Fachbereiche EU 6 und WD 3

„Chatkontrolle“ – zur Grundrechtskonformität von Aufdeckungsanordnungen an interpersonelle Kommunikationsdienste nach der Grundrechtecharta und dem Grundgesetz

© 2025 Deutscher Bundestag

„Chatkontrolle“ – zur Grundrechtskonformität von Aufdeckungsanordnungen an interpersonelle Kommunikationsdienste nach der Grundrechtecharta und dem Grundgesetz

Aktenzeichen:	EU 6 - 3000 - 061/25; WD 3 - 3000 - 080/25
Abschluss der Arbeit:	6. November 2025 (zugleich letzter Abruf)
Fachbereiche:	EU 6: Europa; WD 3: Verfassung und Verwaltung

Die Arbeiten des Fachbereichs Europa geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten des Fachbereichs Europa geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegen, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab der Fachbereichsleitung anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1. Einführung

Der im Mai 2022 von der Europäischen Kommission (Kommission) vorgelegte Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (**CSA-Verordnung** bzw. **VO-Vorschlag**)[1] hat eine breite Diskussion in der Öffentlichkeit und Rechtswissenschaft ausgelöst.[2] In der jüngeren Vergangenheit hat die dänische Ratspräsidentschaft das Thema vorangetrieben und zuletzt im Oktober 2025 einen Kompromisstext[3] vorgelegt, der ebenfalls kontrovers diskutiert wurde. Im Zentrum der Kritik steht die in der Verordnung vorgesehene sog. **Chatkontrolle**. Der Begriff bezieht sich auf behördliche Aufdeckungsanordnungen, mit denen Anbieter interpersoneller Kommunikationsdienste wie WhatsApp oder Signal verpflichtet werden können, sämtliche Kommunikation auf ihrem Dienst automatisiert auf Darstellungen sexualisierter Gewalt zu durchsuchen und zu melden.

Vor diesem Hintergrund wurden die Wissenschaftlichen Dienste und der Fachbereich Europa des Deutschen Bundestages mit der Prüfung beauftragt, ob die sog. Chatkontrolle mit den Grundrechten der Charta der Grundrechte der Europäischen Union (**GRCh**) und jenen des deutschen Grundgesetzes (**GG**) vereinbar ist. Die vorliegende Arbeit erläutert zunächst die Genese und den Inhalt des VO-Vorschlags (Ziff. 2.). Sodann wird die Vereinbarkeit der Chatkontrolle mit Unionsgrundrechten, namentlich dem Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRCh), dem Recht auf Schutz personenbezogener Daten (Art. 8 GRCh) und dem Recht auf Freiheit der Meinungsäußerung (Art. 11 GRCh) geprüft (Ziff. 3). Im Anschluss soll das Verhältnis zum Verfassungsrecht und dem Grundrechtsschutz gemäß dem GG untersucht werden (Ziff. 4).

Gegenstand der Arbeit sind die in der CSA-Verordnung vorgesehenen und gemeinhin als Chatkontrolle bezeichneten **Aufdeckungsanordnungen**. Der Analyse werden grundsätzlich die Regelungen des VO-Vorschlags aus dem Jahr 2022 zugrunde gelegt. Soweit es bei der Prüfung auf abweichende Regelungen des Kompromisstextes vom Oktober 2025 ankommt, wird dies entsprechend kenntlich gemacht.

---

1 Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, KOM(2022) 209 endg., 11. Mai 2022.

2 Auch die wissenschaftlichen Dienste und der Fachbereich Europa des Deutschen Bundestages waren bereits mit der Analyse des Gesetzgebungsverfahrens befasst, siehe insbesondere: Deutscher Bundestag, Fachbereich Europa, Überblick zum Stand der rechtswissenschaftlichen Diskussion zum Vorschlag der Kommission vom 11. Mai 2022, COM(2022), 209 final, PE 6 - 3000 - 032/22, 20. Juni 2022, S. 7 f.; Wissenschaftliche Dienste des Deutschen Bundestags, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 – 3000 – 021/22 vom 21. Mai 2022; Wissenschaftliche Dienste des Deutschen Bundestages, „Chatkontrolle“ – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission, WD 10 – 3000 – 026/22 vom 7. Oktober 2022; Deutscher Bundestag, Fachbereich Europa, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025.

3 Rat der Europäischen Union, 2022/0155(COD), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – Kompromisstext, 3. Oktober 2025, 13095/25.

2. Genese und Inhalt des VO-Vorschlags

Der folgende Abschnitt skizziert überblicksartig die Genese der CSA-Verordnung und die Funktionsweise der Aufdeckungsanordnungen.[4]

2.1. Vorschlag der Kommission (Mai 2022)

Im Mai 2022 legte die Europäische Kommission ihren **Vorschlag der CSA-Verordnung** vor. Ziel der Verordnung ist es, einheitliche Verfahren festzulegen, um im Binnenmarkt gegen den Missbrauch von Diensten der Informationsgesellschaft für sexuellen Kindesmissbrauch im Internet vorzugehen (Art. 1 Abs. 1 VO-Vorschlag). Dafür sollen Diensteanbieter verpflichtet werden, die Verbreitung von Darstellungen sexuellen Kindesmissbrauchs sowie – ursprünglich – die Kontaktaufnahme zu Kindern für sexuelle Zwecke (Art. 2 Buchst. p VO-Vorschlag) (sog. **Grooming**) aufzudecken, zu melden und zu entfernen.

Diese Aufdeckungspflichten gelten nach dem VO-Vorschlag nicht unmittelbar, sondern entstehen erst durch die **Aufdeckungsanordnung** einer nationalen Verwaltungsbehörde. Die Funktionsweise dieser Aufdeckungsanordnungen ist im Wesentlichen in Art. 7 – 11 VO-Vorschlag geregelt und gestaltet sich, chronologisch betrachtet, wie folgt:

Eine Aufdeckungsanordnung kann von einer nationalen Justizbehörde oder unabhängigen Verwaltungsbehörde auf Antrag einer vom Mitgliedstaat benannten Koordinierungsbehörde an einen **Anbieter interpersoneller Kommunikationsdienste**[5] gerichtet werden. **Voraussetzung** für den Erlass ist, dass „Beweise für ein erhebliches Risiko“ vorliegen, dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt wird und dass nach behördlicher Einschätzung die Gründe für den Erlass der Aufdeckungsanordnung schwerer wiegen als die damit einhergehenden negativen Folgen (Art. 7 Abs. 4 VO-Vorschlag).

Ergeht eine solche Aufdeckungsanordnung, ist der Diensteanbieter verpflichtet, die Kommunikationsvorgänge aller Nutzerinnen und Nutzer auf seinem Dienst auf bekannte und neue Darstellungen sexuellen Kindesmissbrauchs und auf Grooming zu überprüfen. Dafür müssen bestimmte, in Art. 10 VO-Vorschlag näher bezeichnete **Technologien** eingesetzt werden**.** Sofern der Anbieter auf diesem Weg Kenntnis von potenziellem Kindesmissbrauch erhält, hat er dies gemäß Art. 12 VO-Vorschlag dem eigens zu gründenden EU-Zentrum zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (**EU-Zentrum**, vgl. Art. 40 ff. VO-Vorschlag), das durch ein Netzwerk nationaler Koordinierungsstellen unterstützt wird, zu **melden**. Die Meldung muss gemäß

---

4 Für eine ausführliche Darstellung siehe: Wissenschaftliche Dienste des Deutscher Bundestages, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 – 3000 – 021/22 vom 21. Mai 2022.

5 Nach Art. 2 Nr. 5 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 321, 17. Dezember 2018, S. 36, ist ein interpersonellen Kommunikationsdienst ein „gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind […]“. Nach Art. 2 Buchst. b VO-Vorschlag soll der Anwendungsbereich auch solche Dienste erfassen, „die einen direkten interpersonellen und interaktiven Informationsaustausch lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen“.

Art. 13 Abs. 1 VO-Vorschlag unter anderem alle Inhaltsdaten sowie Angaben zur Identität der beteiligten Nutzer enthalten und kann beispielsweise die IP-Adresse umfassen. Über die Meldung ist der betreffende Nutzer gemäß Art. 12 Abs. 2 VO-Vorschlag vom Anbieter zu informieren. Das EU-Zentrum prüft die Meldungen und leitet sie, wenn nicht offensichtlich unbegründet, an die Europol und die voraussichtlich zuständige nationale Strafverfolgungsbehörde weiter, vgl. Art. 48 VO-Vorschlag.[6]

2.2. Kompromisstext der dänischen Ratspräsidentschaft (Oktober 2025)

Seit Beginn der Verhandlungen wurden im Rat der EU zahlreiche Änderungsvorschläge diskutiert. Zuletzt schlug die dänische Ratspräsidentschaft am 3. Oktober 2025 einen Kompromisstext zur CSA-Verordnung vor.[7] Der Kompromisstext nimmt **Änderungen** am ursprünglichen Kommissionsvorschlag vor und fügt zusätzliche Regelungen hinzu, um die Cybersicherheit und Verschlüsselung umfassend zu schützen. Relevant sind insbesondere die folgenden Änderungen:

- Der Anwendungsbereich von Aufdeckungsanordnungen wurde eingeschränkt: Umfasst sind künftig **nur Bilder und Videos sowie URLs**, nicht aber Text- und Audioinhalte. Ausgenommen wurden auch dem Berufsgeheimnis unterliegende Kommunikation sowie das sog. „Grooming“.[8]

- Ferner wurde das Verfahren bei **Ende-zu-Ende verschlüsselten Nachrichten** modifiziert: In diesen Fällen soll die Aufdeckung dadurch ermöglicht werden, dass das Scannen vor der Verschlüsselung auf dem Gerät der Nutzerinnen und Nutzer erfolgt (**Client-Side-Scanning - CSS**) und zudem von der Zustimmung der Nutzerinnen und Nutzer abhängig gemacht werden soll (vgl. Art. 10 Abs. 4, 5 Kompromisstext). Die Zustimmung erfolgt im Rahmen der allgemeinen Geschäftsbedingungen (AGB) des Anbieters. Sollte sie verweigert werden, ist ein Versenden von visuellen Inhalten und URL nicht möglich.[9]

- Zudem sollen Meldungen an das EU-Zentrum in einem ersten Schritt **pseudonymisiert** erfolgen, um negative Auswirkungen von „False Positives“ zu begrenzen. Auch soll der Umfang der an das EU-Zentrum zu übermittelnden Metadaten eingegrenzt werden.[10]

---

6 Deutscher Bundestag, Fachbereich Europa, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025.

7 Rat der Europäischen Union, 2022/0155(COD), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – Partielle allgemeine Ausrichtung, 3. Oktober 2025, 13095/25 (im Folgenden: Kompromisstext vom 3. Oktober 2025).

