



Brüssel, den 26. April 2023
(OR. en)

8787/23

LIMITE

JUR 291
ENFOPOL 201
JAI 510

GUTACHTEN DES JURISTISCHEN DIENSTES ¹

Absender:	Juristischer Dienst
Empfänger:	Gruppe „Strafverfolgung“
Betr.:	Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – Aufdeckungsanordnungen für interpersonelle Kommunikation – Artikel 7 und 8 der Charta der Grundrechte – Recht auf Privatleben und den Schutz personenbezogener Daten – Verhältnismäßigkeit

I. EINLEITUNG

1. Die Kommission hat am 11. Mai 2022 einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (im Folgenden „vorgeschlagene Verordnung“², vorgelegt. Ziel der vorgeschlagenen Verordnung ist es, einheitliche Vorschriften festzulegen, um im Binnenmarkt gegen die Nutzung von Diensten der Informationsgesellschaft für sexuellen Kindesmissbrauch im Internet vorzugehen.³ Rechtsgrundlage der vorgeschlagenen Verordnung ist Artikel 114 AEUV.

¹ Die in diesem Dokument enthaltene Rechtsberatung unterliegt dem Schutz nach Artikel 4 Absatz 2 der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission und ist vom Rat der Europäischen Union nicht für die Öffentlichkeit freigegeben worden. Der Rat behält sich vor, im Falle einer unerlaubten Veröffentlichung seine Rechte geltend zu machen.

² COM(2022) 209 final.

³ Artikel 1 Absatz 1 der vorgeschlagenen Verordnung.

2. Die vorgeschlagene Verordnung schafft Verpflichtungen für Anbieter von Diensten der Informationsgesellschaft, i) das Risiko einer Nutzung ihrer Dienste für den sexuellen Kindesmissbrauch im Internet zu bewerten, ii) **sexuellen Kindesmissbrauch im Internet aufzudecken und zu melden** und iii) Darstellungen sexuellen Kindesmissbrauchs in ihren Diensten zu entfernen oder den Zugang dazu zu sperren. Zudem werden Vorschriften in Bezug auf die Benennung und Arbeitsweise der zuständigen Behörden der Mitgliedstaaten, denen die Bekämpfung von sexuellem Kindesmissbrauch im Internet obliegt, sowie für die Zusammenarbeit zwischen diesen festgelegt. Schließlich wird eine neue EU-Agentur – das EU-Zentrum für die Verhütung und Bekämpfung sexuellen Kindesmissbrauchs – eingerichtet.
3. Im Zuge der Beratungen der Gruppe „Strafverfolgung“ wurden ernsthafte rechtliche Bedenken insbesondere hinsichtlich der **Aufdeckungsanordnungen an interpersonelle Kommunikationsdienste** geäußert.⁴
4. Der Juristische Dienst des Rates (JUR) ist ersucht worden, ein schriftliches Gutachten zu dieser Frage vorzulegen. Mit diesem Gutachten erfolgt eine rechtliche Prüfung der **Vereinbarkeit der Aufdeckungsanordnung an interpersonelle Kommunikationsdienste mit den Artikeln 7 und 8 der Charta der Grundrechte (im Folgenden „Charta“) in der Auslegung durch die einschlägige Rechtsprechung des EuGH.** Dabei wird von den mündlichen Ausführungen des Vertreters des Juristischen Dienstes des Rates in der Gruppe „Strafverfolgung“ ausgegangen; der Schwerpunkt liegt auf den diesbezüglich problematischen Aspekten der vorgeschlagenen Verordnung. Das vorliegende Gutachten berührt nicht die rechtliche Prüfung anderer Aspekte der vorgeschlagenen Verordnung, einschließlich insbesondere der Verpflichtungen aus der Aufdeckungsanordnung in Bezug auf *öffentlich zugängliches Material im Internet*.

II. RECHTLICHER RAHMEN

5. Die Aufdeckungspflichten und das Verfahren betreffend den Erlass von Aufdeckungsanordnungen finden sich in Abschnitt 2, Artikel 7 bis 11 der vorgeschlagenen Verordnung. Artikel 44 der vorgeschlagenen Verordnung über die Rolle des EU-Zentrums (der neuen EU-Agentur) beim Errichten, Pflegen und Betreiben von „*Datenbanken mit Indikatoren*“ ist für die vorliegende Analyse ebenfalls von Bedeutung. Die für die Zwecke der vorliegenden Analyse relevanten Aspekte dieser Bestimmungen lassen sich wie folgt zusammenfassen:

⁴ Die Aufdeckungsanordnungen für im Web öffentlich zugängliches Material sowie die Entfernungsanordnungen, Sperranordnungen und Streichungsanordnungen wurden als weniger problematisch erachtet als die Aufdeckungsanordnungen für interpersonelle Kommunikation.

6. Eine **Aufdeckungsanordnung** kann von einer nationalen Justizbehörde oder unabhängigen Verwaltungsbehörde auf Antrag einer Koordinierungsbehörde (der Behörde, die von einem Mitgliedstaat für die Anwendung und Durchsetzung der vorgeschlagenen Verordnung benannt worden ist) erlassen werden, um einen Diensteanbieter aufzufordern, sexuellen Kindesmissbrauch im Internet aufzudecken. Die Aufdeckungsanordnung sollte den spezifischen Dienst angeben, für den die Aufdeckungsanordnung erlassen wird, und gegebenenfalls den betreffenden Teil oder Aspekt desselben (Artikel 8 Absatz 1 Buchstabe d).
7. Zu den Diensten der Informationsgesellschaft, für die die vorgeschlagene Verordnung gelten soll, gehören **interpersonelle Kommunikationsdienste**⁵.
8. Die Diensteanbieter, an die eine Aufdeckungsanordnung gerichtet ist, wären verpflichtet, bereits **bekannte** Darstellungen sexuellen Kindesmissbrauchs, noch **unbekannte** Darstellungen sexuellen Kindesmissbrauchs und **Kontaktaufnahme zu Kindern** aufzudecken. Die Aufdeckungsanordnungen betreffend die Kontaktaufnahme zu Kindern würden für die interpersonelle Kommunikation nur gelten, wenn es sich bei einem der Nutzer um einen minderjährigen Nutzer handelt (Artikel 7 Absatz 8).
9. Eine Aufdeckungsanordnung kann erlassen werden, wenn die Behörde, die sie erlässt, der Ansicht ist, dass die Bedingungen gemäß Artikel 7 Absatz 4 der vorgeschlagenen Verordnung erfüllt sind. Sie wäre **an einen spezifischen Dienst gerichtet**, wenn „*Beweise für ein erhebliches Risiko*“ vorliegen, „*dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet [...] genutzt wird*“ und wenn eine solche Anordnung als verhältnismäßig angesehen würde.⁶ Sie würde die Kommunikationsvorgänge aller Nutzer dieses Dienstes betreffen. Die endgültige Bewertung der „Beweise“, des „erheblichen Risikos“ und der Verhältnismäßigkeit einer Anordnung läge bei der zuständigen nationalen Justizbehörde oder der unabhängigen Verwaltungsbehörde, die die Anordnung erlässt.

⁵ Artikel 2 der vorgeschlagenen Verordnung.

⁶ Artikel 7 Absatz 4 der vorgeschlagenen Verordnung.

