordnung (EU) 2020/1784 des Europäischen Parlaments und des Rates über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten (Zustellung von Schriftstücken)). Diese sehen gegenüber den internationalen Rechtshilferegelungen im Nicht-EU-Ausland zwar durchaus Erleichterungen vor, die Erfahrungen der gerichtlichen Praxis zeigen allerdings, dass gegenüber einer Zustellung im Inland

auch mit den unionsrechtlichen Regelungen ein hoher Aufwand verbunden ist. Die gerichtliche Praxis berichtet hier selbst in Verfahren des vorläufigen Rechtsschutzes teilweise von Zustellungslaufzeiten von sechs Monaten.

Nach der Gesetzesbegründung sieht sich die Bundesregierung in ihrem Entwurf an einer Fortschreibung oder Ausdehnung des bisherigen § 5 NetzDG durch das Urteil des EuGH vom 9. November 2023 (C-376/22) gehindert. Dieses Urteil erachtet abstrakt-generelle Pflichten für Plattformbetreiber, die innerhalb der EU grenzüberschreitend Dienste anbieten, für unvereinbar mit Artikel 3 Absatz 4 der E-Commerce-Richtlinie. Aufgrund der Bedeutung des inländischen Zustellungsbevollmächtigten für die reibungslose Abwicklung von Gerichtsverfahren sollte im weiteren Gesetzgebungsverfahren gleichwohl geprüft werden, ob nicht doch nationalrechtliche Spielräume bestehen. Insbesondere bezieht sich das EuGH-Urteil in seinem begründenden Teil nicht ausdrücklich auf Regelungen zur Zustellungsbevollmächtigung, die rein materiell keine Einschränkung der Dienstleistungsfreiheit bedeuten und auch deutlich prozessualen Charakter haben. Prozessrecht ist Sache der Mitgliedstaaten.

Ungeachtet dessen lässt der Entwurf der Bundesregierung Überlegungen dazu vermissen, ob statt einer abstrakt-generellen Verpflichtung die Rechtsgrundlage für eine behördliche Einzelfallanordnung (zum Beispiel durch die Bundesnetzagentur oder das Bundesamt für Justiz) geschaffen werden könnte, durch die ein Plattformbetreiber mit Sitz im EU-Ausland zur Benennung eines inländischen Zustellungsbevollmächtigten per Bescheid verpflichtet werden kann. Hierfür bietet Artikel 3 der E-Commerce-Richtlinie deutlich größere Spielräume. Die Verpflichtung könnte beispielsweise auch an die Relevanz der Plattform bei der Verbreitung rechtswidriger Inhalte („Schutz der öffentlichen Ordnung“) oder an die besondere Häufigkeit von gerichtlichen Verfahren von Einzelpersonen im Zusammenhang mit der Inhaltmoderation („Schutz der Verbraucher“) geknüpft werden.

In jedem Fall wären klare Regelungen im Unionsrecht wünschenswert, die entweder inländische Zustellungsbevollmächtigte für die Plattformwirtschaft ausdrücklich vorsehen oder zumindest im nationalen Recht ermöglichen. Da Dienste der Plattformwirtschaft nahezu immer grenzüberschreitend angeboten werden, kommt der Erreichbarkeit des Betreibers auch bei gerichtlichen Auseinandersetzungen große Bedeutung zu. Die Bundesregierung ist daher aufzufordern, sich auch unabhängig vom vorliegenden Gesetzgebungsverfahren für entsprechende Regelungen auf EU-Ebene einzusetzen.

U 12. Zu Artikel 32 (Änderung des Barrierefreiheitsstärkungsgesetzes)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren die Übernahme von Zuständigkeiten durch Bundesbehörden für den Vollzug des Barrierefreiheitsstärkungsgesetzes (BFSG) zumindest für einzelne Dienstleistungen im Anwendungsbereich des Gesetzes zu prüfen. Diese Forderung hat der Bundesrat bereits zum Gesetzentwurf zur Umsetzung der Richtlinie (EU) 2019/882 über die

Barrierefreiheitsanforderungen für Produkte und Dienstleistungen erhoben, siehe BR-Drucksache 240/21 (Beschluss), Ziffer 3 vom 7. Mai 2021.

Bereits im geltenden Recht bestehen Zuständigkeiten bei Bundesbehörden, an die der Vollzug des BFGS sowohl in Bezug auf Produkte als auch in Bezug auf Dienstleistungen sinnvollerweise anknüpfen sollte. Auch zeigt Artikel 1 des vorliegenden Gesetzentwurfs, dass eine Übertragung von Aufsichtsaufgaben im Zusammenhang mit digitalen Diensten auf eine Bundesbehörde – hier die Bundesnetzagentur – sachgerecht und sinnvoll ist.