8 Kompromisstext vom 3. Oktober 2025, S. 3 f., ErwG 23a.

9 Kompromisstext vom 3. Oktober 2025, S. 4, ErwG 26a.

10 Kompromisstext vom 3. Oktober 2025, S. 4, ErwG 23a.

Trotz der Änderungen bleibt das **Grundkonzept der Aufdeckungsanordnungen bestehen**: Die Aufdeckungspflichten sind gerichtet auf die Erfassung und Meldung von bekannten und unbekannten Missbrauchsdarstellungen, also Inhaltsdaten – nicht nur Metadaten – der Kommunikation aller Nutzerinnen und Nutzer eines Dienstes.

2.3. Interimsverordnung (bis April 2026)

Zur Vermeidung von Schutzlücken haben sich das Europäische Parlament und der Rat bereits 2021 auf einen befristeten Rechtsrahmen für die Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, die sog. **Interimsverordnung**,[11] geeinigt und diese inzwischen bis April 2026 verlängert.[12]

Die **Interimsverordnung** ermöglicht das freiwillige Verarbeiten von Daten durch die Diensteanbieter, indem sie **Ausnahmen** von bestimmten Vorschriften der **ePrivacy-Richtlinie**[13] macht. Sie erlaubt es den Anbietern, „spezielle Technologien für die Verarbeitung personenbezogener und anderer Daten in dem Maße zu verwenden, in dem dies unbedingt erforderlich ist, um sexuellen Missbrauch von Kindern im Internet bei ihren Diensten aufzudecken und zu melden und Online-Material über sexuellen Missbrauch von Kindern aus ihren Diensten zu entfernen“ (Art. 1 Abs. 1 der Interimsverordnung).

Derzeit ist es also möglich, dass Anbieter *freiwillig* die transportverschlüsselte[14] Kommunikation auf ihren Diensten auf Darstellungen sexualisierter Gewalt von Kindern prüfen und diese melden. Was bislang nicht möglich ist, ist ein *verpflichtender* Zugriff, insbesondere auf Ende-zu-

---

11 Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 29. April 2024 zur Änderung der Verordnung (EU) 2021/1232 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, ABl. L 274, 30. Juli 2021, S. 41.

12 Verordnung (EU) 2024/1307 des Europäischen Parlaments und des Rates vom 29. April 2024 zur Änderung der Verordnung (EU) 2021/1232 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, ABl. L 274, 30. Juli 2021, S. 41 (konsolidierte Fassung v. 15. Mai 2024.

13 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, Amtsblatt L 201 vom 31. Juli 2002, S. 37 – 47.

14 Bei der **Transportverschlüsselung** (z.B. E-Mail-Programme, Facebook-Messenger, Instagram-Nachrichten), auch Punkt-zu-Punkt-Verschlüsselung, werden die Daten (nur) während der Übertragung zwischen zwei Punkten verschlüsselt. Am Knotenpunkt, z. B. dem Server, werden sie entschlüsselt, sodass der Server in der Regel Zugang zu den unverschlüsselten Daten hat. Bei der **Ende-zu-Ende-Verschlüsselung** (z.B. bei WhatsApp, Threema, Signal) sind die Daten hingegen auf dem gesamten Weg vom Sender bis zum Empfänger verschlüsselt. Auf den Inhalt können weder der Diensteanbieter noch der Server zugreifen, vgl. Wissenschaftliche Dienste des Deutschen Bundestags, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 – 3000 – 021/22 vom 21. Mai 2022, S. 16, 18.

Ende verschlüsselte Kommunikation. Darüber hinaus ist die Interimsverordnung bis April 2026 befristet, was den Zeitdruck im Rat für die Einigung auf einen Verordnungstext erhöht.

2.4. Aktueller Verhandlungsstand

Der Kompromissvorschlag der dänischen Ratspräsidentschaft vom Oktober 2025 fand unter den Mitgliedstaaten keine qualifizierte Mehrheit, wobei insbesondere die deutsche Bundesregierung jüngst ihre Zustimmung verweigerte.[15] Daraufhin wurde die Abstimmung zunächst vertagt. Jüngsten Presseberichten zufolge hat sich die dänische Ratspräsidentschaft inzwischen von dem Konzept der verpflichtenden Aufdeckungsanordnungen verabschiedet und strebt nun einen neuen Ansatz an, der auf freiwillige Aufdeckungsmaßnahmen im Sinne der o.g. Interimsverordnung setzt.[16] Ob die Mitgliedstaaten, insbesondere jene, die einen ambitionierteren Ansatz verfolgen, den neuen Vorstoß unterstützen werden, wird sich zeigen. Wie das EP auf die Änderungen reagieren wird, bleibt ebenfalls abzuwarten. In seiner Entschließung vom 16. November 2023[17] zum Verordnungsentwurf befürwortet das Parlament den Erlass von Aufdeckungsanordnungen durch Justizbehörden allerdings unter bestimmten Voraussetzungen und als Ultima Ratio. Vor diesem Hintergrund bleibt abzuwarten, wie sich das Gesetzgebungsverfahren weiterentwickelt.

3. Vereinbarkeit mit Unionsgrundrechten

Der folgende Abschnitt prüft, ob die im VO-Vorschlag vorgesehenen und durch den Kompromisstext modifizierten Aufdeckungsanordnungen mit den in der GRCh gewährleisteten Grundrechten in Einklang stehen. Das ist der Fall, wenn der damit verbundene Eingriff in die Unionsgrundrechte aus Art. 7, 8 und 11 GRCh gerechtfertigt wäre.

Zunächst wird die Eröffnung der Schutzbereiche der genannten Grundrechte knapp dargestellt (Ziff. 3.1.).[18] Auf Eingriffsebene stellt sich die Frage, ob die im Kompromisstext vorgesehene Einwilligung einem Eingriff entgegensteht (Ziff. 3.2.). Der Schwerpunkt der Prüfung liegt auf der Rechtfertigungsebene (Ziff. 3.3.), wobei es insbesondere auf die Achtung des Wesensgehalts und die Wahrung des Gesetzesvorbehaltes und des Verhältnismäßigkeitsgrundsatzes ankommt.

---

15 Welt, „Dem wird Deutschland nicht zustimmen“ – Justizministerin lehnt EU-Pläne zur Chatkontrolle ab, veröffentlicht am 9. Oktober 2025.

16 Heise online, Dänemark verabschiedet sich überraschend von Plänen für die Chatkontrolle | heise online, veröffentlicht am 30. Oktober 2025; FAZ, Dänemark: EU-Ratspräsidentschaft stoppt anlasslose Chatkontrolle | FAZ, veröffentlicht am 31. Oktober 2025; ZEIT, Umstrittenes Vorhaben: Verpflichtende "Chatkontrolle" in EU vorerst vom Tisch | DIE ZEIT, veröffentlicht am 31. Oktober 2025.

17 Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, A9-0364/2023.

18 Für eine ausführliche Herleitung der Schutzbereiche siehe: Wissenschaftliche Dienste des Deutschen Bundestages, „Chatkontrolle“ – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission, WD 10 – 3000 – 026/22 vom 7. Oktober 2022 S. 6 ff.

3.1. Schutzbereich

3.1.1. Achtung des Privat- und Familienlebens (Art. 7 GRCh)

Art. 7 GRCh schützt die Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation und statuiert damit ein Recht auf Privatsphäre. Der Begriff Kommunikation umfasst dabei – entgegen dem offenen Wortlaut – ausschließlich die individuelle Kommunikation unter Abwesenden, die sog. **Fernkommunikation**.[19] Das gilt insbesondere bei der Übermittlung der Kommunikation durch Dritte, die spezifische Risiken für die Vertraulichkeit der Kommunikation mit sich bringt.[20] Dabei ist die Erscheinungsform unerheblich und offen für technische Entwicklungen. Erfasst werden beispielsweise Übermittlungen per Post, Telefon oder E-Mail und konsequenterweise auch die Kommunikation mittels **Messengerdiensten** wie WhatsApp oder Signal.[21] Der Schutzbereich von Art. 7 GRCh ist damit eröffnet.

3.1.2. Schutz personenbezogener Daten (Art. 8 GRCh)

Art. 8 Abs. 1 GRCh umfasst das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten. Der Schutzbereich ist eng mit dem Schutz der Kommunikation aus Art. 7 GRCh verknüpft und dann eröffnet, wenn personenbezogene Daten verarbeitet werden.[22] Der Begriff der **Verarbeitung** ist dabei weit zu verstehen und umfasst alle Maßnahmen, welche an personenbezogenen Daten vorgenommen werden.[23] **Personenbezogene Daten** umfassen alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[24] Dabei reicht es aus, dass das Verfahren es ermöglicht, die Person oder Personen erst später zu identifizieren, wie es etwa im vorliegenden Fall der automatisierten Analyse von Daten der Fall ist.[25] Die Aufdeckungsanordnungen berühren daher den Schutzbereich von Art. 8 GRCh.

3.1.3. Freiheit der Meinungsäußerung (Art. 11 GRCh)

Art. 11 Abs. 1 Satz 1 GRCh schützt das Recht jeder Person auf freie Meinungsäußerung. Dieses Recht schließt gemäß Satz 2 die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen

---

19 Vgl. *Bernsdorff*, in: Meyer, EU-Grundrechtecharta, 6. Aufl. 2024, Art. 7 GRCh, Rn. 21; *Gersdorf,* in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 49. Ed. 01.11.2024, Art. 7 EU-GRCharta, Rn. 35.

20 *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 7 GRCh, Rn. 25.

21 *Bernsdorff*, in: Meyer, EU-Grundrechtecharta, 6. Aufl. 2024, Art. 8 GRCh, Rn. 21; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, GRCh Art. 7 Rn. 10.

22 *Bernsdorff*, in: Meyer, EU-Grundrechtecharta, 6. Aufl. 2024, Art. 8 GRCh, Rn. 20.

23 *Bernsdorff*, in: Meyer, EU-Grundrechtecharta, 6. Aufl. 2024, Art. 8 GRC, Rn. 22.

24 *Bernsdorff*, in: Meyer, EU-Grundrechtecharta, 6. Aufl. 2024, Art. 8 GRC, Rn. 20.

