Bundesrat **Drucksache** **567/1/26**

09.11.26

Empfehlungen
der Ausschüsse

EU - DS - FSFJ - In - K - Wi

zu **Punkt ...** der 1070. Sitzung des Bundesrates am 20. November 2026

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Gewährleistung der Verantwortung und Vertrauenswürdigkeit digitaler Räume im Internet (EU KIDS ACT)

COM(2026) 681 final; Ratsdok. 13321/26

Der **federführende Ausschuss für Fragen der Europäischen Union** (EU),

der **Ausschuss für Digitales und Staatsmodernisierung** (DS),

der **Ausschuss für Familie, Senioren, Frauen und Jugend** (FSFJ),

der **Ausschuss für Innere Angelegenheiten** (In),

der **Ausschuss für Kulturfragen** (K) und

der **Wirtschaftsausschuss** (Wi)

empfehlen dem Bundesrat, zu der Vorlage gemäß §§ 3 und 5 EUZBLG wie folgt Stellung zu nehmen:

Zum Verordnungsvorschlag allgemein

EU
K

1. Der Bundesrat begrüßt das Ziel des Vorschlags für einen EU KIDS ACT, Kinder und Jugendliche wirksam vor den nachgewiesenen Gefahren digitaler Dienste zu schützen. Einheitliche europäische Vorgaben sollen ein hohes Schutzniveau in der gesamten EU gewährleisten und zugleich den Binnenmarkt stärken.

...

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

EU DS 2. Der Bundesrat begrüßt das Ziel der Kommission, mit dem EU KIDS ACT den Schutz von Kindern und Jugendlichen im digitalen Raum zu verbessern und hierfür europaweit einheitliche Regelungen zu schaffen. Besonders positiv bewertet der Bundesrat die stärkere Verantwortung der Plattformbetreiber und die konsequente Verankerung des Prinzips „Safety by Design“.

EU FSFJ 3. Der Bundesrat begrüßt den Verordnungsvorschlag für einen europaweit gesetzlichen, verbesserten Online-Jugendmedienschutz. Er behandelt richtigerweise die nachgewiesenen Gefährdungspotentiale, denen Kinder und Jugendliche bei der Nutzung von bestimmten digitalen Diensten ausgesetzt sind.

EU FSFJ 4. Der Bundesrat begrüßt das Ziel der Verordnung, den Schutz von Kindern und Jugendlichen in digitalen Räumen zu stärken, bestehende Schutzlücken zu schließen und einheitliche europäische Rahmenbedingungen für grenzüberschreitend tätige Anbieter digitaler Dienste zu schaffen. Die Rechte von Kindern und Jugendlichen auf Schutz, Förderung und Beteiligung gelten auch im digitalen Raum. Digitale Angebote eröffnen Chancen für Information, Kommunikation, Bildung, Partizipation und soziale Verbundenheit, ersetzen jedoch nicht die Bedeutung analoger Erfahrungs- und Begegnungsräume. Die vorgesehenen Maßnahmen müssen daher einen wirksamen Schutz Minderjähriger gewährleisten und zugleich ihre Selbstbestimmung, und altersgerechte digitale Teilhabe sichern.

EU In 5. Der Bundesrat begrüßt grundsätzlich die in dem Vorschlag für den EU KIDS ACT enthaltenen Ansätze zum Schutz Minderjähriger im digitalen Raum. Der EU KIDS ACT enthält wichtige regulatorische Ansätze, um die Verantwortung von Plattformbetreibern zu stärken und digitale Dienste für Minderjährige sicherer zu gestalten.

EU In 6. In diesem Zusammenhang merkt der Bundesrat an, dass mit dem digitalen Raum als Bestandteil der Lebenswelt Minderjähriger nicht nur Möglichkeiten der Kommunikation, Bildung und gesellschaftlichen Teilhabe einhergehen. Ebenso bestehen auch vielfältige Risiken der digitalen Viktimisierung. Dazu zählen insbesondere Cybergrooming, Cybermobbing, digitale Sexualdelikte sowie neue Risiken durch den zunehmenden Einsatz Künstlicher Intelligenz.

EU In

7. Der Bundesrat ist daher der Auffassung, dass ein wirksamer digitaler Kinderschutz sich nicht allein auf technische Schutzmaßnahmen, Altersbeschränkungen und die Regulierung von Plattformbetreibern beschränken sollte. Diese Maßnahmen sollten stärker mit den Möglichkeiten der digitalen Kriminalprävention, der staatlichen Erreichbarkeit und der tatsächlichen Unterstützung von Minderjährigen verbunden werden. Von besonderer Bedeutung sind dabei die Berücksichtigung digitaler Polizeiarbeit, die Schaffung kindgerechter polizeilicher Onlineanlaufstellen, die Weiterentwicklung der Moderationsstandards sowie die stärkere Berücksichtigung kriminalitätsbezogener Risiken durch Onlinespiele und KI-Systeme. Ergänzend sollte der Schutz von Kinderbildern bei Veröffentlichungen durch Erwachsene oder andere Minderjährige stärker berücksichtigt werden.

Zu Artikel 2 (Anwendungsbereich)

EU Wi

8. Der Bundesrat lehnt die Einbeziehung von Anbietern von Betriebssystemen in den Anwendungsbereich der Verordnung ab. Die von der Verordnung erfassten Gefährdungen von Minderjährigen gehen regelmäßig von Anwendungen und Diensten, nicht jedoch vom Betriebssystem als solchem aus.

Begründung (nur gegenüber dem Plenum):

Gemäß Artikel 2 Absatz 1 Buchstabe e) fallen auch Anbieter von Betriebssystemen unter die Regelungen der Verordnung. Betriebssysteme dienen jedoch lediglich der Sicherstellung, dass Anwendungen (Apps oder Programme) mit bestimmter Hardware interagieren können und dazu, dass Hardware mit anderer Hardware interagieren kann (z. B. USB-Sticks).

Die von der Verordnung erfassten Gefährdungen von Minderjährigen gehen regelmäßig von Anwendungen und Diensten (soziale Netzwerke, Chatbots etc.), nicht jedoch vom Betriebssystem als solchem aus. Die Regulierung von Anbietern von Betriebssystemen ist daher nicht nur unverhältnismäßig, sondern faktisch nicht erforderlich.