10. Die Darstellungen sexuellen Kindesmissbrauchs müssten vom Diensteanbieter durch die **Installation und den Betrieb von Technologien** aufgedeckt werden, mit denen die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern erkannt werden kann; dies würde mithilfe der entsprechenden vom EU-Zentrum bereitgestellten Indikatoren erfolgen. Aufdeckung würde bedeuten, dass der Inhalt aller Kommunikationsvorgänge abgerufen und gescannt werden müsste; dies würde mittels verfügbarer automatisierter Instrumente erfolgen, deren genaue Beschaffenheit im Vorschlag nicht festgelegt wurde, da die Technologieneutralität der Verordnung gewahrt werden soll.⁷
11. Gemäß der vorgeschlagenen Verordnung gilt für die Technologien Folgendes: i) Sie tragen wirksam zur Erkennung der Verbreitung derartigen Materials bei; ii) mit ihnen können aus der einschlägigen Kommunikation nur die Informationen extrahiert werden, die unbedingt notwendig sind, um derartiges Material aufzudecken; iii) sie beruhen auf der Verwendung der Indikatoren entsprechend dem neuesten Stand der Technik in der Branche und den am wenigsten in die Rechte der Nutzer auf Privatleben und Datenschutz eingreifenden Maßnahmen, und iv) sie sind hinreichend zuverlässig (sodass die Fehlerquote bei der Erkennung soweit wie möglich minimiert wird). Die Technologien müssten vom EU-Zentrum zur Verfügung gestellt (aber nicht konzipiert) werden. Jedoch wären, solange die in der Verordnung festgelegten Anforderungen erfüllt sind, Diensteanbieter nicht zur Nutzung bestimmter – einschließlich der vom EU-Zentrum zur Verfügung gestellten – Technologien verpflichtet. Zudem würde die Verantwortung in Bezug auf die Einhaltung dieser Anforderungen und für etwaige Entscheidungen, die im Zusammenhang mit oder infolge der Nutzung der vom EU-Zentrum zur Verfügung gestellten Technologien zu treffen sind, beim Diensteanbieter liegen.⁸
12. Die Technologien zur Erkennung müssten auf den „*Indikatoren*“ für bekannte Darstellungen sexuellen Kindesmissbrauchs, für unbekannte Darstellungen sexuellen Kindesmissbrauchs und für Kontaktaufnahme zu Kindern beruhen, die vom EU-Zentrum bereitgestellt werden. Zwei Arten von Instrumenten müssten eingesetzt werden. Für alle Arten der Aufdeckung wären die entsprechenden Diensteanbieter gezwungen, **Instrumente zur Prüfung von Inhalten** einzusetzen, um alle Inhalte auf das Vorhandensein von bekannten und unbekannten Darstellungen sexuellen Kindesmissbrauchs zu prüfen. Zudem müssten sie für die Aufdeckung von Kontaktaufnahme mit Kindern (nicht näher beschriebene) **Instrumente zur Prüfung des Alters** einsetzen, um zwischen erwachsenen und minderjährigen Nutzern zu unterscheiden.⁹

⁷ Artikel 10 und 46 der vorgeschlagenen Verordnung.

⁸ Artikel 10 Absätze 2 und 3 und Artikel 50 der vorgeschlagenen Verordnung.

⁹ Artikel 7, 10 und 44 der vorgeschlagenen Verordnung.

13. Die Geltungsdauer der Aufdeckungsanordnungen bliebe „auf das unbedingt erforderliche Maß beschränkt“, sollte jedoch bei Aufdeckungsanordnungen betreffend die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs bzw. die Kontaktaufnahme zu Kindern 24 bzw. 12 Monate nicht überschreiten.¹⁰

III. RECHTLICHE PRÜFUNG

14. Gemäß Artikel 52 Absatz 1 der Charta muss – hinsichtlich des Anwendungsbereichs und der Tragweite der darin garantierten Rechte – jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Europäischen Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.
15. Wie in den Unterabschnitten 2 und 3 näher erläutert wird, besteht kein Zweifel daran, dass mit der Aufdeckungsanordnung für interpersonelle Kommunikation einerseits eine dem Gemeinwohl dienende Zielsetzung verfolgt wird, andererseits jedoch das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten erheblich eingeschränkt wird. Die wichtigsten rechtlichen Bedenken betreffend die Einhaltung der Charta in der Auslegung durch die Rechtsprechung des Gerichtshofs erwachsen aus der Frage, ob diese Einschränkungen in ausreichendem Maße gesetzlich geregelt sind, den Wesensgehalt dieser Grundrechte beeinträchtigen und im Hinblick auf das verfolgte Ziel verhältnismäßig sind. In den Unterabschnitten 1, 4 und 5 im Folgenden werden diese Aspekte näher ausgeführt.

¹⁰ Artikel 7 Absatz 8 Buchstabe c und Absatz 9 der vorgeschlagenen Verordnung.

1. Die Einschränkungen der Grundrechte müssen gesetzlich vorgesehen sein

16. Nach ständiger Rechtsprechung sowohl des EGMR als auch des EuGH¹¹ bedeutet das Erfordernis einer *gesetzlichen Grundlage* für jede Einschränkung der Ausübung der Grundrechte, dass der Rechtsakt, der den Eingriff in diese Rechte ermöglicht, den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss. Daher bezieht sich ein solches Erfordernis nicht nur darauf, dass es eine „gesetzliche“ Grundlage geben muss – was im vorliegenden Fall nicht in Frage steht –, sondern es bedeutet auch, dass der Rechtsakt, der den Eingriff in diese Rechte ermöglicht, den Umfang der Einschränkung selbst klar und präzise festlegen muss. Die fragliche Maßnahme muss zugänglich und vorhersehbar sein und echte gerichtliche Kontrolle ermöglichen, wobei dies nicht ausschließt, dass die fragliche Einschränkung hinreichend offen formuliert ist, um Anpassungen an verschiedene Fallgruppen und an Änderungen der Lage zu erlauben.¹²
17. Die Erfordernisse der Klarheit, Genauigkeit und Vollständigkeit sind angesichts des Ausmaßes und der Schwere des Eingriffs in die Grundrechte, der durch die Regelungen der Aufdeckungsanordnungen für interpersonelle Kommunikation verursacht würde, im Hinblick auf die vorliegende Verordnung umso relevanter. Angesichts der Tragweite des Eingriffs in Grundrechte wäre eine gerichtliche Prüfung durch den Gerichtshof durchaus strikt und bliebe nicht auf offensichtliche Fehler beschränkt, wodurch der Ermessensspielraum des Unionsgesetzgebers verringert würde.¹³ Diese Intensität der gerichtlichen Prüfung verstärkt die Bedeutung klarer, genauer und vollständiger gesetzlicher Bestimmungen im Sinne eines rechtlich fundierten Ansatzes.

¹¹ Siehe Urteil des EGMR vom 25. Mai 2021, Big Brother Watch u. a. gegen United Kingdom, CE:ECHR:2021:0525JUD005817013, Rn. 333 und die dort angeführte Rechtsprechung. Siehe. u. a. Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 175 und die dort angeführte Rechtsprechung.

¹² Siehe Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, Rn. 114.

¹³ Siehe Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 47 und 48 und die dort angeführte Rechtsprechung.

18. Zudem handelt es sich bei dieser Maßnahme um eine Verordnung, die „*unmittelbar in jedem Mitgliedstaat gilt*“¹⁴ und im Gegensatz zu einer Richtlinie grundsätzlich nicht den Erlass von Maßnahmen zur *Umsetzung* der Verpflichtungen zur Aufdeckungsanordnung für interpersonelle Kommunikation in einzelstaatliches Recht erfordert. Dies bedeutet, dass im Falle einer gerichtlichen Prüfung die Einhaltung der Grundrechte bei der Regelung der Aufdeckungsanordnungen im Einzelfall auf der Grundlage der Klarheit und Genauigkeit, wie vom Unionsgesetzgeber festgelegt, beurteilt werden müsste. Bei der Anwendung des Grundsatzes der konformen Auslegung wäre es im Fall dieser Rechte nicht möglich, sich auf den Beurteilungsspielraum der Mitgliedstaaten der bei der Umsetzung einer Richtlinie zu berufen.¹⁵
19. Daher ist zunächst darauf hinzuweisen, dass die vorgeschlagene Verordnung ein umfassendes Regelwerk enthält, das insbesondere die Risikobewertung, die Risikominderung, die Risikoberichte und den Erlass von Aufdeckungsanordnungen durch Justizbehörden oder unabhängige Verwaltungsbehörden betrifft, wobei dies wesentliche Elemente sind, aus denen zu schließen wäre, dass das erste Erfordernis gemäß Artikel 52 der Charta erfüllt ist.
20. Dieser Schluss ist jedoch in zwei wichtigen Aspekten nicht haltbar; diese sind einerseits die Schlüsselrolle und die Auswirkungen der Technologie bei der Einschränkung der betreffenden Grundrechte, andererseits das Fehlen einer Definition der wichtigsten Bedingungen für den Erlass einer Aufdeckungsanordnung.
21. Hinsichtlich des **ersten** Aspekts, betreffend die Technologie, besteht – Artikel 7 Absatz 1 und Artikel 10 Absatz 1 der vorgeschlagenen Verordnung zusammengefasst – im Wesentlichen darin, dass einem spezifischen Diensteanbieter die Verpflichtung auferlegt wird, eine Technologie zu installieren und zu betreiben, mit der Darstellungen sexuellen Kindesmissbrauchs erkannt werden können. Dennoch sind in Artikel 7 Absätze 1, 3, Buchstabe a, und 8, Artikel 10 Absätze 2 und 3, und Artikel 44 der vorgeschlagenen Verordnung die Beschaffenheit und die Merkmale der Technologien, die zu diesem Zweck zur Verfügung gestellt werden müssen, nicht hinreichend detailliert festgelegt.

