Fachbereich Europa - EU 6

Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“

© 2025 Deutscher Bundestag

Fragen zur EuGH-Rechtsprechung über die Vorratsdatenspeicherung und zu ihrer Übertragbarkeit auf die diskutierte „Chatkontrolle“

Aktenzeichen:	EU 6 - 3000 - 044/25
Abschluss der Arbeit:	27. August 2025
Fachbereich:	EU 6: Fachbereich Europa

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

Inhaltsverzeichnis

1.	**Fragestellung**	**4**
2.	**Position des EuGH zur Vorratsdatenspeicherung**	**4**
2.1.	Überblick über die Urteile in den Rs. C-470/21 und verb. Rs. C-511/18 u. a.	4
2.1.1.	Rechtlicher Rahmen	5
2.1.2.	Schwerer Eingriff bei Rückschlüssen auf das Privatleben	7
2.1.3.	Kein schwerer Eingriff bei bloßer Identitätsfeststellung	8
2.1.4.	Näheres zu den Verpflichtungen zur Vorratsdatenspeicherung	8
2.1.5.	Näheres zum behördlichen Zugang zu den auf Vorrat gespeicherten Daten	9
2.1.6.	Aussagen zu online begangenen Straftaten	9
2.2.	Einordnung der Rs. C-470/21 unter Berücksichtigung der Rezeption im rechtswissenschaftlichen Schrifttum	10
2.3.	Gesamtüberblick über die EuGH-Rechtsprechung zur nationalen Vorratsdatenspeicherung	12
3.	**Bedeutung der Entscheidung zur Rs. C-470/21 für die rechtlichen Rahmenbedingungen einer „Chatkontrolle“**	**13**
3.1.	Überblick über das Vorhaben der CSA-Verordnung	14
3.1.1.	Näher zu den Aufdeckungsanordnungen	15
3.1.2.	Näher zur Durchführung von Aufdeckungsanordnungen	16
3.1.3.	Zusammenfassung des Konzepts der Aufdeckungsanordnungen	17
3.2.	Zur Relevanz der Entscheidung zur Rs. C-470/21 für die Chatkontrolle	18
3.2.1.	Übertragbarkeit der Rechtsprechung zur Vorratsdatenspeicherung	19
3.2.2.	Zur Eingriffsintensivität der geplanten CSA-Verordnung, insbesondere zur Sensibilität von Inhaltsdaten	20
3.2.3.	Übertragung der Rechtfertigungsanforderungen der allgemeinen und unterschiedslosen oder der gezielten Vorratsdatenspeicherung von Verkehrs- und Standortdaten	23
4.	**Ergebnis**	**27**

1. Fragestellung

Der Fachbereich Europa wurde beauftragt, darzustellen, welche Änderungen der Europäische Gerichtshof (EuGH) in seiner Position zur Vorratsdatenspeicherung zuletzt vorgenommen hat (dazu Ziff. 2) und welche Auswirkungen dies auf die rechtlichen Rahmenbedingungen für die auf EU-Ebene diskutierte sog. „Chatkontrolle“[1] hat (dazu Ziff. 3).

2. Position des EuGH zur Vorratsdatenspeicherung

Der Auftraggeber möchte wissen, ob der EuGH in seinem Urteil in der Rechtssache (Rs.) **C-470/21** (La Quadrature du Net u. a.)[2] die Rechtfertigungsanforderungen an die Vorratsdatenspeicherung im Vergleich zu vorgehenden Entscheidungen, insbesondere zu den **verbundenen** (verb.) **Rs. C-511/18, C-512/18 und C-520/18** (La Quadrature du Net u. a.)[3] abgesenkt hat.

Hierzu wird zunächst auf die **Ausarbeitung des Fachbereichs Europa** vom 8. August 2024 mit dem Titel „EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen – Einordnung in die bisherige Rechtsprechung“ verwiesen.[4] Wesentliche Aspekte dieser Arbeit werden nachfolgend unter den Ziff. 2.1. und Ziff. 2.2. dargestellt. Ziff. 2.3. enthält eine Übersicht über die Rechtsprechung des EuGH zur Vorratsdatenspeicherung.

2.1. Überblick über die Urteile in den Rs. C-470/21 und verb. Rs. C-511/18 u. a.

Die Entscheidungen betrafen die Frage, ob mitgliedstaatliche Regelungen über die allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen[5] einer Kommunikationsquelle[6] mit Art. 15 der E-Privacy-Richtlinie[7] und der EU-Grundrechtecharta (GRCh) vereinbar sind.

---

1 Gemeint sind die im Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention des sexuellen Missbrauchs von Kindern, KOM(2022) 209 endg., 11. Mai 2022, enthaltenen Verpflichtungen für Anbieter interpersoneller Kommunikationsdienste.

2 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon.

3 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a.

4 Fachbereich Europa, EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen – Einordnung in die bisherige Rechtsprechung, EU 6 - 3000 - 027/24, 8. August 2024.

5 Die Rs. C-470/21 betraf zwar die Rechtfertigung des behördlichen Zugangs zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind. Dieser Zugang setzte aber voraus, dass die Betreiber elektronischer Kommunikationsdienste über die IP-Adressen verfügen, weshalb der EuGH die Zulässigkeit dieser Vorratsdatenspeicherung von IP-Adressen prüfte, vgl. EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 74.

6 Dies ist die IP-Adresse, die einem Nutzer zugewiesen ist, von dem eine Kommunikation ausgeht. Abzugrenzen ist diese von IP-Adressen, die dem Adressaten einer Kommunikation zugewiesen sind.

7 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, 31. Juli 2002, S. 37 (konsolidierte Fassung v. 19. Dezember 2009).

