EDSA-EDSB

Gemeinsame Stellungnahme 4/2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern

Angenommen am 28. Juli 2022

INHALTSVERZEICHNIS

Zusammenfassung

Am 11. Mai 2022 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.

Mit diesem Vorschlag würden den Anbietern von Hostingdiensten, interpersonellen Kommunikationsdiensten und anderen Diensten qualifizierte Verpflichtungen in Bezug auf die Erkennung, Meldung und Sperrung von bekannten und neuen Darstellungen sexuellen Kindesmissbrauchs sowie die Kontaktaufnahme zu Kindern auferlegt. In dem Vorschlag ist auch die Einrichtung einer neuen, dezentralen EU-Agentur („EU-Zentrum“) und eines Netzwerks nationaler Koordinierungsbehörden für Fragen des sexuellen Missbrauchs von Kindern vorgesehen, um die Durchsetzung der vorgeschlagenen Verordnung zu ermöglichen. Wie in der Begründung des Vorschlags anerkannt wird, würden die in dem Vorschlag enthaltenen Maßnahmen die Ausübung der Grundrechte der Nutzer der betreffenden Dienste berühren.

Der sexuelle Missbrauch von Kindern ist eine besonders schwere und verabscheuungswürdige Straftat. Deshalb ist das Ziel, eine wirksame Bekämpfung dieses Phänomens zu ermöglichen, ein von der Union anerkanntes, dem Gemeinwohl dienendes Ziel zum Schutz der Rechte und Freiheiten der Opfer. Gleichzeitig verweisen der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) darauf, dass jede Einschränkung der Grundrechte, wie sie in dem Vorschlag vorgesehen ist, den Anforderungen von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union entsprechen muss.

Der EDSA und der EDSB betonen, dass der Vorschlag Anlass zu ernsthaften Bedenken hinsichtlich der Verhältnismäßigkeit der geplanten Eingriffe und Einschränkungen des Schutzes der Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten gibt. In diesem Zusammenhang weisen der EDSA und der EDSB darauf hin, dass Verfahrensgarantien materielle Schutzvorkehrungen nie vollständig ersetzen können. Ein komplexes Eskalationssystem von der Risikobewertung und den Maßnahmen zur Risikominderung bis hin zur Aufdeckungsanordnung kann die erforderliche Klarheit der materiellen Verpflichtungen nicht ersetzen.

Der EDSA und der EDSB sind der Ansicht, dass es dem Vorschlag an Klarheit in Bezug auf Schlüsselelemente fehlt, z. B. in Bezug auf Begriffe wie „erhebliches Risiko“. Darüber hinaus verfügen die für die Anwendung dieser Schutzvorkehrungen zuständigen Stellen, angefangen bei den privaten Akteuren bis hin zu den Verwaltungs- und/oder Justizbehörden, über einen sehr großen Ermessensspielraum, wodurch Rechtsunsicherheit bei der Abwägung der Rechte entsteht, die in jedem einzelnen Fall auf dem Spiel stehen. Der EDSA und der EDSB heben hervor, dass der Gesetzgeber, wenn er besonders schwerwiegende Eingriffe in die Grundrechte zulässt, Rechtsklarheit darüber schaffen muss, wann und wo Eingriffe zulässig sind. Der EDSA und der EDSB erkennen zwar an, dass die Rechtsvorschriften nicht zu präskriptiv sein dürfen und eine gewisse Flexibilität bei ihrer praktischen Anwendung ermöglichen müssen, sind jedoch der Auffassung, dass der Vorschlag aufgrund des Mangels an klaren materiellen Normen zu viel Raum für potenziellen Missbrauch lässt.

Hinsichtlich der Notwendigkeit und Verhältnismäßigkeit der geplanten Aufdeckungsmaßnahmen äußern der EDSA und der EDSB insbesondere Bedenken, wenn es um die Maßnahmen geht, die für die Aufdeckung von unbekanntem Material über sexuellen Kindesmissbrauch oder der Kontaktaufnahme zu Kindern („Grooming“) in interpersonellen Kommunikationsdiensten vorgesehen sind. Aufgrund ihrer Auswirkungen

auf die Grundrechte, ihres zufälligen Charakters und der Fehlerquoten, die mit solchen Technologien einhergehen, sind der EDSA und der EDSB der Ansicht, dass der durch diese Maßnahmen verursachte Eingriff über das notwendige und verhältnismäßige Maß hinausgeht. Darüber hinaus sind Maßnahmen, die den Behörden einen allgemeinen Zugriff auf den Inhalt einer Nachricht ermöglichen, um die Kontaktaufnahme zu Kindern aufzudecken, eher als Eingriff in den Wesensgehalt der in Artikel 7 und 8 der Charta garantierten Rechte zu betrachten. Daher sollten die entsprechenden Bestimmungen über die Kontaktaufnahme zu Kindern aus dem Vorschlag gestrichen werden. Zudem ist das Durchsuchen von Audiokommunikation nicht vom Anwendungsbereich des Vorschlags ausgenommen. Der EDSA und der EDSB sind der Auffassung, dass das Durchsuchen von Audiokommunikation ein besonders schwerwiegender Eingriff ist und daher nicht in den Anwendungsbereich der in der vorgeschlagenen Verordnung festgelegten Aufdeckungspflichten fallen darf, sowohl in Bezug auf Sprachnachrichten als auch auf Live-Kommunikation.

Der EDSA und der EDSB bekunden auch Zweifel an der Wirksamkeit von Sperrmaßnahmen und sind der Ansicht, dass es unverhältnismäßig wäre, von Anbietern von Internetzugangsdiensten zu verlangen, Online-Kommunikation zu entschlüsseln, um die Kommunikation in Bezug auf Material über sexuellen Kindesmissbrauch zu sperren.

Ferner weisen der EDSA und der EDSB darauf hin, dass Verschlüsselungstechnologien wesentlich zur Achtung des Privatlebens und der Vertraulichkeit der Kommunikation, zur Freiheit der Meinungsäußerung sowie zur Innovation und zum Wachstum der digitalen Wirtschaft beitragen, die auf dem hohen Maß an Vertrauen und Sicherheit beruhen, das diese Technologien bieten. In Erwägungsgrund 26 des Vorschlags wird nicht nur die Wahl der Erkennungstechnologien, sondern auch der technischen Maßnahmen zum Schutz der Vertraulichkeit der Kommunikation, z. B. Verschlüsselung, unter den Vorbehalt gestellt, dass diese gewählte Technologie den Anforderungen der vorgeschlagenen Verordnung entsprechen muss, d. h., sie muss die Erkennung ermöglichen. Dies stützt den aus Artikel 8 Absatz 3 und Artikel 10 Absatz 2 des Vorschlags abgeleiteten Gedanken, dass ein Anbieter die Ausführung einer Aufdeckungsanordnung nicht mit der Begründung der technischen Unmöglichkeit verweigern kann. Der EDSA und der EDSB sind der Auffassung, dass es ein besseres Gleichgewicht zwischen dem gesellschaftlichen Interesse an sicheren und privaten Kommunikationskanälen und der Bekämpfung ihres Missbrauchs geben sollte. In dem Vorschlag sollte klar formuliert werden, dass nichts in der vorgeschlagenen Verordnung als Verbot oder Schwächung der Verschlüsselung ausgelegt werden sollte.

Der EDSA und der EDSB begrüßen zwar die Aussage in dem Vorschlag, dass die Befugnisse und Zuständigkeiten der Datenschutzbehörden gemäß der Datenschutz-Grundverordnung (DSGVO) nicht berührt werden, sind jedoch der Auffassung, dass das Verhältnis zwischen den Aufgaben der Koordinierungsbehörden und denen der Datenschutzbehörden besser geregelt werden sollte. In dieser Hinsicht begrüßen der EDSA und der EDSB die Rolle, die dem EDSA in dem Vorschlag zugewiesen wird, indem seine Beteiligung an der praktischen Umsetzung des Vorschlags gefordert wird, darunter insbesondere die Anforderung an den EDSA, eine Stellungnahme zu den Technologien abzugeben, die das EU-Zentrum für die Ausführung von Aufdeckungsanordnungen bereitstellen würde. Es sollte jedoch geklärt werden, welchem Zweck die Stellungnahme in dem Verfahren dient und wie das EU-Zentrum nach Erhalt einer Stellungnahme des EDSA handeln würde.

Schließlich stellen der EDSA und der EDSB fest, dass in dem Vorschlag eine enge Zusammenarbeit zwischen dem EU-Zentrum und Europol vorgesehen ist, die sich „einander den größtmöglichen Zugang zu einschlägigen Informationen und Informationssystemen“ gewähren. Der EDSA und der EDSB unterstützen zwar grundsätzlich die Zusammenarbeit der beiden Agenturen, sprechen aber angesichts der Tatsache, dass das EU-Zentrum keine Strafverfolgungsbehörde ist, dennoch mehrere Empfehlungen zur Verbesserung der

entsprechenden Bestimmungen aus. Dazu gehört, dass die Übermittlung personenbezogener Daten zwischen dem EU-Zentrum und Europol nur auf Einzelfallbasis nach einem ordnungsgemäß bewerteten Ersuchen über ein sicheres Kommunikationsinstrument wie das SIENA-Netzwerk erfolgten sollte.

Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte —

gestützt auf Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (im Folgenden „EU-DSVO“)[1],

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung[2],

gestützt auf das Ersuchen der Europäischen Kommission um eine gemeinsame Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten vom 12. Mai 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.[3]

HABEN FOLGENDE GEMEINSAME STELLUNGNAHME ANGENOMMEN:

1. HINTERGRUND

1. Am 11. Mai 2022 veröffentlichte die Europäische Kommission (im Folgenden „Kommission“) einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (im Folgenden „Vorschlag“ oder „vorgeschlagene Verordnung“ oder „Verordnungsvorschlag“).[4]

2. Der Vorschlag wurde im Anschluss an die 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 (im Folgenden „Interims-Verordnung“) veröffentlicht[5] Nach der Interims-verordnung sind die betreffenden Diensteanbieter nicht verpflichtet, Maßnahmen zur Aufdeckung von Material über sexuellen Kindesmissbrauch (z. B. Bilder, Videos usw.) oder der Kontaktaufnahme

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.
[3] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2022) 209 final).
[4] Ebd.
[5] Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 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 vom 30.7.2021, S. 41).

zu Kindern (auch als „Grooming“ bezeichnet) in ihren Diensten zu ergreifen, sondern können dies auf freiwilliger Basis unter den in dieser Verordnung festgelegten Bedingungen tun.[6]

3. Der Vorschlag besteht aus zwei wesentlichen Bausteinen: Erstens werden den Anbietern von Hostingdiensten, interpersonellen Kommunikationsdiensten und anderen Diensten Verpflichtungen in Bezug auf die Aufdeckung, Meldung, Entfernung und Sperrung von bekanntem und neuem Material über sexuellen Kindesmissbrauch und die Kontaktaufnahme zu Kindern auferlegt. Zweitens wird im Rahmen des Vorschlags ein neues EU-Zentrum für Fragen des sexuellen Kindesmissbrauchs als dezentrale Agentur (im Folgenden „EU-Zentrum für Fragen des sexuellen Kindesmissbrauchs“ oder „EU-Zentrum“) eingerichtet, um die Durchführung der vorgeschlagenen Verordnung zu ermöglichen.[7]

4. Wie in der Begründung des Vorschlags anerkannt wird, würden die in dem Vorschlag enthaltenen Maßnahmen die Ausübung der Grundrechte der Nutzer der betreffenden Dienste berühren. Zu diesen Rechten gehören insbesondere das Grundrecht auf Achtung der Privatsphäre (einschließlich der Vertraulichkeit der Kommunikation als Teil des umfassenderen Rechts auf Achtung des Privat- und Familienlebens), der Schutz der personenbezogenen Daten sowie die Freiheit der Meinungsäußerung und Informationsfreiheit.[8]

5. Außerdem sollen die vorgeschlagenen Maßnahmen auf den bestehenden EU-Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre aufbauen und diese bis zu einem gewissen Grad ergänzen. In der Begründung heißt es insbesondere wie folgt:

> „Der Vorschlag baut auf der Datenschutz-Grundverordnung (DSGVO) auf. In der Praxis neigen Anbieter dazu, verschiedene in der DSGVO vorgesehene Verarbeitungsgründe geltend zu machen, um personenbezogene Daten zu verarbeiten, die mit der freiwilligen Aufdeckung und Meldung von sexuellem Missbrauch von Kindern im Internet verbunden sind. In dem Vorschlag wird ein System gezielter Aufdeckungsanordnungen eingeführt und werden die Bedingungen für die Aufdeckung festgelegt, wodurch mehr Rechtssicherheit für diese Tätigkeiten geschaffen wird. Was die obligatorischen Aufdeckungstätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten betrifft, so wird mit dem Vorschlag und insbesondere mit den auf seiner Grundlage erlassenen Aufdeckungsanordnungen der Grund für eine solche Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c DSGVO festgelegt, wonach die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung im Rahmen des Rechts der Union oder eines Mitgliedstaats, dem der Verantwortliche unterliegt, vorgesehen ist.
>
> Der Vorschlag bezieht sich unter anderem auf Anbieter, die interpersonelle elektronische Kommunikationsdienste anbieten und daher nationalen Vorschriften zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation und ihrer vorgeschlagenen Überarbeitung unterliegen, über die derzeit verhandelt wird. Mit den in dem Vorschlag vorgesehenen Maßnahmen wird in einigen Punkten der Anwendungsbereich der Rechte und Pflichten aus den einschlägigen Bestimmungen der genannten Richtlinie beschränkt, insbesondere in Bezug auf Tätigkeiten, die für die Ausführung von Aufdeckungsanordnungen

[6]Siehe auch die Stellungnahme 7/2020 zum Vorschlag über eine vorübergehende Ausnahme von der Richtlinie 2002/58/EG zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet des EDSB (10. November 2020).
[7] COM(2022) 209 final, S. 17.
[8] COM(2022) 209 final, S. 12.

unbedingt erforderlich sind. In diesem Zusammenhang ist in dem Vorschlag die analoge Anwendung von Artikel 15 Absatz 1 der genannten Richtlinie vorgesehen."[9]

6. Angesichts der Schwere der geplanten Eingriffe in die Grundrechte ist der Vorschlag von besonderer Bedeutung für den Schutz der Rechte und Freiheiten des Einzelnen bei der Verarbeitung personenbezogener Daten. So beschloss die Kommission am 12. Mai 2022, den Europäischen Datenschutzausschuss (EDSA) und den Europäischen Datenschutzbeauftragten (EDSB) gemäß Artikel 42 Absatz 2 der EU-DSV zu konsultieren.

2. ANWENDUNGSBEREICH DER STELLUNGNAHME

7. In der vorliegenden gemeinsamen Stellungnahme werden die gemeinsamen Ansichten des EDSA und des EDSB zu dem Vorschlag dargelegt. Sie ist auf die Aspekte des Vorschlags beschränkt, die sich auf den Schutz der Privatsphäre und personenbezogener Daten beziehen. In der gemeinsamen Stellungnahme wird insbesondere auf die Bereiche hingewiesen, in denen durch den Vorschlag kein ausreichender Schutz der Grundrechte auf Privatsphäre und Datenschutz gewährleistet wird oder eine weitere Angleichung an den EU-Rechtsrahmen zum Schutz der Privatsphäre und personenbezogener Daten erforderlich ist.

8. Wie in dieser gemeinsamen Stellungnahme weiter ausgeführt, gibt der Vorschlag Anlass zu ernsthaften Bedenken hinsichtlich der Notwendigkeit und Verhältnismäßigkeit der geplanten Eingriffe und Einschränkungen des Schutzes der Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten. Allerdings ist es nicht das Ziel dieser gemeinsamen Stellungnahme, eine erschöpfende Liste aller durch den Vorschlag aufgeworfenen Fragen zum Schutz der Privatsphäre und des Datenschutzes zu liefern oder spezifische Vorschläge zur Verbesserung des Wortlauts der Formulierung zu machen. Stattdessen werden in dieser gemeinsamen Stellungnahme die wichtigsten Punkte des Vorschlags, die der EDSA und der EDSB ermittelt haben, ausführlich erörtert. Nichtsdestotrotz stehen der EDSA und der EDSB weiterhin zur Verfügung, um den Mitgesetzgebern während des Gesetzgebungsverfahrens zu dem Vorschlag weitere Hinweise und Empfehlungen zu geben.

3. ALLGEMEINE AUSFÜHRUNGEN ZU DEN RECHTEN AUF VERTRAULICHKEIT DER KOMMUNIKATION UND AUF DEN SCHUTZ PERSONENBEZOGENER DATEN

9. Die Vertraulichkeit der Kommunikation ist ein zentraler Bestandteil des Grundrechts auf Achtung des Privat- und Familienlebens, wie es in Artikel 7 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") verankert ist.[10] In Artikel 8 der Charta ist zudem das Recht auf den Schutz personenbezogener Daten verankert. Das Recht auf Vertraulichkeit der Kommunikation und das Recht auf Achtung des Privat- und Familienlebens sind auch in Artikel 8 der Europäischen

[9] COM(2022) 209 final, S. 4.

[10] Siehe z. B. die Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der ePrivacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation (25. Mai 2018).