¹⁴ Artikel 288 AEUV.

¹⁵ Siehe Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, Rn. 87 bis 89, in dem sich der Gerichtshof für die Bewertung der Rechtmäßigkeit der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. L 119 vom 4.5.2016, S. 132) bei der Anwendung des Grundsatzes der konformen Auslegung ebenfalls auf den Beurteilungsspielraum der Mitgliedstaaten bei der Umsetzung der Richtlinie berief.

22. Insbesondere ist nicht näher ausgeführt, was unter „*hinreichend zuverlässigen Erkennungstechnologien*“ zu verstehen ist, und was die „*Fehlerquote*“ bei der Erkennung wäre, die im Hinblick auf ein ausgewogenes Verhältnis zwischen „*Wirksamkeit*“ und der Notwendigkeit, die „*am wenigsten eingreifenden Maßnahmen*“ zu treffen, akzeptabel wäre. Zudem sollen die „*Indikatoren*“, die zur Aufdeckung bekannter Darstellungen sexuellen Kindesmissbrauchs, unbekannter Darstellungen sexuellen Kindesmissbrauchs und von Kontaktaufnahme zu Kindern eingesetzt werden sollen, vom EU-Zentrum zu einem späteren Zeitpunkt erarbeitet und bereitgestellt werden. Gleiches gilt für die nicht näher beschriebenen Instrumente, die erforderlich sind, um bei der Aufdeckung von Kontaktaufnahme zu Kindern zwischen erwachsenen und minderjährigen Nutzern zu unterscheiden (Instrumente zur Prüfung des Alters). In diesem Zusammenhang wird das Erfordernis der Einhaltung der Grundrechte nicht im Rechtsakt selbst festgelegt sondern weitgehend dem Diensteanbieter überlassen, der für die Wahl der Technologie und die mit dem Betreiben der Technologie verbundenen Konsequenzen verantwortlich bleibt.¹⁶
23. Um nur ein Beispiel zu nennen: Die Wahl der Technologie zur Prüfung des Alters (Mass Profiling und/oder biometrische Identifizierung und oder digitale Identitätszertifikate) könnte sich erheblich auf den Umfang des Eingriffs durch das System auswirken; daher würde dies die gesamte weitere Bewertung der Vereinbarkeit der Regelungen der Aufdeckungsanordnungen mit der Charta stark beeinflussen.
24. Hinsichtlich des **zweiten** Aspekts, betreffend die Bedingungen für den Erlass einer Aufdeckungsanordnung, ist, wenngleich gemäß Artikel 7 bestimmte Erfordernisse im Detail festgelegt sind, in der vorgeschlagenen Verordnung die Methode, mit der das Risiko, dass ein spezifischer Dienst zum Zwecke des sexuellen Kindesmissbrauchs genutzt wird, bewertet werden soll, oder ein sinnvoller Schwellenwert für das Niveau des Risikos, bei dem die Einführung einer Aufdeckungsanordnung gerechtfertigt wäre, nicht festgelegt. In Artikel 7 Absätze 4 bis 7 wird auf die Konzepte des „*erheblichen Risikos*“, der „*negativen Folgen für die Rechte und berechtigten Interessen*“ der Nutzer, eines „*angemessenen Gleichgewichts zwischen den Grundrechten*“, der „*Risikominderungsmaßnahmen*“ oder der „*potenziellen Folgen*“ für alle Beteiligten hingewiesen. Je nachdem, ob die Aufdeckungsanordnung bekannte oder unbekannte Darstellungen sexuellen Kindesmissbrauchs oder Kontaktaufnahme zu Kindern betrifft, werden diese Konzepte ihrerseits weiter definiert, indem auf weitere nicht hinlänglich genaue Konzepte verwiesen wird, wie auf die Verwendung von Diensten oder vergleichbarer Dienste „*in beträchtlichem Umfang*“ für Zwecke der Verbreitung von Darstellungen sexuellen Kindesmissbrauchs oder auf eine „*beträchtliche Anzahl von Meldungen*“ in diesem Zusammenhang.

¹⁶ Siehe Urteil vom 5. September 2012, Europäisches Parlament gegen Rat der Europäischen Union, C- 355/10, EU:C:2012:516, Rn. 77.

25. Die verwendeten Begriffe – z. B. die Bezugnahme auf die Notwendigkeit, dass eine Maßnahme „*wirksam*“ ist – in Verbindung mit der Tatsache, dass die Verantwortung für die Wahl der „wirksamen“ Technologie letztlich bei den Diensteanbietern liegt, geben Anlass zu ernsthaften Zweifeln an der Vorhersehbarkeit der Auswirkungen dieser Maßnahmen auf die betreffenden Grundrechte.
26. Fazit: Die in der vorgeschlagenen Verordnung verwendeten Konzepte zur Bestimmung der Einschränkungen der betreffenden Grundrechte, die sich aus der Verwendung von Aufdeckungsanordnungen ergeben würden, sowie die Tatsache, dass diese Einschränkungen im Wesentlichen von Technologien und Methoden abhängen würden, die erst festgelegt werden müssen, machen es schwierig, das Ausmaß des Eingriffs in die Grundrechte zu beurteilen. Im Wesentlichen würde die Verpflichtung, das Ausmaß solcher Eingriffe näher zu bestimmen, letztlich bei denjenigen liegen, die für die Konzeption der einschlägigen Technologie, die Parameter für die indikatorenbasierten Screenings und die Umsetzung der Aufdeckungsanordnung im Einzelfall zuständig sind (EU-Zentrum, nationale Behörden, Richter, Dienstleister). Der Umfang des damit verbundenen Ermessensspielraums könnte zu einem sehr breiten Spektrum möglicher unterschiedlicher Auslegungen und Bedenken hinsichtlich der Einhaltung der Grundrechte führen.
27. Vor diesem Hintergrund laufen die derzeit in der vorgeschlagenen Verordnung vorgesehenen Regelungen der Aufdeckungsanordnungen Gefahr, nicht hinreichend klar, genau und vollständig zu sein und daher nicht dem Erfordernis, dass Einschränkungen der Grundrechte gesetzlich vorgesehen sein müssen, entsprechen. Die vorgeschlagene Verordnung sollte detailliertere Elemente sowohl zu den Einschränkungen der Grundrechte, die die spezifische Art und die Merkmale der einzusetzenden Technologie mit sich bringen würden, als auch zu den damit verbundenen möglichen Schutzmaßnahmen enthalten.

2. Die Bekämpfung von sexuellem Kindesmissbrauch ist eine dem Gemeinwohl dienende Zielsetzung

28. Zur Frage, ob die in der vorgeschlagenen Verordnung festgelegten Aufdeckungsanordnungen eine von der Union anerkannte **dem Gemeinwohl dienende Zielsetzung verfolgen** oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer dienen, hat der Gerichtshof bestätigt, dass die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit eine dem Gemeinwohl dienende Zielsetzung darstellt.¹⁷ Ferner benennt der Gerichtshof ausdrücklich „*sexuelle Ausbeutung von Kindern und Kinderpornografie*“ unter den strafbaren Handlungen, die „*ihrem Wesen nach einen unbestreitbar hohen Schweregrad aufweisen*“.¹⁸ Dies ist auch in den einschlägigen EU-Rechtsvorschriften zum sexuellen Missbrauch von Kindern wiedergegeben.¹⁹
29. Der Gerichtshof bekräftigt, dass „*[...] in Bezug insbesondere auf die wirksame Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, zu berücksichtigen [ist], 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 Artikel 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Artikeln 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben*“.