Eine allgemeine und unterschiedslose Vorratsdatenspeicherung kann fast die gesamte Bevölkerung betreffen, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme vorgenommen wird.[8] Demgegenüber versteht der EuGH unter „gezielter Vorratsdatenspeicherung“ nationale Regelungen, die die Speicherung auf Personen oder Orte begrenzen, welche in zumindest mittelbarem Zusammenhang mit dem verfolgten Ziel stehen.[9] Als „umgehende Sicherung“ bezeichnet der EuGH die Anordnung der fortdauernden Datenspeicherung nach Ablauf der maßgeblichen gesetzlichen Fristen zur Bekämpfung schwerer Kriminalität oder zum Schutz der nationalen Sicherheit.[10]

2.1.1. Rechtlicher Rahmen

Die Vorratsdatenspeicherung als solche und der behördliche Zugang zu den auf Vorrat gespeicherten Daten weichen von dem in der E-Privacy-RL normierten Grundsatz ab, dass Daten nicht ohne Einwilligung des Betroffenen auf Vorrat gespeichert werden dürfen.[11] Sie stellen rechtfertigungsbedürftige Eingriffe in die Datenschutzgrundrechte aus Art. 7 und Art. 8 GRCh sowie in die Meinungsfreiheit aus Art. 11 GRCh dar.

Aus Art. 15 Abs. 1 E-Privacy-RL folgt, dass nationale Regelungen zur Vorratsdatenspeicherung grundsätzlich mit folgenden Ziele gerechtfertigt werden können:

- Schutz der nationale Sicherheit,
- Landesverteidigung,
- öffentliche Sicherheit,
- **Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten**,
- Verhütung des unzulässigen Gebrauchs elektronischer Kommunikationssysteme.

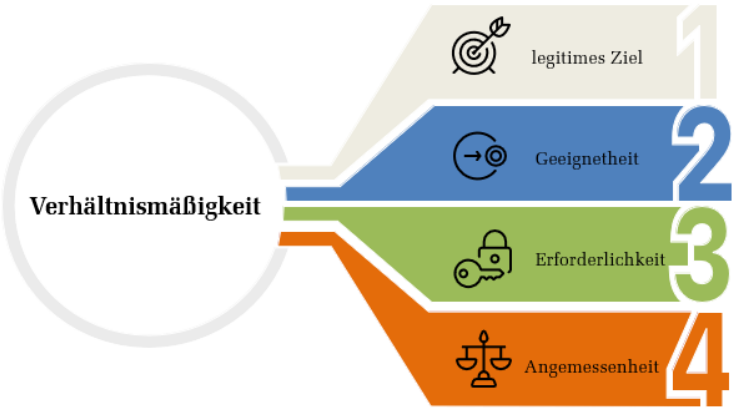
---

8 Vgl. EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 66; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 143.

9 Vgl. EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 76 ff.; Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 104 ff.

10 Vgl. EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 114 ff.; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 85 ff.

11 Vgl. etwa EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 32 ff.; Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 49 ff.



Aus Art. 15 Abs. 1 E-Privacy-RL und Art. 52 Abs. 1 GRCh ergibt sich, dass Regelungen über die Vorratsdatenspeicherung, die eines der vorgenannten Ziele verfolgen, **verhältnismäßig** sein müssen. Das heißt, die Regelungen müssen **geeignet** sein, eines der **legitimen Gemeinwohlziele** zu erreichen. Sie müssen zudem **erforderlich** sein, was bedeutet, dass kein gleich geeignetes, milderes Mittel zur Verfügung steht. Schließlich müssen sie **angemessen** sein. Das heißt, dass die durch Regelungen zur Vorratsdatenspeicherung verursachten Nachteile in einem angemessenen Verhältnis zur Bedeutsamkeit des angestrebten Ziels stehen müssen.[12] Diese Prüfungsschritte entsprechen denen, die das Bundesverfassungsgericht im Rahmen der Verhältnismäßigkeitsprüfung von Grundrechtseingriffen prüft.[13]

Der EuGH hat zu den legitimen Gemeinwohlzielen und der Geeignetheit entschieden, dass Regelungen zur Vorratsdatenspeicherung den in Art. 15 E-Privacy-RL **abschließend aufgezählten Zielen tatsächlich strikt dienen** müssen.[14] Rechtsvorschriften zur Vorratsdatenspeicherung müssen daher objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen, also beispielsweise geeignet sein, zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beizutragen.[15]

Hinsichtlich der Erforderlichkeit ist nach der Rechtsprechung des EuGH relevant, ob der Umfang und die Dauer der Vorratsdatenspeicherung sowie der behördliche Zugang auf das Erforderliche bzw. **auf absolut Notwendige beschränkt**[16] sind.[17] In den Urteilen zur Rs. C-470/21 und den verb. Rs. C-511/18, C-512/18 und C-520/18 misst der EuGH dem Umstand Bedeutung zu, dass es

---

12 Vgl. *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GRCh, Rn. 17; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 52 GRCh, Rn. 65 ff., jeweils m. N. aus der Rechtsprechung.

13 Siehe dazu: *Sommermann*, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 20 GG, Rn. 313 ff.

14 EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 41; Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 58.

15 EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 55 m. w. N.

16 Die hohe Anforderung der Beschränkung auf das „absolut Notwendige“ findet sich auch bei sonstigen Einschränkungen des Schutzes personenbezogener Daten, vgl. etwa EuGH, Urteil vom 9. November 2010, verb. Rs. C-92/09, C-93/09, Volker und Markus Schecke und Eifert, Rn. 77; *Jarass*, in: Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GRCh, Rn. 17.

17 Vgl. EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 93, 113; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 130, 156. Vgl. auch: EuGH, Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur (Conditions d’accès aux données relatives aux communications électroniques), Rn. 38.

jeweils um **online begangene Straftaten** ging. In beiden Entscheidungen ging der EuGH davon aus, dass der Zugang zu IP-Adressen **die einzige Ermittlungsmaßnahme sein könne, die eine effektive Identifizierung ermögliche**. Bei einem Verzicht auf die Vorratsdatenspeicherung der IP-Adresse der Kommunikationsquelle drohe daher eine systemische Straflosigkeit. Dies spreche dafür, dass der Grundrechtseingriff zwingend erforderlich sei.[18] Jedenfalls seien andere Optionen – wie die Prüfung aller Online-Aktivitäten – eingriffsintensiver.[19]