Zu Artikel 6 ff. (Hinausgezögerte Einrichtung und Nutzung von Konten)

EU DS K

9. Der Bundesrat begrüßt die im Vorschlag eines EU KIDS ACT angelegten abgestuften Zugangsregelungen für bestimmte Dienste und Altersstufen. Nach Ansicht des Bundesrates ist diese Herangehensweise besser geeignet, einen angemessenen Ausgleich zwischen Schutz, Befähigung und Teilhabe zu erreichen, als dies durch pauschale Altersgrenzen möglich wäre.

EU FSFJ

10. Der Bundesrat betont, dass die im Verordnungsvorschlag vorgesehene Einführung von abgestuften Zugangsbeschränkungen für Social Media Dienste und Video-Sharing-Plattformen im Sinne des Kinder- und Jugendschutzes erforderlich ist.

Zu Artikel 8 ff. (Verpflichtungen für Online-Dienste sozialer Netzwerke und Video-Sharing-Plattform-Dienste)

EU FSFJ

11. Der Bundesrat unterstützt den Regelungsansatz der Gestaltungsvorgaben für Online Angebote im Sinne des Safety-by-Design-Ansatzes ausdrücklich. Dies umfasst u. a. das Verbot suchtfördernder Mechanismen, Schutz von Schlaf- und Schulzeiten, Interaktions- und Kontaktschutz sowie Anpassung von Empfehlungssystemen.

EU FSFJ

12. Der Bundesrat unterstreicht, dass die Verantwortung für einen wirksamen Schutz Minderjähriger nicht allein Kindern und Jugendlichen oder ihren Eltern übertragen werden darf. Insbesondere Anbieter digitaler Dienste müssen Verantwortung für die Gestaltung ihrer Angebote und Geschäftsmodelle übernehmen. Von Bedeutung sind wirksame Altersüberprüfungen, sichere Voreinstellungen sowie eine datensparsame, altersgerechte und nicht manipulative Gestaltung digitaler Dienste. Erforderlich sind außerdem wirksame Melde- und Beschwerdewege sowie eine konsequente Durchsetzung bestehender Regeln.

EU DS 13. Plattformbetreiber müssen verpflichtet werden, ihre Angebote von vornherein altersgerecht und sicher zu gestalten. Dazu gehören insbesondere sichere Voreinstellungen, die Einschränkung suchtfördernder Mechanismen und die Begrenzung profilbasierter Empfehlungssysteme. Die Wirksamkeit dieser Maßnahmen muss überprüfbar sein. Die Verantwortung darf nicht allein auf Eltern und Minderjährige verlagert werden.

EU K 14. Der Bundesrat begrüßt, dass die Verantwortung für eine sichere Gestaltung digitaler Dienste vorrangig bei den betreffenden Anbietern und nicht bei den Eltern liegt. Der Bundesrat spricht sich dafür aus, in den weiteren Verhandlungen zum EU KIDS ACT zu prüfen, ob die beschriebene Verantwortungsverteilung zwischen Anbietern und Eltern in allen Einzelpunkten angemessen und konsequent vorgenommen wird.

EU Wi 15. Der Bundesrat misst dem Kinder- und Jugendschutz im digitalen Raum höchste Bedeutung bei. Der von der Kommission vorgeschlagene EU KIDS ACT ist jedoch in seiner derzeitigen Ausgestaltung nur bedingt geeignet, einen wirksamen, zielgerichteten Schutz von Kindern und Jugendlichen im digitalen Raum zu gewährleisten.

EU Wi 16. Dies gilt insbesondere mit Blick auf die Regulierung von Klein- und Kleinstanbietern sozialer Netzwerke, die durch die vorgesehenen Anforderungen, die sich in erster Linie an den großen Anbietern (Instagram, TikTok etc.) orientieren, vor große Herausforderungen gestellt werden. Der Bundesrat hält es für erforderlich, dass eine Anpassung der Anforderungen für Klein- und Kleinstanbieter erfolgt, die den Belangen des Jugendschutzes Rechnung trägt, zugleich aber auch die Größe und Leistungsfähigkeit der Anbieter angemessen berücksichtigt.

Begründung zu Ziffern 15 und 16 (nur gegenüber dem Plenum):

Der Bundesrat unterstützt das Ziel, Kinder und Jugendliche wirksam vor Gefährdungen im digitalen Raum zu schützen. Die hierfür vorgesehenen Maßnahmen müssen jedoch verhältnismäßig sein und dürfen nicht über das zur Erreichung des Schutzziels notwendige Maß hinausgehen. Insbesondere müssen die unterschiedlichen Voraussetzungen und Möglichkeiten der betroffenen Anbieter berücksichtigt werden.

Die Verordnung enthält zahlreiche dem Jugendschutz dienende neue Anforderungen, die in ihrer Zielrichtung nachvollziehbar sind, die jedoch in ihrer Fülle

insbesondere für Klein- uns Kleinstanbieter nur mit großem Aufwand umsetzbar sein dürften. So dürfen nach Artikel 6 auch – oftmals von Privatpersonen betriebene – Internetforen (Austauschplattform zu speziellen Themen, wie z. B. PC-Hardware, Kochen, Stricken etc.) Personen unter 15 Jahren die Einrichtung eines Kontos nicht mehr ermöglichen. Weiterhin müssen diese Betreiber bei ihren Anwendungen sicherstellen, dass bestimmte Einstellungen bei Minderjährigen nicht aktiv sind oder anders funktionieren als bei Erwachsenen (z. B. Benachrichtigungen nicht während der Kernschlafzeiten und Schulzeiten). Um sicherzustellen, dass die Betreiber keinen Personen unter 15 Jahren Zugriff auf ihre Plattform gewähren, müssen sie ein EU-zertifiziertes Überprüfungssystem einsetzen, z. B. die europäische Brieftasche (EUDI-Wallet), die in Deutschland als d-You-App umgesetzt werden soll. Ebenso müssen Lösungen eingeführt werden, die es Erziehungsberechtigten erlauben, ihren Kindern den Zugriff auf eigentlich gesperrte Anwendungen zu geben, wenn die Kinder mindestens 13 Jahre alt sind. Vorgesehen ist ferner, dass die Anbieter alle bereits bestehenden Konten einer Kontrolle unterziehen müssen, um so Minderjährige unter 15 Jahren zu identifizieren und die Konten sperren zu können.