25 Vgl. Juristischer Dienst des Rates, Gutachten, Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – Aufdeckungsanordnungen für interpersonelle Kommunikation – Artikel 7 und 8 der Charta der Grundrechte – Recht auf Privatleben und den Schutz personenbezogener Daten – Verhältnismäßigkeit (im Folgenden: JD, Gutachten vom 26. April 2023), Dok. Nr. 8787/23 vom 26. April 2023, Rn. 35.

ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Unter Meinungen sind insbesondere **Werturteile** zu verstehen; Informationen meinen dagegen vor allem **Tatsachenbehauptungen**. Geschützt sind das Bilden, Haben, Äußern und Verbreiten von Meinungen sowie auch das Recht, eine Meinung *nicht* zu haben oder zu äußern.[26] Die Informationsfreiheit schützt insbesondere den Empfang von Informationen und Meinungen und schützt den gesamten Prozess der Informationsbeschaffung.[27]

Was die Aufdeckungsanordnungen betrifft, so wurden Bedenken geäußert, dass diese **eine abschreckende Wirkung** auf die freie Äußerung der eigenen Meinung haben könnten.[28] So könnten Betroffene ein Gefühl der ständigen Überwachung entwickeln und das Vertrauen in die Vertraulichkeit ihrer Kommunikation verlieren. Dies könnte das Kommunikationsverhalten beeinflussen und dazu führen, dass sich manche Menschen im digitalen Raum weniger frei äußern. Insofern ist die Meinungsfreiheit aus Art. 11 Abs. 1 GRCh jedenfalls mittelbar betroffen.

3.2. Eingriff, insb. Einwilligung (vgl. Art. 8 Abs. 2 Satz 1 GRCh)

Die Aufdeckungsanordnungen haben eine nachteilige Wirkung auf die grundrechtsberechtigten Nutzerinnen und Nutzer der Messengerdienste, stellen also grundsätzlich einen Eingriff in die geschützten Grundrechtspositionen aus Art. 7, 8 und 11 GRCh dar.

Zweifel an dem Vorliegen eines Eingriffs könnten sich allerdings aus der im Kompromisstext vorgesehenen **Zustimmung** der Nutzerinnen und Nutzer in den Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Dienstes ergeben (Art. 10 Abs. 4, 5 Kompromisstext).[29] Denn aus Art. 8 Abs. 2 S. 1 GRCh ergibt sich, dass ein Eingriff dann nicht vorliegt, wenn der Grundrechtsinhaber in Kenntnis der Sachlage in die Verarbeitung seiner Daten einwilligt.[30]

Allerdings setzt der Eingriffsausschluss **Freiwilligkeit** voraus, was anhand aller Umstände des Einzelfalls zu beurteilen ist. Zur Konkretisierung der Anforderungen an die datenschutzrechtliche Einwilligung kann auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zum europäischen Datenschutzrecht zurückgegriffen werden.[31] Danach setzt Freiwilligkeit insbesondere

---

26 *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 11 GRCh, Rn. 10 ff.

27 *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 11 GRCh, Rn. 15.

28 JD, Gutachten vom 26. April 2023, Rn. 33.

29 Siehe auch Kompromisstext vom 3. Oktober 2025, S. 4, ErwG 26a.

30 *Jarass*, in Jarass: Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 Rn. 10; Jarass, in Jarass: Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 18.

31 Vgl. *Johlen*, in: Stern/Sachs, 1. Aufl. 2016, Europäische Grundrechte-Charta, Art. 8 Rn. 13; *Jarass*, in Jarass: Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 Rn. 13; siehe auch Der Bayerische Landesbeauftragte für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe vom 1. September 2021, Seite 11, Rn. 1.

voraus, dass der Verzicht auf die Grundrechtsposition nicht **durch gewichtige Umstände erzwungen** sein darf.[32] So urteilte der EuGH in der Rechtssache Schwarz, dass nicht davon ausgegangen werden könne, dass diejenigen, die einen Reisepass beantragen, in eine solche Verarbeitung auch eingewilligt hätten, schließlich sei dies zwingende Voraussetzung für Reisen außerhalb der Europäischen Union (EU).[33] Ferner geht aus der Rechtsprechung des EuGH hervor, dass es den betroffenen Personen freistehen sollte, im Zusammenhang mit politischer Werbung ihre Einwilligung zu bestimmten Datenverarbeitungsvorgängen zu verweigern, **ohne ganz** auf den Zugang zu einer Dienstleistung **verzichten** zu müssen. Nach Auffassung des Gerichtshofs sollte den Betroffenen eine gleichwertige Alternative angeboten werden, die nicht mit einer Datenverarbeitung einhergehe.[34]

Diese Maßstäbe sind nunmehr auf den Vorschlag der dänischen Ratspräsidentschaft hinsichtlich der Zustimmung in den AGB der Diensteanbieter zu übertragen: Der Kompromisstext sieht vor, dass das CSS nur unter der Voraussetzung der ausdrücklichen Zustimmung des Nutzers im Rahmen der AGB des Anbieters stattfindet. Nutzer, die ihre Zustimmung nicht erteilen, sollten den Teil des Dienstes, der nicht das Versenden von visuellen Inhalten und URL umfasst, weiterhin nutzen können (vgl. Art. 10 Abs. 4, 5 Kompromisstext).[35] Das bedeutet, dass ein Versenden von visuellen Inhalten und URL ohne Einwilligung in die Chatkontrolle nicht mehr möglich ist – und zwar auf keinem Dienst.

Diesbezüglich ist zunächst festzustellen, dass Nutzerinnen und Nutzer als Konsequenz für eine verweigerte Zustimmung in die Datenverarbeitung nicht *ganz* auf die Nutzung des jeweiligen Dienstes verzichten müssten, sondern lediglich auf das Versenden von visuellen Inhalten – also Bildern und Videos – sowie URLs. Für den Versand von Text- und Audionachrichten stünde ihnen die Nutzung des Dienstes weiterhin frei – insofern scheint den Anforderungen des EuGH auf den ersten Blick Genüge getan zu sein.

Allerdings ist fraglich, ob insoweit eine „gleichwertige“ Alternative vorliegt. Bei der Versandmöglichkeit von Bildern, Videos und URLs handelt es sich um essenzielle Bestandteile der täglichen Kommunikation auf Messengerdiensten. Im Fall einer verweigerten Zustimmung könnte der Nutzer diese Inhalte auf keinem Dienst mehr versenden, da alle Dienste zur Aufnahme der Zustimmung in ihre AGB verpflichtet sind. Eine digitale Kommunikation ohne Bilder, Videos und URLs ist aus dem Alltag der Nutzerinnen und Nutzer kaum wegzudenken, sodass durchaus eine vergleichbare Situation wie bei den durch den EuGH bereits beurteilten Reisepässen vorläge. Dies spricht im Ergebnis gegen das Vorliegen einer eingriffsausschließenden Einwilligung.

---

32 EuGH, Urteil vom 17. Oktober 2013, Rs. C-291/12, Schwarz, Rn. 32; *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 Rn. 10; *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 18.

33 EuGH, Urteil vom 17. Oktober 2013, Rs. C-291/12, Schwarz, Rn. 32.

34 EuGH, Urteil vom 4. Juli 2023, Rs. C-252/21, Meta Platforms u.a. (Conditions générales d’utilisation d’un réseau social), Rn. 150.

35 Siehe auch Kompromisstext vom 3. Oktober 2025, S. 4, ErwG 26a.

3.3. Rechtfertigung

Der Eingriff in Art. 7, 8 und 11 GRCh kann gerechtfertigt werden, wenn der Wesensgehalt der Grundrechte geachtet (Ziff. 3.3.1.), eine ausreichende gesetzliche Grundlage besteht (Ziff. 3.3.2.) und der Grundsatz der Verhältnismäßigkeit gewahrt ist (Ziff. 3.3.3.).

3.3.1. Wesensgehalt (Art. 52 Abs. 1 Satz 1 GRCh)

Nach Art. 52 Abs. 1 Satz 1 GRCh muss jede Einschränkung den Wesensgehalt des betroffenen Grundrechts achten. Dagegen sind Regelungen, die den Wesensgehalt eines Grundrechts nicht achten, nicht rechtfertigungsfähig und schon deshalb grundrechtswidrig.[36] Der Wesensgehalt umfasst einen **unantastbaren Kernbereich** der Grundrechte und erfordert eine Einzelfallbetrachtung, die die Besonderheiten des jeweiligen Grundrechts berücksichtigt.[37] Mit dem Wesensgehalt der Kommunikationsgrundrechte aus Art. 7 und Art. 8 GRCh[38] hat sich der EuGH bisher im Kontext der Vorratsdatenspeicherung befasst. Ob diese Rechtsprechung unmittelbar auf den vorliegenden Fall übertragbar ist, ist im Einzelnen umstritten, geht es doch bei den Aufdeckungspflichten darum, Kommunikationsinhalte zu scannen, statt sie auf Vorrat zu speichern.[39] Die Rechtsprechung kann aber jedenfalls indiziell herangezogen werden und generelle Anhaltspunkte für die Haltung des EuGH zum Wesensgehalt von Art. 7 und 8 GRCh liefern.

Aus den Urteilen des EuGH zur Vorratsdatenspeicherung ergibt sich, dass bestimmte Eingriffe in den **Inhalt** interpersoneller Kommunikation den Wesensgehalt von Art. 7 und 8 GRCh beeinträchtigen können. In der Rechtssache Digital Rights Ireland stellte der EuGH zu einer Regelung über die allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten fest, dass diese deshalb *nicht* geeignet war, den Wesensgehalt von Art. 7 GRCh anzutasten, weil sie die „Kenntnisnahme des Inhalts elektronischer Kommunikation“ nicht gestattete.[40] Auch in der Rechtssache Tele2 Sverige entschied der EuGH, dass die dort in Rede stehende Regelung *nicht* den Wesensgehalt der Art. 7, 8 GRCh antaste, weil sie nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubte.[41] Daraus kann im Umkehrschluss gefolgert werden: Wenn der Wesensgehalt dann gewahrt ist, wenn eine Kenntnisnahme des Inhalts nicht möglich ist, so

---

36 Deutscher Bundestag, Fachbereich Europa, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025, S. 21; vgl. *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 28.

37 *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 28 f.; *Pache*, in: Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV, GRCh Art. 52 Rn. 31.

38 Da die Meinungsfreiheit aus Art. 11 GRCh nur peripher betroffen ist (vgl. Ziff. 3.1.3.), kommt diesbezüglich eine Wesensgehaltsverletzung nicht infrage.

39 Siehe dazu ausführlich: Deutscher Bundestag, Fachbereich Europa, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025.