Der letzte Prüfungspunkt – die **Angemessenheit** oder auch „**Zweck-Mittel-Relation**" – spielt in den Entscheidungen zur Rs. C-470/21 und den verb. Rs. C-511/18, C-512/18 und C-520/18 eine wichtige Rolle. Hinsichtlich der Frage, wie gewichtig das mit der Vorratsdatenspeicherung verfolgte Gemeinwohlziel ist, kommt es auch darauf an, welche Rechte und Freiheiten anderer durch die Maßnahmen geschützt werden. Es kommen insofern insbesondere das Recht auf Sicherheit aus Art. 6 GRCh sowie – im Zusammenhang mit dem Opferschutz bei der Kriminalitätsbekämpfung – staatliche Schutzverpflichtungen aus Art. 7 GRCh sowie aus Art. 3, 4 GRCh hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit in Betracht.[20] Sofern Maßnahmen zum Schutz von Kindern getroffen werden, ist auch Art. 24 Abs. 2 GRCh relevant, der Schutz des Kindeswohls grundrechtlich verankert. Auf die Gewichtung von Eingriffsschwere und Bedeutsamkeit des Gemeinwohlziels wird nachfolgend unter Ziff. 2.1.2. und Ziff. 2.1.3. näher eingegangen.

2.1.2. Schwerer Eingriff bei Rückschlüssen auf das Privatleben

Der EuGH urteilte zu den verb. Rs. C-511/18, C-512/18 und C-520/18 sowie in weiteren Entscheidungen, dass nationale Vorschriften, die eine **allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen einer Kommunikationsquelle** vorsehen, nur zum Schutz der nationalen Sicherheit, zur **Bekämpfung schwerer Kriminalität** und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit unionsrechtlich zulässig sein können.[21] Dies begründete der EuGH mit der **Schwere der Grundrechtseingriffe**. Diese resultierten nach Ansicht des EuGH daraus, dass die IP-Adressen zur **umfassenden Nachverfolgung** der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden konnten, sodass diese Daten die Erstellung eines **detaillierten Profils des Nutzers** ermöglichten.[22] Die in Rede stehenden nationalen Regelungen ließen nach Einschätzung des EuGH **sehr genaue Schlüsse auf das Privatleben der Betroffenen** zu. Dies lag daran, dass nach den in Rede stehenden nationalen Regelungen

18 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 117 f.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 154.

19 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 120 f.

20 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 63 ff.; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 48 f. m. w. N.

21 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 156 sowie EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 102; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 70.

22 Vgl. EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 153 sowie EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 78 f.

nicht nur die IP-Adressen, sondern auch **weitere Daten gespeichert** wurden und eine Verknüpfung dieser Informationen möglich war.[23]

2.1.3. Kein schwerer Eingriff bei bloßer Identitätsfeststellung

In der Rs. C-470/21 stellte der EuGH klar, dass **nicht jede allgemeine und unterschiedslose Vorratsspeicherung** von **IP-Adressen zwangsläufig einen schweren Eingriff** in Art. 7, Art. 8, Art. 11 GRCh darstelle.[24] Ein schwerer Eingriff im Zusammenhang mit der Speicherung von IP-Adressen liege dann nicht vor, wenn **tatsächlich ausgeschlossen** sei, dass durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten **genaue Schlüsse auf den Betroffenen gezogen** werden können. Sofern dies gewährleistet sei, liege kein schwerer Eingriff vor, weshalb eine Rechtfertigung mit dem Ziel der **Bekämpfung von Straftaten im Allgemeinen** möglich sei.[25]

2.1.4. Näheres zu den Verpflichtungen zur Vorratsdatenspeicherung

Wollen Mitgliedstaaten eine Pflicht zur Vorratsdatenspeicherung mit dem Ziel der Bekämpfung von Straftaten im Allgemeinen einführen, müssen sie nach der Entscheidung zur Rs. C-470/21 klare und präzise Regeln für die Modalitäten der Speicherung vorsehen, die **ausschließen**, dass die **IP-Adressen** mit anderen auf Vorrat gespeicherten **Verkehrs- und Standortdaten**[26] dergestalt **kombiniert** werden, dass genaue Schlüsse auf das Privatleben des Betroffenen möglich sind.[27] Werden die IP-Adressen hingegen nur mit Identitätsdaten[28] verknüpft, um die Identität des Verdächtigen herauszufinden, sieht der EuGH hierin keinen schwerwiegenden Eingriff.

Der EuGH hat entschieden, dass es zwar Sache der Mitgliedstaaten sei, die Trennung der Datenkategorien sicherzustellen. Der Gerichtshof gibt aber **Modalitäten** vor, die hierbei zu beachten sind. Nationale Regelungen müssen u. a. sicherstellen, dass die strikte Trennung der verschiedenen Datenkategorien (Identitätsdaten, IP-Adressen, sonstige Verkehrsdaten, Standortdaten) durch

---

23 Vgl. EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 80 f. unter Verweis auf EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 82 f.

24 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 79.

25 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 82, 90.

26 Verkehrsdaten sind nach Art. 2 Buchst. b E-Privacy-RL „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“. Standortdaten sind nach Art. 2 Buchst. c E-Privacy-RL „Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben“.

27 Vgl. im Einzelnen EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 82 ff. Siehe auch die Zusammenfassung von *Roßnagel*, Datenschutzrecht: EuGH lockert Voraussetzungen zur Vorratsdatenspeicherung – Anmerkung, EuZW 2024, S. 657 (665 f.).

28 D.h. Daten, die allein der Identifizierung einer Person dienen, wie Name, Vorname und Adresse, vgl. EuGH, Urteil vom 2. Oktober 2018, Rs. C-207/16, Ministerio Fiscal, Rn. 59, 63.

eine **abgesicherte und zuverlässige Datenverarbeitungseinrichtung stattfindet**. Soweit die Möglichkeit vorgesehen ist, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, muss ein leistungsfähiges technisches Verfahren erlauben, die Wirksamkeit der strikten Trennung dieser Datenkategorien sicherstellen.[29]

Daraus folgt, dass die Betreiber elektronischer Kommunikationsdienste, soweit sie ihren Pflichten zur Vorratsdatenspeicherung nachkommen,[30] **keine Technologien** – wie etwa KI-Anwendungen – **einsetzen dürfen, die die vorgenannten Anforderungen nicht erfüllen**.