Die Gesamtzahl der Anforderungen ist dazu geeignet, insbesondere Klein- und Kleinstanbieter von sozialen Plattformen zu überfordern, so dass damit zu rechnen ist, dass viele ihre Dienste einstellen werden. An Klein- und Kleinstanbieter dieselben Anforderungen zu stellen wie an große internationale Konzerne erscheint daher unverhältnismäßig und wäre im Sinne eines vielfältigen Angebots an Möglichkeiten zur sozialen Interaktion nicht wünschenswert. Eine Regulierung sollte daher die Größe und Leistungsfähigkeit der Anbieter berücksichtigen und möglichst auch das vom jeweiligen Angebot ausgehende Gefährdungspotenzial angemessen berücksichtigen.

Dabei muss zweifelsohne ein hinreichendes Maß an Kinder- und Jugendschutz für alle Angebote gewährleistet sein. Die konkreten Anforderungen an die Anbieter sollten jedoch nach Art, Funktion und Gefährdungspotenzial des jeweiligen Angebots differenziert ausgestaltet werden. Insbesondere das Risiko einer übermäßigen Nutzung sowie Gefahren der Kontaktaufnahme mit Minderjährigen durch Dritte oder der Zugänglichmachung jugendgefährdender Inhalte können je nach Ausgestaltung und Funktionalität eines Angebots erheblich variieren.

Zu Artikel 14 (Vorgaben für KI-Begleiter und allgemeine dialogbasierte Chatbots)

EU
FSFJ

17. Der Bundesrat hebt die Risiken durch KI-generierte und manipulierte Bild-, Video- und Tonaufnahmen, algorithmische Mechanismen sowie damit verbundene sexualisierte Gewalt und Belästigung hervor. Täuschend echt wirkende Deepfakes können Kindern und Jugendlichen Äußerungen oder Handlungen zuschreiben, die sie nicht getätigt oder vorgenommen haben. Sie können zur Bloßstellung und Erniedrigung der Betroffenen sowie im Zusammenhang mit

sexualisierter Gewalt eingesetzt werden. Bei der Gestaltung digitaler Angebote sind zudem manipulative Gestaltungs- und Interaktionsformen zu unterbinden, die etwa durch personalisierte Ansprache, wiederkehrende Interaktionsanreize, endloses Scrollen, automatisch startende Inhalte, wiederholte Benachrichtigungen und personalisierte Empfehlungssysteme eine übermäßige Nutzung fördern können. Bei KI-gestützten Dialogsystemen und sogenannten KI-Begleitangeboten ist darauf zu achten, dass keine emotionale Abhängigkeit begünstigt wird.

EU
In

18. Kriminalitätsbezogene Risiken durch Künstliche Intelligenz

In Artikel 14 Absatz 1 Buchstaben e und f des Verordnungsvorschlags sind die Anforderungen an die Evaluierung von Risiken und die Beobachtung neu auftretender Gefährdungen im Zusammenhang mit KI-Systemen festgelegt. Artikel 14 Absatz 2 bezieht sich außerdem auf KI-Funktionen innerhalb sozialer Medien, Video-Sharing-Dienste und Onlinespiele. Spezifische, kriminalitätsbezogene Gefährdungen durch KI-Systeme werden jedoch nicht als eigenständige Risikokategorien benannt. Eine ausdrückliche Berücksichtigung kriminalitätsbezogener Gefährdungen von Minderjährigen im Rahmen der Risikobewertungen nach Artikel 14 ist sinnvoll. Dies betrifft insbesondere sexualisierte Interaktionen, manipulative Vertrauensbildung, KI-gestützte Kontaktanbahnung und die mögliche Förderung sexueller Ausbeutung Minderjähriger. Dabei sollten nicht nur die Risiken durch den missbräuchlichen Einsatz von KI durch menschliche Täter, sondern auch die Gefährdungen durch das Verhalten der KI-Systeme selbst berücksichtigt werden. KI-Systeme entwickeln sich zunehmend zu eigenständigen Kommunikations- und Interaktionspartnern, mit denen Minderjährige unmittelbar in Kontakt treten können. Dadurch können neuartige Gefährdungslagen entstehen, die nicht mit den bisherigen Vorstellungen menschlicher Tatbegehung erfasst werden können. Insbesondere die Möglichkeit einer automatisierten, individualisierten und möglicherweise langfristigen Kommunikation mit Minderjährigen wirft neue Fragen für die Kriminalprävention und den Schutz vor sexueller Manipulation auf. Es erscheint daher angezeigt, kriminalitätsbezogene Gefährdungen Minderjähriger bei den Risikobewertungen nach Artikel 14 ausdrücklich zu berücksichtigen.

Zu Artikel 15 (Verpflichtungen für Anbieter von Online-Spielen)

EU
In

19. Schutz vor Cybergrooming und digitalen Straftaten in Onlinespielen

Artikel 15 Absatz 1 Buchstabe c des Verordnungsvorschlags erstreckt bestimmte Schutzvorkehrungen des Artikels 12 bereits auf Onlinespiele. Dabei wird jedoch nicht ausdrücklich auf Artikel 12 Absatz 2 verwiesen, der Schutzmaßnahmen gegen die Manipulation Minderjähriger zur Genehmigung direkter Kontakte vorsieht. Artikel 15 Absatz 2 berücksichtigt das Risiko einer Verlagerung von Kontakten auf andere Dienste, jedoch nicht die direkte Kontaktaufnahme mit Minderjährigen. Artikel 19 Absatz 1 nennt bei den kindgerechten Meldesystemen wiederum nur Videospielplattformen, nicht jedoch sämtliche Onlinespiele. Es erscheint daher sinnvoll, eine ausdrückliche Einbeziehung von Artikel 12 Absatz 2 in Artikel 15 Absatz 1 Buchstabe c zu prüfen. Darüber hinaus sollten die Pflichten zur Bereitstellung kindgerechter Meldemechanismen nach Artikel 19 Absatz 1 grundsätzlich auch für Onlinespiele mit relevanten Kommunikations- und Interaktionsfunktionen gelten.