40 EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 39.

41 EuGH, Urteil vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige, Rn. 101.

müsse umgekehrt das Vorhaben der Kommission, das sich gerade auf die Inhalte elektronischer Kommunikation bezieht, den Wesensgehalt von Art. 7 GrCh verletzen.[42]

Ferner urteilte der EuGH in der Rechtssache Schrems, dass „eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens [verletze]“.[43] Der Juristische Dienst des Rates (JD) sieht auf dieser Grundlage eine ernste Gefahr, dass der EuGH – würde er mit den entsprechenden Regelungen des VO-Vorschlags befasst – eine Verletzung des Wesensgehalts von Art. 7 GRCh feststellen würde. Dies begründet er damit, dass mit der Auferlegung von Aufdeckungspflichten der generelle Zugriff auf die Inhalte interpersoneller elektronischer Kommunikation des verpflichteten Dienstes sowie die generelle Weiterverarbeitung gestattet würde.[44]

Besonderes Augenmerk muss allerdings auf die Einschränkung „**generell**“ in der Rechtssache Schrems gelegt werden. Laut EuGH meint das Merkmal „generell“ den uneingeschränkten behördlichen Zugang zu sämtlichen personenbezogenen Daten aller Personen, deren Daten (aus der Union in die Vereinigten Staaten) übermittelt wurden.[45] Das ist, wie die Kommission argumentiert,[46] bei den Aufdeckungsanordnungen gerade nicht der Fall. Es gehe nicht darum, privaten oder staatlichen Akteuren umfassenden Zugriff auf Inhaltsdaten zu geben. Vielmehr sei nach dem VO-Vorschlag die Extraktion, also Weitergabe von Inhalten als Ergebnis des Scannens des Gesamtinhalts, auf das unbedingt Notwendige beschränkt (Art. 10 Abs. 3 Buchst. b VO-Vorschlag). Inhaltsdaten würden zwar „generell“ verarbeitet, aber nicht „generell“ weitergegeben, sondern vorher extrahiert. Dementsprechend ermöglichen sie auch keinen vollständigen Überblick über das Privatleben der betroffenen Person.[47]

Vor diesem Hintergrund ist der Ausgang der Wesensgehaltsprüfung durch den EuGH offen. Für eine Wahrung des Wesensgehalts spricht jedenfalls, dass diese erst eine differenzierte Abwägung auf Rechtfertigungsebene eröffnet.

---

42 *Tuchtfeld*, „Vielen Dank, Ihre Post ist unbedenklich“ – Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte, Verfassungsblog vom 25. Mai 2022.

43 EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 94.

44 JD, Gutachten vom 26. April 2023, Rn. 56.

45 Vgl. EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 93.

46 Commission services, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Balancing the rights of children with users' rights, Dok. Nr. 9512/23 (im Folgenden: KOM, Non-Paper) vom 16. Mai 2023, Rn. 27.

47 KOM, Non-Paper vom 16. Mai 2023, Rn. 38 ff.; ähnlich: *Vasel*, Datenschutz versus Kinderschutz?, ZRP 2022, 191 (193).

3.3.2. Gesetzesvorbehalt (Art. 52 Abs. 1 Satz 1 GRCh)

Gemäß Art. 52 Abs. 1 S. 1 GRCh muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten „gesetzlich vorgesehen“ sein. Dieses Erfordernis einer gesetzlichen Grundlage, auch Gesetzesvorbehalt genannt,[48] bezieht sich nicht nur auf das bloße *Vorliegen* eines Gesetzes. Vielmehr muss der Unionsgesetzgeber auch die Voraussetzungen und den genauen Umfang dieser Einschränkung **klar, vollständig und präzise** festlegen, damit die Adressaten die Auswirkungen vorhersehen und ihr Verhalten darauf einrichten können.[49] Dabei sind angesichts der Schwere der verbundenen Grundrechtseingriffe sowie der Tatsache, dass die vorgeschlagene VO in den Mitgliedstaaten unmittelbar gelten würde, besonders strenge Anforderungen an die gesetzliche Regelungsdichte zu stellen.[50] Gleichzeitig erkennt der EuGH an, dass die Einschränkung hinreichend offen formuliert sein muss, um Anpassungen an unterschiedliche Fallkonstellationen und sich verändernde Gegebenheiten zu ermöglichen.[51]

Letzteren Punkt betont die Kommission in ihrem Non-Paper zur Abwägung der Rechte des Kindes mit denen der Dienstenutzerinnen und -nutzer: Sie verweist darauf, dass in der Rechtsprechung des EuGH anerkannt sei, dass Regelungen, die privaten Diensteanbietern Pflichten auferlegen, **hinreichend offen** sein müssen, um ihnen eine Abwägung der berührten (gegenläufigen) Unionsgrundrechte zu ermöglichen.[52] Ferner sei eine begriffliche Offenheit bei vergleichbaren Rechtsvorschriften in Bereichen, die einem schnellen technologischen und kommerziellen Wandel unterlägen, nicht unüblich und der den Diensteanbietern eröffnete Handlungsspielraum in einen detaillierten rechtlichen Rahmen eingebettet, der Grenzen und Schutzmaßnahmen vorschreibe. Zudem würde die Kommission auf der Grundlage von Art. 11 VO-Vorschlag konkretisierende Leitlinien zu den Aufdeckungspflichten erarbeiten, um die Vorhersehbarkeit zu erhöhen.[53]

Demgegenüber haben sowohl der JD des Rates als auch der Wissenschaftliche Dienst des Europäischen Parlaments (European Parliamentary Research Service – EPRS) angesichts der im VO-Vorschlag verwendeten **unbestimmten Rechtsbegriffe** Zweifel geäußert, ob es sich bei den Bestimmungen um eine hinreichend klare, präzise und vollständige gesetzliche Grundlage i. S. v.

---

48 *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 23.

49 EuGH, Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, Rs. C-311/18, Rn. 175; *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 11 GRCh, Rn. 13 f.

50 JD, Gutachten vom 26. April 2023, Rn. 17 f.

51 EuGH, Urteil vom 21. Juli 2022, Ligue des droits humains, Rs. C-817/19, Rn. 114; Vgl. JD, Gutachten vom 26. April 2023, Rn. 16.

52 KOM, Non-Paper vom 16. Mai 2023, Rn. 22 unter Verweis auf EuGH, Urteil vom 26. April 2022, Rs. C-401/19, Polen/EP und Rat, Rn. 75.

53 KOM, Non-Paper vom 16. Mai 2023, Rn. 20 ff.

Art. 52 Abs. 1 Satz 1 GRCh handelt.[54] Anlass dafür gibt die Vielzahl von **unbestimmten Rechtsbegriffen**, die den VO-Vorschlag sowohl auf Tatbestands- als auch auf Rechtsfolgenseite der Aufdeckungsanordnungen prägen:

Auf Tatbestandsseite setzt Art. 7 Abs. 4 VO-Vorschlag unter anderem voraus, dass „**Beweise für ein erhebliches Risiko“** vorliegen, dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt wird. Dieses Tatbestandsmerkmal lässt sich anhand des VO-Vorschlags kaum konkretisieren. So setzt Art. 7 Abs. 5 für die Annahme eines erheblichen Risikos voraus, dass der Dienst „in beträchtlichem Umfang“ für die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs genutzt wird und Beweise dafür vorliegen, dass der Dienst oder ein „vergleichbarer Dienst“ in den letzten zwölf Monaten in beträchtlichem Umfang für die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs genutzt wurde. Es ist ungeklärt, ab wann von einem „beträchtlichen Umfang“ oder „vergleichbaren Dienst“ auszugehen ist, sodass an dieser Stelle das Bestimmtheitsgebot nicht gewahrt sein dürfte.[55]

Auf Rechtsfolgenseite ist Art. 10 VO-Vorschlag zu beachten. Gemäß Art. 10 Abs. 1 VO-Vorschlag führen Anbieter interpersoneller Kommunikationsdienste, die eine Aufdeckungsanordnung erhalten, diese durch die „**Installation und den Betrieb von Technologien**“ aus, mit denen die Verbreitung von Darstellungen sexuellen Kindesmissbrauchs „mithilfe der entsprechenden vom EU-Zentrum gemäß Art. 46 bereitgestellten Indikatoren“ erkannt werden kann. Allerdings wird die Beschaffenheit dieser Technologien nicht hinreichend detailliert festgelegt. Es bleibt offen, welche Technologien wie genau eingesetzt werden sollen, um Darstellungen sexuellen Kindesmissbrauchs zu erkennen. Dies ist auch deswegen relevant, da mit unterschiedlichen technischen Verfahren unterschiedliche Grundrechte berührt sein, bestimmte Technologien höhere Fehleranfälligkeiten aufweisen können und auch das Potential für die Gefahr von Missbrauch dieser Technologien steigen könnte.[56] Darüber hinaus sieht Art. 10 keine Beschränkung oder Eingrenzung dahingehend vor, welche Art von Daten verarbeitet werden soll. Auch wird nicht geregelt, wie mit erhobenen Daten umgegangen werden soll, die nicht zum Zweck der Erkennung von Darstellungen sexuellen Kindesmissbrauchs benötigt werden. Letztendlich wird insoweit die staatliche Verantwortung in erheblichem Maße auf die Anbieter interpersoneller Kommunikationsdienste gewissermaßen delegiert. Aufseiten der Betroffenen bleibt eine große Unsicherheit, was konkret mit ihren Daten geschieht.[57]

Angesichts der unklaren Auslegung der unbestimmten Rechtsbegriffe auf Tatbestands- und Rechtsfolgenseite dürften erhebliche **Anwendungsspielräume** auf Behörden- und Anbieterseite

---

54 Vgl. JD, Gutachten vom 26. April 2023, Rn. 16 ff.; EPRS, Proposal for a regulation laying down the rules to prevent and combat child sexual abuse, Complementary impact assessment (im Folgenden: EPRS, Folgenabschätzung), April 2023, S. 52 f.

55 Vgl. EPRS, Folgenabschätzung, April 2023, S. 52 f.

56 Vgl. auch: *Zurawski*, EU-Kommission: Vorschlag „Chatkontrolle“ – Verhältnisse der Überwachung, ZD-Aktuell 2022, 01240; *Etteldorf*, EU-Kommission: Verordnungsvorschlag zum besseren Schutz von Kindern vor sexuellem Missbrauch, MMR-Aktuell 2022, 449230.