2.1.5. Näheres zum behördlichen Zugang zu den auf Vorrat gespeicherten Daten

Auch hinsichtlich des behördlichen Zugangs zu den auf Vorrat gespeicherten Daten geht es in der Rs. C-470/21 darum, ob das Vorliegen eines schweren Eingriffs ausgeschlossen werden kann, sodass eine Rechtfertigung durch die Bekämpfung von Straftaten im Allgemeinen in Betracht kommt.[31]

Insofern ist nach Ansicht des EuGH sicherzustellen, dass Behörden die IP-Adressen nur zur Identifizierung des Verdächtiger nutzen. Sie dürfen nicht dazu dienen, die Online-Aktivität dieser Person zu überwachen und ihre Kontakte oder ihren Standort herauszufinden. Sei dies gewährleistet, betreffe der Zugang zur IP-Adresse diese als Identitätsdatum und nicht als Verkehrsdatum. Es liege dann kein schwerwiegender Eingriff vor.[32]

2.1.6. Aussagen zu online begangenen Straftaten

Wie unter Ziff. 2.1.1. zur Erforderlichkeitsprüfung erwähnt, misst der EuGH sowohl in der Rs. C-470/21 als auch in den verb. Rs. C-511/18, C-512/18, C-520/18 der Frage Bedeutung zu, ob die Straftaten, die bekämpft werden sollen, online begangen werden. Der EuGH weist darauf hin, dass auch für die im Rahmen der Angemessenheitsprüfung erforderliche Abwägung widerstreitender Interessen relevant sei, dass der Zugang zu IP-Adressen bei der Verfolgung von Online-Straftaten ggf. das einzige effektive bzw. das am wenigsten einschneidende Mittel zur Identifikation mutmaßlicher Straftäter sei. Der eigentlich vorrangige Schutz der Freiheit der Meinungsäußerung und der Schutz der Vertraulichkeit personenbezogener Daten könne insbesondere dann hinter die Verfolgung von Allgemeininteressen zurücktreten, wenn andernfalls die Wirksamkeit

---

29 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 85-89; Fachbereich Europa, EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen – Einordnung in die bisherige Rechtsprechung, EU 6 - 3000 - 027/24, 8. August 2024, S. 13 f.

30 Die Rechtmäßigkeit sonstiger Tätigkeiten der Betreiber elektronischer Kommunikationsdienste ist an rechtlichen Maßstäben zu messen, die außerhalb der Vorratsdatenspeicherung gelten.

31 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 95 f.

32 Vgl. EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 95 ff., 101; Fachbereich Europa, EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen – Einordnung in die bisherige Rechtsprechung, EU 6 - 3000 - 027/24, 8. August 2024, S. 14 ff.

strafrechtlicher Ermittlungen, einschließlich der Identifizierung des Straftäters, behindert werde.[33]

Der Generalanwalt, auf dessen Schlussanträge der EuGH in diesem Zusammenhang Bezug nimmt, wies darauf hin, dass sich die Situation bei Online-Straftaten von der Mehrheit der Strafverfolgungen unterscheide. Denn normalerweise hänge die Wirksamkeit der Strafverfolgung nicht von einem einzigen Ermittlungsinstrument ab.[34] Bei Online-Straftaten sei der Zugang zu IP-Adressen zugeordneten Identitätsdaten aber das einzige Mittel zur Aufdeckung und Verfolgung.[35] Hierin dürfte insbesondere der Unterschied zu nicht online begangenen Straftaten liegen, zu deren Aufdeckung die Behörden in der Regel über weitere Ermittlungsmöglichkeiten verfügen.

2.2. Einordnung der Rs. C-470/21 unter Berücksichtigung der Rezeption im rechtswissenschaftlichen Schrifttum

Im rechtswissenschaftlichen **Schrifttum** wurde das Urteil zur Rs. C-470/21 teils als „**Wende**“[36] oder **„Abweichung“**[37] bzw. „**Lockerung**“[38] der bisherigen Rechtsprechung zur Vorratsdatenspeicherung eingestuft. Andere Stimmen bewerteten die Entscheidung demgegenüber als „**Erweiterung und Konkretisierung**“[39] oder nur als „**Konkretisierung**“[40] bzw. „**Präzisierung**“[41].

Hierzu ist zunächst festzustellen, dass sich das Urteil ausschließlich auf die Vorratsdatenspeicherung der IP-Adressen einer Kommunikationsquelle bezieht. Diese hat der EuGH bereits in seiner

---

33 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 116.

34 Vgl. auch EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u. a., Rn. 69.

35 GA *Szpunar*, Schlussanträge vom 28. September 2023 zu EuGH, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 60 f.

36 *Seyda/Zurawski*, Glatteis für „Quick Freeze“ – schon überholt von Hessen und dem EuGH?, ZD-Aktuell 2024, 01696.

37 Vgl. *Hartl/Vogl*, EuGH: Lockerung der Voraussetzungen zur Vorratsdatenspeicherung – Urteilsanmerkung, NJW 2024, S. 2099 (2107). So wohl auch: *Veeck/Jechel*, EuGH: Der EuGH zur Vorratsdatenspeicherung – Völlige Abkehr von der bisherigen Rechtsprechung?, LTZ 2024, S. 340 (349).

38 Vgl. *Hartl/Vogel*, Lockerungen der Voraussetzungen zur Vorratsdatenspeicherung, NJW 2024, S. 2099 (2107); LTO, EuGH erlaubt Vorratsdatenspeicherung bei allen Straftaten, 2. Mai 2024. Vgl. auch *Seyda/Zurawski*, Glatteis für „Quick Freeze“ – schon überholt von Hessen und dem EuGH?, ZD-Aktuell 2024, 01696, die von einer „scheinbaren Lockerung“ sprechen.

39 *Eifinger*, Vorratsdatenspeicherung zur Bekämpfung von Urheberrechtsverletzungen zulässig, GRUR-Prax 2024, S. 433.

40 *Ferner*, in: BeckOK StPO, 52. Edition Juli 2024, § 174 TKG, Rn. 35.1.