Menschenrechtskonvention (EMRK) garantiert und gehören zu den gemeinsamen Verfassungstraditionen der Mitgliedstaaten.[11]

10. Der EDSA und der EDSB weisen erneut darauf hin, dass die in den Artikeln 7 und 8 der Charta verankerten Rechte keine absoluten Rechte sind, sondern im Zusammenhang mit ihrer Funktion in der Gesellschaft betrachtet werden müssen.[12] Der sexuelle Missbrauch von Kindern ist eine besonders verabscheuungswürdige Straftat, und das Ziel, eine wirksame Bekämpfung des sexuellen Missbrauchs von Kindern im Internet zu ermöglichen, entspricht sowohl einer von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzung als auch den Erfordernissen des Schutzes der Rechte und Freiheiten der Opfer. Im Hinblick auf die wirksame Bekämpfung von Straftaten, deren Opfer Minderjährige und andere schutzbedürftige Personen sind, hat der Gerichtshof der Europäischen Union (im Folgenden „EuGH“) hervorgehoben, dass sich aus Artikel 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens ergeben können. Solche Verpflichtungen können sich aus den Artikeln 3 und 4 der Charta hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit von Einzelpersonen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben.[13]

11. Gleichzeitig muss jede Einschränkung der durch die Charta garantierten Rechte, wie im Vorschlag vorgesehen,[14] den Anforderungen von Artikel 52 Absatz 1 der Charta genügen. Bei jeder Maßnahme, die in das Recht auf Vertraulichkeit der Kommunikation und das Recht auf Privat- und Familienleben eingreift, muss in erster Linie der Wesensgehalt der betreffenden Rechte gewahrt werden.[15] Der Wesensgehalt eines Rechts wird beeinträchtigt, wenn das Recht seines grundlegenden Inhalts beraubt wird und der Einzelne es nicht ausüben kann.[16] Der Eingriff darf im Verhältnis zum verfolgten Ziel keinen derart unverhältnismäßigen und nicht tragbaren Eingriff darstellen, der das so gewährleistete Recht in seinem Wesensgehalt antasten würde.[17] Das bedeutet, dass selbst ein Grundrecht, das nicht absolut ist, wie das Recht auf Vertraulichkeit der Kommunikation und das Recht auf den Schutz personenbezogener Daten, einige Kernbestandteile hat, die nicht eingeschränkt werden dürfen.

12. Der EuGH hat bei mehreren Gelegenheiten den „Wesensgehalt eines Rechts“ im Bereich der Privatsphäre in der elektronischen Kommunikation geprüft. In der Rechtssache *Tele2 Sverige und*

---

[11] In fast allen europäischen Verfassungen ist das Recht auf den Schutz der Vertraulichkeit der Kommunikation verankert. Siehe z. B. Artikel 15 der Verfassung der Italienischen Republik, Artikel 10 des Grundgesetzes der Bundesrepublik Deutschland, Artikel 22 der Verfassung des Königreichs Belgiens und Artikel 13 der Verfassung des Königreichs der Niederlande.

[12] Siehe unter anderem das Urteil des Gerichtshofs vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, ECLI:EU:C:2020:559, Rn. 172 und die darin zitierte Rechtsprechung. Siehe auch Erwägungsgrund 4 DSGVO.

[13] Siehe das Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2020, La Quadrature du Net u. a., verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791, Rn. 126–128. Siehe auch die Stellungnahme 7/2020 zum Vorschlag über eine vorübergehende Ausnahme von der Richtlinie 2002/58/EG zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet des Europäischen Datenschutzbeauftragten (10. November 2020), Rn. 12.

[14] Vgl. COM(2022) 209 final, S. 12–13.

[15] Artikel 52 Absatz 1 der Charta.

[16] Siehe die Leitlinien des EDSB zur Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19. Dezember 2019), S. 8, abrufbar unter https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[17] Urteil des Gerichtshofs der Europäischen Union vom 14. Januar 2021, *OM*, C-393/19, ECLI:EU:C:2021:8, Rn. 53.

Watson entschied der Gerichtshof, dass eine Regelung, die keine Vorratsspeicherung des Inhalts einer Kommunikation erlaubt, den Wesensgehalt der Grundrechte auf Privatleben und den Schutz der personenbezogenen Daten nicht antastet.[18] In der Rechtssache *Schrems* urteilte der EuGH, dass insbesondere eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens verletzt.[19] In der Rechtssache *Digital Rights Ireland und Seitlinger u. a.* entschied das Gericht, dass die Vorratsspeicherung von Daten nach der Richtlinie 2006/24/EG zwar einen besonders schwerwiegenden Eingriff in das Grundrecht auf Achtung des Privatlebens und die übrigen in Artikel 7 der Charta verankerten Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.[20] Aus dieser Rechtsprechung lässt sich ableiten, dass Maßnahmen, die den Behörden einen allgemeinen Zugriff auf den Inhalt einer Nachricht ermöglichen, eher als Eingriff in den Wesensgehalt der in Artikel 7 und 8 der Charta garantierten Rechte zu betrachten sind. Diese Überlegungen gelten auch für Maßnahmen zur Aufdeckung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern, wie sie in dem Vorschlag vorgesehen sind.

13. Darüber hinaus hat der EuGH festgestellt, dass Datensicherheitsmaßnahmen eine Schlüsselrolle spielen, um zu gewährleisten, dass der Wesensgehalt des in Artikel 8 der Charta niedergelegten Rechts auf Schutz personenbezogener Daten gewahrt ist.[21] Im digitalen Zeitalter sind technische Lösungen zur Sicherung und zum Schutz der Vertraulichkeit der elektronischen Kommunikation, einschließlich Maßnahmen zur Verschlüsselung, von zentraler Bedeutung, um die Wahrnehmung aller Grundrechte zu wahren.[22] Dies sollte bei der Bewertung der Maßnahmen zur obligatorischen Aufdeckung von Material über sexuellen Kindesmissbrauch gebührend berücksichtigt werden, insbesondere wenn sie zu einer Schwächung oder Verschlechterung der Verschlüsselung führen würden.[23]

14. In Artikel 52 Absatz 1 der Charta ist außerdem vorgesehen, dass jede Einschränkung der Ausübung eines in der Charta anerkannten Grundrechts gesetzlich vorgesehen sein muss. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[24] Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die den wirksamen Schutz dieser Daten vor

---

[18] Urteil des Gerichtshofs der Europäischen Union vom 21. Dezember 2016, *Tele2 Sverige und Watson*, C-203/15 und C-698/15, ECLI:EU:C:2016:970, Rn. 101.

[19] Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, *Schrems/Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, Rn. 94.

[20] Urteil des Gerichtshofs der Europäischen Union vom 8. April 2014, *Digital Rights Ireland und Seitlinger u. a.*, verbundene Rechtssachen C-293/12 und C-594/12, ECLI:EU:C:2014:238, Rn. 39.

[21] Ebd., Rn. 40.

[22] Siehe Menschenrechtsrat, Resolution 47/16 über die Förderung, den Schutz und den Genuss der Menschenrechte im Internet, UN-Dok. A/HRC/RES/47/16 (26. Juli 2021).

[23] Siehe auch Erwägungsgrund 25 der vorgeschlagenen Verordnung.

[24] Siehe „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit“, 11. April 2019, abrufbar unter https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf..

Missbrauchsrisiken ermöglichen.[25] In der Regelung muss insbesondere angegeben werden, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut notwendige Maß beschränkt wird.[26] Der EuGH hat klargestellt, dass das Erfordernis, über solche Garantien zu verfügen, umso bedeutsamer ist, wenn die personenbezogenen Daten automatisiert verarbeitet werden und es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht.[27]

15. Mit dem Vorschlag würde die Ausübung der in Artikel 5 Absätze 1 und 3 und Artikel 6 Absatz 1 der Richtlinie 2002/58/EG (im Folgenden „Datenschutzrichtlinie für elektronische Kommunikation“)[28] vorgesehenen Rechte und Pflichten insoweit eingeschränkt, als dies für die Ausführung der gemäß Kapitel 1 Abschnitt 2 des Vorschlags erteilten Aufdeckungsanordnungen erforderlich ist. Der EDSA und der EDSB sind daher der Ansicht, dass es erforderlich ist, den Vorschlag nicht nur im Lichte der Charta und der DSGVO, sondern auch im Hinblick auf die Artikel 5, 6 und 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation zu bewerten.

[25] Siehe das Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2020, *La Quadrature du Net u. a.*, verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791, Rn. 132.
[26] Ebd.
[27] Ebd.
[28] 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), geändert durch die Richtlinien 2006/24/EG und 2009/136/EG.

4. SPEZIFISCHE ANMERKUNGEN

4.1 Zusammenspiel mit bestehenden Rechtsvorschriften

4.1.1 Zusammenspiel mit der DSGVO und der Datenschutzrichtlinie für elektronische Kommunikation

16. In dem Vorschlag heißt es, dass die Verordnung unbeschadet der Vorschriften gilt, die sich aus anderen Rechtsakten der Union ergeben, insbesondere aus der DSGVO [29] und der Datenschutzrichtlinie für elektronische Kommunikation. Im Gegensatz zur Interims-Verordnung ist in dem Vorschlag keine ausdrückliche vorübergehende Ausnahme von der Datenschutzrichtlinie für elektronische Kommunikation vorgesehen, sondern eine Einschränkung der Ausübung der in Artikel 5 Absätze 1 und 3 und Artikel 6 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation festgelegten Rechte und Pflichten. Ferner ist zu beachten, dass in der Interims-Verordnung eine Ausnahme von den Bestimmungen in Artikel 5 Absatz 1 und Artikel 6 Absatz 1 und nicht von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehen ist.

17. In dem Vorschlag wird ferner auf Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation verwiesen, wonach die Mitgliedstaaten Rechtsvorschriften erlassen dürfen, die die Rechte und Pflichten gemäß den Artikeln 5 und 6 dieser Richtlinie beschränken, sofern eine solche Beschränkung unter anderem für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Dem Vorschlag zufolge wird Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation analog angewandt, wenn der Vorschlag die Ausübung der in Artikel 5 Absatz 1, Artikel 5 Absatz 3 und Artikel 6 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehenen Rechte und Pflichten einschränkt.

18. Der EDSA und der EDSB betonen, dass der EuGH klargestellt hat, dass Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation eng auszulegen ist, was bedeutet, dass die Ausnahme vom Grundsatz der Vertraulichkeit der Kommunikation nach Artikel 15 Absatz 1 eine Ausnahme bleiben muss und nicht zur Regel werden darf.[30] Wie nachfolgend in dieser gemeinsamen Stellungnahme dargelegt, sind der EDSA und der EDSB der Ansicht, dass die Anforderungen der (strikten) Notwendigkeit, Wirksamkeit und Verhältnismäßigkeit im Vorschlag nicht erfüllt werden. Ferner kommen der EDSA und der EDSB zu dem Schluss, dass der Vorschlag dazu führen würde, dass die Einschränkung der Vertraulichkeit der Kommunikation eher die Regel als die Ausnahme sein könnte.

4.1.2 Zusammenspiel mit der Verordnung (EU) 2021/1232 und Auswirkungen auf die freiwillige Aufdeckung von sexuellem Kindesmissbrauch im Internet

19. Gemäß Artikel 88 des Vorschlags würde damit die Interims-Verordnung aufgehoben, in der eine vorübergehende Ausnahme von bestimmten Bestimmungen der Datenschutzrichtlinie für

[29] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR) (ABl. L 119 vom 4.5.2016, S. 1).

[30] Urteil des Gerichtshofs der Europäischen Union vom 21. Dezember 2016, *Tele2 Sverige AB und Watson*, verbundene Rechtssachen C-203/15 und C-698-15, ECLI:EU:C:2016:970, Rn. 89.

elektronische Kommunikation vorgesehen ist, um den freiwilligen Einsatz von Technologien zur Erkennung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zu ermöglichen. Somit gäbe es ab dem Zeitpunkt der Anwendung der vorgeschlagenen Verordnung keine Ausnahmeregelung von der Datenschutzrichtlinie für elektronische Kommunikation, durch die die freiwillige Aufdeckung von Material über sexuellen Kindesmissbrauch im Internet durch solche Anbieter ermöglicht würde.

20. Da die mit dem Vorschlag eingeführten Aufdeckungspflichten nur für Empfänger von Aufdeckungsanordnungen gelten würden, wäre es wichtig, im Text der vorgeschlagenen Verordnung klarzustellen, dass der freiwillige Einsatz von Technologien zur Erkennung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern nur insoweit zulässig bleibt, als er nach der Datenschutzrichtlinie für elektronische Kommunikation und der DSGVO zulässig ist. Dies würde beispielsweise bedeuten, dass Anbieter von nummernunabhängigen interpersonellen Kommunikationsdiensten daran gehindert würden, solche Technologien auf freiwilliger Grundlage zu nutzen, es sei denn, dies wäre nach den nationalen Rechtsvorschriften zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation gemäß Artikel 15 Absatz 1 der genannten Richtlinie und der Charta zulässig.

21. Insgesamt wäre es von Vorteil, wenn die vorgeschlagene Verordnung mehr Klarheit über den Status der freiwilligen Aufdeckung von sexuellem Kindesmissbrauch im Internet nach dem Beginn der Anwendung der vorgeschlagenen Verordnung und über den Übergang von der Regelung der freiwilligen Aufdeckung der Interims-Verordnung zu den Aufdeckungspflichten der vorgeschlagenen Verordnung schaffen würde. So schlagen der EDSA und der EDSB beispielsweise vor, klarzustellen, dass in der vorgeschlagenen Verordnung keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum alleinigen Zweck der freiwilligen Aufdeckung von sexuellem Kindesmissbrauch im Internet vorgesehen ist.

4.2 Rechtsgrundlage gemäß der DSGVO

22. Mit dem Vorschlag soll eine Rechtsgrundlage im Sinne der DSGVO für die Verarbeitung personenbezogener Daten zur Aufdeckung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern geschaffen werden. In der Begründung heißt es wie folgt: „Was die obligatorischen Aufdeckungstätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten betrifft, so wird mit dem Vorschlag und insbesondere mit den auf seiner Grundlage erlassenen Aufdeckungsanordnungen der Grund für eine solche Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c DSGVO festgelegt, wonach die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung im Rahmen des Rechts der Union oder eines Mitgliedstaats, dem der Verantwortliche unterliegt, vorgesehen ist.“[31]

23. Der EDSA und der EDSB begrüßen die Entscheidung der Kommission, die Rechtsunsicherheit in Bezug auf die Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu beseitigen, die durch die Interims-Verordnung entstanden ist. Der EDSA und der EDSB stimmen auch mit der Schlussfolgerung der Kommission überein, dass die Folgen des Einsatzes von Aufdeckungsmaßnahmen zu weitreichend und schwerwiegend sind, um die Entscheidung über die Durchführung solcher Maßnahmen den Diensteanbietern zu überlassen.[32] Gleichzeitig stellen der EDSA und der EDSB fest, dass jede Rechtsgrundlage, nach der Diensteanbieter verpflichtet werden, in die Grundrechte auf Datenschutz

[31] Ebd., S. 4.
[32] Vgl. Vorschlag (COM(2022) 209 final), S. 14.

und Schutz der Privatsphäre einzugreifen, nur dann gültig ist, wenn sie die in Artikel 52 Absatz 1 der Charta festgelegten Bedingungen erfüllt, wie in den folgenden Abschnitten analysiert wird.

4.3 Risikobewertungs- und Risikominderungspflichten

24. Nach Kapitel II Abschnitt 1 des Vorschlags müssen Anbieter von Hostingdiensten und Anbieter interpersoneller Kommunikationsdienste für jeden von ihnen angebotenen Dienst das Risiko seiner Nutzung zum Zwecke des sexuellen Kindesmissbrauchs im Internet ermitteln, analysieren und bewerten, und dann versuchen, das ermittelte Risiko durch „angemessene Risikominderungsmaßnahmen, die auf das [...] ermittelte Risiko zugeschnitten sind“, zu minimieren.

25. Der EDSA und der EDSB stellen fest, dass der Anbieter bei der Durchführung einer Risikobewertung insbesondere die in Artikel 3 Absatz 2 Buchstaben a bis e des Vorschlags aufgeführten Elemente berücksichtigen sollte, darunter in den allgemeinen Geschäftsbedingungen festgelegte Verbote und Beschränkungen, die Art und Weise, wie die Nutzer ihren Dienst in Anspruch nehmen, und die damit verbundenen Auswirkungen auf dieses Risiko, und die Art und Weise der Konzeption und des Betriebs des Dienstes, einschließlich des Geschäftsmodells, der Unternehmensführung und der einschlägigen Systeme und Prozesse, sowie die damit verbundenen Auswirkungen auf dieses Risiko. Im Hinblick auf das Risiko der Kontaktaufnahme zu Kindern wird vorgeschlagen, folgende Aspekte zu berücksichtigen: den Umfang, in dem der Dienst von Kindern genutzt wird bzw. voraussichtlich genutzt werden wird, die Altersgruppen und das Risiko der Kontaktaufnahme in Bezug auf diese Altersgruppen, die Verfügbarkeit von Funktionen, die eine Nutzersuche ermöglichen, Funktionen, die es den Nutzern ermöglichen, direkten Kontakt zu anderen Nutzern herzustellen, insbesondere durch private Mitteilungen, und Funktionen, die es den Nutzern ermöglichen, Bilder oder Videos mit anderen Nutzern auszutauschen.

26. Der EDSA und der EDSB erkennen zwar an, dass diese Kriterien relevant zu sein scheinen, sind aber dennoch besorgt darüber, dass sie einen ziemlich großen Spielraum für die Auslegung und Bewertung lassen. Einige Kriterien sind sehr allgemein gehalten (z. B. „die Art und Weise, wie die Nutzer ihren Dienst in Anspruch nehmen, und die damit verbundenen Auswirkungen auf dieses Risiko“) oder beziehen sich auf grundlegende Funktionen, die vielen Online-Diensten gemeinsam sind (z. B. die „Möglichkeit für Nutzer, Bilder oder Videos mit anderen Nutzern auszutauschen“). Daher scheinen die Kriterien eher einer subjektiven (als einer objektiven) Bewertung zu unterliegen.

27. Nach Ansicht des EDSA und des EDSB gilt dies auch für die gemäß Artikel 4 des Vorschlags zu ergreifenden Risikominderungsmaßnahmen. Maßnahmen wie die Anpassung der Systeme des Anbieters zur Moderation von Inhalten oder seiner Empfehlungssysteme durch geeignete technische und operative Maßnahmen und Personalausstattung scheinen geeignet, das ermittelte Risiko zu verringern. Werden diese Kriterien jedoch im Rahmen eines komplexen Risikobewertungsprozesses angewandt und mit abstrakten und vagen Begriffen zur Beschreibung des annehmbaren Risikos (z. B. „beträchtlicher Umfang“) kombiniert, erfüllen sie nicht die Kriterien der Rechtssicherheit und Vorhersehbarkeit, die erforderlich sind, um einen Eingriff in die Vertraulichkeit der Kommunikation zwischen Privatpersonen zu rechtfertigen, der einen eindeutigen Eingriff in die Grundrechte auf Privatsphäre und Freiheit der Meinungsäußerung darstellt.