¹⁷ Siehe Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, Rn. 42, vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, 125, EU:C:2020:79, Rn. 126. Der Gerichtshof stellt fest, dass nach Artikel 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat. Jedoch führt der Gerichtshof aus, dass, da diese Bestimmung einen Freiheitsentzug durch eine staatliche Stelle betrifft, Artikel 6 der Charta nicht dahin ausgelegt werden kann, dass er die staatlichen Stellen verpflichtet, spezifische Maßnahmen zur Ahndung bestimmter Straftaten zu erlassen.

¹⁸ Siehe Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, Rn. 149.

¹⁹ Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1 und Berichtigung ABl. L 18 vom 21.1.2012, S. 7).

30. Der Gerichtshof gelangt zu dem Schluss, dass gemäß „Artikel 4 und 7 der Charta“ insbesondere „materielle und prozedurale Vorschriften zu erlassen sowie praktische Maßnahmen zu treffen sind, die eine wirksame Bekämpfung von Straftaten gegen Personen mittels effektiver Ermittlungen und Verfolgung gestatten. Diese Verpflichtung ist umso wichtiger, wenn das körperliche und geistige Wohlergehen eines Kindes bedroht ist“.²⁰
31. Hier ist anzumerken, dass einerseits in Artikel 1 (*Gegenstand und Anwendungsbereich*) das Ziel der vorgeschlagenen Verordnung darin besteht, „im Binnenmarkt gegen den Missbrauch einschlägiger Dienste der Informationsgesellschaft für den sexuellen Kindesmissbrauch im Internet vorzugehen“; andererseits bezieht sich die vorgeschlagene Verordnung in Artikel 2 Buchstaben l bis n (Begriffsbestimmungen) auf die Definitionen der Darstellungen sexuellen Kindesmissbrauchs gemäß der Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und nicht auf die Definition der damit zusammenhängenden Straftaten auf dem Gebiet des sexuellen Missbrauchs gemäß jener Richtlinie. Somit bleibt der Anwendungsbereich der in der vorgeschlagenen Verordnung vorgesehenen Aufdeckungsanordnung nicht auf die Aufdeckung strafbaren Verhaltens beschränkt.
32. Vor diesem Hintergrund besteht kein Zweifel daran, dass die Aufdeckungsanordnung der wichtigen dem Gemeinwohl dienende Zielsetzung der Verhütung, Aufdeckung, Ermittlung und Strafverfolgung von Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch dienen soll. Jedoch umfasst der Umfang einer solchen Aufdeckung, wie er in der vorgeschlagenen Verordnung festgelegt ist, mehr als die Aufdeckung strafbaren Verhaltens. Dies ist ein Aspekt, der bei der Beurteilung der Erfordernisse gemäß Artikel 52 der Charta in der Auslegung durch den Gerichtshof zu berücksichtigen ist.

²⁰ Siehe Urteile vom 6 Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 128, vom 20. September 2022, *SpaceNet AG*, C-793/19 und C-794/19, EU:C:2022:702, Rn. 63 bis 65.

3. Einschränkungen der Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten

33. Das Screening interpersoneller Kommunikation infolge des Erlasses einer Aufdeckungsanordnung greift zweifelsfrei in das nach Artikel 7 der Charta garantierte Grundrecht auf Achtung des Privatlebens ein, da Zugriff auf interpersonelle Kommunikation (Textnachrichten, E-Mails, Audio-Kommunikation, Bilder oder jede andere Art ausgetauschter personenbezogener Informationen) ermöglicht und deren Vertraulichkeit beeinträchtigt wird. Zudem kann es abschreckende Wirkungen in Bezug auf die Ausübung der durch Artikel 11 der Charta gewährleisteten Freiheit der Meinungsäußerung entfalten.²¹ Dabei kommt es nicht darauf an, ob die betreffenden Informationen über das Privatleben als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben.²²
34. Zudem stellt ein derartiges Screening die Verarbeitung personenbezogener Daten nach Artikel 8 der Charta dar und greift in den durch diese Bestimmung garantierten Schutz personenbezogener Daten ein.²³
35. In diesem Zusammenhang ist darauf hinzuweisen, dass der Umstand, dass nach ständiger Rechtsprechung eine automatisierte Analyse auf der Grundlage vorab festgelegter Indikatoren es als solche nicht ermöglicht, alle Nutzer zu identifizieren, deren Daten dieser Analyse unterzogen werden, der Einstufung solcher Daten als „personenbezogene Daten“ nicht entgegensteht. Da das Verfahren es gestattet, die Person oder die Personen, deren Daten Gegenstand der automatisierten Analyse waren, später zu identifizieren. Nach der Definition in Artikel 4 Nr. 1 der Datenschutz-Grundverordnung (DSGVO) sind aber u. a. Informationen, die sich auf eine **identifizierbare Person** beziehen, personenbezogene Daten.²⁴ Daher setzt das Screening der gesamten Kommunikation in einem Dienst mithilfe einer automatisierten Operation systematischen Zugriff auf alle und systematische Verarbeitung aller Informationen voraus und bedeutet daher einen Eingriff in den Datenschutz, unabhängig davon wie die Daten in weitere Folge verwendet werden. Insbesondere ist die Frage, ob die zuständige Behörde in weiterer Folge auf diese Informationen zugreift, nicht relevant.

²¹ Siehe Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 173.

²² Siehe Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, Rn. 96.

²³ Siehe analog dazu Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, Rn. 93 und 94.

²⁴ Siehe Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, Rn. 171.

36. Was die Schwere des Eingriffs betrifft, den die Verwendung einer Aufdeckungsanordnung für interpersonelle Kommunikation mit sich bringen würde, so hat der Gerichtshof in der Rechtssache *La Quadrature du Net*²⁵ die nationale Regelung geprüft, mit der zum Schutz der nationalen Sicherheit einschließlich im Hinblick auf Terrorismus den Betreibern elektronischer Kommunikationsdienste aufgegeben wurde, in ihren Netzen Maßnahmen umzusetzen, die es ermöglichen, Verkehrs- und Standortdaten automatisiert zu analysieren.
37. In der Rechtssache *La Quadrature du Net* kam der Gerichtshof zu dem Schluss, dass eine automatisierte Analyse, die „*im Wesentlichen einer Filterung aller von den Betreibern elektronischer Kommunikationsdienste gespeicherten Verkehrs- und Standortdaten, die von ihnen auf Ersuchen der zuständigen nationalen Behörden in Anwendung der von diesen festgelegten Parametern vorgenommen wird,*“ entspricht, einen **besonders schwerwiegenden Eingriff** bedeutet, da sie sich **allgemein und unterschiedslos** auf die Daten der Nutzer elektronischer Kommunikationsmittel erstreckt, sich aus diesen Daten die Art der im Internet konsultierten Informationen entnehmen lässt, und da sie auch bei Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit terroristischen Aktivitäten stehen könnte, angewendet werden.²⁶
38. Die vom Gerichtshof in den Randnummern 171 bis 180 des Urteils *La Quadrature du Net* geprüfte nationale Maßnahme ist den Aufdeckungsanordnungen in der vorgeschlagenen Verordnung ähnlich. In beiden Fällen wird den Anbietern ein automatisiertes Screening der Kommunikationsdaten aufgegeben. In beiden Fällen erfolgt das Screening auf der Grundlage von durch öffentliche Behörden bereitgestellten „*Indikatoren*“. Bei beiden Maßnahmen sind elektronische Kommunikationsdienste betroffen, und die Art der im Internet konsultierten Informationen lässt sich entnehmen. Zudem kommen beide Maßnahmen auch bei Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit den betroffenen kriminellen Aktivitäten stehen könnte, zur Anwendung.

²⁵ Siehe Urteile vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18, Rn. 172 bis 180.

²⁶ Siehe Urteile vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18, Rn. 174.