57 Vgl. im Einzelnen: JD, Gutachten vom 26. April 2023, Rn. 21 ff. Der JD weist darauf hin, dass weder ausgeführt werde, was unter „hinreichend zuverlässigen Erkenntnistechnologien“ zu verstehen sei, noch welche „Fehlerquote“ angemessen wäre oder welche Indikatoren zum Einsatz kämen.

verbleiben. Die Betroffenen dürften entsprechend Schwierigkeiten haben, die Voraussetzungen und das Ausmaß der Überwachung vorherzusehen. Berücksichtigt man die eingangs hergeleiteten hohen Anforderungen an die Präzision der Verordnung, fehlt es im Ergebnis an einer ausreichend klaren und präzisen gesetzlichen Grundlage i. S. d. Art. 52 Abs. 1 Satz 1 GRCh.

3.3.3. Verhältnismäßigkeit (Art. 52 Abs. 1 Satz 2 GRCh)

Nach dem in Art. 52 Abs. 1 Satz 2 GRCh normierten Grundsatz der Verhältnismäßigkeit darf eine hoheitliche Maßnahme nicht außer Verhältnis zu dem angestrebten Ziel stehen. Das ist der Fall, wenn sie zur Erreichung des zulässigerweise verfolgten Ziels geeignet und erforderlich und überdies angemessen ist.[58]

3.3.3.1. Legitimes Ziel

Die CSA-Verordnung verfolgt gemäß Art. 1 Abs. 1 VO-Vorschlag das Ziel, im Binnenmarkt gegen den Missbrauch einschlägiger Dienste der Informationsgesellschaft für den sexuellen Kindesmissbrauch im Internet vorzugehen. Dabei handelt es sich um eine dem Gemeinwohl dienende Zielsetzung, nämlich die Bekämpfung schwerer Kriminalität.[59] Ob dies im vorliegenden Fall als legitime Zielsetzung ausreicht, ist umstritten.

Grundsätzlich reichen nach Art. 52 Abs. 1 Satz 2 GRCh die „von der Union anerkannten dem **Gemeinwohl** dienenden Zielsetzungen“ oder der „Schutz der Rechte und Freiheiten anderer“ als legitimes Ziel aus. Der JD des Rates und der EPRS verweisen bezüglich der erhöhten Anforderungen an das legitime Ziel u. a. auf die Rechtsprechung des EuGH zur Vorratsdatenspeicherung. Danach ist die allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten nur zum **Schutz der nationalen Sicherheit** zulässig,[60] wohingegen die gezielte Vorratsdatenspeicherung von Verkehrs- und Standortdaten auch mit der Bekämpfung **schwerer Kriminalität** gerechtfertigt werden kann.[61]

---

58 EuGH, Urteil von 17. Dezember 2020, Rs. C-336/19, Centraal Israëlitisch Consistorie van België u.a., Rn. 64; Urteil vom 11. Juli 1989, Rs. C-265/87, Schräder/Hauptzollamt Gronau, Rn. 21; *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 34; *Kingreen*, in: Calliess/Ruffert, 6. Aufl. 2022, GRCh Art. 52 Rn. 65.

59 Laut EuGH ist die Bekämpfung des Kindesmissbrauchs als schwere Kriminalität einzustufen, vgl. EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 149.

60 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor.

61 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor.

Wie oben unter Ziff. 3.3.1. dargestellt, ist umstritten, ob die Rechtsprechung zur Vorratsdatenspeicherung ohne Weiteres auf den vorliegenden Fall übertragen werden kann.[62] Unterstellt man aber ihre Anwendbarkeit, kommt es folgerichtig darauf an, ob in den Aufdeckungsanordnungen eine **gezielte** oder eine **allgemeine und unterschiedslose Maßnahme** zu sehen ist. Nach der Rechtsprechung des EuGH setzt eine gezielte Maßnahme voraus, dass zumindest ein mittelbarer Zusammenhang zwischen den zu bekämpfenden Straftaten und dem betroffenen Personenkreis besteht. Daneben kann eine gezielte Maßnahme auch auf ein geografisches Gebiet beschränkt werden, in dem ein erhöhtes Risiko der Begehung von Straftaten besteht.[63]

Davon ausgehend lassen sich verschiedene Argumente für das Vorliegen einer **gezielten Maßnahme** anführen: Die Aufdeckungsanordnung richtet sich nicht an alle elektronischen Kommunikationsdienste, sondern (zunächst) nur an einen bestimmten Diensteanbieter. Zudem folgen die Aufdeckungspflichten nicht pauschal aus dem Gesetz, sondern erst aus einer konkreten Einzelfallentscheidung einer Behörde für eine begrenzte Dauer. Sie betreffen also gerade nicht die gesamte Bevölkerung, sondern sind von einem zuvor identifizierten Risiko und einer behördlichen Abwägungsentscheidung im Einzelfall abhängig. Was das geografische Kriterium betrifft, so argumentiert die Kommission, dass eine geografische Eingrenzung auf einen bestimmten Ort mit „digitalen Orten“ vergleichbar und daher noch gezielt sei.[64]

Dieser Argumentation lässt sich allerdings die enorme Reichweite zumindest einiger Messengerdienste entgegenhalten, die keineswegs vergleichbar ist mit eng umgrenzten Örtlichkeiten wie Flughäfen und Bahnhöfen. Vielmehr sind manche Messengerdienste sehr verbreitet. Beispielsweise nutzen über 80 Prozent aller Internetnutzerinnen und -nutzer – generationsübergreifend – WhatsApp als Messenger.[65] Bedenkt man, dass sich die Aufdeckungsanordnungen faktische auf sämtliche Nutzerinnen und Nutzer eines Dienstes beziehen, ohne dass es darauf ankäme, ob die jeweiligen Personen eine auch nur mittelbare Verbindung zu Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch hätten, hat die Aufdeckungsanordnung eine **weitreichende Wirkung**.[66] Hinzu kommt, dass es voraussichtlich nicht bei einer Aufdeckungsanordnung an einen Dienst bliebe: Im Fall einer Aufdeckungsanordnung an einen Dienst würden die betroffenen

---

62 Für eine ausführliche Darstellung siehe Deutscher Bundestag, Fachbereich Europa, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025: JD und EPRS gehen davon aus, dass die Verhältnismäßigkeit der Aufdeckungsanordnung unter Berücksichtigung der EuGH-Rechtsprechung zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu beurteilen sei. Demgegenüber hält die Kommission die Rechtsprechung zur Vorratsdatenspeicherung und automatischen Analyse von Verkehrs- und Standortdaten für nicht übertragbar.

63 EuGH, Urteil vom 22. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet u.a., Rn. 105 ff.

64 KOM, Non-Paper vom 16. Mai 2023, Rn. 26 ff.; ähnlich auch Deutscher Bundestag, Fachbereich Europa, Ausarbeitung, Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“, EU 6 - 3000 - 044/25 vom 27. August 2025, S. 24 ff.

65 Statista, Ranking der beliebtesten Social Networks und Messenger nach dem Anteil der Nutzer an den Internetnutzern in Deutschland im Jahr 2024; Anteil der Nutzer von WhatsApp nach Generationen in Deutschland im Jahr 2024, vgl. JD, Gutachten vom 26. April 2023, Rn. 44; vgl. *Woerlein*, Gesetzesvorschlag im Kampf gegen Kindesmissbrauch, ZD-Aktuell 2022, 01251.

66 Vgl. JD, Gutachten vom 26. April 2023, Rn. 39 ff.

Straftäter ihre Aktivitäten kurzfristig auf einen anderen Messenger verlagern, der in der Folge Gegenstand einer weiteren Aufdeckungsanordnung werden müsste. Das Ergebnis wäre eine nahezu flächendeckende Betroffenheit.

Nach dem Vorgesagten spricht einiges dafür, die Aufdeckungsanordnungen als **allgemeine und unterschiedslose Maßnahme** einzuordnen,[67] die nach der Rechtsprechung zur Vorratsdatenspeicherung nur mit dem Schutz der nationalen Sicherheit zu rechtfertigen wäre, worauf die betreffenden Regelungen der VO gerade nicht gestützt werden. Letztlich obläge es dem EuGH, zunächst die Rechtfertigungsanforderungen für Aufdeckungsanordnungen im Sinne des VO-Vorschlags zu entwickeln und diese sodann auf die CSA-Verordnung anzuwenden.

3.3.3.2. Eignung

Die Maßnahme muss geeignet sein, die mit der fraglichen Regelung verfolgten Ziele zu erreichen.[68] Nur dann kann sie dem Ziel „tatsächlich entsprechen“ i. S. v. Art. 52 Abs. 1 Satz 2 GRCh. Dabei ist es ausreichend, dass die Maßnahme einen **Beitrag zur Zielerreichung** leistet.[69] Zudem besteht hier ein gewisser Einschätzungsspielraum des Unionsgesetzgebers.[70] Demnach lässt sich argumentieren, dass das umfangreiche Scannen von privater Kommunikation auf einem Messengerdienst den Zweck der Aufdeckung und Verhinderung der Verbreitung von Missbrauchsdarstellungen zumindest fördert.

Gleichwohl bestehen berechtigte Zweifel, ob die Aufdeckungsanordnungen wirklich ein wirksames Instrument für einen besseren Schutz von Kindern und Jugendlichen vor sexualisierter Gewalt darstellen. So ist es bereits fraglich, zu welchem Grad die ins Visier genommenen Messengerdienste tatsächlich für die Verbreitung kinderpornographischer Inhalte verwendet werden. In der Regel wird das kinderpornographische Material von den Tätern verschlüsselt und die Schlüssel im Darknet verbreitet. Spätestens, wenn eine Aufdeckungsanordnung an einen der gängigen Messengerdienste ergeht, würden die Täter in kürzester Zeit auf einen anderen Messengerdienst, dezentrale Kommunikationsdienste oder das Darknet ausweichen. Insofern ist die Maßnahme **leicht zu umgehen**.[71]

Ein weiterer Aspekt, der die Eignung der Aufdeckungsanordnungen infrage stellt, sind die begrenzten **Ermittlungsressourcen** in den Mitgliedstaaten. Es steht zu befürchten, dass die zu verwendenden Algorithmen eine große Masse von – berechtigten und unberechtigten – Verdachts-

---

67 So auch EPRS, Folgenabschätzung, April 2023, S. 62; JD, Gutachten vom 26. April 2023, Rn. 72 ff.

68 EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 46; *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 37 f.

69 *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 37.

70 EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 47 f; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, GRCh Art. 52 Rn. 68.