28. Zwar sind die Anbieter nicht befugt, im Rahmen ihrer Risikobewertungs- und Risikominderungsprozesse in die Vertraulichkeit der Kommunikation einzugreifen, bevor sie eine Aufdeckungsanordnung erhalten, doch es besteht ein direkter Zusammenhang zwischen den Verpflichtungen zur Risikobewertung und -minderung und den sich daraus ergebenden Aufdeckungspflichten. Nach Artikel 7 Absatz 4 des Vorschlags ist der Erlass einer

Aufdeckungsanordnung davon abhängig, dass ein erhebliches Risiko besteht, dass der betreffende Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt werden könnte. Bevor eine Aufdeckungsanordnung erlassen wird, muss ein komplexes Verfahren durchlaufen werden, an dem Anbieter, die Koordinierungsbehörde und die für den Erlass der Anordnung zuständige Justizbehörde oder andere unabhängige Verwaltungsbehörde beteiligt sind. Erstens müssen die Anbieter das Risiko der Nutzung ihrer Dienste zum Zwecke des sexuellen Kindesmissbrauchs im Internet bewerten (Artikel 3 des Vorschlags) und mögliche Maßnahmen zur Risikominderung (Artikel 4 des Vorschlags) prüfen, um dieses Risiko zu verringern. Die Ergebnisse dieser Prüfung sind dann der zuständigen Koordinierungsbehörde zu berichten (Artikel 5 des Vorschlags). Ergibt die Risikobewertung, dass trotz der Bemühungen zur Risikominderung weiterhin ein erhebliches Risiko besteht, hört die Koordinierungsstelle den Anbieter zu einem Entwurf eines Ersuchens um Erlass einer Aufdeckungsanordnung an und gibt ihm Gelegenheit zur Stellungnahme. Der Anbieter ist ferner verpflichtet, einen Durchführungsplan vorzulegen, einschließlich einer Stellungnahme der zuständigen Datenschutzbehörde im Falle der Aufdeckung der Kontaktaufnahme zu Kindern. Verfolgt die Koordinierungsbehörde den Fall weiter, wird um eine Aufdeckungsanordnung ersucht und diese schließlich von einer Justizbehörde oder einer anderen unabhängigen Verwaltungsbehörde erlassen. Daher sind die anfängliche Risikobewertung und die Maßnahmen, die zur Verringerung des festgestellten Risikos gewählt wurden, eine maßgebliche Grundlage für die Beurteilung durch die Koordinierungsbehörde sowie durch die zuständige Justiz- oder unabhängige Verwaltungsbehörde, ob eine Aufdeckungsanordnung erforderlich ist.

29. Der EDSA und der EDSB nehmen die komplexen Schritte zur Kenntnis, die zum Erlass einer Aufdeckungsanordnung führen. Dazu gehören eine erste Risikobewertung durch den Anbieter und der Vorschlag des Anbieters für Maßnahmen zur Risikominderung sowie die weitere Interaktion des Anbieters mit der zuständigen Koordinierungsbehörde. Der EDSA und der EDSB sind der Ansicht, dass der Anbieter in erheblichem Maße die Möglichkeit hat, das Ergebnis des Prozesses zu beeinflussen. In diesem Zusammenhang stellen der EDSA und der EDSB fest, dass in dem Erwägungsgrund 17 des Vorschlags vorgesehen ist, dass die Anbieter in der Lage sein sollten, „ihre Bereitschaft zu bekunden, gegebenenfalls eine Aufdeckungsanordnung [...] auszuführen“. Daher kann nicht davon ausgegangen werden, dass jeder Anbieter versuchen wird, den Erlass einer Aufdeckungsanordnung zu vermeiden, um die Vertraulichkeit der Kommunikation seiner Nutzer zu wahren, indem er die wirksamsten, aber am wenigsten eingreifenden Risikominderungsmaßnahmen anwendet, insbesondere dann, wenn diese Maßnahmen die unternehmerische Freiheit des Anbieters gemäß Artikel 16 der Charta beeinträchtigen.

30. Der EDSA und der EDSB möchten betonen, dass Verfahrensgarantien materielle Schutzvorkehrungen nie vollständig ersetzen können. Daher sollte das oben beschriebene komplexe Verfahren, das zum Erlass einer Aufdeckungsanordnung führen kann, mit klaren materiellen Pflichten einhergehen. Der EDSA und der EDSB sind der Auffassung, dass es dem Vorschlag an Klarheit in Bezug auf mehrere Schlüsselelemente mangelt (z. B. die Begriffe „erhebliches Risiko“, „beträchtliches Risiko“ usw.), was nicht durch das Vorhandensein mehrerer Schichten von Verfahrensgarantien behoben werden kann. Dies ist umso wichtiger, als die für die Anwendung dieser Schutzvorkehrungen zuständigen Stellen (z. B. Anbieter, Justizbehörden usw.) über einen großen Ermessensspielraum bei der Abwägung der Rechte verfügen, die in jedem einzelnen Fall auf dem Spiel stehen. Angesichts der weitreichenden Eingriffe in die Grundrechte, die sich aus der Annahme des Vorschlags ergeben würden, sollten die Gesetzgeber dafür sorgen, dass in dem Vorschlag mehr Klarheit darüber geschaffen wird, wann und wo solche Eingriffe zulässig sind. Der EDSA und der EDSB erkennen zwar an, dass die gesetzgeberischen Maßnahmen nicht zu präskriptiv sein dürfen und eine gewisse Flexibilität bei ihrer praktischen Anwendung ermöglichen müssen, sind jedoch der Auffassung, dass der derzeitige

Wortlaut des Vorschlags aufgrund des Mangels an klaren materiellen Normen zu viel Raum für potenziellen Missbrauch lässt.

31. Angesichts der potenziell erheblichen Auswirkungen auf eine sehr große Anzahl von betroffenen Personen (d. h. potenziell alle Nutzer interpersoneller Kommunikationsdienste) betonen der EDSA und der EDSB, dass ein hohes Maß an Rechtssicherheit, Klarheit und Vorhersehbarkeit der Gesetzgebung erforderlich ist, um sicherzustellen, dass mit den vorgeschlagenen Maßnahmen das mit ihnen verfolgte Ziel wirklich erreicht wird und gleichzeitig die Grundrechte, um die es geht, möglichst wenig beeinträchtigt werden.

4.4 Bedingungen für den Erlass von Aufdeckungsanordnungen

32. In Artikel 7 des Vorschlags ist vorgesehen, dass die Koordinierungsbehörde am Niederlassungsort befugt ist, bei der zuständigen Justizbehörde des Mitgliedstaats, der sie benannt hat, oder einer anderen unabhängigen Verwaltungsbehörde dieses Mitgliedstaats den Erlass einer Aufdeckungsanordnung zu beantragen, mit der ein Anbieter von Hostingdiensten oder ein Anbieter interpersoneller Kommunikationsdienste verpflichtet wird, die in Artikel 10 genannten Maßnahmen zu ergreifen, um sexuellen Kindesmissbrauch im Internet in einem bestimmten Dienst aufzudecken.

33. Der EDSA und der EDSB berücksichtigen gebührend die folgenden Elemente, die vor dem Erlass einer Aufdeckungsanordnung erfüllt sein müssen:

a. Es gibt Beweise für ein erhebliches Risiko, dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt wird, im Sinne von Artikel 7 Absätze 5, 6 und 7;

b. die Gründe für den Erlass der Aufdeckungsanordnung wiegen schwerer als die negativen Folgen für die Rechte und berechtigten Interessen aller betroffenen Parteien, wobei insbesondere was die notwendige Herstellung eines angemessenen Gleichgewichts zwischen den Grundrechten dieser Parteien betrifft.

34. Die Bedeutung der Begriffe „erhebliches Risiko“ wird in Artikel 7 Absatz 5 ff. je nach Art der betreffenden Aufdeckungsanordnung erläutert. In Bezug auf Aufdeckungsanordnungen betreffend die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs gilt das erhebliche Risiko als gegeben, wenn die folgenden Bedingungen erfüllt sind:

a. Trotz etwaiger Risikominderungsmaßnahmen, die vom Anbieter ergriffen wurden oder noch ergriffen werden, ist davon auszugehen, dass der Dienst in beträchtlichem Umfang für die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs genutzt wird;

b. es liegen Beweise dafür vor, dass der Dienst oder – falls der betreffende Dienst zum Zeitpunkt des Antrags auf Erlass der Aufdeckungsanordnung noch nicht in der Union angeboten wurde – ein vergleichbarer Dienst in den letzten zwölf Monaten in beträchtlichem Umfang für die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs genutzt wurde.

35. Um eine Aufdeckungsanordnung in Bezug auf neues Material über sexuellen Kindesmissbrauch zu erlassen, müssen sich die Wahrscheinlichkeit und der Sachverhalt auf neues Material über sexuellen Kindesmissbrauch beziehen und es muss eine frühere Aufdeckungsanordnung für bekanntes Material erlassen worden sein, die zu einer erheblichen Anzahl von Meldungen über Material über sexuellen Kindesmissbrauch durch den Anbieter geführt hat (Artikel 7 Absatz 6 des Vorschlags). Bei einer Aufdeckungsanordnung betreffend die Kontaktaufnahme zu Kindern wird davon ausgegangen, dass ein erhebliches Risiko besteht, wenn der Anbieter als Anbieter interpersoneller Kommunikationsdienste gilt, wenn davon auszugehen ist, dass der Dienst in beträchtlichem Umfang

für die Kontaktaufnahme zu Kindern genutzt wird und wenn Beweise vorliegen, dass der Dienst in beträchtlichem Umfang für die Kontaktaufnahme zu Kindern genutzt wird (Artikel 7 Absatz 7 des Vorschlags).

36. Der EDSA und der EDSB stellen fest, dass selbst mit den Klarstellungen in Artikel 7 Absätze 5 bis 7 des Vorschlags die Bedingungen für den Erlass einer Aufdeckungsanordnung von vagen Rechtsbegriffen wie „beträchtlicher Umfang“ und „erhebliche Anzahl“ beherrscht werden und sich zum Teil wiederholen, da Beweise für früheren Missbrauch häufig dazu beitragen, die Wahrscheinlichkeit eines künftigen Missbrauchs zu ermitteln.

37. In dem Vorschlag ist ein System vorgesehen, bei dem bei der Entscheidung, ob eine Aufdeckungsanordnung erforderlich ist, eine vorausschauende Entscheidung über die künftige Nutzung eines Dienstes zum Zwecke des sexuellen Kindesmissbrauchs im Internet getroffen werden muss. Es ist daher nachvollziehbar, dass die in Artikel 7 aufgeführten Elemente einen prognostischen Charakter haben. Da in dem Vorschlag jedoch vage Begriffe verwendet werden, ist es sowohl für die Anbieter als auch für die zuständigen Justiz- oder anderen unabhängigen Verwaltungsbehörden schwierig, die durch den Vorschlag eingeführten rechtlichen Anforderungen auf vorhersehbare und nicht willkürliche Weise anzuwenden. Der EDSA und der EDSB befürchten, dass diese weit gefassten und vagen Begriffe zu einem Mangel an Rechtssicherheit sowie zu erheblichen Unterschieden bei der konkreten Umsetzung des Vorschlags in der Union führen werden, je nachdem, wie Begriffe wie „Wahrscheinlichkeit“ und „beträchtlicher Umfang“ von den Justiz- oder anderen unabhängigen Verwaltungsbehörden in den Mitgliedstaaten ausgelegt werden. Ein solches Ergebnis wäre nicht hinnehmbar angesichts der Tatsache, dass die Bestimmungen über Aufdeckungsanordnungen für Anbieter interpersoneller Kommunikationsdienste „Einschränkungen“ des in Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation verankerten Grundsatzes der Vertraulichkeit der Kommunikation darstellen werden und ihre Klarheit und Vorhersehbarkeit daher von größter Bedeutung ist, um sicherzustellen, dass diese Einschränkungen in der gesamten Union einheitlich angewendet werden.

4.5 Analyse der Notwendigkeit und Verhältnismäßigkeit der geplanten Maßnahmen[33]

38. Wie bereits erwähnt, können drei Arten von Aufdeckungsanordnungen erlassen werden: Aufdeckungsanordnungen betreffend die Verbreitung von bekannten Darstellungen sexuellen Kindesmissbrauchs (Artikel 7 Absatz 5 des Vorschlags), Aufdeckungsanordnungen betreffend die Verbreitung von neuen Darstellungen sexuellen Kindesmissbrauchs (Artikel 7 Absatz 6 des Vorschlags) und Aufdeckungsanordnungen betreffend die Kontaktaufnahme zu Kindern (Artikel 7 Absatz 7 des Vorschlags). Für jede Aufdeckungsanordnung wird im Regelfall eine andere Technologie für die praktische Umsetzung benötigt. Folglich wird damit in unterschiedlichem Maße in die Privatsphäre eingegriffen, was unterschiedliche Auswirkungen auf das Recht auf Privatsphäre und den Schutz personenbezogener Daten hat.

39. Die Technologien zur Aufdeckung von Material über sexuellen Kindesmissbrauch im Internet sind in der Regel Abgleichstechnologien in dem Sinne, dass sie sich auf eine bestehende Datenbank mit

[33] Siehe auch „The EDPS quick guide to necessity and proportionality“ (Leitfaden des EDSB zur Notwendigkeit und Verhältnismäßigkeit), abrufbar unter https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

bekanntem Material über sexuellen Kindesmissbrauch stützen, das mit Bildern (einschließlich Standbildern aus Videos) verglichen wird. Für den Abgleich müssen sowohl die Bilder, die der Anbieter verarbeitet, als auch die Bilder in der Datenbank digitalisiert werden, in der Regel durch Umwandlung in Hashwerte. Diese Art von Hashing-Technologie hat eine geschätzte Falsch-Positiv-Rate von nicht mehr als 1 zu 50 Milliarden (d. h. 0,000000002 %).[34]

40. Für die Erkennung von neuem Material über sexuellen Kindesmissbrauch wird in der Regel eine andere Art von Technologie verwendet, darunter Klassifikatoren und künstliche Intelligenz (KI).[35] Die Fehlerquoten sind jedoch meistens deutlich höher. Im Bericht über die Folgenabschätzung wird beispielsweise darauf hingewiesen, dass es Technologien zur Erkennung von neuem Material über sexuellen Kindesmissbrauch gibt, deren Genauigkeit auf 99,9 % (d. h. eine Falsch-Positiv-Rate von 0,1 %) eingestellt werden kann. Mit dieser Genauigkeit können jedoch nur 80 % des gesamten Materials über sexuellen Kindesmissbrauch in dem betreffenden Datensatz identifiziert werden.[36]

41. Hinsichtlich der Aufdeckung der Kontaktaufnahme zu Kindern in textbasierter Kommunikation wird im Bericht über die Folgenabschätzung erklärt, dass dies in der Regel auf der Erkennung von Mustern beruht. Im Bericht über die Folgenabschätzung heißt es, dass einige der bestehenden Technologien zur Erkennung der Kontaktaufnahme zu Kindern eine Genauigkeit von 88 % haben.[37] Nach Angaben der Kommission bedeutet dies, „dass von 100 Gesprächen, bei denen auf eine mögliche strafbare Kontaktaufnahme zu Kindern hingewiesen wird, dies bei 12 Gesprächen nach einer Überprüfung [laut dem Vorschlag durch das EU-Zentrum] ausgeschlossen werden kann und keine Meldung an die Strafverfolgungsbehörden erfolgt“[38]. Obwohl der Vorschlag – im Gegensatz zur Interims-Verordnung – auch auf Audiokommunikation Anwendung finden würde, wird im Bericht über die Folgenabschätzung nicht näher auf die technischen Lösungen eingegangen, die zur Aufdeckung der Kontaktaufnahme zu Kindern in einem solchen Umfeld eingesetzt werden könnten.

4.5.1 Wirksamkeit der Aufdeckung

42. „Notwendigkeit“ impliziert das Erfordernis einer kombinierten, faktengestützten Bewertung der Wirksamkeit der Maßnahme mit Blick auf das angestrebte Ziel und auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist.[39] Ein weiterer Faktor, der bei der Prüfung der Verhältnismäßigkeit einer vorgeschlagenen Maßnahme zu berücksichtigen ist, ist die Wirksamkeit der vorhandenen Maßnahmen gegenüber der geplanten.[40] Wenn es bereits

---

[34] Siehe Europäische Kommission, Arbeitsunterlage der Kommissionsdienststellen mit dem Titel „Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse“ (Bericht über die Folgenabschätzung zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern), SWD(2022) 209 final (im Folgenden „Bericht über die Folgenabschätzung“ oder „SWD(2022) 209 final“), S. 281, Fußnote 511.

[35] Folgenabschätzung, S. 281.

[36] Ebd., S. 282.

[37] Ebd., S. 283.

[38] Siehe den Vorschlag (COM(2022) 209 final), S. 14, Fußnote 32.

[39] EDSB, „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener einschränken: Ein Toolkit“ (11. April 2017), S. 5; Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19. Dezember 2019), S. 8.

[40] Siehe die Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19. Dezember 2019), S. 11.

Maßnahmen für denselben oder einen ähnlichen Zweck gibt, sollte deren Wirksamkeit im Rahmen der Beurteilung der Verhältnismäßigkeit bewertet werden. Wird die Wirksamkeit bestehender Maßnahmen, die denselben oder einen ähnlichen Zweck verfolgen, nicht bewertet, kann die Prüfung der Verhältnismäßigkeit für eine neue Maßnahme nicht als ordnungsgemäß durchgeführt angesehen werden.