Die ausdrückliche Berücksichtigung von Onlinespielen im Verordnungsvorschlag ist bereits ein wichtiger Schritt. Allerdings sind Onlinespiele längst nicht mehr ausschließlich digitale Spielangebote, sondern vielfach auch soziale Kommunikations- und Interaktionsräume. Sprach- und Textchats, Freundeslisten, Gruppenfunktionen und private Kommunikationsmöglichkeiten können vergleichbare Gefährdungslagen hervorrufen wie klassische soziale Medien. Dies betrifft insbesondere Cybergrooming, unerwünschte Kontaktaufnahmen – auch durch Extremisten – und die Verlagerung entsprechender Kontakte auf externe Kommunikationsdienste. Aus einer risikoorientierten Perspektive erscheint es daher sinnvoll, Schutzmaßnahmen stärker an den tatsächlichen Kommunikationsmöglichkeiten und weniger an der formalen Einordnung eines Dienstes auszurichten.

Zu Artikel 17 (Verhaltenskodizes für die Alterseinstufung und für Online-Spiele)

EU FSFJ

20. Der Bundesrat begrüßt auch die Zielsetzung, europaweit harmonisierte Kodizes für die Altersklassifizierung von Online-Spielen zu entwickeln, die auf den Alterseinstufungssystemen der Mitgliedstaaten aufbauen und auch Interaktionsrisiken und Monetarisierungspraktiken berücksichtigen sollen. Dabei ist sicherzustellen, dass die zugrunde liegenden Einstufungsmaßstäbe nicht hinter den Stand der in Deutschland nach dem Jugendschutzgesetz geltenden Regelungen und Verfahren zurückfallen oder diese verdrängen.

EU FSFJ

21. Der Bundesrat sieht beim derzeitigen Verordnungsentwurf bezüglich der Thematik der Online Spiele (Artikel 2 Absatz 1 Buchstabe d), welche grundsätzlich auch für Spiele auf Datenträgern gilt sobald diese auch eine Online-Komponente enthalten, jedoch die Gefahr, dass der bewährte hohe Standard des deutschen Jugendschutzes bei der Alterskennzeichnung von Computerspielen im Rahmen einer harmonisierten europäischen Lösung künftig abgesenkt werden könnte. Auch wenn nationale Systeme in Erwägungsgrund 40 des Vorschlags genannt werden, so ist dies kein verbindlicher Schutz, da diese Erwägungsgründe nicht verbindlich sind. Es besteht daher die Gefahr, dass sie im weiteren Verfahren entfallen.

EU FSFJ

22. Der Bundesrat bittet daher die Bundesregierung, sich in den Verhandlungen im Rat und gegenüber der Kommission dafür einzusetzen, dass die Öffnung für nationale Alterseinstufungssysteme aus der bisherigen Ausführung im Rahmen des Erwägungsgrunds 40 in den verfügenden Teil (konkret in Artikel 17 Absatz 2 Buchstabe f), übernommen wird.

Zu Artikel 19 (Kindgerechte Meldemechanismen und Instrumente zur Unterstützung Minderjähriger)

EU In

23. Kindgerechte polizeiliche Onlineanlaufstellen

Gemäß Artikel 19 Absatz 1 und 4 des Verordnungsvorschlags müssen kindgerechte Meldemechanismen und Informationen über Unterstützungsangebote be-

reitgestellt werden. Artikel 33 Absatz 1 Buchstabe a verlangt darüber hinaus nationale Hilfekanäle, die für Minderjährige einfach, kostenlos und vertraulich zugänglich sein sollen. Erwägungsgrund 42 berücksichtigt ebenfalls die Möglichkeit, auf Kontaktdaten von Strafverfolgungsbehörden hinzuweisen. Eine ausdrückliche Berücksichtigung eigenständiger, kindgerechter polizeilicher Onlineanlaufstellen oder einer unmittelbaren Verbindung zu entsprechenden Angeboten ist hingegen nicht vorgesehen.

Daher sind Artikel 19 und 33 um die Berücksichtigung kindgerechter polizeilicher Onlineanlaufstellen zu ergänzen. Denkbar wäre die Einrichtung einer Kinderonlinewache, über die Minderjährige unkompliziert und altersgerecht Kontakt zur Polizei aufnehmen, Straftaten melden und Unterstützung erhalten können. Ein solches Angebot könnte auch auf europäischer Ebene bereitgestellt werden. KI-gestützte Anwendungen könnten eine mehrsprachige Bereitstellung des Angebots unterstützen. Entsprechende Angebote sollten möglichst unmittelbar aus sozialen Medien, Onlinespielen und anderen digitalen Kommunikationsdiensten erreichbar sein. Die konkrete organisatorische Ausgestaltung könnte im Rahmen nationaler Strategien durch die Mitgliedstaaten erfolgen.

Gerade bei digitalen Sexualdelikten, Cybergrooming und anderen Formen digitaler Viktimisierung können Minderjährige häufig nur schwer beurteilen, ob sie von einer Straftat betroffen sind. Ein kindgerechtes polizeiliches Angebot sollte daher nicht nur die Möglichkeit einer formalen Strafanzeige bieten, sondern auch eine niedrigschwellige erste Kontaktaufnahme ermöglichen.

EU
In

24. Rechtssichere Sicherung digitaler Beweismittel

In Artikel 19 Absatz 1 bis 4 des Verordnungsvorschlags wird die Meldung problematischer Inhalte sowie die Unterstützung betroffener Minderjähriger geregelt. Eine spezifische Verpflichtung zur Sicherung strafrechtlich relevanter digitaler Beweismittel ist dort jedoch nicht enthalten. Artikel 12 Absatz 3 Buchstabe e des Verordnungsvorschlags sieht darüber hinaus technische Schutzmaßnahmen gegen das Herunterladen und die Anfertigung von Screenshots bestimmter Inhalte von Minderjährigen vor. Ergänzend bestehen bereits Verpflichtungen nach Artikel 18 des Digital Services Act, die bei einer möglichen Erweiterung zu berücksichtigen sind. Vor diesem Hintergrund könnte geprüft werden, ob Artikel 19 um geeignete Verfahren zur anlassbezogenen, rechtssicheren und datenschutzkonformen Sicherung gemeldeter, strafrechtlich relevanter Inhalte ergänzt werden könnte. Dabei sollte insbesondere berücksichtigt

werden, wie Inhalte bei einem konkreten Verdacht gesichert und auf Grundlage bestehender gesetzlicher Befugnisse den zuständigen Strafverfolgungsbehörden zugänglich gemacht werden können.