41 *Bär*, in: BeckOK StPO, 52. Edition Juli 2024, § 100g StPO, Rn. 69a. So wohl auch: *Roßnagel*, Datenschutzrecht: EuGH lockert Voraussetzungen zur Vorratsdatenspeicherung – Anmerkung, EuZW 2024, S. 657 (665 f.).

vorherigen Rechtsprechung als weniger sensibel als sonstige Verkehrsdaten eingestuft.[42] Das Urteil betraf **nicht die Vorratsdatenspeicherung sonstiger Verkehrs- und Standortdaten**, sodass insofern Änderungen der bisherigen Rechtsprechung ausscheiden.

Eine Abweichung von der bisherigen Rechtsprechung liegt aber insofern vor, als der EuGH in vorherigen Urteilen entschieden hatte, dass eine allgemeine und unterschiedslose Vorratsspeicherung der **IP-Adressen einer Kommunikationsquelle** nur durch die gewichtigen Gemeinwohlziele der nationalen Sicherheit, Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit gerechtfertigt werden könne. In der Rs. C-470/21 wird der weniger gewichtige Rechtfertigungsgrund der Bekämpfung von Straftaten im Allgemeinen anerkannt. Der EuGH betont aber, dass es sich hierbei **nicht um eine Lockerung der etablierten rechtlichen Maßstäbe**, sondern um ihre Anwendung auf den konkreten – von vorherigen Entscheidungen abweichenden – Sachverhalt handele. Der EuGH bestätigt seine Rechtsprechung, nach der schwere Grundrechtseingriffe im Zusammenhang mit der Vorratsdatenspeicherung nur durch gewichtige Gemeinwohlziele der E-Privacy-RL gerechtfertigt werden können (wie die Bekämpfung schwerer Kriminalität).[43] Demgegenüber entsprach es der Rechtsprechung bereits vor der Rs. C-470/21, dass nicht schwerwiegende Grundrechtseingriffe durch das Ziel Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein können.[44] Auf dieser Grundlage gelangte der EuGH zu der Einschätzung, dass der Grundrechtseingriff in der Rs. C-470/21 – bei Beachtung der im Urteil formulierten Modalitäten – weniger schwer wog als die in früheren Verfahren durch eine Vorratsdatenspeicherung von IP-Adressen ausgelösten Eingriffe.[45]

---

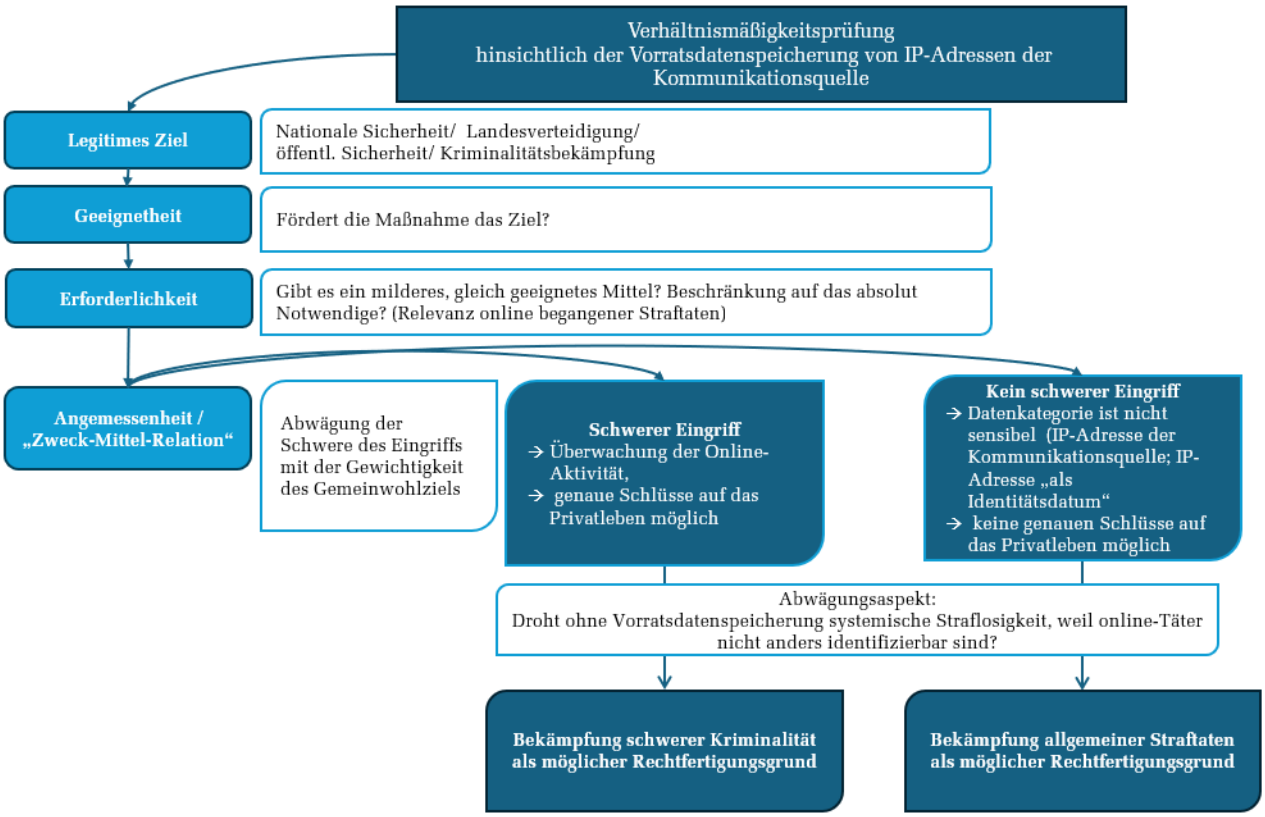
42 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 152. Ebenso: EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 76. Kritisch: *Vettermann*, »Don't stop me now!«: Speicherung von IP-Adressen auf Vorrat zur Prävention von Urheberrechtsverletzungen, ZUM 2024, S. 722 (724).

43 EuGH, Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 33 ff. m. w. N.

44 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 73; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u. a., Rn. 59; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 140 m. w. N.

45 So auch: *Hartl/Vogl*, EuGH: Lockerung der Voraussetzungen zur Vorratsdatenspeicherung – Urteilsanmerkung NJW 2024, S. 2099 (2107).