43. Die Aufdeckung von Material über sexuellen Kindesmissbrauch oder der Kontaktaufnahme zu Kindern durch Anbieter von Hostingdiensten und Anbieter von interpersonellen Kommunikationsdiensten kann zum übergeordneten Ziel der Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern und der Verbreitung von Material über sexuellen Kindesmissbrauch im Internet beitragen. Gleichzeitig ergeben sich aus der Notwendigkeit, die Wirksamkeit der in dem Vorschlag vorgesehenen Maßnahmen zu bewerten, drei zentrale Fragen:

- Können die Maßnahmen zur Aufdeckung von sexuellem Kindesmissbrauch im Internet leicht umgangen werden?
- Welche Auswirkungen haben die Aufdeckungstätigkeiten auf die Maßnahmen der Strafverfolgungsbehörden?[41]
- Wie würde die Rechtsunsicherheit durch den Vorschlag verringert?

44. Es obliegt nicht dem EDSA und dem EDSB, auf diese Fragen eine detaillierte Antwort zu geben. Der EDSA und der EDSB stellen jedoch fest, dass weder der Bericht über die Folgenabschätzung noch der Vorschlag vollständige Antworten auf diese Fragen enthalten.

45. Hinsichtlich der Möglichkeit, die Aufdeckung von Material über sexuellen Kindesmissbrauch zu umgehen, ist anzumerken, dass es derzeit keine technische Lösung zu geben scheint, um Material über sexuellen Kindesmissbrauch zu erkennen, das in verschlüsselter Form weitergegeben wird. Daher kann jede Aufdeckungstätigkeit – selbst das Durchsuchen auf Anbieterseite, womit das Ziel verfolgt wird, die vom Anbieter angebotene Ende-zu-Ende-Verschlüsselung zu umgehen[42] – leicht umgangen werden, indem die Inhalte vor dem Senden oder Hochladen mithilfe einer separaten Anwendung verschlüsselt werden. Daher könnten sich die in dem Vorschlag vorgesehenen Aufdeckungsmaßnahmen geringer auf die Verbreitung von Material über sexuellen Kindesmissbrauch im Internet auswirken als erhofft.

46. Ferner erwartet die Kommission, dass die Zahl der Meldungen von sexuellem Kindesmissbrauch an die Strafverfolgungsbehörden mit der Verabschiedung der durch den Vorschlag eingeführten Aufdeckungspflichten steigen wird. [43] Allerdings wird weder in dem Vorschlag noch in der Folgenabschätzung erläutert, wie die Mängel des derzeitigen Stands der Dinge behoben werden sollen. Angesichts der begrenzten Ressourcen der Strafverfolgungsbehörden scheint es notwendig zu sein, besser zu verstehen, ob eine gesteigerte Zahl der Meldungen eine sinnvolle Auswirkung auf die Strafverfolgungsmaßnahmen gegen sexuellen Kindesmissbrauch haben würde. In jedem Fall möchten der EDSA und der EDSB betonen, dass solche Meldungen zeitnah bewertet werden sollten, um sicherzustellen, dass eine Entscheidung über die strafrechtliche Relevanz des gemeldeten Materials

[41] Laut dem Bericht über die Folgenabschätzung (Anhang II, S. 132) äußerten 85,71 % der befragten Strafverfolgungsbehörden ihre Besorgnis in Bezug auf die steigende Zahl von Fällen von sexuellem Kindesmissbrauch in den letzten zehn Jahren und den Mangel an Ressourcen (d. h. Personal und Technologie).
[42] Siehe auch Abschnitt 4.10 unten.
[43] Siehe unter anderem Anhang 3 des Berichts über die Folgenabschätzung (SWD(2022) 209 final), S. 176.

so früh wie möglich getroffen wird und um die Speicherung irrelevanter Daten so weit wie möglich zu begrenzen.

4.5.2 Keine weniger eingreifende Maßnahme

47. Vorausgesetzt, dass die von der Kommission angestrebten positiven Auswirkungen der Aufdeckung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern verwirklicht werden können, muss die Aufdeckung die am wenigsten eingreifende Maßnahme sein. In Artikel 4 des Vorschlags heißt es, dass Anbieter in einem ersten Schritt angemessene Risikominderungsmaßnahmen für die Nutzung ihres Dienstes zum Zwecke des sexuellen Kindesmissbrauchs im Internet erwägen sollten, um die Schwelle zu unterschreiten, die den Erlass einer Aufdeckungsanordnung rechtfertigt. Wenn es Risikominderungsmaßnahmen gibt, die zu einer erheblichen Verringerung des Umfangs der Kontaktaufnahme zu Kindern oder des Austauschs von Material über sexuellen Kindesmissbrauch innerhalb des betreffenden Dienstes führen kann, würden diese Maßnahmen im Vergleich zu einer Aufdeckungsanordnung oftmals weniger eingreifend sein.[44] Für den Fall, dass der betreffende Anbieter solche Maßnahmen nicht freiwillig ergreift, sollte die zuständige unabhängige Verwaltungsbehörde oder Justizbehörde die Möglichkeit haben, die Durchführung von Risikominderungsmaßnahmen verbindlich vorzuschreiben und durchzusetzen, anstatt eine Aufdeckungsanordnung zu erlassen. Nach Ansicht des EDSA und des EDSB ist die Tatsache, dass die Koordinierungsbehörde nach Artikel 5 Absatz 4 des Vorschlags in der Lage ist, den Anbieter „aufzufordern", Risikominderungsmaßnahmen einzuführen, zu überprüfen, einzustellen oder zu erweitern, nicht ausreichend, da eine solche Aufforderung nicht eigenständig durchsetzbar wäre; die Nichteinhaltung würde lediglich durch die Aufdeckungsanordnung „sanktioniert".

48. Daher sind der EDSA und der EDSB der Auffassung, dass die Koordinierungsbehörde oder die zuständige unabhängige Verwaltungsbehörde bzw. die Justizbehörde ausdrücklich ermächtigt werden sollte, weniger eingreifende Risikominderungsmaßnahmen vor oder anstelle einer Aufdeckungsanordnung anzuordnen.

4.5.3 Verhältnismäßigkeit im engeren Sinne

49. Damit eine Maßnahme dem in Artikel 52 Absatz 1 der Charta festgelegten Grundsatz der Verhältnismäßigkeit Genüge tut, sollten die sich aus der Maßnahme ergebenden Vorteile nicht durch die Nachteile aufgewogen werden, die die Maßnahme im Hinblick auf die Achtung der Ausübung von Grundrechten mit sich bringt. Daher „schränkt er [der Grundsatz der Verhältnismäßigkeit] die Behörden in der Ausübung ihrer Befugnisse ein, weil er ein Gleichgewicht zwischen den eingesetzten Mitteln und dem angestrebten Ziel (oder dem erreichten Ergebnis) verlangt".[45]

---

[44] So könnten beispielsweise Maßnahmen wie die Blockierung der Übertragung von Material über sexuellen Kindesmissbrauch aufseiten des Anbieters durch die Verhinderung des Hochladens und der Übermittlung von Inhalten der elektronischen Kommunikation in Erwägung gezogen werden, da sie in bestimmten Kontexten helfen könnten, die Verbreitung von bekanntem Material über sexuellen Kindesmissbrauch zu verhindern.

[45] Siehe Urteil des Gerichtshofs der Europäischen Union vom 8. Juli 2010, *Afton Chemical/Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, Rn. 45; Urteil des Gerichtshofs der Europäischen Union vom 9. November 2010, *Volker und Markus Schecke und Hartmut Eifert/Land Hessen*, verbundene Rechtssachen C-92/09 und C-93/09, ECLI:EU:C:2010:662, Rn. 74; Urteil des Gerichtshofs der Europäischen Union vom 23. Oktober 2012, *Nelson u. a.*, verbundene Rechtssachen C-581/10 und C-629/10, ECLI:EU:C:2012:657, Rn. 71; Urteil des Gerichtshofs der Europäischen Union vom 22. Januar 2013, *Sky Österreich*, C-283-11,

50. Zur Beurteilung der Auswirkungen einer Maßnahme auf die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten ist es besonders wichtig, Folgendes genau zu ermitteln: [46]

- den **Umfang der Maßnahme**, einschließlich der Anzahl der betroffenen Personen, ob sie „kollaterale Eingriffe" zur Folge hat, d. h. Eingriffe in die Privatsphäre von Personen, die eigentlich nicht Gegenstand der Maßnahme sind,
- die **Tragweite der Maßnahme**, einschließlich der Menge der erfassten Informationen, die zeitliche Dauer, ob die zu prüfende Maßnahme die Erhebung und Verarbeitung besonderer Datenkategorien erfordert,
- das **Ausmaß des Eingriffs** durch die Maßnahme unter Berücksichtigung: der Art der Tätigkeit, die Gegenstand der Maßnahme ist (ob sie Tätigkeiten betrifft, die unter die Geheimhaltungspflicht fallen oder nicht, Anwalt-Mandanten-Beziehung, medizinische Tätigkeit), des Kontextes, ob sie auf Profiling der betroffenen Personen hinausläuft oder nicht, ob die Verarbeitung die Nutzung eines (teilweise oder vollständig) automatisierten Entscheidungsfindungssystems mit einer „Fehlermarge" beinhaltet,
- ob sie **schutzbedürftige Personen** betrifft oder nicht,
- ob sie auch **andere Grundrechte** berührt (z. B. das Recht auf Freiheit der Meinungsäußerung, wie in den Rechtssachen *Digital Rights Ireland und Seitlinger u. a.* und *Tele2 Sverige und Watson*).[47]

51. In diesem Zusammenhang sei darauf hingewiesen, dass die Auswirkungen für die betroffene Person gering sein können, für das Kollektiv/die Gesellschaft insgesamt jedoch erheblich bzw. äußerst erheblich.[48]

52. Bei allen drei Arten von Aufdeckungsanordnungen (Aufdeckung von bekanntem Material über sexuellen Kindesmissbrauch, Aufdeckung von neuem Material über sexuellen Kindesmissbrauch, Aufdeckung der Kontaktaufnahme zu Kindern) beruhen die derzeit verfügbaren Technologien auf der automatisierten Verarbeitung der Inhaltsdaten aller betroffenen Nutzer. Die für die Analyse der Inhalte verwendeten Technologien sind oft komplex und erfordern in der Regel den Einsatz von KI. Infolgedessen ist das Verhalten dieser Technologie für den Nutzer des Dienstes möglicherweise nicht vollständig nachvollziehbar. Darüber hinaus ist bekannt, dass die derzeit verfügbaren Technologien, insbesondere diejenigen zur Aufdeckung von neuem Material über sexuellen Missbrauch oder der Kontaktaufnahme zu Kindern, relativ hohe Fehlerquoten aufweisen.[49] Darüber hinaus besteht das

---

ECLI:EU:C:2013:28, Rn. 50; Urteil des Gerichtshofs der Europäischen Union vom 17. Oktober 2013, *Schaible/Land Baden-Württemberg*, C-101/12, ECLI:EU:C:2013:661, Rn. 29. [45] Siehe auch EDSB, „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener einschränken: Ein Toolkit" (11. April 2017).

[46] Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19. Dezember 2019), S. 23.

[47] Siehe auch die Stellungnahme 7/2020 zum Vorschlag über eine vorübergehende Ausnahme von der Richtlinie 2002/58/EG zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet des Europäischen Datenschutzbeauftragten (10. November 2020), Rn. 9 ff.

[48] Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19. Dezember 2019), S. 20.

[49] Einzelheiten siehe oben, Abschnitt 4.5, und nachfolgend in Unterabschnitt 4.8.2.

Risiko, dass dem EU-Zentrum gemäß Artikel 12 Absatz 1 und Artikel 48 Absatz 1 des Vorschlags „potenzielle“ Darstellungen sexuellen Kindesmissbrauchs gemeldet werden.

53. Darüber hinaus können die allgemeinen Bedingungen für den Erlass einer Aufdeckungsanordnung im Rahmen des Vorschlags, z. B. die Anwendung auf einen gesamten Dienst und nicht nur auf ausgewählte Mitteilungen[50], die Geltungsdauer von bis zu 24 Monaten für bekannte oder neue Darstellungen sexuellen Kindesmissbrauchs bzw. zwölf Monaten für die Kontaktaufnahme zu Kindern[51] usw., in der Praxis zu einem sehr breiten Anwendungsbereich der Anordnung führen. Infolgedessen wäre die Überwachung in der Praxis eher allgemein und willkürlich und nicht zielgerichtet.

54. In Anbetracht dessen sind der EDSA und der EDSB auch besorgt über die mögliche abschreckende Wirkung für die Ausübung des Rechts auf Freiheit der Meinungsäußerung. Der EDSA und der EDSB weisen darauf hin, dass eine solche abschreckende Wirkung umso wahrscheinlicher ist, je unklarer die Rechtsvorschriften sind.

55. In Ermangelung der erforderlichen Spezifität, Präzision und Klarheit, um dem Erfordernis der Rechtssicherheit zu genügen,[52] und in Anbetracht des breiten Anwendungsbereichs, d. h. alle Anbieter einschlägiger Dienste der Informationsgesellschaft, die solche Dienste in der Union anbieten,[53] wird mit dem Vorschlag nicht sichergestellt, dass nur ein gezielter Ansatz zur Aufdeckung von Darstellungen sexuellen Kindesmissbrauchs und der Kontaktaufnahme zu Kindern tatsächlich erfolgt. Daher sind der EDSA und der EDSB der Ansicht, dass der Vorschlag in der Praxis die Grundlage für ein *faktisch* allgemeines und unterschiedsloses Durchsuchen des Inhalts praktisch aller Arten von elektronischer Kommunikation aller Nutzer in der EU/im EWR werden könnte. Dies kann dazu führen, dass Menschen davon absehen, legale Inhalte weiterzugeben, weil sie befürchten, dass sie aufgrund ihrer Handlung verfolgt werden könnten.

56. Vor diesem Hintergrund merken der EDSA und der EDSB an, dass verschiedene Maßnahmen zur Bekämpfung des sexuellen Kindesmissbrauchs im Internet unter Umständen unterschiedlich starke Grundrechtseingriffe darstellen. Vorab stellen der EDSA und der EDSB dazu fest, dass eine automatische Analyse von Sprache oder Texten im Hinblick auf die Erkennung möglicher Fälle der Kontaktaufnahme zu Kindern wahrscheinlich ein stärkerer Eingriff ist als der Abgleich von Bildern oder Videos auf der Grundlage von bereits bekannten Darstellungen des sexuellen Kindesmissbrauchs mit dem Ziel, die Verbreitung dieser Darstellungen aufzudecken. Außerdem sollte zwischen der Erkennung von „bekanntem Material über sexuellen Kindesmissbrauch“ und „neuem Material über sexuellen Kindesmissbrauch“ unterschieden werden. Zusätzlich sollte bei den Auswirkungen weiter unterschieden werden zwischen den Maßnahmen, die sich an die Anbieter von Hostingdiensten richten, und denen, die den Anbietern von interpersonellen Kommunikationsdiensten auferlegt werden.

[50] Siehe Artikel 7 Absatz 1 des Vorschlags.
[51] Siehe Artikel 7 Absatz 9 Unterabsatz 3 des Vorschlags.
[52] Vgl. Urteil des Gerichtshofs der Europäischen Union vom 13. März 1997, Kommission/Französische Republik, C-197/96, ECLI:EU:C:1997:155, Rn. 15.
[53] Siehe Artikel 1 Absatz 2 des Vorschlags.

4.5.4 Aufdeckung von bekanntem Material über sexuellen Kindesmissbrauch

57. Obwohl der Vorschlag laut Erwägungsgrund 4 „technologieneutral“ sein soll, werden sowohl die Wirksamkeit der vorgeschlagenen Aufdeckungsmaßnahmen als auch ihre Auswirkungen auf den Einzelnen stark von der Wahl der angewandten Technologie und den ausgewählten Indikatoren abhängen. Diese Tatsache wird von der Kommission in Anhang 8 des Berichts über die Folgenabschätzung[54] anerkannt und durch andere Studien bestätigt, z. B. die gezielte substituierende Folgenabschätzung des Wissenschaftlichen Dienstes des Europäischen Parlaments zum Vorschlag der Kommission über eine vorübergehende Ausnahme von der Datenschutzrichtlinie für elektronische Kommunikation zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet vom Februar 2021[55].

58. In Artikel 10 des Vorschlags wird eine Reihe von Anforderungen an die zu Aufdeckungszwecken einzusetzenden Technologien festgelegt, insbesondere in Bezug auf ihre Wirksamkeit, Zuverlässigkeit und den geringsten Eingriff in die Rechte der Nutzer auf Privat- und Familienleben, einschließlich der Vertraulichkeit der Kommunikation, sowie auf den Schutz personenbezogener Daten.

59. In diesem Zusammenhang stellen der EDSA und der EDSB fest, dass die einzigen Technologien, die derzeit in der Lage zu sein scheinen, diese Normen generell zu erfüllen, diejenigen sind, die zur Aufdeckung von bekanntem Material über sexuellen Kindesmissbrauch verwendet werden, d. h. Abgleichstechnologien, die sich auf eine Datenbank mit Hashwerten als Referenz stützen.

4.5.5 Aufdeckung von bisher unbekanntem Material über sexuellen Kindesmissbrauch

60. Die Bewertung der Maßnahmen, die auf die Aufdeckung von bisher unbekanntem (neuem) Material über sexuellen Kindesmissbrauch abzielen, lässt unterschiedliche Schlussfolgerungen hinsichtlich ihrer Wirksamkeit, Zuverlässigkeit und Begrenzung der Auswirkungen auf die Grundrechte auf Privatsphäre und Datenschutz zu.

61. Wie im Bericht über die Folgenabschätzung zu dem Vorschlag erläutert, gehören zu den Technologien, die derzeit für die Aufdeckung von bisher unbekanntem Material über sexuellen Kindesmissbrauch eingesetzt werden, Klassifikatoren und KI. Ein Klassifikator ist ein Algorithmus, der Daten durch Mustererkennung in gekennzeichnete Klassen oder Informationskategorien einteilt.[56] Daher liefern diese Technologien unterschiedliche Ergebnisse und haben unterschiedliche Auswirkungen in Bezug auf Genauigkeit und Wirksamkeit und führen zu unterschiedlichen Eingriffen. Gleichzeitig sind sie aber auch anfälliger für Fehler.