71 *Woerlein*, Gesetzesvorschlag im Kampf gegen Kindesmissbrauch, ZD-Aktuell 2022, 01251; vgl. Wissenschaftliche Dienste des Deutschen Bundestags, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 – 3000 – 021/22 vom 21. Mai 2022, S. 21 f.

fällen auswerfen würden, die sodann über das EU-Zentrum an die mitgliedstaatlichen Strafverfolgungsbehörden weitergeleitet würden. In der Folge besteht die Gefahr, dass die ohnehin schon ausgelasteten Behörden mit zum Teil irrelevantem Material überschwemmt und dadurch gehemmt würden, gezielte Ermittlungen voranzutreiben.[72]

Insofern ergeben sich Zweifel an der Eignung der Aufdeckungsanordnungen. Vor dem Hintergrund des Einschätzungsspielraums des EU-Gesetzgebers bei gleichzeitig geringen Anforderungen an die Eignung (bloßer „Beitrag zur Zielerreichung“) kann die Maßnahme dennoch grundsätzlich als geeignet angesehen werden. Der geringe zu erwartende Nutzen wird aber spätestens auf Ebene der Angemessenheit erneut relevant.

3.3.3.3. Erforderlichkeit

Eingriffe sind dann „erforderlich“ i. S. v. Art. 52 Abs. 1 Satz 2 GRCh, wenn es kein zur Erreichung des Ziels gleich geeignetes Mittel gibt, das für die Betroffenen weniger einschneidend wirkt.[73] Darüber hinaus begrenzt der Grundsatz der Erforderlichkeit auch den Umfang des Mittels: So dürfen die eingesetzten Mittel nicht über das hinausgehen, was zur Erreichung des angestrebten Ziels zwingend notwendig ist, sowohl in inhaltlicher als auch in zeitlicher Hinsicht.[74] Speziell zu Art. 8 GRCh fordert der EuGH, dass kompensatorische Schutzregelungen getroffen werden, also technische und organisatorische Maßnahmen zum Schutz der gespeicherten Daten vor Missbrauch und unberechtigter Nutzung der Daten.[75]

Als **mildere Mittel** zum Schutz von Kindern vor sexualisierter Gewalt ist an umfangreiche Präventionsmaßnahmen und eine geeignete Ausstattung der Strafverfolgungsbehörden (technische Experten und Infrastruktur) zur gezielten Verfolgung von Verdachtsfällen zu denken, um sicherzustellen, dass Missbrauchsdarstellungen konsequent verfolgt und gelöscht werden. Diese Maßnahmen erscheinen für die Grundrechte aus Art. 7, 8 und 11 GRCh weniger eingriffsintensiv, wobei die gleiche oder höhere Eignung im Einschätzungsspielraum des Unionsgesetzgebers liegt (s. Ziff. 3.3.3.2.).[76]

Was die **Begrenzung des Umfangs der Maßnahme** angeht, so finden sich im Text des VO-Vorschlags zahlreiche Schutzregelungen, die den Anwendungsbereich der Aufdeckungsanordnungen auf das unbedingt Erforderliche begrenzen. Beispielsweise sieht Art. 7 Abs. 8 VO-Vorschlag

---

72 Wissenschaftliche Dienste des Deutschen Bundestags, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 – 3000 – 021/22 vom 21. Mai 2022, S. 21 f.

73 EuGH, Urteil vom 17 Oktober 2013, Rs. C-101/12, Schaible, Rn. 29; Urteil vom 11. Juli 1989, Rs. C-265/87, Schräder/Hauptzollamt Gronau, Rn. 21; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, GRCh Art. 52 Rn. 69.

74 EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 66-68; EuGH, Urteil vom 9. November 2010, Rs. C-92/09, Schecke, Rn. 74; EuGH, Urteil vom 17. Oktober 2013, Rs. C-291/12, Schwarz, Rn. 40; *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 40.

75 Stern/Sachs/Krämer, 1. Aufl. 2016, GRCh Art. 52 Rn. 51; EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 40.

76 *Bering/Windwehr,* Digitale Silver Bullets, Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz, Verfassungsblog vom 30. August 2024.

vor, dass die Aufdeckungsanordnung so zielgerichtet und spezifisch zu formulieren ist, dass die negativen Folgen auf das **unbedingt erforderliche Maß** beschränkt bleiben. Die nationalen Erlassbehörden müssen unter anderem dafür Sorge tragen, dass Aufdeckungsmaßnahmen – sofern das identifizierte Risiko auf einen identifizierbaren Teil oder Aspekt des Dienstes beschränkt ist – nur in Bezug auf diesen konkret risikobehafteten Teil oder Aspekt des jeweiligen Dienstes Anwendung finden. Die **Geltungsdauer** muss befristet und auf das unbedingt erforderliche Maß beschränkt sein. Sogar die Definition der Erforderlichkeit – dass von mehreren gleichermaßen wirksamen Maßnahmen die am wenigsten eingreifenden Maßnahmen getroffen werden müssen – ist in Abs. 8 eigens erwähnt.

Ähnliche Formulierungen finden sich auch in Art. 10, der eigens mit „Schutzvorkehrungen" überschrieben ist. Die Technologien dürfen nach Art. 10 Abs. 3 VO-Vorschlag nur Informationen extrahieren, die „**unbedingt notwendig**" sind, um mithilfe der Indikatoren Muster zu erkennen, die auf die Verbreitung relevanten Materials hindeuten. Sie müssen hinreichend zuverlässig sein, sodass die Fehlerquote bei der Erkennung so weit wie möglich minimiert wird. Nach Art. 10 Abs. 4 VO-Vorschlag haben Anbieter u. a. sicherzustellen, dass die ergriffenen Maßnahmen auf das „**unbedingt Erforderliche**" beschränkt sind. Sie müssen wirksame interne Verfahren festlegen, um den Missbrauch der eingesetzten Technologie zu verhindern und für eine regelmäßige menschliche Aufsicht sowie erforderlichenfalls menschliches Eingreifen sorgen.

Aus dem Vorstehenden ergibt sich, dass die Kommission großen Wert auf die explizite Aufnahme von Schutzvorkehrungen in den VO-Vorschlag gelegt hat, um den Umfang der Aufdeckungsanordnungen zu begrenzen und die Erforderlichkeit zu wahren. Dass die dazu gewählten Formulierungen – „unbedingt erforderlich", „unbedingt notwendig" und „am wenigsten eingreifende Maßnahmen" – vage und formelhaft wirken, ist keine Frage der Erforderlichkeit, sondern des Gesetzesvorbehalts (siehe dazu bereits unter Ziff. 3.3.2.).

3.3.3.4. Angemessenheit

Schließlich müssten die Aufdeckungsanordnungen in einem **angemessenen Verhältnis** zu dem verfolgten Zweck stehen, also einen angemessenen Ausgleich zwischen den widerstreitenden Interessen herstellen.[77] Hier kollidieren die Kommunikationsgrundrechte aus Art. 7, 8 und 11 GRCh mit dem Schutz der Kinder, der in Art. 24 GRCh seinen expliziten Niederschlag findet und zudem auch Art. 3 und Art. 4 GRCh berührt.[78] Zur Beurteilung des konkreten durch den VO-Vorschlag getroffenen Interessenausgleichs müssen insbesondere die Eingriffsschwere (Ziff. 3.3.3.4.1.) und der zu erwartende Nutzen (Ziff. 3.3.3.4.2.) gegenübergestellt werden.

---

77 EuGH, Urteil vom 9. November 2010, Rs. C-92/09, Schecke, Rn. 72; *Jarass*, in: Jarass; Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 41.

78 Vgl. *Vasel*, Datenschutz versus Kinderschutz?, ZRP 2022, 191 (192).

3.3.3.4.1. Besondere Eingriffsschwere

Die im VO-Vorschlag vorgesehenen Aufdeckungsanordnungen stellen nach verbreiteter Auffassung einen **besonders schweren Eingriff** dar. Selbst die Kommission hält Eingriffe in die Kommunikationsinhalte für „sensibel“ („sensitive“), sodass sie einer starken Rechtfertigung bedürfen.[79] Nachfolgend werden einige ausgewählte, die Eingriffsintensität begründende bzw. erhöhende Aspekte dargestellt.

An erster Stelle ist hervorzuheben, dass Aufdeckungsanordnungen – ungeachtet der formalen Einordnung als allgemeine und unterschiedslose bzw. gezielte Maßnahme (s. dazu Ziff. 3.3.3.1.) – einen **großen Personenkreis** treffen, werden doch Messengerdienste von weiten Teilen Bevölkerung genutzt. Die Mehrzahl der von einer Aufdeckungsanordnung betroffenen Personen hat **keine eigene Verbindung zu den zu verfolgenden Straftaten**, einzige Verbindung ist die Nutzung eines als riskant eingestuften Messengerdienstes und eine schwer vorhersehbare Abwägungsentscheidung einer Behörde.[80] Auf Rechtsfolgenseite steht die Verarbeitung nicht nur von Verkehrs- und Standortdaten, sondern auch von **Kommunikationsinhalten**, die nach der Rechtsprechung des EuGH als besonders sensibel einzustufen sind.[81]

Hinzu kommt, dass die nach dem VO-Vorschlag zu verwendende Technik als **fehleranfällig** gilt, was zugleich die Eingriffsintensität erhöht und den zu erwartenden Nutzen schmälert (dazu sogleich). Diesbezüglich ist zwischen der Aufdeckung von bekanntem (Art. 7 Abs. 5 VO-Vorschlag) und unbekanntem (Art. 7 Abs. 6 VO-Vorschlag) Material zu differenzieren.[82] Während das sog. „Hashing“[83] bekannter Bilder vergleichsweise geringe Fehlerraten aufweist, gelten die zur Detektion von neuen Inhalten verwendeten Technologien, die die Einbindung Künstlicher Intelligenz erfordern, als technisch nicht verlässlich.[84]

Eingriffserschwerend kommt hinzu, dass die von den Anbietern eingerichteten Cybersicherheitsmaßnahmen, insbesondere die **Ende-zu-Ende-Verschlüsselung**, umgangen werden müsste. Dazu sieht der Kompromisstext der Ratspräsidentschaft vor, dass die Inhalte im Wege des CSS unmit-

---

79 KOM, Non-Paper vom 16. Mai 2023, Rn. 45.

80 JD, Gutachten vom 26. April 2023, Rn. 44.

81 Vgl. EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 117, 184 ; EuGH, Urteil vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige, Rn. 99, so auch JD, Gutachten vom 26. April 2023, Rn. 49.

82 Dafür plädiert etwa *Vasel*, Datenschutz versus Kinderschutz?, ZRP 2022, 191 (193), ebenso EPRS, Folgenabschätzung, April 2023, S. 58 ff.