Die Verhältnismäßigkeitsprüfung des EuGH hinsichtlich der Vorratsdatenspeicherung von IP-Adressen der Kommunikationsquelle lässt sich vereinfacht wie folgt darstellen:



2.3. Gesamtüberblick über die EuGH-Rechtsprechung zur nationalen Vorratsdatenspeicherung

Die Rechtsprechung des EuGH zur Vorratsdatenspeicherung zeichnet sich durch die Gewichtung der Sensibilität betroffener Datenkategorien auf der einen Seite und der Bedeutsamkeit des Gemeinwohlziels auf der anderen Seite aus. Sie lässt sich wie folgt zusammenfassen:

- Eine **allgemeine und unterschiedslose** Vorratsdatenspeicherung von **Verkehrs- und Standortdaten** ist nur zulässig zum **Schutz der nationalen Sicherheit**.[46]
- Eine **gezielte** Vorratsdatenspeicherung von **Verkehrs- und Standortdaten**, die die Speicherung auf Personen oder Orte begrenzt, welche in zumindest mittelbarem Zusammenhang

46 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 1. Siegelstrich; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor 1, 1. Spiegelstrich. Vgl. auch EuGH, Urteil vom 17. November 2022, Rs. C-350/21, Spetsializirana prokuratura () und à la localisation), Tenor 1, wonach eine präventive allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auch für einen begrenzten Zeitraum von sechs Monaten nicht mit dem Ziel der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit gerechtfertigt werden kann.

mit dem verfolgten Ziel stehen, kann mit dem **Schutz der nationalen Sicherheit**, der **Bekämpfung schwerer Kriminalität** und der **Verhütung schwerer Bedrohungen der öffentlichen Sicherheit** gerechtfertigt werden.[47]

- Eine allgemeine und unterschiedslose Vorratsdatenspeicherung von **Identitätsdaten** kann mir der **Bekämpfung von Straftaten im Allgemeinen**, dem Schutz der nationalen Sicherheit und der öffentlichen Sicherheit gerechtfertigt werden.[48]
- Nach der Entscheidung zur **Rs. C-470/21** kann eine **allgemeine und unterschiedslose** Vorratsdatenspeicherung von **IP-Adressen der Kommunikationsquelle** zur Identifikation mutmaßlicher Straftäter mit der **Bekämpfung von Straftaten im Allgemeinen** gerechtfertigt sein, sofern sichergestellt ist, dass kein schwerwiegender Grundrechtseingriff vorliegt. Die **IP-Adresse** fungiert dann **als Identitätsdatum**. Sofern hingegen mit der IP-Vorratsdatenspeicherung der Kommunikationsquelle ein schwerwiegender Grundrechtseingriff einhergeht, kommen als rechtfertigende Gemeinwohlziele nur der Schutz der nationalen Sicherheit, die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit in Betracht.[49]
- Durch Anordnung einer zuständigen Behörde kann den Betreibern elektronischer Kommunikationsdienste, nach Ablauf der maßgeblichen gesetzlichen Fristen, aufgegeben werden ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern („**Quick-Freeze**“), wenn dies zur **Bekämpfung schwerer Kriminalität** oder zum **Schutz der nationalen Sicherheit** erforderlich ist.[50]

3. Bedeutung der Entscheidung zur Rs. C-470/21 für die rechtlichen Rahmenbedingungen einer „Chatkontrolle“

Der Auftraggeber möchte wissen, ob sich aus dem EuGH-Urteil zur Rs. C-470/21 Änderungen der juristischen Rahmenbedingungen für die auf EU-Ebene diskutierte „Chatkontrolle“ ergeben. Hier-

---

47 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 2. Siegelstrich; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Tenor 1, 1. Spiegelstrich; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor 1, 2. Spiegelstrich.

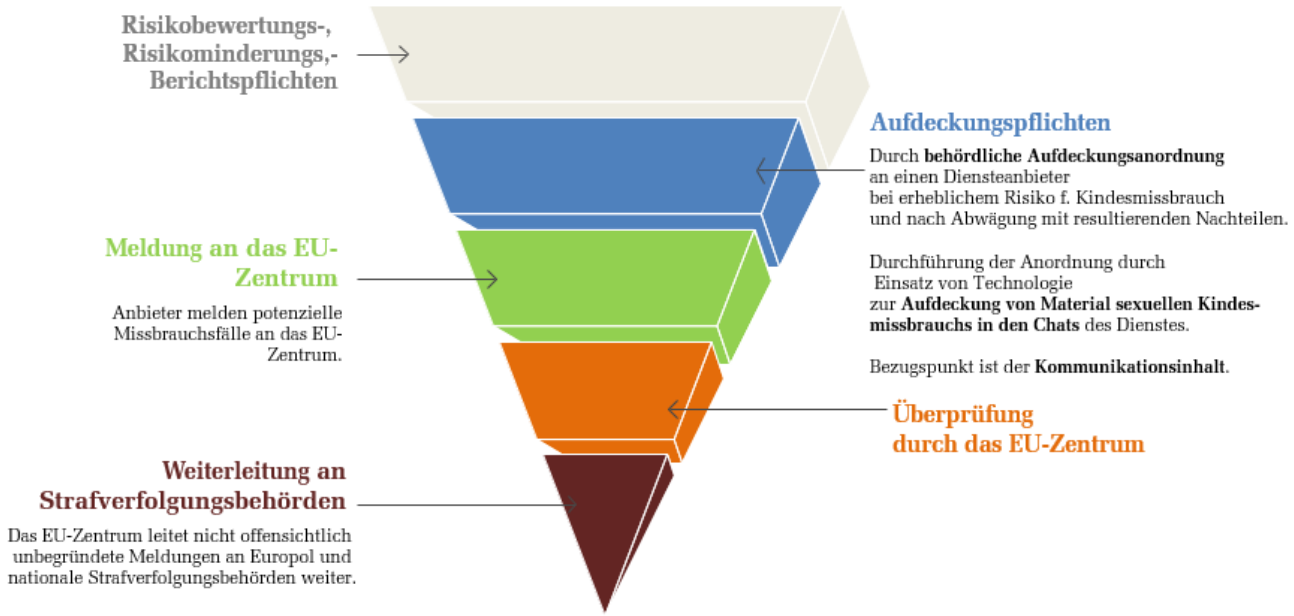
48 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 4. Siegelstrich; Urteil vom 2. Oktober 2018, Rs. C-207/16, Ministerio Fiscal, Tenor.