62. Die Technologien zur Aufdeckung von bisher bekanntem Material von sexuellem Kindesmissbrauch ähneln denen zur Aufdeckung der Kontaktaufnahme zu Kindern, da beide nicht auf einfachen Abgleichstechnologien, sondern auf Vorhersagemodellen unter Verwendung von KI-Technologien

---

[54] Vgl. die Informationen über die Falsch-Positiv-Raten in Anhang 8 des Berichts über die Folgenabschätzung (S. 279 ff.).

[55] Vgl. die Studie mit dem Titel „Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment“ (Vorschlag der Kommission über eine vorübergehende Ausnahme von der Datenschutzrichtlinie für elektronische Kommunikation zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet: eine gezielte substituierende Folgenabschätzung), Wissenschaftlicher Dienst des Europäischen Parlaments, Februar 2021, S. 14 f.

[56] Anhang 8 des Berichts über die Folgenabschätzung (S. 281).

beruhen. Der EDSA und der EDSB sind der Ansicht, dass bei der Aufdeckung von bisher unbekanntem Material über sexuellen Kindesmissbrauch ein hohes Maß an Vorsicht geboten ist, da ein Fehler des Systems schwerwiegende Folgen für die betroffenen Personen hätte, da sie automatisch als Personen gekennzeichnet würden, die möglicherweise eine sehr schwere Straftat begangen haben und ihre personenbezogenen Daten und Einzelheiten ihrer Kommunikation gemeldet würden.

63. Zweitens lassen die in der Literatur gefundenen Leistungsindikatoren, von denen einige in dem dem Vorschlag beigefügten Bericht über die Folgenabschätzung[57] hervorgehoben werden, nur sehr wenig Rückschlüsse auf die Bedingungen, die für ihre Berechnung verwendet wurden, und auf ihre Angemessenheit unter realen Bedingungen zu, was bedeutet, dass ihre Leistung in der realen Welt deutlich geringer sein könnte als erwartet, was zu einer geringeren Genauigkeit und einem höheren Prozentsatz an „falsch-positiven" Ergebnissen führt.

64. Drittens sollten die Leistungsindikatoren im spezifischen Kontext der Verwendung der jeweiligen Erkennungstools betrachtet werden und einen umfassenden Einblick in das Verhalten der Erkennungstools bieten. Bei der Anwendung von Algorithmen der künstlichen Intelligenz auf Bilder oder Texte ist gut dokumentiert, dass es zu Verzerrungen und Diskriminierung kommen kann, da bestimmte Bevölkerungsgruppen in den zum Trainieren des Algorithmus verwendeten Daten nicht repräsentiert sind. Diese Verzerrungen sollten ermittelt, gemessen und auf ein akzeptables Maß verringert werden, damit die Erkennungssysteme für die Gesellschaft als Ganzes wirklich von Nutzen sind.

65. Obwohl eine Studie über die für die Erkennung verwendeten Technologien durchgeführt wurde,[58] sind der EDSA und der EDSB der Ansicht, dass weitere Analysen erforderlich sind, um die Zuverlässigkeit der vorhandenen Instrumente zu bewerten. Bei dieser Analyse sollten erschöpfende Leistungsindikatoren zugrunde gelegt und die Auswirkungen möglicher Fehler unter realen Bedingungen für alle von dem Vorschlag betroffenen Personen bewertet werden.

66. Wie bereits erwähnt, haben der EDSA und der EDSB ernsthafte Zweifel daran, inwieweit die in Artikel 7 Absatz 6 des Vorschlags vorgesehenen Verfahrensgarantien ausreichen, um diese Risiken auszugleichen. Außerdem stellen sie – wie bereits erwähnt – fest, dass im Vorschlag abstrakte und vage Begriffe zur Beschreibung des akzeptablen Risikos verwendet werden (z. B. „beträchtlicher Umfang").

67. Der EDSA und der EDSB befürchten, dass diese weit gefassten und vagen Begriffe zu einem Mangel an Rechtssicherheit sowie zu starken Divergenzen bei der konkreten Umsetzung des Vorschlags in der Union führen werden, je nachdem, wie Begriffe wie „Wahrscheinlichkeit" und „beträchtlicher Umfang" von den Justiz- oder anderen unabhängigen Verwaltungsbehörden in den Mitgliedstaaten ausgelegt werden. Dieser Umstand ist auch deshalb bedenklich, weil die Bestimmungen über die Aufdeckungsanordnungen „Einschränkungen" des in Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation verankerten Grundsatzes der Vertraulichkeit darstellen werden. Daher müssen sie in der vorgeschlagenen Verordnung klarer und vorhersehbarer formuliert werden.

4.5.6 Aufdeckung der Kontaktaufnahme zu Kindern („Grooming")

68. Der EDSA und der EDSB stellen fest, dass die vorgeschlagenen Maßnahmen zur Aufdeckung der Kontaktaufnahme zu Kindern („Grooming"), die eine automatisierte Analyse von Sprache oder Text

[57] Anhang 8 des Berichts über die Folgenabschätzung, S. 281–283.
[58] Bericht über die Folgenabschätzung, S. 279 f.

umfassen, wahrscheinlich den stärksten Eingriff in die Rechte der Nutzer auf Privat- und Familienleben, einschließlich der Vertraulichkeit der Kommunikation, und auf den Schutz personenbezogener Daten darstellen werden.

69. Während die Aufdeckung von bekanntem oder sogar neuem Material über sexuellen Kindesmissbrauch auf die Analyse von Bildern und Videos beschränkt werden kann, würde sich die Aufdeckung der Kontaktaufnahme zu Kindern per Definition auf alle textbasierten (und möglicherweise akustischen) Mitteilungen erstrecken, die in den Anwendungsbereich einer Aufdeckungsanordnung fallen. Infolgedessen ist die Stärke des Eingriffs in die Vertraulichkeit der betroffenen Kommunikation viel größer.

70. Der EDSA und der EDSB sind der Ansicht, dass die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit nicht gewahrt sind, wenn textbasierte Mitteilungen, die über interpersonelle Kommunikationsdienste übermittelt werden, *faktisch* allgemein und willkürlich automatisiert analysiert werden, um die potenzielle Kontaktaufnahme zu Kindern aufzudecken. Selbst wenn die verwendete Technologie auf den Einsatz von Indikatoren beschränkt ist, sind der EDSA und der EDSB der Ansicht, dass der Einsatz einer solchen allgemeinen und willkürlichen Analyse übertrieben ist und sogar den Wesensgehalt des in Artikel 7 der Charta verankerten Grundrechts auf Privatsphäre berühren kann.

71. Wie bereits erwähnt, kann der Mangel an materiellen Schutzvorkehrungen im Zusammenhang mit den Maßnahmen zur Aufdeckung der Kontaktaufnahme zu Kindern nicht allein durch Verfahrensgarantien ausgeglichen werden. Darüber hinaus ist das Problem der mangelnden Rechtsklarheit und -sicherheit (z. B. die Verwendung vager juristischer Formulierungen wie „in beträchtlichem Umfang“) bei der automatisierten Analyse textbasierter persönlicher Mitteilungen noch gravierender als beim Abgleich von Bildmaterialien auf der Grundlage der Hashing-Technologie.

72. Ferner sind der EDSA und der EDSB der Ansicht, dass die abschreckende Wirkung auf die Freiheit der Meinungsäußerung besonders groß ist, wenn die Text-(oder Sprach-)Nachrichten von Einzelpersonen in großem Umfang durchsucht und analysiert werden. Der EDSA und der EDSB weisen darauf hin, dass eine solche abschreckende Wirkung umso schwerwiegender ist, je unklarer die Rechtsvorschriften sind.

73. Darüber hinaus ist, wie im Bericht über die Folgenabschätzung [59] und in der Studie des Wissenschaftlichen Dienstes des Europäischen Parlaments [60] dargelegt, die Genauigkeit von Technologien zur Aufdeckung der textbasierten Kontaktaufnahme zu Kindern viel niedriger als die Genauigkeit von Technologien zur Aufdeckung von Material über sexuellen Kindesmissbrauch.[61] Die Techniken zur Aufdeckung der Kontaktaufnahme zu Kindern sind so gestaltet, dass jeder Aspekt einer Konversation analysiert und mit einer Wahrscheinlichkeitsbewertung versehen wird. Daher halten der EDSA und der EDSB sie auch für fehleranfällig und anfällig für Missbrauch.

4.5.7 Schlussfolgerung zur Notwendigkeit und Verhältnismäßigkeit der geplanten Maßnahmen

74. Im Hinblick auf die Notwendigkeit und Verhältnismäßigkeit der geplanten Aufdeckungsmaßnahmen äußern der EDSA und der EDSB insbesondere Bedenken hinsichtlich der Maßnahmen, die zur

[59] Anhang 8 des Berichts über die Folgenabschätzung (S. 281–283).
[60] S. 15–18.
[61] Siehe Rn. 40 oben.

Aufdeckung von unbekanntem Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern (Grooming) vorgesehen sind, da sie aufgrund der potenziellen Gewährung des Zugriffs auf den Inhalt der Kommunikation in allgemeiner Form, ihres wahrscheinlichkeitsbasierten Charakters und der mit solchen Technologien verbundenen Fehlerquoten zu einem Eingriff in die Privatsphäre führen.

75. Zudem lässt sich aus der Rechtsprechung des EuGH ableiten, dass Maßnahmen, die den Behörden einen allgemeinen Zugriff auf den Inhalt einer Nachricht ermöglichen, eher als Eingriff in den Wesensgehalt der in Artikel 7 und 8 der Charta garantierten Rechte zu betrachten sind. Diese Überlegungen sind insbesondere im Hinblick auf die im Vorschlag vorgesehenen Maßnahmen zur Aufdeckung der Kontaktaufnahme zu Kindern relevant.

76. Der EDSA und der EDSB sind in jedem Fall der Ansicht, dass der Eingriff, der insbesondere durch die Maßnahmen zur Aufdeckung der Kontaktaufnahme zu Kindern entsteht, über das unbedingt notwendige und verhältnismäßige Maß hinausgeht. Diese Maßnahmen sollten daher aus dem Vorschlag gestrichen werden.

4.6 Meldepflichten

77. Der EDSA und der EDSB empfehlen, die Liste der speziellen Anforderungen an Meldungen in Artikel 13 des Vorschlags durch die Anforderung zu ergänzen, in die Meldung Informationen über die spezifische Technologie aufzunehmen, die es dem Anbieter ermöglicht hat, von den relevanten missbräuchlichen Inhalten Kenntnis zu erlangen, falls der Anbieter von dem potenziellen sexuellen Missbrauch von Kindern infolge von Maßnahmen zur Ausführung einer gemäß Artikel 7 des Vorschlags erlassenen Aufdeckungsanordnung Kenntnis erlangt hat.

4.7 Entfernungs- und Sperrpflichten

78. Eine der Maßnahmen, die in dem Vorschlag zur Minderung der Risiken der Verbreitung von Material über sexuellen Kindesmissbrauch vorgesehen ist, ist der Erlass von Entfernungs- und Sperranordnungen, wonach Anbieter dazu verpflichtet würden, Material über sexuellen Kindesmissbrauch im Internet zu entfernen oder den Zugang dazu zu sperren oder zu blockieren.[62]

79. Zwar sind die Auswirkungen von Entfernungsanordnungen auf den Datenschutz und den Schutz der Vertraulichkeit der Kommunikation eher begrenzt, aber der EDSA und der EDSB möchten allgemein daran erinnern, dass der übergreifende Grundsatz eingehalten werden muss, dass jede Maßnahme dieser Art so gezielt wie möglich sein sollte.

80. Gleichzeitig weisen der EDSA und der EDSB darauf hin, dass Anbieter von Internetzugangsdiensten nur dann Zugang zur genauen URL von Inhalten haben, wenn diese Inhalte im Klartext zur Verfügung gestellt werden. Jedes Mal, wenn Inhalte über HTTPS zugänglich gemacht werden, hat der Anbieter von Internetzugangsdiensten keinen Zugriff auf die genaue URL, es sei denn, er durchbricht die Verschlüsselung der Kommunikation. Daher haben der EDSA und der EDSB Zweifel an der Wirksamkeit von Sperrmaßnahmen und sind der Ansicht, dass es unverhältnismäßig wäre, von Anbietern von Internetzugangsdiensten zu verlangen, Online-Kommunikation zu entschlüsseln, um die Kommunikation in Bezug auf Material über sexuellen Kindesmissbrauch zu sperren.

[62] Artikel 14 und 16 des Vorschlags.

81. Darüber hinaus und ganz allgemein ist anzumerken, dass das Sperren des Zugriffs auf ein digitales Objekt ein Vorgang ist, der auf Netzwerkebene stattfindet und dessen Umsetzung sich im Falle mehrerer (möglicherweise ähnlicher und nicht identischer) Kopien desselben Objekts als unwirksam erweisen kann. Ferner kann sich ein solcher Vorgang als unverhältnismäßig erweisen, wenn die Sperrung andere, nicht illegale digitale Objekte betrifft, die auf demselben Server gespeichert sind, der durch Netzwerkbefehle (z. B. IP-Adresse oder DNS-Blacklisting) unzugänglich gemacht wurde. Außerdem sind nicht alle Ansätze zur Sperrung auf Netzwerkebene gleich wirksam und einige können mit einfachen technischen Kenntnissen leicht umgangen werden.

82. Schließlich sollten die Befugnisse von Koordinierungsbehörden in Bezug auf den Erlass von Sperranordnungen in dem Verordnungsvorschlag klargestellt werden. So geht aus dem derzeitigen Wortlaut von Artikel 16 Absatz 1 und Artikel 17 Absatz 1 nicht eindeutig hervor, ob die Koordinierungsbehörden befugt sind, Sperranordnungen zu erlassen oder ob sie den Erlass von Sperranordnungen lediglich beantragen.[63]

4.8 Einschlägige Technologien und Schutzvorkehrungen

4.8.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

83. Die im Vorschlag enthaltenen Anforderungen an die Technologien, die zur Aufdeckung von Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern eingesetzt werden sollen, scheinen nicht streng genug zu sein. Der EDSA und der EDSB haben insbesondere festgestellt, dass der Vorschlag – im Gegensatz zu den entsprechenden Bestimmungen in der Interims-Verordnung[64] – keinen ausdrücklichen Verweis auf den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen enthält und es nicht vorgesehen ist, dass Technologien, die zum Durchsuchen von Text in Mitteilungen verwendet werden, nicht in der Lage sein dürfen, den wesentlichen Inhalt der Kommunikation zu erschließen. In Artikel 10 Absatz 3 Buchstabe b des Vorschlags ist lediglich vorgesehen, dass mit den Technologien aus der einschlägigen Kommunikation nur die Informationen extrahiert werden können, die unbedingt notwendig sind. Dieser Standard scheint jedoch nicht streng genug zu sein, da es möglich sein könnte, aus dem Inhalt einer Kommunikation andere Informationen *zu erschließen*, ohne der Mitteilung als solcher Informationen zu *entnehmen*.

84. Daher empfehlen der EDSA und der EDSB, einen Erwägungsgrund in den Vorschlag aufzunehmen, in dem festgelegt wird, dass der in Artikel 25 der Verordnung (EU) 2016/679 festgelegte Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen für die in Artikel 10 des Vorschlags genannten Technologien von Rechts wegen gilt und daher im Rechtstext nicht wiederholt werden muss. Überdies sollte Artikel 10 Absatz 3 Buchstabe b geändert werden, um dafür Sorge zu tragen, dass nicht nur keine anderen Informationen extrahiert, sondern diese auch

[63] In Artikel 16 Absatz 1 des Vorschlags heißt es: „Die Koordinierungsbehörde am Niederlassungsort ist befugt, bei der zuständigen Justizbehörde des Mitgliedstaats, der sie benannt hat, oder einer anderen unabhängigen Verwaltungsbehörde dieses Mitgliedstaats den Erlass einer Sperranordnung zu beantragen, [...]“, und in Artikel 17 Absatz 1 heißt es: „Die Koordinierungsbehörde am Niederlassungsort erlässt die in Artikel 16 genannten Sperranordnungen [...]“ (eigene Hervorhebung).

[64] Artikel 3 Absatz 1 Buchstabe b der Interims-Verordnung.

nicht erschlossen werden können, wie es derzeit in Artikel 3 Absatz 1 Buchstabe b des Verordnungsvorschlags vorgesehen ist.

4.8.2 Zuverlässigkeit der Technologien

85. In dem Vorschlag wird davon ausgegangen, dass verschiedene Arten von technischen Lösungen von Diensteanbietern zur Ausführung von Aufdeckungsanordnungen verwendet werden können. Insbesondere wird im Vorschlag angenommen, dass Systeme der künstlichen Intelligenz für die Aufdeckung von unbekanntem Material über sexuellen Kindesmissbrauch und der Kontaktaufnahme zu Kindern verfügbar sind und funktionieren[65] und von einigen Koordinierungsbehörden als Stand der Technik angesehen werden könnten. Die Wirksamkeit des Vorschlags hängt von der Zuverlässigkeit dieser technischen Lösungen ab. Es liegen jedoch nur sehr wenige Informationen über die allgemeine und systematische Verwendung dieser Technologien vor, wodurch eine sorgfältige Prüfung gerechtfertigt ist.

86. Hinzu kommt, dass die Leistungsindikatoren für Erkennungstechnologien, die in dem Bericht über die Folgenabschätzung, der dem Vorschlag beigefügt ist, genannt wurden, kaum Informationen darüber enthalten, wie sie bewertet wurden und ob sie die tatsächliche Leistung der betreffenden Technologien widerspiegeln; der EDSA und der EDSB mussten diese Indikatoren mangels Alternativen bei ihrer Beurteilung der Verhältnismäßigkeit heranziehen. Es gibt keine Informationen über die Tests und Benchmarks, die von den Technologieanbietern zur Messung dieser Leistungen zugrunde gelegt wurden. Ohne diese Informationen ist es nicht möglich, die Tests zu wiederholen oder die Gültigkeit der Leistungsangaben zu bewerten. In diesem Zusammenhang ist anzumerken, dass die Leistungsindikatoren zwar so ausgelegt werden könnten, dass einige Erkennungstools eine hohe Genauigkeit aufweisen (z. B. liegt die Genauigkeit bestimmter Tools zur Aufdeckung der Kontaktaufnahme zu Kindern bei 88 %),[66] dass diese Indikatoren jedoch im Lichte des geplanten praktischen Einsatzes der Erkennungstools und der Schwere der Risiken, die eine falsche Bewertung von bestimmtem Material für die betroffene Person mit sich bringen würde, betrachtet werden sollten. Darüber hinaus sind der EDSA und der EDSB der Ansicht, dass bei einer solch risikoreichen Verarbeitung eine Fehlerquote von 12 % ein hohes Risiko für die betroffenen Personen darstellt, die von falsch positiven Ergebnissen betroffen sind, selbst wenn es Schutzvorkehrungen gibt, um falsche Meldungen an die Strafverfolgungsbehörden zu verhindern. Es ist überaus unwahrscheinlich, dass Diensteanbieter hinreichend Ressourcen bereitstellen können, um einen solchen Prozentsatz an falsch-positiven Ergebnissen zu überprüfen.