39. Für die Beurteilung der Frage, ob eine Aufdeckungsanordnung für interpersonelle Kommunikation im Lichte dieser Rechtsprechung einen **besonders schwerwiegenden Eingriff** darstellen würde, ist jedoch erstens die Frage, ob die Aufdeckungsanordnung sich *allgemein und unterschiedslos* auf die Daten von Personen, die elektronische Kommunikationssysteme im Sinne dieser Rechtsprechung nutzen, erstrecken würde, und zweitens die Art der betroffenen Daten zu prüfen.
40. **Erstens** dürfte der Umstand, dass eine Aufdeckungsanordnung an einen bestimmten Diensteanbieter und nicht an alle interpersonellen Kommunikationsdienste gerichtet würde, als solcher kein stichhaltiges Argument für die Annahme sein, dass die Maßnahme nicht **allgemeiner und unterschiedsloser** Natur wäre.
41. Hier ist darauf hinzuweisen, dass der Gerichtshof bei der Beurteilung, ob es sich um **gezielte** oder **allgemeine und unterschiedslose** Maßnahmen handelt, die spezifische Art der Maßnahme berücksichtigt.²⁷ Der maßgebliche Faktor, den der Gerichtshof in seiner Rechtsprechung zur Vorratsspeicherung von Kommunikation von *Metadaten* berücksichtigt, ist insbesondere, ob die automatische Verarbeitung von Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums begrenzt ist, oder ob objektive und nicht diskriminierende Kriterien herangezogen werden können, um eine zumindest indirekte Verbindung zwischen den schweren Straftaten und den Personen, deren Daten auf Vorrat gespeichert werden, herzustellen.²⁸ Die Notwendigkeit einer solchen *Verbindung*, die der Gerichtshof im Zusammenhang mit der Vorratsspeicherung von Metadaten (Verkehrs- und Standortdaten) festgestellt hat, sollte in Bezug auf den Zugriff auf Inhaltsdaten (Inhalte interpersoneller Kommunikation) anders beurteilt werden; denn hierbei handelt es sich um einen schwerwiegenderen Eingriff in die Grundrechte.

²⁷ Siehe z B. Urteil vom 26. Januar 2023, Ministerstvo na vatreshnite raboti, C-205/21, EU:C:2023:49, Rn. 129.

²⁸ Siehe Urteil vom 20 September 2022, SpaceNet AG, C-793/19 und C-794/19, Rn. 75, 83 bis 84, 112 und 113.

42. Die in der vorgeschlagenen Verordnung vorgesehenen Verpflichtungen aufgrund der Aufdeckungsanordnungen wären zwar an einen bestimmten Diensteanbieter gerichtet, würden jedoch bedeuten, dass Inhalte der gesamten interpersonellen Kommunikation, die über diesen Dienst (oder gegebenenfalls den entsprechenden Teil oder Aspekt desselben)²⁹ erfolgt, mithilfe automatisierter Instrumente abgerufen und gescannt werden müssen. Daher bliebe eine solche Verarbeitung von Daten nicht auf die interpersonelle Kommunikation von Personen begrenzt, in Bezug auf die berechtigter Grund zu der Annahme besteht, dass sie in irgendeiner Weise an der Begehung einer Straftat im Zusammenhang mit sexuellem Kindesmissbrauch beteiligt sind oder eine derartige Straftat begangen haben, oder bei denen es zumindest eine indirekte Verbindung zu Straftaten im Zusammenhang mit sexuellem Missbrauch gibt.
43. Die vorgeschlagenen Rechtsvorschriften sehen ein allgemeines Screening der von einem bestimmten Diensteanbieter verarbeiteten Daten ohne weitere Unterscheidung im Hinblick auf die Personen vor, die diesen spezifischen Dienst nutzen. Der Umstand, dass die Aufdeckungsanordnungen an einen spezifischen Dienst gerichtet würden, wenn Beweise für ein erhebliches Risiko vorliegen, dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt wird, würde auf einer Verbindung zwischen dem Dienst und den Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch beruhen, und nicht auf einer zumindest indirekten Verbindung zwischen den schweren Straftaten und den Personen, deren Daten gescannt werden. Die Daten aller Personen, die diesen spezifischen Dienst nutzen, würden gescannt, ohne dass sich die Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte, wobei die Nutzung dieses konkreten Dienstes der einzige diesbezüglich relevante Faktor wäre.
44. In diesem Zusammenhang ist zu berücksichtigen, dass interpersonelle Kommunikationsdienste nahezu von der gesamten Bevölkerung genutzt werden und auch für die Verbreitung von Darstellungen sexuellen Kindesmissbrauchs und/oder für die Kontaktaufnahme zu Kindern genutzt werden können. An diese Dienste gerichtete Aufdeckungsanordnungen würden ein variables – jedoch in jedem Fall sehr breites – Spektrum automatisierter Analysen personenbezogener Daten und Zugriff auf personenbezogene und vertrauliche Informationen mit sich bringen, wobei eine überaus große Zahl von Personen betroffen wäre, bei denen keine, auch nur indirekte, Verbindung zu Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch besteht.

²⁹ Siehe Artikel 8 Absatz 1 Buchstabe d der vorgeschlagenen Verordnung.

45. Diese Bedenken werden auch dadurch bestärkt, dass in der vorgeschlagenen Verordnung keinerlei echte Schutzmaßnahmen vorgesehen sind, um das Risiko zu vermeiden, dass die kumulierte Wirkung der Anwendung der Aufdeckungsanordnungen durch nationale Behörden in verschiedenen Mitgliedstaaten dazu führen könnte, dass alle in der Union verfügbaren interpersonellen Kommunikationsdienste betroffen wären.
46. Da der Erlass einer Aufdeckungsanordnung in Bezug auf einen bestimmten Anbieter interpersoneller Kommunikationsdienste das Risiko mit sich bringen würde, die Nutzung anderer Dienste zu Zwecken des sexuellen Kindmissbrauchs zu fördern, besteht darüber hinaus eindeutig die Gefahr, dass Aufdeckungsanordnungen, um wirksam zu sein, auf andere Anbieter ausgedehnt werden müssten und de facto zu einer ständigen Überwachung der gesamten interpersonellen Kommunikation führen würden.
47. Daher ist es, wenngleich die Aufdeckungsanordnung an einen einzigen Diensteanbieter, im Hinblick auf einen spezifischen interpersonellen Kommunikationsdienst oder einen Aspekt desselben gerichtet ist, sehr wahrscheinlich, dass im Fall einer gerichtlichen Prüfung eine Verpflichtung zum Daten-Screening wie jene, die sich aus den Verpflichtungen durch die Aufdeckungsanordnung ergibt, als *allgemein und unterschiedslos* angesehen würde – und daher nicht als *gezielte* Verarbeitung von Daten.
48. Angesichts ihres allgemeinen und unterschiedslosen Charakters würde eine solche Screening-Verpflichtung daher im Lichte der unter den Nummern 36 und 37 (oben) angeführten Rechtsprechung einen ***besonders schwerwiegenden Eingriff*** in die Grundrechte darstellen.
49. **Zweitens** wird dieser Schluss durch die Tragweite des Eingriffs bestätigt, die – angesichts der betreffenden Datenkategorien – bei der Aufdeckungsanordnung deutlich über jene in der Rechtssache *La Quadrature du Net* hinausgeht. In der Rechtssache *La Quadrature du Net* betraf das allgemeine Screening die Metadaten (Verkehrs- und Standortdaten), während die Aufdeckungsanordnung das Screening von *Kommunikationsinhalten* betreffen würde. Die Verarbeitung von Metadaten bedeutet einen geringeren Eingriff als eine ähnliche Verarbeitung von Inhaltsdaten.