49 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 155 f.

50 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 5. Siegelstrich; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Tenor 1, 4. Spiegelstrich; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor 1, 5. Spiegelstrich.

mit sind die seit 2022 diskutierten Regelungen für Anbieter interpersoneller Kommunikationsdienste[51] im Verordnungsvorschlag zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSA-Verordnung) gemeint.[52] Nachfolgend wird ein Überblick über die vorgeschlagenen Regelungen der CSA-Verordnung gegeben (Ziff. 3.1.). Dann wird auf die Anwendbarkeit der Entscheidung zur Rs. C-470/21 auf diese Regelungen eingegangen (Ziff. 3.2.).

3.1. Überblick über das Vorhaben der CSA-Verordnung



Pflichten der Anbieter interpersoneller Kommunikationsdienste nach dem Vorschlag der CSA-Verordnung

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

52 KOM(2022) 209 endg., 11. Mai 2022. Übergangsweise gilt die 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, 30. Juli 2021, S. 41 (konsolidierte Fassung v. 15. Mai 2024). Die Verordnung gilt nach Art. 10 der konsolidierten Fassung bis April 2026. Vgl. zu ihrem Inhalt: Deutscher Bundestag, Wissenschaftliche Dienste, Sachstand, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 - 3000 - 021/22, 21. Mai 2022, S. 9.

Der Vorschlag der Kommission (im Folgenden VO-Vorschlag) zielt darauf, einheitliche Vorschriften festzulegen, um gegen den Missbrauch von Diensten der Informationsgesellschaft für sexuellen Kindesmissbrauch im Internet vorzugehen, vgl. Art. 1 Abs. 1 VO-Vorschlag.

Hierfür sollen u. a. Anbietern interpersoneller Kommunikationsdienste Verpflichtungen auferlegt werden.[53] Diese umfassen Risikobewertungs-, Risikominderungs- und Berichtspflichten (vgl. Art. 3 ff. VO-Vorschlag). Darüber hinaus sieht der VO-Vorschlag vor, dass einem Diensteanbieter unter bestimmten Voraussetzungen durch **nationale Behörden** auch sog. **Aufdeckungspflichten** auferlegt werden können. Danach muss der jeweilige Anbieter Technologien einsetzen, um bereits bekanntes oder neues **Material über den sexuellen Kindesmissbrauch** bzw. das sog. **Grooming** (d. h. Kontaktaufnahme zu Kindern für sexuelle Zwecke) aufzudecken (vgl. Art. 2 Buchst. m – o, Art. 7 ff. VO-Vorschlag).

Sofern der Anbieter auf diesem Weg Kenntnis von potenziellem Kindesmissbrauch erhält, hat er dies gemäß Art. 12 VO-Vorschlag dem **EU-Zentrum** zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (EU-Zentrum, vgl. Art. 40 ff. VO-Vorschlag) zu **melden**). In dieser Meldung müssen nach Art. 13 Abs. 1 Buchst. c, d, f, g VO-Vorschlag u. a. **alle Inhaltsdaten**, einschließlich Bilder, Videos und Texte, **alle sonstigen verfügbaren Daten, Angaben zum geografischen Standort**, der mit dem potenziellen sexuellen Kindesmissbrauch im Internet zu tun hat, (bspw. die **IP-Adresse**) und **Angaben zur Identität** aller am potenziellen sexuellen Kindesmissbrauch im Internet beteiligten Nutzer enthalten sein. Das EU-Zentrum prüft die Meldungen und leitet sie, wenn sie nicht offensichtlich unbegründet sind, an die Europol und die voraussichtlich zuständige nationale Strafverfolgungsbehörde weiter, vgl. Art. 48 VO-Vorschlag.

3.1.1. Näher zu den Aufdeckungsanordnungen

Die genannten Aufdeckungspflichten sollen nach dem VO-Vorschlag **nicht unmittelbar gesetzlich**, sondern aufgrund einer **Aufdeckungsanordnung** einer Justiz- oder unabhängigen Verwaltungsbehörde entstehen. Für deren Erlass sind verfahrensrechtliche und materiell-rechtliche Voraussetzungen formuliert, um die Verhältnismäßigkeit der Maßnahme zu gewährleisten, vgl. Art. 7, 10 VO-Vorschlag.[54] Unter anderem müssen im Rahmen eines mehrstufigen Verfahrens unter Beteiligung des EU-Zentrums und des Diensteanbieters sowie unter Berücksichtigung der von ihm ergriffenen Risikobewertungs- und Risikominderungsmaßnahmen folgende materielle Erlassvoraussetzungen gegeben sein: (1) Vorliegen von Beweisen für ein **erhebliches, näher definiertes Risiko** der Nutzung des jeweiligen Dienstes für den sexuellen Kindesmissbrauch und (2) behördliche Einschätzung, dass die Gründe für den Erlass der Aufdeckungsanordnung **schwerer wiegen**

53 Verpflichtungen sind auch für Anbieter von Hostingdiensten, Internetzugangsdiensten und von Diensten der Informationsgesellschaft vorgesehen, vgl. Art. 1 VO-Vorschlag. Für die Frage der Chatkontrolle sind aber die Verpflichtungen der Anbieter interpersoneller Kommunikationsdienste relevant.