87. Wie bereits erwähnt,[67] sollten die Leistungsindikatoren einen umfassenden Einblick in das Verhalten der Erkennungstools liefern. Bei der Anwendung von Algorithmen der künstlichen Intelligenz auf Bilder oder Texte ist gut dokumentiert, dass es zu Verzerrungen und Diskriminierung kommen kann, da bestimmte Bevölkerungsgruppen in den zum Trainieren des Algorithmus verwendeten Daten nicht repräsentiert sind. Diese Verzerrungen sollten ermittelt, gemessen und auf ein akzeptables Maß verringert werden, damit die Erkennungssysteme für die Gesellschaft als Ganzes wirklich von Nutzen sind.

---

[65] Siehe Bericht über die Folgenabschätzung, S. 281–282.
[66] Ebd., S. 283.
[67] Siehe die Randnummern 63–64 oben.

88. Es wurde zwar eine Studie über die für die Erkennung verwendeten Technologien durchgeführt,[68] aber der EDSA und der EDSB sind der Auffassung, dass weitere Analysen erforderlich sind, um die Zuverlässigkeit der vorhandenen Instrumente in realen Anwendungsfällen unabhängig zu analysieren. Bei dieser Analyse sollten erschöpfende Leistungsindikatoren zugrunde gelegt und die Auswirkungen möglicher Fehler unter realen Bedingungen für alle von dem Vorschlag betroffenen Personen bewertet werden. Da diese Technologien die Grundlage des Vorschlags bilden, halten der EDSA und der EDSB diese Analyse für äußerst wichtig, um die Angemessenheit des Vorschlags zu beurteilen.

89. Der EDSA und der EDSB stellen zudem fest, dass der Vorschlag keine technologiespezifischen Anforderungen enthält, sei es in Bezug auf die Fehlerquoten, die Verwendung von Klassifikatoren und deren Validierung oder andere Einschränkungen. Damit bleibt es Aufgabe der Anwender, solche Kriterien zu entwickeln, wenn es darum geht, die Verhältnismäßigkeit des Einsatzes einer bestimmten Technologie zu beurteilen, was zu einem weiteren Mangel an Präzision und Klarheit beiträgt.

90. In Anbetracht der Bedeutung der Konsequenzen für die betroffenen Personen im Falle eines falsch-positiven Ergebnisses sind der EDSA und der EDSB der Ansicht, dass die Falsch-Positiv-Raten auf ein Mindestmaß reduziert werden müssen und dass diese Systeme unter Berücksichtigung der Tatsache weiterentwickelt werden müssen, dass die überwiegende Mehrheit der elektronischen Kommunikation weder Material über sexuellen Kindesmissbrauch noch eine Kontaktaufnahme zu Kindern umfasst und dass selbst eine sehr niedrige Falsch-Positiv-Rate angesichts der Menge der zu erfassenden Daten eine sehr hohe Anzahl von falsch-positiven Ergebnissen impliziert. Grundsätzlich befürchten der EDSA und der EDSB auch, dass die im Bericht über die Folgenabschätzung angegebene Leistung der verfügbaren Tools keine präzisen und vergleichbaren Indikatoren für die Falsch-Positiv- und Falsch-Negativ-Raten widerspiegelt, und sind der Ansicht, dass vergleichbare und aussagekräftige Leistungsindikatoren für diese Technologien herausgegeben werden sollten, bevor sie als verfügbar und wirksam gelten.

4.8.3 Durchsuchen von Audiokommunikation

91. Im Gegensatz zur Interims-Verordnung [69] wird das Durchsuchen von Audiokommunikation im Zusammenhang mit der Aufdeckung der Kontaktaufnahme zu Kindern im Vorschlag nicht vom Anwendungsbereich ausgeschlossen. [70] Der EDSA und der EDSB sind der Ansicht, dass das Durchsuchen von Audiokommunikation einen besonderen Eingriff darstellt, da üblicherweise ein aktives, laufendes „Echtzeit"-Abhören erforderlich wäre. Darüber hinaus wird die Vertraulichkeit des gesprochenen Wortes in einigen Mitgliedstaaten besonders geschützt.[71] Da im Prinzip der gesamte Inhalt der Audiokommunikation analysiert werden müsste, dürfte diese Maßnahme außerdem den Wesensgehalt der in Artikel 7 und Artikel 8 der Charta garantierten Rechte berühren. Daher sollte diese Aufdeckungsmethode nicht in den Anwendungsbereich der in der vorgeschlagenen Verordnung festgelegten Aufdeckungspflichten fallen, und zwar sowohl in Bezug auf Sprachnachrichten als auch auf Echtzeit-Kommunikation, zumal im Bericht über die Folgenabschätzung, der dem Vorschlag beigefügt ist, keine spezifischen Risiken oder Veränderungen in der Bedrohungslandschaft festgestellt wurden, die ihren Einsatz rechtfertigen würden.[72]

---

[68] Siehe Bericht über die Folgenabschätzung, S. 279 f.
[69] Vgl. Artikel 1 Absatz 2 der Interims-Verordnung.
[70] Vgl. Artikel 1 des Vorschlags.
[71] Siehe z. B. § 201 des deutschen Strafgesetzbuches.
[72] Siehe den Bericht über die Folgenabschätzung.

4.8.4 Altersüberprüfung

92. Die Anbieter werden durch den Vorschlag angeregt, Maßnahmen zur Altersüberprüfung und -beurteilung zu ergreifen, um minderjährige Nutzer ihrer Dienste zu identifizieren.[73] In diesem Zusammenhang stellen der EDSA und der EDSB fest, dass es derzeit keine technologische Lösung gibt, die in der Lage ist, das Alter eines Nutzers in einem Online-Kontext mit Sicherheit zu bestimmen, ohne sich auf eine offizielle digitale Identität zu stützen, die derzeit nicht für jede europäische Bürgerin bzw. jeden europäischen Bürger verfügbar ist.[74] Daher könnte der im Vorschlag vorgesehene Einsatz von Maßnahmen zur Altersüberprüfung möglicherweise dazu führen, dass z. B. jung aussehende Erwachsene vom Zugang zu Online-Diensten ausgeschlossen werden oder dass sehr aufdringliche Instrumente zur Altersüberprüfung eingesetzt werden, die die rechtmäßige Nutzung der betroffenen Dienste behindern oder die Nutzer davon abhalten könnten.

93. In diesem Zusammenhang und obwohl in Erwägungsgrund 16 des Vorschlags auf Instrumente der elterlichen Kontrolle als mögliche Risikominderungsmaßnahmen hingewiesen wird, empfehlen der EDSA und der EDSB, den Verordnungsvorschlag dahingehend zu ändern, dass es den Anbietern ausdrücklich gestattet wird, sich zusätzlich oder alternativ zur Altersüberprüfung auf Mechanismen der elterlichen Kontrolle zu verlassen.

4.9 Informationsbewahrung

94. In Artikel 22 des Vorschlags werden die Zwecke eingeschränkt, für die die Anbieter, die dem Vorschlag unterliegen, die Inhaltsdaten und sonstigen Daten, die in Verbindung mit den zur Einhaltung dieser Verordnung getroffenen Maßnahmen verarbeitet werden, aufbewahren dürfen. In dem Vorschlag wird jedoch darauf hingewiesen, dass die Anbieter die Informationen auch aufbewahren können, um bei der Ausführung einer erlassenen Aufdeckungsanordnung die Wirksamkeit und Genauigkeit der Technologien zur Aufdeckung des sexuellen Kindesmissbrauchs im Internet zu verbessern. Für diesen Zweck dürfen sie jedoch keine personenbezogenen Daten speichern.[75]

95. Der EDSA und der EDSB sind der Ansicht, dass nur die Anbieter, die ihre eigenen Erkennungstechnologien verwenden, die Möglichkeit haben sollten, Daten zur Verbesserung der Wirksamkeit und Genauigkeit der Technologien zu speichern, während diejenigen, die vom EU-Zentrum bereitgestellte Technologien verwenden, diese Möglichkeit nicht nutzen können sollten. Darüber hinaus weisen der EDSA und der EDSB darauf hin, dass es in der Praxis schwierig sein könnte, sicherzustellen, dass keine personenbezogenen Daten zu diesem Zweck gespeichert werden, da die meisten Inhaltsdaten und anderen Daten, die zu Erkennungszwecken verarbeitet werden, wahrscheinlich als personenbezogene Daten zu betrachten sind.

4.10 Auswirkungen auf die Verschlüsselung

96. Die europäischen Datenschutzbehörden haben sich stets für die generelle Verfügbarkeit von starken Verschlüsselungswerkzeugen und gegen jede Art von Hintertüren ausgesprochen.[76] Verschlüsselung

[73] Siehe Artikel 4 Absatz 3, Artikel 6 Absatz 1 Buchstabe c und Erwägungsgrund 16 des Vorschlags.
[74] Siehe CNIL, Empfehlung 7: Check the age of the child and parental consent while respecting the child's privacy (Alter des Kindes und die Einwilligung der Eltern überprüfen und dabei die Privatsphäre des Kindes wahren) (9. August 2021).
[75] Artikel 22 Absatz 1 des Vorschlags.
[76] Siehe z. B. Artikel-29-Datenschutzgruppe, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (Erklärung der nach

ist schließlich wichtig, um die Wahrnehmung aller Menschenrechte offline und online zu gewährleisten.[77] Zudem tragen Verschlüsselungstechnologien wesentlich zur Achtung sowohl des Privatlebens als auch der Vertraulichkeit der Kommunikation sowie zur Innovation und zum Wachstum der digitalen Wirtschaft bei, die auf dem hohen Maß an Vertrauen und Sicherheit beruhen, das diese Technologien bieten.

97. Im Zusammenhang mit der zwischenmenschlichen Kommunikation ist die Ende-zu-Ende-Verschlüsselung ein entscheidendes Instrument zur Sicherstellung der Vertraulichkeit der elektronischen Kommunikation, da sie starke technische Schutzvorkehrungen gegen den Zugriff auf den Inhalt der Kommunikation durch andere Personen als den Absender und den/die Empfänger, einschließlich des Anbieters, bietet. Würde die Nutzung der Ende-zu-Ende-Verschlüsselung in irgendeiner Weise verhindert oder erschwert oder würden Diensteanbieter verpflichtet, elektronische Kommunikationsdaten für andere Zwecke als die Erbringung ihrer Dienste zu verarbeiten oder elektronische Kommunikation proaktiv an Dritte weiterzuleiten, bestünde die Gefahr, dass Anbieter weniger verschlüsselte Dienste anbieten, um den Verpflichtungen besser nachkommen zu können, wodurch die Rolle der Verschlüsselung im Allgemeinen geschwächt und die Achtung der Grundrechte der europäischen Bürgerinnen und Bürger untergraben würde. Es sei darauf hingewiesen, dass die Ende-zu-Ende-Verschlüsselung zwar eine der am häufigsten verwendeten Sicherheitsmaßnahmen im Zusammenhang mit der elektronischen Kommunikation ist, dass aber auch andere technische Lösungen (z. B. die Verwendung anderer kryptografischer Verfahren) für die Sicherheit und den Schutz der Vertraulichkeit der digitalen Kommunikation ebenso wichtig sein oder werden können. Daher sollte ihre Verwendung weder verhindert noch erschwert werden.

98. Der Einsatz von Tools zum Abhören und Analysieren zwischenmenschlicher elektronischer Kommunikation steht im grundsätzlichen Widerspruch zur Ende-zu-Ende-Verschlüsselung, da letztere darauf abzielt, technisch zu gewährleisten, dass eine Kommunikation zwischen Sender und Empfänger vertraulich bleibt.

99. Selbst wenn in dem Vorschlag keine systematische Abhörverpflichtung für die Anbieter vorgesehen ist, dürfte die bloße Möglichkeit einer Aufdeckungsanordnung die technischen Entscheidungen der Anbieter stark beeinflussen, insbesondere angesichts des begrenzten Zeitrahmens, der ihnen für die Ausführung einer solchen Anordnung zur Verfügung steht, und der hohen Sanktionen, die sie bei Nichterfüllung zu erwarten hätten.[78] In der Praxis könnte dies dazu führen, dass bestimmte Anbieter die Ende-zu-Ende-Verschlüsselung nicht mehr nutzen.

100. Die Auswirkungen des Vorschlags, die die Nutzung der Ende-zu-Ende-Verschlüsselung beeinträchtigen oder davon abhalten könnten, müssen angemessen bewertet werden. Jede der Techniken zur Umgehung der datenschutzfreundlichen Merkmale der Ende-zu-Ende-Verschlüsselung, die in dem Bericht über die Folgenabschätzung zu dem Vorschlag vorgestellt wurden, würde Sicherheitslücken

---

Artikel 29 eingesetzten Datenschutzgruppe über Verschlüsselung und ihre Auswirkungen auf den Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten in der EU) (11. April 2018).

[77] Siehe Menschenrechtsrat, Resolution 47/16 über die Förderung, den Schutz und den Genuss der Menschenrechte im Internet, UN-Dok. A/HRC/RES/47/16 (26. Juli 2021).

[78] Vgl. Artikel 35 des Vorschlags.

schaffen. [79] So würde das Durchsuchen aufseiten der Anbieter [80] wahrscheinlich zu einem umfangreichen, ungezielten Zugriff auf unverschlüsselte Inhalte und deren Verarbeitung auf den Geräten der Endnutzer führen. Eine solche erhebliche Verschlechterung der Vertraulichkeit würde vor allem Kinder betreffen, da die von ihnen genutzten Dienste mit größerer Wahrscheinlichkeit von Aufdeckungsanordnungen betroffen sind und sie somit anfällig für Überwachung oder Abhörmaßnahmen sind. Gleichzeitig ist das *serverseitige* Durchsuchen auch grundsätzlich unvereinbar mit dem Modell der Ende-zu-Ende-Verschlüsselung, da der zwischen den Endnutzern verschlüsselte Kommunikationskanal aufgebrochen werden müsste, was zu einer Massenverarbeitung personenbezogener Daten auf den Servern der Anbieter führen würde.

101. Zwar heißt es in dem Vorschlag, dass „den betreffenden Anbietern mit dieser Verordnung die Wahl der zur Erfüllung der Aufdeckungsanordnungen zu betreibenden Technologien überlassen [wird], wobei dies nicht als Anreiz für die Nutzung bzw. Nichtnutzung einer bestimmten Technologie verstanden werden sollte“ [81] , doch wird die strukturelle Unvereinbarkeit einiger Aufdeckungsanordnungen mit der Ende-zu-Ende-Verschlüsselung in der Tat zu einem starken Anreiz für die Nichtnutzung der Ende-zu-Ende-Verschlüsselung führen. Die Unmöglichkeit des Zugangs zu und der Nutzung der Ende-zu-Ende-Verschlüsselung (die den derzeitigen Stand der Technik in Bezug auf die technische Gewährleistung der Vertraulichkeit darstellt) könnte eine abschreckende Wirkung auf die Freiheit der Meinungsäußerung und die legitime private Nutzung von elektronischen Kommunikationsdiensten haben. Die negative Beziehung zwischen der Aufdeckung von Material über sexuellen Kindesmissbrauch und der Ende-zu-Ende-Verschlüsselung wird auch von der Kommission anerkannt, da sie im Bericht über die Folgenabschätzung[82] auf die Wahrscheinlichkeit hinweist, dass die Einführung der Ende-zu-Ende-Verschlüsselung durch Facebook im Jahr 2023 dazu führen wird, dass das freiwillige Durchsuchen durch Facebook beendet wird.

102. Damit gewährleistet ist, dass die vorgeschlagene Verordnung nicht die Sicherheit oder Vertraulichkeit der elektronischen Kommunikation der europäischen Bürgerinnen und Bürger untergräbt, halten es der EDSA und der EDSB für erforderlich, dass im verfügenden Teil des Vorschlags (in einem der Artikel des Vorschlags) eindeutig festgelegt wird, dass nichts in der vorgeschlagenen Verordnung als Verbot oder Schwächung der Verschlüsselung ausgelegt werden sollte, wie es in Erwägungsgrund 25 der Interims-Verordnung steht.

4.11 Überwachung, Durchsetzung und Zusammenarbeit

4.11.1 Rolle der nationalen Aufsichtsbehörden im Rahmen der DSGVO

103. In dem Vorschlag ist die Einrichtung eines Netzwerks von nationalen Koordinierungsbehörden vorgesehen, die für die Anwendung und Durchsetzung der vorgeschlagenen Verordnung zuständig sind. [83] Zwar heißt es in Erwägungsgrund 54 des Vorschlags, dass die „in dieser Verordnung

[79] Siehe Abschnitt 4.2 in Abelson, Harold, Anderson, Ross J., Bellovin, Steven M., Benaloh, Josh, Blaze, Matt, Callas, John L., Diffie, Whitfield, Landau, Susan, Neumann, Peter G., Rivest, Ronald L., Schiller, Jeffrey I., Schneier, Bruce, Teague, Vanessa und Troncoso, Carmela: Bugs in our Pockets: The Risks of Client-Side Scanning (Wanzen in unseren Taschen: Risiken des Durchsuchens aufseiten der Anbieter). ArXiv abs/2110.07450 (2021).