Gerade bei digitalen Sexualdelikten, Cybergrooming und Cybermobbing können Kommunikationsinhalte kurzfristig gelöscht werden oder aus anderen Gründen nicht mehr verfügbar sein. Dadurch besteht die Gefahr, dass wichtige Beweismittel verloren gehen, bevor Betroffene Hilfe erhalten oder die Strafverfolgungsbehörden tätig werden können. Wirksame Meldesysteme sollten deshalb auch geeignete Verfahren vorsehen, die es ermöglichen, gemeldete Inhalte bei konkreten Anhaltspunkten für strafrechtlich relevante Sachverhalte zeitnah, rechtssicher und datenschutzkonform zu sichern, soweit hierfür eine tragfähige Rechtsgrundlage besteht.

EU
In

25. Verbindliche Standards für Moderation und die Qualifikation von Moderierenden

Während Artikel 8 des Verordnungsvorschlags allgemeine Anforderungen an die sichere Gestaltung digitaler Dienste enthält, sieht Artikel 19 Absatz 3 eine vorrangige und zügige Bearbeitung von Meldungen Minderjähriger vor. Es werden jedoch keine ausdrücklichen Mindestanforderungen an die fachliche Qualifikation und Fortbildung der hierfür verantwortlichen Moderierenden festgelegt. Ergänzend dazu sieht Artikel 42 Absatz 2 Buchstaben a und b des Digital Services Act Berichtspflichten für sehr große Online-Plattformen bezüglich der Qualifikation und Schulung ihres Moderationspersonals vor. Auch die EU-Kinderschutzleitlinien von 2025, insbesondere Abschnitt 6.7, enthalten Empfehlungen für wirksame Moderationsstrukturen und menschliche Überprüfungen (unter anderem Nummer 72). Vor diesem Hintergrund sollte geprüft werden, ob Artikel 19 um risikobasierte Mindeststandards für die Moderation digitaler Kommunikationsräume, die von Minderjährigen genutzt werden, ergänzt werden könnte. Dazu könnten insbesondere Anforderungen an die fachliche Qualifikation, regelmäßige Fortbildung und transparente Verfahren zum Umgang mit schwerwiegenden Gefährdungen gehören. Denkbar wären anerkannte oder zertifizierbare Qualifizierungsstandards für Moderierende, die neben technischen und organisatorischen Kenntnissen auch Grundlagen des digitalen Kinderschutzes, einschlägiger Kriminalitätsphänomene und der Zusammenarbeit mit zuständigen Hilfs- und Strafverfolgungsstellen berücksichtigen.

Die Wirksamkeit von Schutzmaßnahmen hängt nicht allein von technischen Meldesystemen, sondern wesentlich auch von der Qualität der anschließenden Moderationsentscheidungen ab. Gerade bei Cybergrooming, Cybermobbing und digitalen Sexualdelikten sind Kenntnisse über typische Tatbegehungsweisen, Risikokonstellationen, angemessene Reaktionen und den Umgang mit betroffenen Minderjährigen erforderlich. Eine stärkere Standardisierung könnte dazu beitragen, die Qualität entsprechender Moderationsverfahren zu verbessern und den Umgang mit schwerwiegenden Gefährdungen nachvollziehbarer zu gestalten. Dabei wäre eine verhältnismäßige Ausgestaltung erforderlich, um insbesondere kleine Anbieter und ehrenamtliche Moderationsstrukturen nicht unverhältnismäßig zu belasten.

EU
In

26. Schutz Minderjähriger bei der Veröffentlichung ihrer Bilder durch Dritte

Artikel 12 Absatz 3 des Verordnungsvorschlags enthält Schutzmaßnahmen für Informationen und Inhalte, die von Minderjährigen selbst geteilt werden. Artikel 19 Absatz 4 Buchstabe c des Verordnungsvorschlags berücksichtigt zudem Warnhinweise vor riskanten Veröffentlichungen durch Minderjährige. Eine ausdrückliche Regelung zu besonderen Schutzmaßnahmen bei der Veröffentlichung von Kinderbildern, insbesondere in sozialen Medien durch Erwachsene beziehungsweise Erziehungsberechtigte, ist hingegen nicht vorgesehen. Dabei sind die bestehenden Anforderungen der Datenschutz-Grundverordnung und die nationalen Persönlichkeitsrechte ergänzend zu berücksichtigen. Es erscheint daher sinnvoll, zu prüfen, ob Artikel 12 und 19 um geeignete Schutzmechanismen bei der Veröffentlichung von Bildern Minderjähriger durch Dritte ergänzt werden könnten. Denkbar wären insbesondere deutliche Warnhinweise bei der Veröffentlichung von Kinderbildern in der Öffentlichkeit, einfache Meldemöglichkeiten für betroffene Minderjährige und wirksame Verfahren zur Wahrnehmung bestehender Löschungsrechte. Besondere Berücksichtigung könnte dabei die kommerzielle Veröffentlichung von Kinderbildern, beispielsweise durch Familien-Influencer, erfahren. Oftmals werden Kinderbilder durch Erwachsene veröffentlicht, ohne dass die betroffenen Minderjährigen hierauf einen nennenswerten Einfluss nehmen können. Damit sind Risiken für die Persönlichkeitsrechte, die Privatsphäre und die langfristige Kontrolle über eigene Bildinformationen verbunden. Hinzu kommen Gefährdungen durch die unkontrollierte Weiterverbreitung, die Zusammenführung mit anderen personenbezogenen Daten und die Möglichkeiten KI-gestützter Bildmanipulation. Gerade mit der

zunehmenden Verfügbarkeit generativer KI-Systeme erscheint es deshalb sinnvoll, die Schutzverantwortung nicht ausschließlich auf Minderjährige als aktive Nutzer digitaler Dienste zu konzentrieren. Dabei sollten auch der Wille und die Persönlichkeitsrechte der betroffenen Kinder entsprechend ihrem Alter und ihrer Reife berücksichtigt werden.