50. Darüber hinaus müsste das Screening von Kommunikationsinhalten auch in einer verschlüsselten Umgebung wirksam sein, denn verschlüsselte Umgebungen sind bei interpersoneller Kommunikation weit verbreitet. Das würde bedeuten, dass die Anbieter in Erwägung ziehen müssten, i) wirksame Ende-zu-Ende-Verschlüsselung aufzugeben oder ii) eine Art „Backdoor“ einzuführen, um auf verschlüsselte Inhalte zuzugreifen, oder iii) auf Inhalte auf dem Gerät des Nutzers zuzugreifen, bevor sie verschlüsselt werden („Client-Side-Scanning“).³⁰
51. Daher scheint es, dass das allgemeine Screening von Inhalten von Kommunikation, eine Schwächung oder anderweitige Umgehung von Cybersicherheitsmaßnahmen (insbesondere Ende-zu-Ende-Verschlüsselung) erfordern würde, um ein solches Screening zu ermöglichen. Die entsprechenden Auswirkungen auf Cybersicherheitsmaßnahmen, sofern sie von Wirtschaftsakteuren auf dem Markt bereitgestellt werden, selbst unter der Kontrolle der zuständigen Behörden, würden zu einem stärkeren Eingriff in die betreffenden Grundrechte führen und könnten zusätzliches Eingreifen in andere Grundrechte und legitime Ziele wie den Schutz der Datensicherheit bewirken.
52. Darüber hinaus würde das Screening von Audio-Kommunikation oder schriftlichen Mitteilungen, um Kontaktaufnahme zu Kindern zu erkennen, notwendigerweise eine Prüfung/Verifizierung des Alters erfordern, die sich allgemein auf alle Nutzer des betroffenen Dienstes erstrecken würde. Ohne das genaue Alter aller Nutzer zu bestimmen, wäre es nämlich nicht möglich, herauszufinden, ob eine mutmaßliche Kontaktaufnahme an ein Kind gerichtet ist. Ein solches Verfahren müsste entweder durch i) Mass Profiling der Nutzer oder ii) durch biometrische Analyse des Gesichts und/oder der Stimme der Nutzer oder iii) durch ein digitales Identifizierungs-/Zertifizierungssystem erfolgen. Die Umsetzung einer dieser Maßnahmen durch die Anbieter von Kommunikationsdiensten würde zwangsläufig zu einer weiteren Ebene der Beeinträchtigung der Rechte und Freiheiten der Nutzer führen.

³⁰ Siehe dazu auch Vorabentscheidungsersuchen, Landgericht Berlin (Deutschland), vorgelegt am 24. Oktober 2022 – Strafverfahren gegen M.N., anhängige Rechtssache C-670/22, betreffend die Verwendung von Beweismitteln aus der Überwachung von Ende-zu-Ende-verschlüsselter Telekommunikation, einschließlich Kommunikationsinhalte, wobei alle Nutzer eines Kommunikationsdienstes, ohne konkrete Hinweise auf Begehung schwerwiegender Straftaten durch diese Nutzer, betroffen waren.

53. Daraus folgt, dass die Anwendung von Aufdeckungsanordnungen auf interpersonelle Kommunikation, wie vorgeschlagen, einen besonders schwerwiegenden Eingriff in die Grundrechte bedeuten würde.

4. Der Wesensgehalt der Rechte auf Privatleben und den Schutz personenbezogener Daten

54. In diesem Zusammenhang könnte sich auch die Frage stellen, ob im Lichte der Rechtsprechung der Eingriff, den die vorgeschlagene Aufdeckungsanordnung für interpersonelle Kommunikation mit sich bringen würde, sogar den Wesensgehalt³¹ des Rechts auf Achtung des Privat- und Familienlebens sowie des Rechts auf Schutz personenbezogener Daten beeinträchtigen könnte.
55. Tatsächlich „*verletzt 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*“, so die Feststellung des Gerichtshofs.³² Aus der Rechtsprechung lässt sich zudem ableiten, dass der Eingriff durch eine derartige Regelung in die nach Artikel 7 und 8 der Charta garantierten Rechte einen weitreichenden, besonders schwerwiegenden Eingriff in diese Rechte darstellt, und geeignet ist, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.³³

³¹ Die Verpflichtung, den Wesensgehalt der betroffenen Rechte zu achten, ist gemäß Artikel 52 Absatz 1 der Charta eine der Voraussetzungen für die Rechtmäßigkeit einer Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten.

³² Siehe Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 94.

³³ Siehe Urteile vom 8. April 2014, Digital Rights Ireland and u.a., C-293/12 und C-594/12, Rn. 39; vom 6. Oktober 2015, Schrems, C-362/14, Rn. 94; vom 21. Dezember 2016, Tele2 Sverige gegen Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 100 und 101.

56. Da die Aufdeckung, die gestattet werden könnte, generellen Zugriff auf die Inhalte interpersoneller elektronischer Kommunikation sowie generelle Weiterverarbeitung dieser Inhalte mit sich brächte, würde das Briefgeheimnis seiner Wirksamkeit und seines Inhalts entleert, denn es gäbe weder Einschränkungen hinsichtlich der Inhalte noch der betroffenen Personen, auf die ein Diensteanbieter die Aufdeckungsanordnung anzuwenden hätte. Angesichts der genannten Rechtsprechung birgt ein derartiger Eingriff daher sogar die ernsthafte Gefahr einer Beeinträchtigung des Wesensgehalts des Grundrechts auf Achtung des Privatlebens.
57. Zwar gilt nach Artikel 10 Absatz 3 Buchstabe b der vorgeschlagenen Verordnung für die Technologien, die verfügbar gemacht und von den Betreibern verwendet werden müssen Folgendes: „*Mit ihnen können aus der einschlägigen Kommunikation nur die Informationen extrahiert werden, die unbedingt notwendig sind, um [...] Darstellungen sexuellen Kindesmissbrauchs [zu erkennen]*“, und „*sie entsprechen dem neuesten Stand der Technik in der Branche und greifen am wenigsten [in die Rechte der Nutzer auf Privatleben und den Schutz personenbezogener Daten] ein.*“ Jedoch ist in diesem Zusammenhang darauf hinzuweisen, dass der Umstand, dass irrelevante Informationen nicht extrahiert werden, an sich nicht die Notwendigkeit ausschließt, im Wege einer automatisierten Analyse alle Daten der interpersonellen Kommunikation aller Nutzer des spezifischen Kommunikationsdienstes, an den die Anordnung gerichtet ist, also auch bei Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit Straftaten des sexuellen Kindesmissbrauchs stehen könnte, zu scannen.
58. In Anbetracht der vorstehenden Ausführungen kann der Schluss gezogen werden, dass die Aufdeckungsanordnung, die gemäß der vorgeschlagenen Verordnung in Bezug auf interpersonelle Kommunikation vorgesehen ist, die ernsthafte Gefahr birgt, dass festgestellt würde, dass sie den Wesensgehalt der nach Artikel 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und Datenschutz beeinträchtigt, da mit der Aufdeckungsanordnung angestrebt würde, generellen Zugriff mittels Überwachung durch automatisiertes und systematisches Screening auf die Inhalte der elektronischen Kommunikation und die personenbezogenen Daten aller Nutzer eines spezifischen Dienstes zu gestatten, unabhängig davon ob bei diesen eine direkte oder indirekte Verbindung zu kriminellen Aktivitäten im Zusammenhang mit sexuellem Kindesmissbrauch besteht.³⁴

³⁴ Siehe analog dazu, Urteil vom 21. Juli 2022, Ligue des droits humains, C-817/19, Rn. 92 bis 111.

5. Einhaltung des Grundsatzes der Verhältnismäßigkeit

59. Ungeachtet der vorstehenden Ausführungen müsste, für den Fall, dass davon ausgegangen wird, dass die fraglichen Maßnahmen den Wesensgehalt der Grundrechte achten, ihre Vereinbarkeit mit der Charta unter dem Aspekt der Verhältnismäßigkeit beurteilt werden, da sie, wie oben unter den Nummern 33 bis 53 dargelegt, in jedem Fall **besonders schwerwiegende** Einschränkungen dieser Rechte bzw. Eingriffe in diese Rechte mit sich bringen.
60. Nach ständiger Rechtsprechung verlangt der Grundsatz der Verhältnismäßigkeit, dass die Beschränkungen, die insbesondere durch EU-Rechtsakte an in der Charta verankerten Rechten und Freiheiten vorgenommen werden können, nicht die Grenzen dessen überschreiten, was zur Erreichung der mit dieser Regelung zulässigerweise verfolgten Ziele oder zum Schutz der Rechte und Freiheiten anderer **angemessen und notwendig** ist; stehen mehrere geeignete Maßnahmen zur Auswahl, ist die am wenigsten belastende zu wählen, und die durch sie bedingten Nachteile müssen in angemessenem Verhältnis zu den angestrebten Zielen stehen. Sind mehrere in den Verträgen verankerte Grundrechte und Grundsätze betroffen, so ist zudem bei der Beurteilung der Einhaltung des Grundsatzes der Verhältnismäßigkeit darauf zu achten, dass die mit dem Schutz der verschiedenen Rechte und Grundsätze verbundenen Erfordernisse miteinander in Einklang gebracht werden und dass zwischen ihnen ein angemessenes Gleichgewicht besteht.³⁵
61. Das Erfordernis, zu gewährleisten, dass der Eingriff in das Privatleben und den Datenschutz auf das unbedingt erforderliche Maß beschränkt bleibt, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht.³⁶ Dies trifft auf Daten, die in Inhalten interpersoneller Kommunikation enthalten sind, eindeutig zu.