83 „**Hashing**“ bezeichnet eine Technik, die verwendet wird, um bestimmte Inhalte wie Bilder oder Videos zu identifizieren, ohne diese tatsächlich zu speichern oder zu durchsuchen. Die Hash-Werte („Fingerabdrücke“) eines Bildes werden mit einer Datenbank verglichen, die Hashes von bereits bekannten kinderpornographischen Inhalten enthalten. Wenn der Hash eines neuen Inhalts mit einem bekannten Hash in der Datenbank übereinstimmt, wird dieser Inhalt als potenziell problematisch markiert und kann zur weiteren menschlichen Überprüfung weitergeleitet werden.

84 *Vasel*, Datenschutz versus Kinderschutz?, ZRP 2022, 191 (193).

telbar auf den Geräten der Nutzerinnen und Nutzer überprüft werden, bevor eine Verschlüsselung erfolgt. Eine Verweigerung des CSS bei vollständiger Weiternutzung des Dienstes ist indes faktisch nicht möglich (siehe dazu Ziff. 3.2.). In der Folge muss die Verschlüsselung selbst zwar nicht „durchbrochen" werden, doch ist deren Bedeutung infrage zu stellen, wenn das Gerät ohnehin direkt überwacht wird.[85]

Schließlich stehen die zu schützenden **Kinder** paradoxerweise auch auf der anderen Seite der Abwägung, denn auch und gerade Kinder müssen vor Eingriffen in ihre Privatsphäre geschützt werden. Minderjährige sind im digitalen Raum besonders vulnerabel und könnten, etwa durch Familienchats oder einvernehmliche intime Chats („Sexting") unter Jugendlichen, vermehrt Gegenstand von Fehlanzeigen der Algorithmen werden. Mit diesen Argumenten hat sich sogar der Kinderschutzbund gegen die Pläne zur Chatkontrolle gestellt.[86]

3.3.3.4.2. Geringer Nutzen

Dieser besonderen Eingriffsschwere steht ein potenziell **geringer Nutzen** gegenüber. Zwar ist das übergeordnete Ziel der Verordnung, die Verbreitung von Missbrauchsdarstellungen über das Internet zu verhindern, von besonderem Gewicht. Es ist jedoch nicht davon auszugehen, dass das hier gewählte Instrument der Aufdeckungsanordnungen ein effektives Mittel zur Verfolgung des hehren Ziels darstellt. Diesbezüglich kann auf die Ausführungen zur Eignung unter Ziff. 3.3.3.2. verwiesen werden: Die ins Visier genommenen Messengerdienste sind nicht die primäre Plattform für den Austausch von Kinderpornographie. Spätestens nach Ergehen einer Aufdeckungsanordnung würden die Täter auf andere Plattformen ausweichen und die Maßnahme damit umgehen. Schließlich könnten die nationalen Strafverfolgungsbehörden durch eine Flut teils unbegründeter Verdachtsmeldungen überlastet werden, wodurch der eigentliche Schutz von Kindern vor sexualisierter Gewalt schlimmstenfalls eher behindert als verbessert würde.

Vor diesem Hintergrund erscheint es fraglich, ob der potenziell geringe Nutzen die enorme Eingriffsschwere der vorgesehenen Aufdeckungsanordnungen zu rechtfertigen vermag.

3.4. Fazit

Im Ergebnis sprechen **schwerwiegende Gründe gegen die Vereinbarkeit** der im VO-Vorschlag vorgesehenen und im Kompromisstext der Ratspräsidentschaft modifizierten Aufdeckungsanordnungen mit den in Art. 7, 8 und 11 GRCh garantierten Grundrechten.

Eine der Eingriffsqualität entgegenstehende Einwilligung dürfte in der durch den Kompromissvorschlag eingeführten Zustimmung in den AGB der Dienste nicht zu sehen sein. Ob der VO-Vorschlag den Wesensgehalt von Art. 7, 8 und 11 GRCh wahrt, ist angesichts der Rechtsprechung zur

---

85 Vgl. Chaos Computer Club, Aus Sicherheitsgründen: Bundesregierung muss der Chatkontrolle eine Absage erteilen, Online-Beitrag vom 3. Oktober 2025; *Bering* und *Windwehr* bezeichnen das CSS als „Taschenspielertrick", siehe Digitale Silver Bullets, Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz, Verfassungsblog vom 30. August 2024.

86 *Reuter*, EU-Überwachungsgesetz: Kinderschutzbund stellt sich gegen Chatkontrolle, Online-Beitrag auf Netzpolitik.org vom 6. Oktober 2025.

Vorratsdatenspeicherung zumindest zweifelhaft. Auch den Anforderungen an eine klare und präzise gesetzliche Grundlage dürfte der VO-Vorschlag wohl nicht genügen. Spätestens auf Ebene der Verhältnismäßigkeit würde eine Rechtfertigung des gravierenden Eingriffs durch einen nur zweifelhaften Nutzen für die Bekämpfung von Kinderpornographie voraussichtlich scheitern. In ihrer jetzigen Ausgestaltung erscheinen die Regelungen zu Aufdeckungsanordnungen aus hiesiger Sicht unverhältnismäßig.

Die **abschließende Beurteilung** der Grundrechtskonformität der Aufdeckungsanordnungen obliegt dem **EuGH**. Über den Kompromissvorschlag vom 3. Oktober 2025 wird der Gerichtshof voraussichtlich nicht entscheiden können, da dieser bereits von der dänischen Ratspräsidentschaft aufgegeben wurde. Vor diesem Hintergrund bleibt abzuwarten, ob im weiteren Verlauf des Gesetzgebungsverfahrens eine Ausgestaltung der CSA-Verordnung gewählt wird, die mit den Unionsgrundrechten vereinbar ist.

4. Vereinbarkeit des VO-Vorschlags mit dem Grundgesetz

Gemäß dem Prüfungsauftrag soll weiter untersucht werden, ob und inwieweit die mit dem VO-Vorschlag vorgesehenen Maßnahmen zur Prävention und Bekämpfung des sexuellen Kindesmissbrauchs im Internet mit dem grundrechtlichen Schutz der Kommunikation über Messengerdienste auf Basis des GG vereinbar wären.

4.1. Anwendungsvorrang des Unionsrechts

Im Rahmen einer Grundrechtsprüfung im Zusammenhang mit europäischen Rechtsakten gilt jedoch, dass europäisches Recht grundsätzlich in der Anwendung dem nationalen Recht und damit auch dem nationalen Verfassungsrecht vorgeht. So hat das Bundesverfassungsgericht (BVerfG) bereits im Jahr 1986 in einer Grundsatzentscheidung erkannt:

> „Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte oder Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen […].“[87]

Zum Zeitpunkt dieser Entscheidung war die GRCh noch nicht in Kraft. Das BVerfG war jedoch der Auffassung, dass mittlerweile im Hoheitsbereich der Europäischen Gemeinschaften ein Maß an **Grundrechtsschutz** erwachsen war, das **nach Konzeption, Inhalt und Wirkungsweise** dem

87 BVerfG, Beschluss vom 22.10.1986 – 2 BvR 197/83 (Solange II).

Grundrechtsstandard des Grundgesetzes **im Wesentlichen gleichwertig** ist.[88] Dieser Grundrechtsstandard sei insbesondere durch die Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften inhaltlich ausgestaltet worden, gefestigt und zureichend gewährleistet.[89]

Eine weitere Grundsatzentscheidung zum Anwendungsvorrang des Unionsrechts folgte im Jahr 2019, als das BVerfG feststellte:

> „Bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen sind nach dem Grundsatz des Anwendungsvorrangs des Unionsrechts in aller Regel nicht die Grundrechte des Grundgesetzes, sondern allein die Unionsgrundrechte maßgeblich. Der Anwendungsvorrang steht unter anderem unter dem Vorbehalt, dass der Schutz des jeweiligen Grundrechts durch die stattdessen zur Anwendung kommenden Grundrechte der Union hinreichend wirksam ist.“[90]

Der Europäischen Union sind nach Art. 23 Abs. 1 Satz 2 GG Hoheitsbefugnisse übertragen worden. Das BVerfG hat hierzu ausgeführt, dass wenn im Rahmen dieser Befugnisse **unionsweite Regelungen** geschaffen und in der gesamten Union einheitlich angewendet werden sollen, auch der bei der Anwendung dieser Regelungen zu gewährleistende **Grundrechtsschutz einheitlich** sein müsse. Dies werde durch die GRCh gewährleistet. Die deutschen Grundrechte seien in diesen Fällen nicht anwendbar, weil ihre Anwendung das Ziel der Rechtsvereinheitlichung konterkarieren würde.[91]

Das BVerfG hat mit dieser Entscheidung auch klargestellt, dass es die Anwendung des Unionsrechts durch deutsche Stellen am Maßstab der Unionsgrundrechte selbst kontrolliert, soweit die Grundrechte des GG durch den Anwendungsvorrang des Unionsrechts verdrängt werden.[92] Die Grundrechte des GG werden aber dann nicht verdrängt, wenn das Unionsrecht keinen gleichwertigen, wirksamen Schutz bietet, ihnen kommt daher noch eine **Reservefunktion** zu.[93]

Entscheidend für die Prüfung der Vereinbarkeit von Maßnahmen des VO-Vorschlags mit den Grundrechten des GG ist daher, ob es sich bei dem VO-Vorschlag um eine **unionsrechtlich vollständig vereinheitlichte Regelung** handelt und ob auf Unionsebene ein vergleichbares **Schutzniveau** wie durch die einschlägigen Grundrechte des GG gewährleistet ist.[94] Ist dies der Fall, so kommt eine Grundrechtsprüfung am Maßstab des GG nicht mehr in Betracht.

---

88 BVerfG, Beschluss vom 22.10.1986 – 2 BvR 197/83 (Solange II), Rn. 112.

89 BVerfG, Beschluss vom 22.10.1986 – 2 BvR 197/83 (Solange II), Rn. 113.

90 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II).

91 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 44.

92 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 50.

93 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 42, 48.