Zu Artikel 27 ff. (Allgemeine Grundsätze für die Altersfeststellung)

EU DS

27. Für digitale Angebote sollen europaweit einheitliche, transparente und risikobasierte Kriterien zur Altersklassifizierung entwickelt werden. Neben den Inhalten müssen dabei insbesondere Interaktionsmöglichkeiten, Empfehlungsalgorithmen und suchtfördernde Mechanismen berücksichtigt werden. Bewährte Modelle wie die Altersklassifizierung nach FSK und USK können hierfür als Vorbild dienen.

EU FSFJ

28. Der Bundesrat sieht in wirksamen und datensparsamen Möglichkeiten der Altersüberprüfung ein wichtiges Instrument des Kinder- und Jugendmedienschutzes. Sie kann ihren Schutzzweck nur erreichen, wenn sie in eine kohärente Schutzarchitektur eingebettet ist. Dazu gehören sichere Voreinstellungen, eine kindgerechte Gestaltung digitaler Dienste, wirksame Beschwerdewege und die Stärkung von Medienkompetenz. Verfahren zur Altersfeststellung müssen barrierefrei, diskriminierungsfrei und für unterschiedliche Lebenslagen praktikabel ausgestaltet werden. Dabei sind insbesondere die Belange von Kindern mit Behinderungen sowie von Familien zu berücksichtigen, denen digitale Identitätsnachweise oder geeignete technische Mittel nicht ohne Weiteres zur Verfügung stehen. Derartige Barrieren bei der Altersfeststellung dürfen nicht dazu führen, dass Kinder und Jugendliche von zulässigen digitalen Angeboten ausgeschlossen werden. Deshalb sollten wirksame, kostenfreie und niedrigschwellige Möglichkeiten zur Überprüfung und Anfechtung einer Altersentscheidung vorgesehen werden. Altersgrenzen und technische Schutzmechanismen sind so auszugestalten, dass sie Schutz vor digitalen Gefährdungen bieten, ohne den Zugang zu altersgerechten Informations-, Bildungs-, Kommunikations-, Beratungs- und Beteiligungsangeboten unangemessen zu erschweren.

EU K

29. Der Bundesrat fordert technologieoffene Vorgaben für Altersverifikationssysteme (AVS). Der EU KIDS ACT darf den Markt nicht frühzeitig auf eine einzelne technische Lösung verengen. Systeme, die einheitliche Kriterien und Standards erfüllen, müssen unionsweit eingesetzt werden können, um Praktikabilität und Effektivität zu gewährleisten.

EU K

30. Aus Sicht des Bundesrates ist es nicht zwingend erforderlich, dass die Anerkennung von AVS in den Mitgliedstaaten bei einer staatlichen Behörde verortet werden. Der Regelungstext sollte hier eine Öffnung auch für andere Stellen vorsehen, sofern dort ausreichende Expertise im Bereich der AVS besteht, wie dies in Deutschland im bewährten System der regulierten Selbstregulierung der Fall ist.

EU FSFJ

31. Die in Artikel 31 des Verordnungsvorschlags vorgesehenen elektronischen Nachweise der elterlichen Verantwortung können insbesondere im Zusammenhang mit Vormundschaften und geflüchteten Familien Auswirkungen auf Schulen, Kinder- und Jugendhilfe sowie Jugendämter haben. Die Länder sind frühzeitig und umfassend in die weiteren Beratungen über die Umsetzung einzubeziehen. Dabei sind die technische und organisatorische Umsetzbarkeit, zusätzliche Verwaltungsaufwände, erforderliche personelle Voraussetzungen und mögliche finanzielle Auswirkungen zu berücksichtigen.

Artikel 33 (Nationale Maßnahmen zur Vorbereitung und Unterstützung Minderjähriger)

EU In

32. Digitale Polizeiarbeit und Kriminalprävention

In Artikel 33 Absatz 1 und 2 des Verordnungsvorschlags sind nationale Maßnahmen zur Unterstützung Minderjähriger geregelt. Berücksichtigt werden dabei unter anderem Hilfsangebote und die Förderung digitaler Kompetenzen. Eine ausdrückliche Berücksichtigung der digitalen Polizeiarbeit, der polizeilichen Präsenz und der polizeilichen Kriminalprävention in den digitalen Lebenswelten Minderjähriger erfolgt hier jedoch nicht.

Daher ist Artikel 33 um eine entsprechende Berücksichtigung dieser Aspekte im Rahmen nationaler Strategien zum Schutz Minderjähriger zu ergänzen. Dies könnte die Förderung einer im digitalen Raum sichtbaren und niedrigschwellig

erreichbaren Polizei umfassen, beispielsweise durch digitale Polizeistreifen und polizeiliche Präventionsangebote in sozialen Medien und Onlinespielen.

Während polizeiliche Präsenz und Kriminalprävention im analogen öffentlichen Raum selbstverständlich sind, ist eine vergleichbare Erreichbarkeit staatlicher Sicherheitsbehörden in digitalen Lebenswelten bislang nur eingeschränkt gegeben. Gerade angesichts der zunehmenden Bedeutung digitaler Kommunikations- und Interaktionsräume erscheint es deshalb notwendig, dass die Polizei auch dort sichtbar, ansprechbar und präventiv tätig werden kann.

EU In

33. Digitale Bildung und Vermittlung rechtlicher Normen

In Artikel 33 Absatz 1 Buchstabe b des Verordnungsvorschlags sind bereits Maßnahmen zur Förderung digitaler Kompetenzen bzw. Bildung berücksichtigt. Eine ausdrückliche Berücksichtigung der digitalen Kriminalprävention und der Vermittlung grundlegender rechtlicher Normen findet sich dort jedoch nicht. Artikel 33 Absatz 1 Buchstabe b sollte dahingehend präzisiert werden, dass nationale Strategien neben technischen Kompetenzen auch eine umfassendere digitale Bildung umfassen. Dazu sollten insbesondere Kenntnisse über rechtliche Normen, digitale Ethik, Formen digitaler Kriminalität, Viktimisierungsrisiken und Möglichkeiten staatlicher Unterstützung gehören. Entsprechende Bildungsangebote sollten sich nicht nur an Minderjährige, sondern auch an Eltern und andere Erziehungsberechtigte richten.