³⁵ Siehe Urteil von 17. Dezember 2020, Centraal Israëlitisch Consistorie van België u. a., C-336/19, EU:C:2020:1031, Rn. 64.

³⁶ Siehe Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18 und die dort angeführte Rechtsprechung, Rn. 132.

62. In seiner bisherigen Rechtsprechung war der Gerichtshof noch nie mit der Verhältnismäßigkeit einer verpflichtenden Überprüfung der *Inhalte interpersoneller Kommunikation* zu Strafverfolgungszwecken, wie sie in der vorgeschlagenen Verordnung vorgesehen ist, direkt befasst – aus dem einfachen Grund, dass noch keine solche Maßnahme von der Union oder einem ihrer Mitgliedstaaten erlassen worden ist. Rechtsvergleichung ist ebenfalls nur in begrenztem Maße hilfreich.³⁷ Das Ergebnis der Verhältnismäßigkeitsprüfung ließe sich jedoch aus einer Reihe von Entscheidungen ableiten, die insbesondere Binnenmarktvorschriften (Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation³⁸) betroffen haben, die die Verhältnismäßigkeit von Maßnahmen im Zusammenhang mit Kommunikationsdaten zum Gegenstand hatten. Diese Rechtsprechung ist hier umso relevanter, als sich die vorgeschlagene Verordnung, wie auch die oben genannte Richtlinie, auf Artikel 114 AEUV stützt.
63. Die vom Gerichtshof entwickelte Methode zur Bewertung der Verhältnismäßigkeit besonders schwerwiegender Eingriffe in Grundrechte im Zusammenhang mit der Vorratsdatenspeicherung oder dem Zugriff auf *Metadaten* ist für die Zwecke der Bewertung der fraglichen Maßnahmen relevant.
64. In diesem Zusammenhang hat der Gerichtshof in Bezug auf die Artikel 7, 8 und 11 und Artikel 52 Absatz 1 der Charta festgestellt, dass **erstens** jene Bestimmungen Rechtsvorschriften nicht entgegenstehen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen.³⁹

³⁷ Siehe jedoch Ausführungen über das Scannen von Kommunikationsdaten nach den Rechtsvorschriften der Vereinigten Staaten (Urteile vom 6. Oktober 2015, Schrems, C-362/14 und die dort angeführte Rechtsprechung, und vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18 und die dort angeführte Rechtsprechung). In Bezug ein anderes aber mit diesem zusammenhängendes Thema, die Massenüberwachung von Kommunikation durch Nachrichtendienste für Zwecke der nationale Sicherheit, siehe Urteil des EGMR vom 25. Mai 2021, Big Brother Watch u. a. gegen das Vereinigte Königreich, CE:ECHR:2021:0525JUD005817013 und Centrum för Rättvisa gegen Schweden, CE:ECHR:2021:0525JUD003525208.

³⁸ 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); ABl. L 201 vom 31.7.2002.

³⁹ Siehe Urteil vom 20. September 2022, SpaceNet AG, C-793/19 und C-794/19 und die dort angeführte Rechtsprechung, Rn. 75.

65. Der Gerichtshof hat jedoch ausgeführt, dass selbst die positiven Verpflichtungen, die sich, je nach Fall, für die Mitgliedstaaten aus den Artikeln 3, 4 und 7 der Charta ergeben können und die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen, keine so schwerwiegenden Eingriffe rechtfertigen können, wie sie mit einer Regelung, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, für die Grundrechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen.⁴⁰
66. Angesichts dieser Rechtsprechung und unter Berücksichtigung der vorstehend in den Nummern 39 bis 47 genannten Erwägungen besteht die ernsthafte Gefahr der Nichteinhaltung des Grundsatzes der Verhältnismäßigkeit, da die Aufdeckungsanordnungen den *allgemeinen und unterschiedslosen Zugriff* eines bestimmten Diensteanbieters auf die Inhalte der persönlichen Kommunikation erfordern würden und ohne Unterscheidung auf alle Personen anzuwenden wären, die diesen spezifischen Dienst in Anspruch nehmen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte.

⁴⁰ Siehe Urteile vom 6 Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18 und die dort angeführte Rechtsprechung, Rn. 145, und vom 20. September 2022, *SpaceNet AG*, C-793/19 und C-794/19, EU:C:2022:702, Rn. 24. In diesem Zusammenhang ist darauf hinzuweisen, dass der Gerichtshof die Vereinbarkeit mit der Charta von Bestimmungen bestätigt hat, die darauf abzielen, in Bezug auf eine Person, bei der die berechtigte Annahme besteht, dass sie an einer schweren Straftat beteiligt ist, und nach einer individuellen Bewertung der Notwendigkeit und Verhältnismäßigkeit, eine wirksame und schnelle Beschaffung von Informationen zu ermöglichen (siehe Urteile vom 15. Dezember 2015, *WebMindLicenses*, C-419/14, EU:C:2015:832, Rn. 69, und vom 16. Februar 2023, *HYA u. a.*, C-349/21, EU:C:2023:102, Rn. 49).

67. In diesem Zusammenhang ist darauf hinzuweisen, dass die Herstellung *eines zumindest mittelbaren Zusammenhangs* zwischen den Inhalten interpersoneller Kommunikation und dem mit der der Maßnahme verfolgten Ziel auch von der Tatsache beeinflusst wird, dass im Lichte von Nummer 31, oben, die Aufdeckungsanordnungen nicht auf kriminelle Inhalte begrenzt sind. Die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie legt Mindestvorschriften zur Definition der entsprechenden Straftaten fest und überlässt es den Mitgliedstaaten, mehrere Elemente der entsprechenden Straftaten in nationalem Recht selbst zu definieren (siehe insbesondere „Alter der sexuellen Mündigkeit“, unterhalb dessen die Vornahme sexueller Handlungen mit einem Kind nach dem nationalen Recht verboten ist). Folglich kann das Screening auf EU-Ebene sich auf Material erstrecken, das nicht immer in allen Mitgliedstaaten Straftaten im Zusammenhang mit sexuellem Kindesmissbrauch bedeutet oder zu diesen führt.
68. Zudem würde das Risiko der Nichteinhaltung des Grundsatzes der Verhältnismäßigkeit noch dadurch verschärft, dass die Aufdeckungsanordnung im Gegensatz zu den Maßnahmen, die in der Rechtsprechung genannt sind, auf die unter Nummer 64 verwiesen wird, die Inhalte der interpersonellen Kommunikation und nicht die Verkehrs- und Standortdaten betreffen würde.
69. **Zweitens** hat der Gerichtshof festgestellt, dass EU-Recht **einer allgemeinen Vorratsspeicherung der die Identität sowie IP-Adressen betreffenden Daten** für die Zwecke der Bekämpfung der Kriminalität im Allgemeinen nicht entgegensteht.⁴¹

⁴¹ Die Identität betreffende Daten sind von Bedeutung beim Erwerb elektronischer Kommunikationsmittel, beispielsweise beim Erwerb einer Prepaid SIM-Karte, wenn der Verkäufer die offiziellen Dokumente, aus denen die Identität des Käufers hervorgeht, überprüfen, die betreffenden Informationen registrieren und für den Fall, dass die zuständigen nationalen Behörden dies verlangen, ihnen Zugang zu diesen Informationen gewähren muss. IP- Adressen gehören zu den Verkehrsdaten, werden aber ohne Anknüpfung an eine bestimmte Kommunikation erzeugt und dienen in erster Linie dazu, über die Betreiber elektronischer Kommunikationsdienste die natürliche Person zu ermitteln, der ein Endgerät gehört, von dem aus eine Kommunikation über das Internet stattfindet. Siehe Urteil vom 20. September 2022, SpaceNet AG, C-793/19 und C-794/19 und die dort angeführte Rechtsprechung, Rn. 99.