U 13. Zum Gesetzentwurf insgesamt

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob der bisher unter anderem im Telemediengesetz, Telekommunikations-Telemedien-Datenschutz-Gesetz, Bürgerlichen Gesetzbuch und Jugendschutzgesetz verwendete Begriff der Telemedien beibehalten werden kann und nicht durch den Begriff der „digitalen Dienste“ abgelöst wird. Der Bundesrat sieht die Gefahr von unerwünschten Regelungslücken und Anwendungsschwierigkeiten, da der Begriff „Telemedien“ weiter ist als der Begriff der „Digitalen Dienste“ und anders als „Digitale Dienste“ auch unentgeltliche Dienstleistungen erfasst. Dies würde beispielsweise nicht nur Vorgaben für die Verwendung von Cookies betreffen, sondern möglicherweise auch Auswirkungen auf den Geltungsbereich der besonderen Schutzvorschriften des BGB für Verträge im elektronischen Geschäftsverkehr haben. Hinzu kommt, dass der EuGH bereits entschieden hat, dass auch eine dem unmittelbaren Nutzer gegenüber unentgeltlich erbrachte Leistung wirtschaftlich ein „Dienst der Informationsgesellschaft“ sein kann. Dies gelte insbesondere, wenn sie von dem Anbieter als Leistung zu Werbezwecken für von ihm verkaufte Güter oder angebotene Dienstleistungen erbracht werde (vergleiche EuGH - Urteil vom 15.09.2016, Rs. C- 484/14). Die Bezugnahme auf den Begriff der „digitalen Dienste“ im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 kann damit aus sich heraus zu Unklarheiten und Fehlvorstellungen führen, zumal die Gesetzesbegründung hierauf nicht näher eingeht.

Begründung:

Die pauschale Ersetzung des Begriffs „Telemedien“ durch den Begriff der „digitalen Dienste“ birgt die Gefahr einer unerwünschten Verengung des Anwendungsbereichs von bisherigen Regelungen unter anderem zum Einsatz von Cookies bei Telemedien und zum Verbraucherschutz im elektronischen Geschäftsverkehr. Zudem entsteht Rechtsunsicherheit, da nicht hinreichend klar wird, dass es bei der Beurteilung, ob ein „digitaler Dienst“ vorliegt, nicht ausschließlich auf die Entgeltlichkeit gegenüber dem unmittelbaren Nutzer des Dienstes abzustellen ist. Andernfalls wären künftig die meisten Online-Plattformen, Video-Sharing-Plattformen oder Suchmaschinen nicht mehr von den entsprechenden Regelungen erfasst. Auch ergibt sich aus der Verordnung (EU) 2022/2065 („Digital Services Act“ - DSA) kein Zwang für den nationalen Gesetzgeber, den Anwendungsbereich von Vorschriften, die nicht denselben Regelungsgegenstand wie die Verordnung haben oder ihrer Umsetzung dienen, ebenfalls einzuschränken.

K 14. Zum Gesetzentwurf allgemein

Im Hinblick auf den Bereich der Forschung bittet der Bundesrat, im weiteren Gesetzgebungsverfahren um Prüfung folgender Anliegen:

- a) Allen akkreditierten Forschenden ist seitens der Plattformen ein gleichartiger Datenzugang zu gewähren, um die Zuverlässigkeit der Forschung nicht durch ungleichen Ressourcenzugang zu gefährden.
- b) Allen akkreditierten Forschenden ist ein kostenfreier, unabhängiger und umfänglicher Zugang zu gewähren. Die Daten müssen maschinenlesbar sein und zum Zwecke der Vergleichbarkeit seitens der Plattform nach einheitlichen Mindeststandards aufbereitet werden, die entsprechend Artikel 40 Absatz 13 DSA nicht einseitig von den Plattformen vorgegeben werden können.
- c) Die Koordinierungsstelle prüft nicht nur individuelle Zugänge von einzelnen Forschenden gemäß Artikel 40 Absatz 8 DSA, sondern ermöglicht eine Akkreditierung auch flexibel für einschlägige Forschungsgruppen.
- d) Die Durchführung der Zulassung von akkreditierten Forschenden sollte möglichst weitgehend vom nationalen Koordinator gemäß Artikel 40 Absatz 9 vorgenommen werden, um eine Überlastung einzelner nationaler Behörden, in deren Zuständigkeitsbereich viele Plattformen ihren EU-Sitz haben, zu vermeiden. Bei alleiniger Zulassung durch den Niederlassungsort ist ein wirksamer Beschwerdemechanismus und eine entsprechende Aus-

stattung der Koordinierungsstelle vorzusehen, um strittigen Zulassungen zeitnah nachgehen zu können.

- e) Die Koordinierungsstelle legt die Anforderungen auch infrastruktureller Art an die Forschungsinstitutionen wie zum Beispiel zur Datensicherheit fest und macht sie öffentlich zugänglich, damit die Institutionen wissen, welche Standards sie für eine erfolgreiche Akkreditierung von Forschenden erreichen müssen.
- f) Zur Sicherung der wissenschaftlichen Qualität ist den akkreditierten Forschenden ein Recht auf Scraping einzuräumen, also des strukturierten Sammelns von Daten in einen Untersuchungskorpus, anhand dessen die Studienergebnisse im Zuge einer Begutachtung überprüft werden können.
- g) Neben den Bußgeldverfahren in Teil 8 des DDG sollten akkreditierten Forschenden selbst Untätigkeitsklagen oder vergleichbare Rechtsmittel zur Verfügung stehen, wenn Plattformen den Zugriff verweigern
- h) Der Bundesrat bittet die Bundesregierung, sich bei der Kommission dafür einzusetzen, dass im delegierten Rechtsakt zum Datenzugang für Forschende die vorgenannten Anliegen angemessen berücksichtigt werden.

B

15. Der Ausschuss für Frauen und Jugend

empfiehlt dem Bundesrat, gegen den Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes keine Einwendungen zu erheben.