Technische Schutzmaßnahmen und Altersbeschränkungen können Risiken zwar reduzieren, Minderjährige jedoch nicht vollständig vor digitaler Viktimisierung schützen. Ein wirksamer digitaler Kinderschutz setzt deshalb voraus, dass Kinder, Jugendliche und Erwachsene über grundlegende Kenntnisse digitaler Risiken und angemessener Handlungsmöglichkeiten verfügen. Dabei sollte digitale Bildung nicht allein auf die Nutzung digitaler Technologien ausgerichtet sein, sondern auch rechtliche, ethische und kriminalpräventive Aspekte berücksichtigen. Dies ist insbesondere deshalb bedeutsam, weil Minderjährige digitale Gefährdungen nicht immer selbstständig als solche erkennen und einordnen können.

EU FSFJ

34. Der Bundesrat betont, dass Kinder und Jugendliche Beratungs- und Hilfeangebote bei Bedarf vertraulich und ohne Kenntnis ihrer Eltern oder sonstiger Sorgeberechtigter nutzen können müssen, soweit die gesetzlichen Voraussetzungen hierfür vorliegen. Instrumente zur elterlichen Kontrolle dürfen diese

Vertraulichkeit nicht beeinträchtigen. Insbesondere sollte verhindert werden, dass Eltern oder Sorgeberechtigte allein aufgrund der Nutzung entsprechender Angebote durch Kontrollwerkzeuge Kenntnis von einer vertraulichen Beratung erhalten. Die vorgesehenen nationalen Strategien und Hilfeangebote sollten einen niedrigschwelligen, kostenfreien, selbständig durch Kinder und Jugendliche nutzbaren und vertraulichen Zugang zu Beratung und Unterstützung gewährleisten. Die Vereinbarkeit mit den einschlägigen nationalen Kinderschutz- und Jugendhilferegelungen ist sicherzustellen.

EU FSFJ

35. Der Bundesrat unterstreicht, dass digitale Medienkompetenz eine wesentliche Voraussetzung für selbstbestimmte Lebensgestaltung, gesellschaftliche Teilhabe und demokratische Resilienz junger Menschen ist. Erforderlich sind insbesondere Informationskompetenz, Quellenkritik, Faktenprüfung, ein Verständnis algorithmischer Mechanismen und die Fähigkeit, KI-generierte Inhalte und Deepfakes kritisch zu hinterfragen. Medien- und Demokratiekompetenz tragen zur Prävention von Desinformation, Hassrede und extremistischer Ansprache sowie zur Förderung reflektierter Urteilsbildung und politischer Mitbestimmung bei.

EU FSFJ

36. Digitale Bildung sollte daher alters- und entwicklungsgerecht entlang der gesamten Bildungsbiografie verankert werden. Dies betrifft die frühkindliche Bildung, Schulen und Ausbildung ebenso wie den außerschulischen Bildungsbereich und die Kinder- und Jugendhilfe. Dazu gehören Inhalte in der Ausbildung pädagogischer Fachkräfte, insbesondere in Sozialpädagogik und Sozialer Arbeit, Fort- und Weiterbildungsangebote zu Social-Media-Anwendungen und Künstlicher Intelligenz sowie Unterstützung für Eltern durch Familienbildung, Gemeinwesenarbeit und Frühe Hilfen. Medienkompetenz soll in pädagogischen Konzepten der Kinder- und Jugendhilfe sowie in schulischen und außerschulischen Bildungsangeboten berücksichtigt und mit MINT-Kompetenzen und Demokratiebildung altersgerecht verbunden werden.

EU FSFJ

37. Der Bundesrat weist darauf hin, dass digitale Angebote analoge Erfahrungs- und Begegnungsräume nicht ersetzen. Familie, Freundeskreise, Schulen, Kindertageseinrichtungen, Jugendarbeit, Vereine und öffentliche Räume ermöglichen soziale Erfahrungen, demokratisches Lernen und Zugehörigkeit. Die Förderung digitaler Teilhabe ist deshalb mit der Stärkung analoger sozialer und pädagogischer Angebote zu verbinden.

EU FSFJ

38. Der Bundesrat stellt fest, dass die Umsetzung der Verordnung die Aufgaben und Zuständigkeiten der Länder berühren kann. Dies betrifft insbesondere die in Artikel 33 vorgesehenen nationalen Strategien zu Hilfekanälen und digitaler Kompetenz sowie die Unterrichtung der Kommission innerhalb der vorgesehenen Frist. Bestehende Strukturen und Zuständigkeiten der Länder sind zu berücksichtigen. Die Kinder- und Jugendhilfe ist als wichtiger außerschulischer Bildungsakteur einzubeziehen. Maßnahmen zur Förderung digitaler Medienkompetenz dürfen nicht auf den schulischen Bereich beschränkt bleiben.

Zu Artikel 34 (Zuständigkeiten, Aufsicht und Durchsetzung)

EU K

39. Der Bundesrat fordert eine klare Abgrenzung der Aufsicht: Die Prüfung und Ahndung einzelner rechtswidriger oder jugendgefährdender Inhalte muss weiterhin den mitgliedstaatlichen Regelungen und Aufsichtsstrukturen unterliegen. Systemische Risiken können auf europäischer Ebene adressiert werden. Doppelstrukturen und Kompetenzkonflikte sind zu vermeiden. Diese Aufteilung ermöglicht ein effektives und effizientes Vorgehen nationaler und europäischer Stellen im Sinne eines weitreichenden Schutzes von Kindern und Jugendlichen.

Zu Artikel 42 (Überprüfung)

EU FSFJ

40. Hinsichtlich der Evaluierung spricht sich der Bundesrat dafür aus, neben der Wirksamkeit der Schutzmaßnahmen insbesondere deren Auswirkungen auf die Rechte und Lebenslagen von Kindern und Jugendlichen zu untersuchen. Dabei sind die Verhältnismäßigkeit von Altersgrenzen und technischen Schutzmechanismen sowie deren tatsächliche Auswirkungen auf den Zugang zu altersgerechten Informations-, Bildungs-, Beratungs- und Beteiligungsangeboten zu bewerten. Einzubeziehen sind auch mögliche Umgehungsmöglichkeiten, Ausschlusswirkungen für besonders benachteiligte Gruppen, die inklusive digitale Teilhabe sowie die Förderung von Medien- und Demokratiekompetenz. Ferner ist zu prüfen, ob Verfahren zur Altersfeststellung barrierefrei und diskriminierungsfrei ausgestaltet sind, wirksame, kostenfreie und niedrigschwellige Möglichkeiten zur Überprüfung und Anfechtung von Altersentscheidungen bestehen und die vertrauliche Nutzung von Beratungs- und Hilfeangeboten gewährleistet bleibt. Die angemessene Beteiligung von Kindern und Jugendlichen sowie ihrer

Interessenvertretungen und die Erfahrungen der Betroffenen und der mit ihnen arbeitenden Fachkräfte sind ebenfalls einzubeziehen. Ziel ist es, Schutzbedürfnisse mit dem Recht auf Information, Beteiligung und altersgerechte digitale Teilhabe in einen angemessenen Ausgleich zu bringen.