[80] Das Durchsuchen aufseiten der Anbieter bezieht sich im weitesten Sinne auf Systeme, die den Inhalt von Nachrichten auf Übereinstimmungen mit einer Datenbank für unerwünschte Inhalte überprüfen, bevor die Nachricht an den vorgesehenen Empfänger übermittelt wird.

[81] Erwägungsgrund 26 des Vorschlags.

[82] Bericht über die Folgenabschätzung, S. 27.

[83] Erwägungsgrund 25 des Vorschlags.

enthaltenen Vorschriften über die Überwachung und Durchsetzung [...] nicht so verstanden werden [sollten], dass sie die Befugnisse und Zuständigkeiten der Datenschutzbehörden gemäß der Verordnung (EU) 2016/679 berühren“, doch sind der EDSA und der EDSB der Ansicht, dass das Verhältnis zwischen den Aufgaben der Koordinierungsbehörden und denen der Datenschutzbehörden besser geregelt werden sollte und dass den Datenschutzbehörden im Verordnungsvorschlag eine wichtigere Rolle zukommen sollte.

104. Insbesondere sollten die Anbieter verpflichtet werden, die Datenschutzbehörden im Rahmen eines Verfahrens der vorherigen Konsultation gemäß Artikel 36 der DSGVO zu konsultieren, bevor sie Maßnahmen zur Aufdeckung von Material über sexuellen Kindesmissbrauch oder der Kontaktaufnahme zu Kindern einsetzen, und zwar nicht ausschließlich in Verbindung mit der Verwendung von Maßnahmen zur Aufdeckung der Kontaktaufnahme zu Kindern, wie es im Vorschlag derzeit vorgesehen ist.[84] Alle Maßnahmen zur Aufdeckung sollten von vornherein als mit „hohem Risiko“ behaftet eingestuft werden und daher ein Verfahren der vorherigen Konsultation durchlaufen, unabhängig davon, ob sie die Kontaktaufnahme zu Kindern oder Material über sexuellen Kindesmissbrauch betreffen, wie es bereits in der Interims-Verordnung der Fall ist.[85] Außerdem sollten die im Rahmen der DSGVO benannten zuständigen Datenschutzbehörden jederzeit die Möglichkeit haben, sich zu den geplanten Aufdeckungsmaßnahmen zu äußern, und nicht nur unter bestimmten Bedingungen.[86]

105. Darüber hinaus sollte mit der vorgeschlagenen Verordnung ein System für die Behandlung und Beilegung von Meinungsverschiedenheiten zwischen den zuständigen Behörden und den Datenschutzbehörden in Bezug auf Aufdeckungsanordnungen eingeführt werden. Insbesondere sollten die Datenschutzbehörden berechtigt sein, eine Aufdeckungsanordnung vor den Gerichten des Mitgliedstaats anzufechten, in dem sich die zuständige Justizbehörde oder unabhängige Verwaltungsbehörde befindet, die die Aufdeckungsanordnung erlassen hat. In diesem Zusammenhang stellen der EDSA und der EDSB fest, dass nach der derzeitigen Fassung des Vorschlags die Stellungnahme der zuständigen Datenschutzbehörden von der zuständigen Behörde beim Erlass einer Aufdeckungsanordnung zurückgewiesen werden kann. Dies kann möglicherweise zu widersprüchlichen Entscheidungen führen, da die Datenschutzbehörden, wie in Artikel 36 Absatz 2 DSGVO bestätigt, das gesamte Spektrum ihrer Untersuchungsbefugnisse gemäß Artikel 58 DSGVO behalten würden, einschließlich der Befugnis, ein Verbot der Verarbeitung anzuordnen.

4.11.2 Rolle des EDSA

106. Der EDSA und der EDSB stellen fest, dass in Artikel 50 Absatz 1 Satz 3 des Vorschlags vorgesehen ist, dass „das EU-Zentrum [...] die Stellungnahme seines Technologieausschusses und des Europäischen Datenschutzausschusses“ einholt, bevor es bestimmte Technologien in die Liste der Technologien aufnimmt, die die Anbieter von Hostingdiensten und Anbieter interpersoneller Kommunikationsdienste in Betracht ziehen können, um Aufdeckungsanordnungen auszuführen. Ferner ist vorgesehen, dass der EDSA seine Stellungnahme innerhalb von acht Wochen abgibt. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit erforderlichenfalls um weitere sechs Wochen verlängert werden. Schließlich wird der EDSA verpflichtet, das EU-Zentrum innerhalb

[84] Artikel 7 Absatz 3 Unterabsatz 2 Buchstabe b des Vorschlags.
[85] Artikel 3 Absatz 1 Buchstabe c der Interims-Verordnung.
[86] Vgl. Artikel 7 Absatz 3 Unterabsatz 2 Buchstabe b des Vorschlags.

eines Monats nach Eingang des Antrags auf Konsultation zu informieren und die Gründe für die Verzögerung anzugeben.

107. Die bestehenden Aufgaben des EDSA sind in Artikel 70 DSGVO und Artikel 51 der Richtlinie (EU) 2016/680 (im Folgenden „JI-Richtlinie“)[87] festgelegt. Zu diesen Aufgaben gehört auch, dass der EDSA die Kommission berät und auf Ersuchen der Kommission, einer nationalen Aufsichtsbehörde oder ihres Vorsitzenden Stellungnahmen abgibt. In Artikel 1 Absatz 3 Buchstabe d des Vorschlags heißt es zwar, dass der Vorschlag die Vorschriften der DSGVO und der JI-Richtlinie unberührt lässt, aber die Befugnis des EU-Zentrums, Stellungnahmen des EDSA anzufordern, geht über die Aufgaben hinaus, die dem EDSA nach der DSGVO und der JI-Richtlinie übertragen wurden. Daher sollte in der vorgeschlagenen Verordnung – zumindest in einem Erwägungsgrund – klargestellt werden, dass das Mandat des EDSA durch den Vorschlag erweitert wird. In diesem Sinne begrüßen der EDSA und der EDSB die wichtige Rolle, die dem EDSA durch den Vorschlag zugewiesen wird, indem dessen Beteiligung an der praktischen Umsetzung der vorgeschlagenen Verordnung gefordert wird. In der Praxis spielt das Sekretariat des EDSA eine zentrale Rolle bei der Bereitstellung der analytischen, verwaltungstechnischen und logistischen Unterstützung, die für die Annahme der Stellungnahmen des EDSA erforderlich ist. Um sicherzustellen, dass der EDSA und seine Mitglieder ihre Aufgaben erfüllen können, ist es daher unerlässlich, dem EDSA ausreichende Finanzmittel und Personal zur Verfügung zu stellen. Bedauerlicherweise geht aus dem Finanzbogen des Vorschlags jedoch nicht hervor, dass zusätzliche Mittel für die Erfüllung der zusätzlichen Aufgaben, die dem EDSA mit dem Vorschlag zugewiesen werden, zur Verfügung gestellt werden.[88]

108. Ferner stellen der EDSA und der EDSB fest, dass in Artikel 50 des Vorschlags nicht angegeben wird, wie das EU-Zentrum nach Erhalt einer Stellungnahme des EDSA vorgehen wird.[89] In Erwägungsgrund 27 des Vorschlags heißt es lediglich, dass die Empfehlungen des EDSA vom EU-Zentrum und auch von der Kommission berücksichtigt werden sollten. Es sollte daher geklärt werden, welchem Zweck die angeforderte Stellungnahme im Rahmen des in Artikel 50 des Vorschlags vorgesehenen Verfahrens dienen soll und wie das EU-Zentrum nach Erhalt einer Stellungnahme des EDSA handeln soll.

109. Überdies sind der EDSA und der EDSB der Ansicht, dass in den Leitlinien des EDSA oder in einer möglichen Stellungnahme zum Einsatz von Erkennungstechnologien der Einsatz solcher Technologien zwar auf allgemeiner Ebene bewertet werden sollte, die nationale Aufsichtsbehörde jedoch für eine vorherige Konsultation gemäß Artikel 36 DSGVO die spezifischen Bedingungen berücksichtigen und eine Einzelfallprüfung der beabsichtigten Verarbeitung durch den jeweiligen Verantwortlichen durchführen muss. Der EDSA und der EDSB stellen fest, dass die Aufsichtsbehörden die in Artikel 36 DSGVO festgelegten Kriterien anwenden werden und sollten, um zu entscheiden, ob es notwendig ist, die in der DSGVO festgelegte Frist für die Abgabe ihrer Stellungnahmen im Anschluss an eine vorherige Konsultation zu verlängern, und dass keine Notwendigkeit besteht, andere Standards anzuwenden, wenn eine vorherige Konsultation den Einsatz einer Erkennungstechnologie betrifft.[90]

---

[87] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

[88] Vgl. Vorschlag, S. 105 f.

[89] Siehe im Gegensatz dazu Artikel 51 Absatz 4 der JI-Richtlinie.

[90] Vgl. Erwägungsgrund 24 des Vorschlags.

110. Schließlich ist in Artikel 11 („Leitlinien zu den Aufdeckungspflichten“) des Vorschlags vorgesehen, dass die Kommission Leitlinien für die Anwendung der Artikel 7 bis 10 des Vorschlags herausgeben kann. Artikel 11 des Vorschlags sollte geändert werden, um klarzustellen, dass neben den Koordinierungsbehörden und dem EU-Zentrum auch der EDSA von der Kommission außerhalb des vorgesehen öffentlichen Konsultationsverfahrens zu den Leitlinienentwürfen konsultiert werden sollte, bevor Leitlinien für die Aufdeckungspflichten erlassen werden.

111. Diese Aufgabe des EDSA sowie seine Rolle innerhalb des Rechtsrahmens, der durch den Vorschlag eingeführt würde, sollte daher vom Gesetzgeber weiter geprüft werden.

4.11.3 Rolle des EU-Zentrums für Fragen des sexuellen Kindesmissbrauchs

112. Mit Kapitel IV des Vorschlags wird das EU-Zentrum als neue dezentrale Agentur eingerichtet, um die Umsetzung des Vorschlags zu ermöglichen. Das EU-Zentrum soll unter anderem den Anbietern den Zugang zu zuverlässigen Erkennungstechnologien ermöglichen, Indikatoren zur Verfügung stellen, die auf der Grundlage von sexuellem Kindesmissbrauch im Internet erstellt und von Gerichten oder unabhängigen Verwaltungsbehörden der Mitgliedstaaten zum Zwecke der Aufdeckung überprüft wurden, auf Verlangen bestimmte Unterstützung bei der Durchführung von Risikobewertungen leisten und bei der Kommunikation mit den zuständigen nationalen Behörden unterstützen.[91]

113. In diesem Zusammenhang begrüßen der EDSA und der EDSB den Wortlaut von Artikel 77 Absatz 2 des Vorschlags, in dem bestätigt wird, dass die Verarbeitung personenbezogener Daten durch das EU-Zentrum der EU-DSVO unterliegt, und in dem vorgesehen ist, dass die Maßnahmen für die Anwendung dieser Verordnung durch das EU-Zentrum und insbesondere für die Bestellung eines Datenschutzbeauftragten des EU-Zentrums nach Anhörung des EDSB getroffen werden. Der EDSA und der EDSB sind jedoch der Meinung, dass mehrere Bestimmungen dieses Kapitels genauer geprüft werden sollten.

114. Erstens stellen der EDSA und der EDSB fest, dass es in Artikel 48 des Vorschlags heißt, dass alle Meldungen, die „nicht offensichtlich unbegründet sind“ [92], an die nationalen Strafverfolgungsbehörden und die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung („Europol“) weiterzuleiten sind. Diese Schwelle für die Weiterleitung von Meldungen an die nationalen Strafverfolgungsbehörden und Europol durch das EU-Zentrum („nicht offensichtlich unbegründet“) erscheint zu niedrig, insbesondere vor dem Hintergrund, dass der Zweck der Einrichtung des EU-Zentrums, wie im Bericht über die Folgenabschätzung der Kommission[93] dargelegt, darin besteht, die Belastung der Strafverfolgungsbehörden und von Europol durch die Filterung von fälschlicherweise als Material über sexuellen Kindesmissbrauch gekennzeichneten Inhalten zu verringern. In dieser Hinsicht ist es unklar, warum das EU-Zentrum als Kompetenzzentrum nicht eine gründlichere rechtliche und faktische Bewertung vornehmen kann, um das Risiko zu begrenzen, dass die Daten unschuldiger Personen an die Strafverfolgungsbehörden übermittelt werden.

115. Zweitens erscheint die Bestimmung über die Dauer der Speicherung personenbezogener Daten durch das EU-Zentrum angesichts der Sensibilität der betreffenden Daten unbestimmt. Selbst wenn es nicht

---

[91] Siehe COM(2022) 209 final, S. 7.

[92] Die Begriffe „offensichtlich unbegründet“ werden in Erwägungsgrund 65 des Vorschlags wie folgt beschrieben: „bei denen ohne eine inhaltliche, rechtliche oder faktische Analyse klar ersichtlich ist, dass es sich bei den gemeldeten Tätigkeiten nicht um einen sexuellen Kindesmissbrauch im Internet handelt.“

[93] Siehe z. B. S. 349 des Berichts über die Folgenabschätzung.

möglich wäre, eine maximale Speicherdauer für diese Daten festzulegen, empfehlen der EDSA und der EDSB, in dem Vorschlag zumindest eine maximale Frist für die Überprüfung der Notwendigkeit einer weiteren Speicherung von Daten festzulegen und eine Rechtfertigung für eine längere Speicherung nach Ablauf dieser Frist zu verlangen.

116. Angesichts der sehr hohen Sensibilität der vom EU-Zentrum zu verarbeitenden personenbezogenen Daten sind der EDSA und der EDSB zudem der Auffassung, dass die Verarbeitung zusätzlichen Schutzvorkehrungen unterliegen sollte, insbesondere um eine wirksame Aufsicht sicherzustellen. Dies könnte die Verpflichtung des EU-Zentrums einschließen, Protokolle für Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen in Bezug auf die Daten zu führen (also die Anforderung für operative personenbezogene Daten gemäß Kapitel IX der EU-DSVO widerzuspiegeln), einschließlich der Protokollierung der Eingabe, Änderung, des Zugriffs, der Abfrage, Weitergabe, Kombination und Löschung personenbezogener Daten. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge, die Identifizierung der Person, die die operativen personenbezogenen Daten abgefragt oder offengelegt hat, und so weit wie möglich die Identität des Empfängers festzustellen. Diese Protokolle würden zur Überprüfung der Rechtmäßigkeit der Verarbeitung, zur Selbstüberwachung und zur Sicherstellung der Integrität und Sicherheit verwendet und dem Datenschutzbeauftragten des EU-Zentrums und dem EDSB auf Anfrage zur Verfügung gestellt.

117. Darüber hinaus wird in dem Vorschlag auf die Verpflichtung der Anbieter verwiesen, die Nutzer über die Aufdeckung von Material über sexuellen Kindesmissbrauch im Rahmen von Aufdeckungsanordnungen sowie über ihr Recht, sich bei der Koordinierungsbehörde zu beschweren, zu informieren.[94] Allerdings ist in dem Vorschlag kein Verfahren für die Ausübung der Rechte der betroffenen Personen vorgesehen, auch nicht in Anbetracht der zahlreichen Orte, an die personenbezogene Daten im Rahmen des Vorschlags übermittelt bzw. wo sie gespeichert werden können (EU-Zentrum, Europol, nationale Strafverfolgungsbehörden). Die Verpflichtung, die Nutzer zu informieren, sollte auch die Verpflichtung umfassen, Einzelpersonen darüber zu informieren, dass ihre Daten an verschiedene Stellen (z. B. nationale Strafverfolgungsbehörden und Europol) weitergeleitet wurden und von ihnen verarbeitet werden. Darüber hinaus sollte es ein zentralisiertes Verfahren für die Entgegennahme und Koordinierung von Anträgen auf Auskunft, Berichtigung und Löschung geben oder alternativ eine Verpflichtung, dass die Stelle, die eine Betroffenenanfrage erhält, sich mit den anderen betreffenden Stellen abstimmt.

118. Der EDSA und der EDSB stellen fest, dass das EU-Zentrum gemäß Artikel 50 des Vorschlags die Liste der Technologien festlegen soll, die für die Ausführung von Aufdeckungsanordnungen verwendet werden können. Nach Artikel 12 Absatz 1 des Vorschlags sind die Anbieter jedoch verpflichtet, alle Informationen zu melden, die auf einen möglichen sexuellen Kindesmissbrauch im Internet hinweisen, und nicht nur diejenigen, die im Rahmen der Ausführung einer Aufdeckungsanordnung gewonnen wurden. Es ist sehr wahrscheinlich, dass ein erheblicher Teil dieser Informationen durch die Anwendung von Risikominderungsmaßnahmen der Anbieter gemäß Artikel 4 des Vorschlags ermittelt werden würde. Es scheint daher unerlässlich, zu ermitteln, wie diese Maßnahmen aussehen könnten, wie hoch die Fehlerquote bei der Meldung von potenziellen Darstellungen sexuellen Kindesmissbrauchs ist und welche Auswirkungen sie auf die Rechte und Freiheiten des Einzelnen hat. Obwohl in Artikel 4 Absatz 5 des Vorschlags vorgesehen ist, dass die Kommission in Zusammenarbeit mit den Koordinierungsbehörden und dem EU-Zentrum nach Durchführung einer öffentlichen

[94] Siehe Artikel 10 Absatz 6 und – nach Vorlage eines Berichts an das EU-Zentrum – Artikel 12 Absatz 2 des Vorschlags.

Konsultation entsprechende Leitlinien herausgeben kann, halten es der EDSA und der EDSB für wichtig, dass der Gesetzgeber in Artikel 50 das EU-Zentrum beauftragt, auch eine Liste empfohlener Risikominderungsmaßnahmen und einschlägiger bewährter Verfahren vorzulegen, die bei der Erkennung von potenziellem sexuellem Kindesmissbrauch im Internet besonders wirksam sind. Da solche Maßnahmen einen Eingriff in die Grundrechte auf Datenschutz und den Schutz der Privatsphäre darstellen können, wird dem EU-Zentrum nahegelegt, vor der Veröffentlichung einer solchen Liste die Stellungnahme des EDSA einzuholen.