70. Der Gerichtshof hat in diesem Zusammenhang bestätigt, dass die Vorratsspeicherung der IP- Adressen aller natürlichen Personen, denen ein Endgerät gehört, der einzige Anhaltspunkt sein kann, der es ermöglicht, unter anderem bei besonders schweren Straftaten im Bereich der Kinderpornografie, etwa wenn Kinderpornographie im Sinne von Artikel 2 Buchstabe c der Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie erworben, verbreitet, weitergegeben oder im Internet bereitgestellt wird, zu ermitteln. Der Gerichtshof hat jedoch zum einen klargestellt, dass die Identität der Nutzer elektronischer Kommunikationssysteme abgesehen von den Kontaktdaten dieser Nutzer, wie ihren Adressen, keine Informationen über die gesendeten Nachrichten und damit über das Privatleben der Nutzer enthält. Der Eingriff, den die Vorratsspeicherung dieser Daten mit sich bringt, kann grundsätzlich nicht als schwerwiegend angesehen werden; was, zum anderen, die IP-Adressen angeht, so können daraus, wenngleich sie Teil der Verkehrsdaten sind, keine Informationen über Dritte entnommen werden, die mit der Person, die die Kommunikation geführt hat, in Kontakt gestanden sind. Diese Kategorie von Daten weist daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf.⁴²
71. Diese Rechtsprechung kann daher nicht als Grundlage für den Schluss herangezogen werden, dass der besonders schwerwiegende Eingriff in das Privatleben und den Datenschutz, den die Verpflichtungen aus den Aufdeckungsanordnungen für interpersonelle Kommunikation mit sich bringen, notwendig und verhältnismäßig wäre, da das Screening von Informationen vorgeschrieben würde, die der Gerichtshof entgegen der oben genannten Rechtsprechung als sehr sensibel (Inhalt interpersoneller Kommunikation) angesehen hat.

⁴² Siehe Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18 und die dort angeführte Rechtsprechung, Rn. 152 bis 158.

72. **Drittens** hat der Gerichtshof in der Rechtssache *La Quadrature du Net* ausgeführt, dass der mit einer allgemeinen und unterschiedslosen Analyse von Verkehrs- und Standortdaten verbundene besonders schwere Eingriff, **dem Erfordernis der Verhältnismäßigkeit nur in Situationen genügen kann, in denen ein Mitgliedstaat einer ernsthaften Bedrohung für die nationale Sicherheit ausgesetzt ist**, die sich als tatsächlich, aktuell oder vorhersehbar erweist, und sofern die Dauer dieser Speicherung auf das absolut Notwendige beschränkt ist. Der Gerichtshof hat klargestellt, dass nur unter diesen Bedingungen ein allgemeines und unterschiedsloses Screening von Daten, aus denen sich die Art der im Internet konsultierten Informationen entnehmen lässt, und auch bei Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit terroristischen Aktivitäten stehen könnte, angewendet werden, im Lichte der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta als gerechtfertigt angesehen werden kann.⁴³
73. Es ist jedoch schwer vorstellbar, wie diese Rechtsprechung als Grundlage für die Rechtfertigung einer Maßnahme dienen kann, die auf die Bekämpfung von Straftaten ausgerichtet ist, die zweifelsfrei schwer sind, aber nicht mit Bedrohungen der nationalen Sicherheit im Zusammenhang stehen.
74. In diesem Zusammenhang hat der Gerichtshof entschieden, dass das Ziel, der Wahrung der nationalen Sicherheit dem zentralen Anliegen entspricht, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft durch die Verhütung und Repression von Tätigkeiten zu schützen, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten. Eine solche Bedrohung unterscheidet sich somit in ihrer Art, in ihrer Schwere und der Besonderheit der sie begründenden Umstände nach von der Gefahr schwerer Straftaten. In diesem Zusammenhang kommt der Gerichtshof zu dem Schluss, dass Kriminalität – auch besonders schwere Kriminalität – nicht mit einer Bedrohung der nationalen Sicherheit gleichgesetzt werden kann.⁴⁴

⁴³ Siehe Urteil vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18 und die dort angeführte Rechtsprechung, Rn. 172 bis 180.

⁴⁴ Siehe Urteile vom 5. April 2022, *Commissioner of the Garda Síochána* u. a., C-140/20, EU:C:2022:258, Rn. 61 und 62, und vom 20. September 2022, *SpaceNet AG*, C-793/19 und C-794/19 und die dort angeführte Rechtsprechung, Rn. 92 bis 94.

75. Wenn also das Screening von *Metadaten* von Kommunikation vom Gerichtshof nur für das Ziel der Wahrung der *nationalen Sicherheit* als verhältnismäßig beurteilt wird, ist es eher wenig wahrscheinlich, dass ein ähnliches Screening *der Inhalte* von Kommunikation zum Zwecke der *Bekämpfung von Kriminalität* im Zusammenhang mit sexuellem Kindesmissbrauch als verhältnismäßig angesehen würde – und umso weniger in Bezug auf Verhalten, das keine Straftat darstellt.
76. Aus den vorstehenden Erwägungen ergibt sich, dass die Regelung der Aufdeckungsanordnung in Bezug auf interpersonelle Kommunikation die ernsthafte Gefahr birgt, die Grenzen dessen überschreiten, was zur Erreichung der zulässigerweise verfolgten Ziele angemessen und notwendig ist, und daher nicht mit dem Grundsatz der Verhältnismäßigkeit vereinbar zu sein.

IV. **FAZIT**

77. Der Juristische Dienst des Rates kommt zu dem Schluss, dass im Lichte der Rechtsprechung des Gerichtshofs zum gegenwärtigen Zeitpunkt die Regelung der Aufdeckungsanordnung, wie sie derzeit in der vorgeschlagenen Verordnung in Bezug auf interpersonelle Kommunikation vorgesehen ist, eine besonders schwerwiegende Einschränkung der in den Artikeln 7 und 8 der Charta verankerten Rechte auf Achtung des Privatlebens und Schutz personenbezogener Daten darstellt.
78. Eine solche Regelung birgt die ernste Gefahr,
- a) nicht hinreichend klar, genau und vollständig zu sein, insbesondere im Hinblick auf die zu erwartende Intensität der gerichtlichen Prüfung einer Maßnahme, die in Grundrechte eingreift, und daher nicht dem Erfordernis, dass Einschränkungen der Grundrechte gesetzlich vorgesehen sein müssen, in Bezug auf die unter den Nummern 20 bis 26 genannten Aspekte zu entsprechen;
 - b) den Wesensgehalt der oben genannten Grundrechte einzuschränken, da sie allgemeinen Zugriff auf Inhalte der interpersonellen Kommunikation ermöglicht würde, oder, alternativ,

c) nicht mit dem Erfordernis der Wahrung des Grundsatzes der Verhältnismäßigkeit vereinbar zu sein, da

- sie allgemeines und unterschiedsloses Screening der von einem spezifischen Diensteanbieter verarbeiteten Daten erfordern und alle Personen betreffen würde, die diesen spezifischen Dienst nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte;
- sie nicht Verkehrs- und Standortdaten betreffen würde, sondern den Inhalt der interpersonellen Kommunikation;
- sie das allgemeine Ziel verfolgen würde, Straftaten des sexuellen Kindesmissbrauchs zu bekämpfen, die, obwohl es sich um schwere Straftaten handelt, keine Gefahr für die nationale Sicherheit darstellen.

79. Sollte der Rat beschließen, die interpersonelle Kommunikation im Anwendungsbereich der Aufdeckungsanordnung zu belassen, so sollte die Regelung in einer Weise gezielt ausgerichtet sein, dass sie auf Personen Anwendung findet, bei denen berechtigter Grund zu der Annahme besteht, dass sie in irgendeiner Weise an der Begehung einer Straftat im Zusammenhang mit sexuellem Kindesmissbrauch beteiligt sind oder eine derartige Straftat begangen haben, oder bei denen es zumindest eine indirekte Verbindung zu Straftaten im Zusammenhang mit sexuellem Missbrauch gibt. Zudem sollte der Verordnungsentwurf detailliertere und aussagekräftigere Elemente in Bezug auf die zu verwendende Technologie und das Ausmaß der Einschränkungen der Grundrechte, die sich aus dieser ergeben könnten, sowie weitere Präzisierungen zu den Bedingungen für den Erlass einer Aufdeckungsanordnung sowie zu damit verbundenen möglichen Schutzmaßnahmen enthalten.