Verhältnis zu anderen Rechtsakten

EU DS

41. Die neuen Regelungen müssen eng mit dem Digital Services Act (DSA) und dem AI Act abgestimmt werden. Doppelregulierungen, zusätzliche Nachweispflichten und neue Verwaltungsstrukturen sind möglichst zu vermeiden. Bestehende europäische Aufsichtsmechanismen sollen genutzt und nationale Übergangsregelungen frühzeitig mit der künftigen europäischen Rechtslage in Einklang gebracht werden.

EU K

42. Der Bundesrat weist darauf hin, dass der EU KIDS ACT trotz seines funktionsbezogenen Ansatzes in Bereiche der Medieninhalte- und Medienvielfaltsregulierung eingreift, die auf nationaler Ebene bisher auf Länderebene im Jugendmedienschutz-Staatsvertrag und im Medienstaatsvertrag adressiert sind. Dies betrifft insbesondere Video-Sharing-Plattformen, Altersverifikations- (AVS) und Altersbewertungssysteme, App-Stores, Empfehlungssysteme, KI-Angebote und die Aufsichtsarchitektur. Die im Hinblick auf die Kulturhoheit der Mitgliedstaaten erforderlichen Handlungsspielräume der Mitgliedstaaten müssen deutlich zum Ausdruck kommen.

EU K

43. Der Bundesrat nimmt zur Kenntnis, dass durch den EU KIDS ACT der bisher recht unbestimmte und nicht ausreichend durchsetzungskräftige Artikel 28 des Gesetzes über digitale Dienste (Digital Services Act, DSA) genauer ausgeformt werden soll. Der Bundesrat begrüßt diese Intention im Grundsatz und betont gleichzeitig, dass eine Verzahnung bestehenden nationalen Rechts mit europäischen Rechtsakten im Sinne eines konsistenten und durchsetzungsstarken Schutzes von Kindern und Jugendlichen weiterhin erforderlich ist. So ist etwa das Zusammenspiel zwischen den Regelungen des EU KIDS ACT und den nationalen Umsetzungen des Artikels 28b der Richtlinie über audiovisuelle Mediendienste nicht hinreichend geklärt. Der Bundesrat spricht sich dafür aus, das Verhältnis des EU KIDS ACT zu anderen Rechtsakten eindeutig zu bestimmen.

EU K

44. Der Bundesrat betont, dass die im EU KIDS ACT vorgesehene Anknüpfung an die Umsetzungssystematik des DSA nicht dazu führen darf, dass eingespielte und funktionierende Strukturen blockiert oder ausgehebelt werden. Der Verordnungsvorschlag der EU sollte die in dieser Hinsicht bestehenden Hürden des DSA für eine effektive Rechtsdurchsetzung ausräumen, anstatt sie durch eine Übertragung auf den EU KIDS ACT weiter zu vertiefen.

EU K

45. Der Bundesrat begrüßt in diesem Zusammenhang ausdrücklich auch, dass der EU KIDS ACT eine Beweislastumkehr vorsieht, der die Anbieter sehr großer Online-Plattformen dazu verpflichtet, die Übereinstimmung ihrer Dienste mit den Regelungen des EU KIDS ACT zu belegen. Der Bundesrat sieht in dieser Umkehr der Compliance-Logik einen wichtigen und notwendigen Schritt dahin, die sehr großen Online-Plattformen (VLOP) stärker in die Verantwortung zu nehmen.

Übrige Anliegen

EU FSFJ

46. Der Bundesrat hält eine wirksame Beteiligung von Kindern und Jugendlichen sowie ihrer Interessenvertretungen an der Ausgestaltung, Umsetzung und Überprüfung der Verordnung für wesentlich. Junge Menschen sind Expertinnen und Experten in eigener Sache. Ihre Perspektiven tragen dazu bei, einen zeitgemäßen und wirksamen Jugendmedienschutz, bedarfsgerechte Medienpädagogik und geeignete Rahmenbedingungen für digitale Teilhabe zu gewährleisten.

EU K

47. Der Bundesrat fordert, dass der altersgerechte Zugang zu Medienvielfalt und Information für Kinder und Jugendliche im EU KIDS ACT verankert wird. Mit den im Vorschlag vorgesehenen Regelungen wird der klare Fokus auf den Schutz von Kindern und Jugendlichen vor Gefährdungspotentialen gelegt. Dabei darf das Bedürfnis insbesondere von Jugendlichen am Informationspotential von Social-Media-Netzwerken und Video-Sharing Plattformen teilzuhaben, nicht vollständig in den Hintergrund geraten. Insbesondere vor dem Hintergrund, dass Minderjährige Social-Media-Angebote und Video-Sharing-Plattformen zunehmend als wesentlichen Zugang zu Informationen nutzen, muss gewährleistet sein, dass sie dort auch weiterhin und trotz aktivierter Schutzeinstellungen Zugang zu einer Vielfalt von journalistisch-redaktionellen medialen Angeboten erhalten.

Verhandlungsführung

EU K

48. Der EU KIDS ACT wird in der Ratsarbeitsgruppe Audiovisuelles und Medien beraten. Der Bundesrat nimmt zur Kenntnis, dass die Bundesregierung die Verhandlungsführung für diesen Rechtsakt übernommen hat. Der Bundesrat fordert die Bundesregierung auf, die Position des Bundesrates bei den Verhandlungen mit Nachdruck zu vertreten und die für die Ratsarbeitsgruppe zuständigen Stellen der Länder frühzeitig und umfassend in die jeweiligen Beratungen einzubinden.

Direktzuleitung

EU FSFJ

49. Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.