119. Schließlich sollten die Sicherheitsanforderungen in Artikel 51 Absatz 4 des Vorschlags klargestellt werden. In diesem Zusammenhang können die Sicherheitsanforderungen anderer Verordnungen für Großsysteme mit risikoreicher Verarbeitung herangezogen werden, wie etwa die Verordnung (EG) Nr. 767/2008[95] (siehe Artikel 32), die Verordnung (EG) Nr. 1987/2006[96] (siehe Artikel 16), die Verordnung (EU) 2018/1862[97] (siehe Artikel 16) und die Verordnung (EU) Nr. 603/2013[98] (siehe Artikel 34).

4.11.4 Rolle von Europol

120. In dem Vorschlag ist eine enge Zusammenarbeit zwischen dem EU-Zentrum und Europol vorgesehen. Nach Kapitel IV des Vorschlags prüft das EU-Zentrum nach Eingang der Meldungen von Anbietern über mutmaßliche Darstellungen sexuellen Kindesmissbrauchs, welche Meldungen verfolgbar (nicht offensichtlich unbegründet) sind, und leitet sie an Europol sowie an die nationalen Strafverfolgungsbehörden weiter.[99] Das EU-Zentrum gewährt Europol Zugang zu seinen Datenbanken mit Indikatoren und Datenbanken mit Meldungen, um die Ermittlungen Europols in Bezug auf den sexuellen Kindesmissbrauch zu unterstützen.[100] Außerdem würde das EU-Zentrum den „größtmöglichen" Zugang zu den Informationssystemen von Europol erhalten.[101] Die beiden

[95] Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) (ABl. L 218 vom 13.8.2008, S. 60).
[96] Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 4).
[97] Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).
[98] Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von „Eurodac" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 180 vom 29.6.2013, S. 1).
[99] Siehe Artikel 48 des Vorschlags.
[100] Siehe Artikel 46 Absätze 4 und 5 des Vorschlags.
[101] Siehe Artikel 53 Absatz 2 des Vorschlags.

Agenturen werden auch Räumlichkeiten und bestimmte (nicht-operative) Infrastrukturen gemeinsam nutzen.[102]

121. Der EDSA und der EDSB stellen fest, dass mehrere Aspekte im Zusammenhang mit der Zusammenarbeit zwischen dem vorgeschlagenen EU-Zentrum und Europol Anlass zur Sorge geben oder einer weiteren Klarstellung bedürfen.

Weiterleitung von Meldungen durch das EU-Zentrum an Europol (Artikel 48)

122. Nach Artikel 48 der vorgeschlagenen Verordnung leitet das EU-Zentrum Meldungen, die nicht offensichtlich unbegründet sind, zusammen mit allen ihm zur Verfügung stehenden zusätzlichen einschlägigen Informationen an Europol und die zuständige(n) Strafverfolgungsbehörde(n) des Mitgliedstaats weiter, der voraussichtlich für die Untersuchung oder strafrechtliche Verfolgung des potenziellen sexuellen Kindesmissbrauchs rechtlich zuständig sein wird. In diesem Artikel wird zwar Europol die Aufgabe zugewiesen, die zuständige Strafverfolgungsbehörde zu ermitteln, wenn unklar ist, welcher Mitgliedstaat betroffen ist, allerdings ist in der Bestimmung auch vorgesehen, dass alle Meldungen an Europol übermittelt werden, unabhängig davon, ob die nationale Behörde ermittelt und die Meldung bereits von dem EU-Zentrum übermittelt wurde.

123. Aus dem Vorschlag geht jedoch nicht hervor, worin der zusätzliche Nutzen der Beteiligung von Europol besteht und welche Rolle Europol nach Erhalt der Meldungen spielen soll, insbesondere in den Fällen, in denen die nationale Strafverfolgungsbehörde festgestellt und parallel dazu benachrichtigt wurde.[103]

124. Der EDSA und der EDSB weisen darauf hin, dass das Mandat von Europol darauf beschränkt ist, die Maßnahmen der zuständigen Behörden der Mitgliedstaaten und ihre gegenseitige Zusammenarbeit bei der Verhütung und Bekämpfung der zwei oder mehr Mitgliedstaaten betreffenden schweren Kriminalität zu unterstützen.[104] Gemäß Artikel 19 der Verordnung (EU) 2016/794[105] in der durch die Verordnung (EU) 2022/991 geänderten Fassung[106] (im Folgenden „geänderte Europol-Verordnung“) ist eine Unionseinrichtung, die Informationen an Europol übermittelt, verpflichtet zu bestimmen, zu welchem Zweck oder welchen Zwecken diese Informationen von Europol verarbeitet werden dürfen, sowie die Bedingungen für die Verarbeitung festzulegen. Sie ist auch dafür verantwortlich, die Richtigkeit der übermittelten personenbezogenen Daten zu gewährleisten.[107]

---

[102] Dies gilt insbesondere für die Bereiche Personalverwaltung und Informationstechnologie (IT), einschließlich Cybersicherheit, sowie für das Gebäude und die Kommunikation.

[103] In Erwägungsgrund 71 des Vorschlags wird lediglich allgemein auf die Erfahrung bei der Ermittlung zuständiger nationaler Behörden in unklaren Situationen sowie seine Datenbank für kriminalpolizeiliche Erkenntnisse, dank derer Verbindungen zu Untersuchungen in anderen Mitgliedstaaten hergestellt werden können, verwiesen.

[104] Siehe Artikel 3 der geänderten Europol-Verordnung.

[105] Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI (ABl. L 135 vom 24.5.2016, S. 53).

[106] Verordnung (EU) 2022/991 des Europäischen Parlaments und des Rates vom 8. Juni 2022 zur Änderung der Verordnung (EU) 2016/794 in Bezug auf die Zusammenarbeit von Europol mit privaten Parteien, die Verarbeitung personenbezogener Daten durch Europol zur Unterstützung strafrechtlicher Ermittlungen und die Rolle von Europol in Forschung und Innovation (ABl. L 169 vom 27.6.2022, S. 1).

[107] Artikel 38 Absatz 2 Buchstabe a der geänderten Europol-Verordnung.

125. Eine pauschale Weiterleitung von Meldungen an Europol würde daher gegen die geänderte Europol-Verordnung verstoßen und wäre mit einer Reihe von Datenschutzrisiken verbunden. Die doppelte Verarbeitung personenbezogener Daten könnte dazu führen, dass mehrere Kopien derselben hochsensiblen personenbezogenen Daten parallel gespeichert werden (z. B. beim EU-Zentrum, bei Europol oder einer nationalen Strafverfolgungsbehörde), wodurch Risiken für die Datengenauigkeit infolge der möglichen mangelnden Synchronisierung der Datenbanken sowie für die Ausübung der Rechte der betroffenen Personen entstehen. Darüber hinaus impliziert die im Vorschlag festgelegte niedrige Schwelle für die Weiterleitung von Meldungen an die Strafverfolgungsbehörden (die „nicht offensichtlich unbegründet" sind) eine hohe Wahrscheinlichkeit, dass falsch-positive Meldungen (d. h. Inhalte, die fälschlicherweise als sexueller Kindesmissbrauch gekennzeichnet sind) in den Informationssystemen von Europol gespeichert werden, und zwar möglicherweise über längere Zeiträume.[108]

126. Der EDSA und der EDSB empfehlen daher, in dem Vorschlag die Umstände und Zwecke, unter denen das EU-Zentrum Meldungen an Europol weiterleiten könnte, im Einklang mit der geänderten Europol-Verordnung klarzustellen und einzuschränken. Dabei sollten ausdrücklich die Fälle ausgeschlossen werden, in denen Meldungen, die keine grenzüberschreitende Dimension aufweisen, an die zuständige Strafverfolgungsbehörde des Mitgliedstaats übermittelt wurden. Darüber hinaus sollte der Vorschlag die Anforderung enthalten, dass das EU-Zentrum nur personenbezogene Daten an Europol übermittelt, die angemessen und sachdienlich sind und sich auf das unbedingt erforderliche Maß beschränken. Es müssen zudem besondere Schutzvorkehrungen zur Gewährleistung der Datenqualität und -zuverlässigkeit vorgesehen werden.

[108] Dem Bericht über die Folgenabschätzung zufolge konnte Europol nur 20 % der 50 Mio. eindeutigen Darstellungen sexuellen Kindesmissbrauchs in seiner Datenbank prüfen, was bedeutet, dass es an Ressourcen mangelt, um die derzeit eingehenden Meldungen über sexuellen Kindesmissbrauch zu bearbeiten. Siehe Bericht über die Folgenabschätzung zum Vorschlag für eine Verordnung mit Vorschriften zur Verhütung und Bekämpfung sexuellen Missbrauchs von Kindern (SWD(2022) 209), S. 47–48.

Artikel 53 Absatz 2 über die Zusammenarbeit zwischen dem EU-Zentrum und Europol

127. Nach Artikel 53 Absatz 2 des Vorschlags gewähren Europol und das EU-Zentrum einander den größtmöglichen Zugang zu einschlägigen Informationen und Informationssystemen im Einklang mit den Rechtsakten der Union, die diesen Zugang regeln, soweit dies für die Erfüllung ihrer jeweiligen Aufgaben erforderlich ist.

128. In Artikel 46 Absätze 4 und 5 des Vorschlags ist ferner festgelegt, dass Europol Zugang zu den Datenbanken mit Indikatoren und den Datenbanken mit Meldungen erhält, und in Artikel 46 Absatz 6 wird das Verfahren für die Gewährung dieses Zugangs festgelegt. Europol übermittelt einen Antrag, in dem dessen Zweck und der für die Erreichung dieses Zwecks erforderliche Umfang des Zugangs angegeben sind, der dann vom EU-Zentrum sorgfältig geprüft wird.

129. Die Kriterien und Schutzvorkehrungen, die den Zugang von Europol zu den aus den Informationssystemen des EU-Zentrums gewonnenen Daten und deren anschließende Verwendung bestimmen, sind nicht festgelegt. Außerdem wird nicht erklärt, warum es erforderlich ist, Europol direkten Zugang zu den Informationssystemen einer Einrichtung zu gewähren, die keine Strafverfolgungsbehörde ist, die hochsensible personenbezogene Daten enthalten, bei denen möglicherweise keine Verbindung zu kriminellen Tätigkeiten und zur Verbrechensverhütung hergestellt wurde. Um ein hohes Datenschutzniveau und die Einhaltung des Grundsatzes der Zweckbindung zu gewährleisten, empfehlen der EDSA und der EDSB, dass die Übermittlung personenbezogener Daten von dem EU-Zentrum an Europol nur auf Einzelfallbasis nach einem ordnungsgemäß bewerteten Ersuchen über ein sicheres Kommunikationsinstrument wie SIENA[109] erfolgt.

130. Artikel 53 Absatz 2 enthält den einzigen Verweis im Vorschlag auf den Zugang des EU-Zentrums zu den Informationssystemen von Europol. Es ist daher nicht klar, zu welchen Zwecken und unter welchen besonderen Schutzvorkehrungen ein solcher Zugang erfolgen würde.

131. Der EDSA und der EDSB erinnern daran, dass Europol eine Strafverfolgungsbehörde ist, die gemäß den EU-Verträgen mit dem Hauptauftrag eingerichtet wurde, schwere Straftaten zu verhüten und zu bekämpfen. Die von Europol verarbeiteten operativen personenbezogenen Daten unterliegen daher strengen Datenverarbeitungsvorschriften und -garantien. Das vorgeschlagene EU-Zentrum ist keine Strafverfolgungsbehörde und sollte unter keinen Umständen direkten Zugang zu den Informationssystemen von Europol erhalten.

132. Der EDSA und der EDSB stellen ferner fest, dass ein großer Teil der Informationen, die für das EU-Zentrum und Europol von gemeinsamem Interesse sind, personenbezogene Daten in Bezug auf Opfer mutmaßlicher Straftaten, personenbezogene Daten in Bezug auf Minderjährige und personenbezogene Daten in Bezug auf das Sexualleben betreffen, die nach der geänderten Europol-Verordnung als besondere Kategorien personenbezogener Daten gelten. In der geänderten Europol-Verordnung sind strenge Vorgaben für den Zugang zu besonderen Kategorien personenbezogener Daten vorgesehen. In Artikel 30 Absatz 3 der geänderten Europol-Verordnung heißt es, dass allein Europol bzw. eine begrenzte Anzahl von Europol-Beamten, die vom Exekutivdirektor ordnungsgemäß ermächtigt wurden, unmittelbaren Zugriff auf diese personenbezogenen Daten hat.[110]

---

[109] Netzanwendung für sicheren Datenaustausch (Secure Information Exchange Network Application; SIENA).

[110] Nach der geänderten Europol-Verordnung sind Ausnahmen von diesem Verbot für die nach Titel V AEUV errichteten Agenturen der EU vorgesehen. In Anbetracht der Rechtsgrundlage des Vorschlags (Artikel 114 AEUV,

133. Der EDSA und der EDSB empfehlen daher, den Wortlaut von Artikel 53 Absatz 2 des Vorschlags klarzustellen, um die nach der geänderten Europol-Verordnung geltenden Beschränkungen korrekt wiederzugeben und die Modalitäten für den Zugang des EU-Zentrums festzulegen. Insbesondere sollte der Zugang zu personenbezogenen Daten, die in den Informationssystemen von Europol verarbeitet werden, nur auf Einzelfallbasis gewährt werden, wenn dies für die Erfüllung der Aufgabe des EU-Zentrums unbedingt erforderlich ist, und zwar auf ausdrückliches Ersuchen, in dem der spezifische Zweck und die Begründung enthalten sind. Europol sollte verpflichtet werden, diese Ersuchen sorgfältig zu prüfen und personenbezogene Daten nur dann an das EU-Zentrum zu übermitteln, wenn dies unbedingt erforderlich ist und in einem angemessenen Verhältnis zu dem beabsichtigten Zweck steht.

Artikel 10 Absatz 6 über die Rolle Europols bei der Unterrichtung der Nutzer infolge der Ausführung einer Aufdeckungsanordnung

134. Der EDSA und der EDSB begrüßen die in Artikel 10 Absatz 6 des Vorschlags enthaltene Anforderung an die Anbieter, die Nutzer darüber zu unterrichten, dass ihre personenbezogenen Daten von der Ausführung einer Aufdeckungsanordnung betroffen sein könnten. Diese Informationen werden den Nutzern erst dann zur Verfügung gestellt, nachdem Europol oder die nationale Strafverfolgungsbehörde eines Mitgliedstaats, die die Meldung gemäß Artikel 48 erhalten hat, bestätigt hat, dass die Information der Nutzer die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch nicht beeinträchtigen würde.

135. Es mangelt jedoch an Klarheit in Bezug auf die praktische Umsetzung dieser Bestimmung. Für den Fall, dass Meldungen sowohl an Europol als auch an eine Strafverfolgungsbehörde eines Mitgliedstaats weitergeleitet werden, wird in dem Vorschlag weder festgelegt, ob eine Bestätigung von einem oder beiden Empfängern erforderlich ist, noch werden die Verfahren bzw. Modalitäten für die Erlangung dieser Bestätigung in dem Vorschlag dargelegt (z. B. ob die Bestätigungen über das EU-Zentrum zu leiten sind). In Anbetracht der großen Menge an Material über sexuellen Kindesmissbrauch, die von Europol und den nationalen Strafverfolgungsbehörden verarbeitet werden könnte, und des Mangels an genauen Fristen für die Erteilung der Bestätigung („unverzüglich“) empfehlen der EDSA und der EDSB, die anwendbaren Verfahren zu klären, um die Verwirklichung dieser Schutzvorkehrung in der Praxis sicherzustellen. Außerdem sollten im Rahmen der Unterrichtungspflicht gegenüber den Nutzern auch Angaben zu den Empfängern der betreffenden personenbezogenen Daten gemacht werden.

Datenerfassung und Transparenzberichterstattung (Artikel 83)

136. In Artikel 83 Absatz 3 des Vorschlags ist vorgesehen, dass das EU-Zentrum Daten erfasst und Statistiken erstellt, die sich auf eine Reihe ihrer Aufgaben im Rahmen der vorgeschlagenen Verordnung beziehen. Zu Überwachungszwecken empfehlen der EDSA und der EDSB, dieser Liste Statistiken über die Anzahl der gemäß Artikel 48 an Europol weitergeleiteten Meldungen sowie über die Anzahl der bei Europol eingegangenen Auskunftsersuchen gemäß Artikel 46 Absätze 4 und 5, einschließlich der Anzahl der vom EU-Zentrum bewilligten und abgelehnten Ersuchen, beizufügen.

5. SCHLUSSFOLGERUNG

der sich auf die Harmonisierung des Binnenmarkts bezieht) würde diese Ausnahme jedoch nicht für das vorgeschlagene EU-Zentrum gelten.

137. Der EDSA und der EDSB begrüßen zwar die Bemühungen der Kommission, wirksame Maßnahmen gegen sexuellen Kindesmissbrauch im Internet sicherzustellen, sind jedoch der Ansicht, dass der Vorschlag ernsthafte Bedenken hinsichtlich des Datenschutzes und des Schutzes der Privatsphäre aufwirft. Daher fordern der EDSA und der EDSB die Mitgesetzgeber auf, den Verordnungsvorschlag zu ändern, um insbesondere sicherzustellen, dass die geplanten Aufdeckungspflichten den geltenden Standards im Hinblick auf Notwendigkeit und Verhältnismäßigkeit entsprechen und nicht zu einer Schwächung oder Verschlechterung der Verschlüsselung im Allgemeinen führen. Der EDSA und der EDSB stehen weiterhin zur Verfügung, um während des Gesetzgebungsverfahrens zu unterstützen, falls ihr Beitrag als notwendig erachtet wird, um die in dieser gemeinsamen Stellungnahme hervorgehobenen Bedenken auszuräumen.

Für den Europäischen Datenschutzbeauftragten	Für den Europäischen Datenschutzausschuss
Europäischer Datenschutzbeauftragter	Die Vorsitzende
(Wojciech Wiewiorowski)	(Andrea Jelinek)