94 BVerfG, Beschluss vom 29.09.2025 – 2 BvR 934/19 (Egenberger), Rn. 150 ff.

4.1.1. Unionsrechtlich vollständig vereinheitlichte Regelungen

Gemäß Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gelten EU-Rechtsverordnungen allgemein, sind in allen Teilen verbindlich und binden die Mitgliedstaaten unmittelbar. Dies stellt Art. 89 des VO-Vorschlags auch ausdrücklich selbst klar. Ziel des VO-Vorschlags ist die **Schaffung eines harmonisierten Rechtsrahmens** für die Prävention und Bekämpfung des sexuellen Kindesmissbrauchs im Internet. So wird in den Erwägungsgründen 3 und 4 des VO-Vorschlags problematisiert, dass die Mitgliedstaaten zunehmend divergierende nationale Rechtsvorschriften zur Prävention und Bekämpfung des sexuellen Kindesmissbrauchs im Internet einführen würden. Angesichts des grenzüberschreitenden Charakters des Internets und der betreffenden Dienstleistungserbringung hätte dies unmittelbar negative Auswirkungen auf den Binnenmarkt. Daher sollten harmonisierte Anforderungen auf Unionsebene festgelegt werden, um die Rechtssicherheit zu erhöhen, Hindernisse für die Dienstleistungserbringung zu beseitigen und gleiche Wettbewerbsbedingungen auf dem Binnenmarkt zu schaffen. Mit dem VO-Vorschlag sollen daher **klare, einheitliche und ausgewogene Vorschriften** festgelegt werden, um den sexuellen Missbrauch von Kindern wirksam zu verhindern und zu bekämpfen.

Spielräume der Mitgliedstaaten für die inhaltliche Umsetzung der Regelungen aus dem VO-Vorschlag dürften nach dessen Sinn und Zweck entsprechend auch nicht gewollt sein. In der einleitenden Begründung zur Wahl des Regelungsinstruments wird argumentiert, dass eine Richtlinie, die einen Spielraum für eine unterschiedliche nationale Umsetzung von EU-Vorschriften lässt, nicht geeignet sei, die einschlägigen Ziele zu erreichen. Mit einer Verordnung werde demgegenüber sichergestellt, dass unionsweit die gleichen Verpflichtungen auf einheitliche Weise eingeführt und eine unterschiedliche Umsetzung in den Mitgliedstaaten verhindert würden.

Folglich wird im VO-Vorschlag an vielen Stellen bereits detailliert festgelegt, wem welche Rechte eingeräumt und Pflichten auferlegt werden, welche Maßnahmen zu unternehmen und welche staatlichen Stellen zu beteiligen sind. Insbesondere werden die Anbieter interpersoneller Kommunikationsdienste unmittelbar verpflichtet, **Risikobewertungen** (Art. 3) und **Risikominderungen** (Art. 4) für deren angebotene Dienste durchzuführen, auf entsprechende behördliche Anordnung bestimmte **Inhalte aufzudecken** (Art. 7, 10), **Inhalte zu melden** (Art. 12) **und für eine bestimmte Zeit aufzubewahren** (Art. 22). Des Weiteren werden die Mitgliedstaaten nach Art. 25 verpflichtet, eine oder mehrere zuständige **Behörden für die Anwendung und Durchsetzung dieser Verordnung** zu benennen sowie eine davon als Koordinierungsbehörde für Fragen des sexuellen Missbrauchs von Kindern vorzusehen. Dazu werden in Art. 26 konkrete Anforderungen, Aufgaben und Befugnisse dieser Behörden definiert. Auch wie einzelne staatliche Maßnahmen umzusetzen sind, wird konkret vorgegeben. So bestimmt beispielsweise Art. 8 Abs. 1, dass die zuständige Behörde die in Art. 7 genannten Aufdeckungsanordnungen unter Verwendung des Musters in Anhang I erlässt. Abs. 1 enthält zudem in den Buchstaben a - j einen Katalog von Angaben, die eine Aufdeckungsanordnung enthalten muss. Auch werden den nationalen Behörden konkrete **Prüfkataloge** und gesetzliche **Vermutungsregeln** vorgegeben (z.B. Art. 7 Abs. 5: „[…] gilt das in Abs. 4 UAbs. 1 Buchst. a genannte erhebliche Risiko als gegeben, wenn die folgenden Bedingungen erfüllt sind: […]“). Die Tatbestandsvoraussetzungen dürften daher nach Sinn und Zweck des Verordnungsentwurfs als abschließend zu verstehen sein. Auf Rechtsfolgenseite werden zudem **bestimmte Höchstgrenzen** festgelegt, zum Beispiel dass gemäß Art. 7 Abs. 9 bei Aufdeckungsanordnungen betreffend die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs die Geltungsdauer 24 Monate nicht überschreiten darf. Für konkrete

Meldepflichten gemäß Art. 12, 13 wird auch die Verwendung der **Muster** im Anhang des VO-Vorschlags vorgegeben, die ebenfalls konkrete Inhaltsangaben vorschreiben.

Soweit die Mitgliedstaaten gemäß Art. 35 zum Erlass von **Vorschriften über Sanktionen** verpflichtet sind, steht ihnen auch insoweit kein nennenswerter Umsetzungsspielraum zu. Denn hier werden im VO-Vorschlag bereits Höchstbeträge für Zwangsgelder festgelegt und im Übrigen Leitlinien für die Verhängung von Sanktionen vorgegeben. Ohnehin handelt es sich nur um einen untergeordneten Teilbereich des VO-Vorschlags.

4.1.2. Zwischenergebnis

Es lässt sich somit feststellen, dass der VO-Vorschlag eine unionsrechtlich vollständig vereinheitlichte Regelung darstellen dürfte. Eingriffe wären damit grundsätzlich nur am Maßstab der Unionsgrundrechte zu prüfen, solange der Grundrechtsschutz auf Unionsebene mit dem des GG gleichwertig ist.

4.2. Gleichwertiges Schutzniveau durch Unionsgrundrechte

Ob der Grundrechtsschutz auf Unionsebene mit dem des GG gleichwertig ist, kann nur im Rahmen einer auf das jeweilige Grundrecht des GG bezogenen **generellen Betrachtung** festgestellt werden.[95] Indem das GG den einzelnen Menschen und seine Grundrechte in den Mittelpunkt seiner Ordnung stellt, deren **Wesensgehalt und Menschenwürdekern** für unantastbar erklärt und diesen Schutz auch im Hinblick auf die Unionsverträge sichert, können die Garantien der Grundrechte nur insoweit durch das Unionsrecht überlagert werden, als deren Schutzversprechen in der Substanz erhalten bleiben.[96] Erforderlich ist deshalb, dass der **Schutz der GRCh** dem vom Grundgesetz jeweils als unabdingbar gebotenen Grundrechtsschutz **im Wesentlichen gleichwertig** ist, zumal den Wesensgehalt der Grundrechte generell verbürgt.[97]

Das BVerfG geht in ständiger Rechtsprechung davon aus, dass diese Voraussetzungen grundsätzlich erfüllt sind und den Grundrechten des GG insoweit nur eine Reservefunktion zukommt.[98]

Unter dem Maßstab der generellen Betrachtung sind bei der Überprüfung des gegenständlichen VO-Vorschlags das **Fernmeldegeheimnis** aus Art. 10 Abs. 1 GG und das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. GG abgeleitete **allgemeine Persönlichkeitsrecht** in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung sowie als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die relevanten Grundrechte.

---

95 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 47.

96 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 47.

97 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 47.

98 BVerfG, Beschluss vom 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 48.

4.2.1. Fernmeldegeheimnis, Art. 10 Abs. 1 GG

Das Fernmeldegeheimnis schützt die **unkörperliche Übermittlung von Informationen** an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs und damit die **auf Vertraulichkeit angelegte Kommunikation**.[99] Auf Unionsebene wird das Fernmeldegeheimnis mit dem Recht auf Wahrung der Kommunikation gemäß **Art. 7 GRCh** gewährleistet. Für die Einzelheiten sei auf die obigen Ausführungen unter Ziffer 3.1.1. verwiesen. Das Recht auf Wahrung der Kommunikation gemäß Art. 7 GRCh entspricht damit im Wesentlichen dem Schutzniveau des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG.

4.2.2. Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung umfasst das Recht, selbst zu bestimmen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[100] Es schützt den Einzelnen vor **Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten**.[101] Auf Unionsebene findet das Recht auf informationelle Selbstbestimmung aus der gemeinsamen Anwendung der Grundrechte auf Achtung des Privat- und Familienlebens aus **Art. 7 GRCh** und auf Schutz personenbezogener Daten aus **Art. 8 GRCh** einen vergleichbaren Grundrechtsschutz.[102] Auch insofern sei für die Einzelheiten auf die obigen Ausführungen unter Ziffer 3.1.2. verwiesen.

4.2.3. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt den Einzelnen davor, dass der Staat sich durch **technische Instrumente** personenbezogene Daten beschafft, die es ihm ermöglichen, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen.[103] Der Schutzbereich erfasst den Zugriff auf einen umfassenden Datenbestand, der auf einem informationstechnischen System gespeichert ist, und wird somit grundsätzlich **quantitativ** vom Recht auf informationelle Selbstbestimmung abgegrenzt.[104] Andererseits endet aber auch der Schutzbereich des Rechts auf informationelle Selbstbestimmung nicht bei einzelnen Datenerhebungen, sodass es für den Wesensgehalt keinen Unterschied machen dürfte, in welchem Umfang Daten erhoben werden.[105] Auf Unionsebene dürfte das Recht

---

99 *Jarass,* in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, 18. Aufl. 2024, Art. 10 GG, Rn. 5, 6.

100 *Martini*, Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, JA 2009, 839 (841).

101 *Gersdorf,* in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 49. Ed. 01.11.2024, Art. 2 GG, Rn. 18.

102 *Eichberger,* in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 2 GG, Rn. 278.

103 *Martini*, Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, JA 2009, 839 (840).

104 *Gersdorf,* in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 49. Ed. 01.11.2024, Art. 2 GG, Rn. 24.

105 *Barczak,* in: Dreier, Grundgesetz-Kommentar, 4. Aufl. 2023, Art. 2 Abs. 1 GG, Rn. 97.

auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme daher ähnlich wie das Recht auf informationelle Selbstbestimmung bereits hinreichend durch **Art. 7 und Art. 8 GRCh** gewährleistet sein.[106] Auch insoweit ist ein im Wesentlichen gleichwertiger Grundrechtsschutz anzunehmen.

4.3. Fazit

Der generellen Betrachtung folgend ist festzustellen, dass der Schutz durch die GRCh ein im Wesentlichen gleiches Schutzniveau wie die einschlägigen Grundrechte des GG bietet. Eine weitergehende verfassungsrechtliche Würdigung des VO-Vorschlags ist daher nach den durch die ständige Rechtsprechung des BVerfG aufgestellten Prüfungsmaßstäben nicht vorzunehmen.

* * *

106 *Gersdorf,* in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 49. Ed. 01.11.2024, Art. 2 GG, Rn. 22.