54 Vgl. näher: Deutscher Bundestag, Fachbereich Europa, Sachstand, Überblick zum Stand der rechtswissenschaftlichen Diskussion zum Vorschlag der Kommission vom 11. Mai 2022, COM(2022), 209 final, PE 6 - 3000 - 032/22, 20. Juni 2022, S. 7.

als die negativen Folgen für die Rechte und Interessen aller betroffenen Parteien. Zu gewährleisten ist ein angemessenen Gleichgewichts zwischen den **Grundrechten** dieser Parteien, vgl. Art. 7 Abs. 3 – 7 VO-Vorschlag.[55]

Art. 7 Abs. 8 VO-Vorschlag sieht vor, dass die Aufdeckungsanordnung so zielgerichtet und spezifisch zu formulieren ist, dass die negativen Folgen auf das **unbedingt erforderliche Maß** beschränkt bleiben. Hierfür müssen die zuständigen nationalen Behörden alle relevanten Parameter berücksichtigen. Dazu gehört die Frage, ob effektive und möglichst geringe Fehlerquoten („False Positives") generierende Technologien zur Verfügung stehen. Die nationalen Erlassbehörden müssen zudem u. a. dafür Sorge tragen, dass Aufdeckungsmaßnahmen – sofern das identifizierte Risiko auf einen identifizierbaren Teil oder Aspekt des Dienstes beschränkt ist – nur in Bezug auf diesen **konkret risikobehafteten Teil** oder **Aspekt des jeweiligen Dienstes** Anwendung finden. Die Geltungsdauer muss auf das unbedingt erforderliche Maß beschränkt bleiben (vgl. im Einzelnen Art. 7 Abs. 8 Satz 2, 3 und Abs. 9 VO-Vorschlag, wobei bei Aufdeckungsanordnungen bzgl. bekannten oder neuen Materials 24 Monate und bzgl. Grooming 12 Monate nicht überschritten werden dürfen).[56]

3.1.2. Näher zur Durchführung von Aufdeckungsanordnungen

Art. 10 VO-Vorschlag regelt, wie die Anbieter eine Aufdeckungsanordnung durchführen sollen.[57]

Nach Art. 10 Abs. 1 VO-Vorschlag haben sie zur Aufdeckung Technologien einzusetzen, die bekannte oder neue Darstellungen sexuellen Kindesmissbrauchs oder des Groomings mithilfe der vom EU-Zentrum bereitgestellter **Indikatoren** (vgl. Art. 44, 46 VO-Vorschlag) erkennen. Die Technologien dürfen nach Art. 10 Abs. 3 VO-Vorschlag u. a. nur **Informationen extrahieren** können,

---

55 Sowohl der Juristische Dienst des Rates (JD) als auch der Wissenschaftliche Dienst des Europäischen Parlaments (European Parliamentary Research Service – EPRS) haben angesichts der im VO-Vorschlag verwendeten unbestimmten Rechtsbegriffe Zweifel geäußert, ob es sich bei den Bestimmungen um eine hinreichend klare, präzise und vollständige gesetzliche Grundlage i. S. v. Art. 52 Abs. 1 GRCh handele. Vgl. JD, Gutachten, Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – Aufdeckungsanordnungen für interpersonelle Kommunikation – Artikel 7 und 8 der Charta der Grundrechte – Recht auf Privatleben und den Schutz personenbezogener Daten – Verhältnismäßigkeit, Dok.-Nr. 8787/23, 26. April 2023, Rn. 24 (im Folgenden JD-Gutachten); EPRS, Proposal for a regulation laying down the rules to prevent and combat child sexual abuse, Complementary impact assessment, April 2023, S. 37 ff. (im Folgenden EPRS-Folgenabschätzung). Vgl. dagegen Kommissionsdienststellen, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Balancing the rights of children with users' rights, Dok.-Nr. 9512/23, 16. Mai 2023, Rn. 20 ff. (im Folgenden KOM-Non-Paper).

56 Der EPRS hat darauf verwiesen, dass die Erneuerung der Anordnung im VO-Vorschlag nicht verboten sei, was zu einer unbegrenzten Geltung führen könne, vgl. EPRS-Folgenabschätzung, S. 52 f.

57 Vgl. auch Deutscher Bundestag, Fachbereich Europa, Sachstand, Überblick zum Stand der rechtswissenschaftlichen Diskussion zum Vorschlag der Kommission vom 11. Mai 2022, COM(2022), 209 final, PE 6 - 3000 - 032/22, 20. Juni 2022, S. 7 f.

die **unbedingt notwendig sind**, um mithilfe der Indikatoren Muster zu erkennen, die auf die Verbreitung relevanten Materials hindeuten. Sie müssen hinreichend zuverlässig sein, sodass die Fehlerquote bei der Erkennung soweit wie möglich minimiert wird.[58]

Nach Art. 10 Abs. 4 VO-Vorschlag haben Anbieter u. a. sicherzustellen, dass die ergriffenen Maßnahmen auf das **unbedingt Erforderliche beschränkt** sind. Sie müssen wirksame interne Verfahren festlegen, um den Missbrauch der eingesetzten Technologie zu verhindern und um für eine regelmäßige **menschliche Aufsicht** sowie erforderlichenfalls menschliches Eingreifen sorgen. Art. 10 Abs. 5 VO-Vorschlag normiert Informationspflichten. Danach muss der jeweilige Anbieter u. a. **darüber informieren**, dass und wie er **Technologien** zur Durchführung einer Aufdeckungsanordnung **einsetzt,** wie sich dies auf die **Vertraulichkeit der Kommunikation** der Nutzer auswirkt und dass er Inhalte ggf. dem EU-Zentrum melden muss.

3.1.3. Zusammenfassung des Konzepts der Aufdeckungsanordnungen

Nach dem VO-Vorschlag sollen Anbieter interpersoneller Kommunikationsdienste nicht rein präventiv aufgrund einer gesetzlichen Regelung zum „Screening“ von Chats verpflichtet werden. Die Aufdeckungspflichten sollen vielmehr erst aufgrund einer an einen bestimmten Dienst gerichteten **behördlichen Aufdeckungsanordnung** entstehen, sofern Beweise für ein erhebliches **Risiko** der Nutzung des jeweiligen Dienstes für den sexuellen Kindesmissbrauch vorliegen und nach behördlicher Einschätzung die Gründe für den Erlass der Aufdeckungsanordnung schwerer wiegen als die damit einhergehenden negativen Folgen.

Der **Verordnungsvorschlag** zielt auf die Erfassung und ggf. Meldung von **Kommunikationsinhalten**.[59] Bei der **Meldung** potenziellen Kindesmissbrauchs an das EU-Zentrum sollen nach Art. 13 VO-Vorschlag **zusätzlich Meta- und Identitätsdaten** übermittelt werden (Ziff. 3.1.).

Es bleibt abzuwarten, welche **Änderungen im weiteren Gesetzgebungsverfahren** hinsichtlich der Aufdeckungsanordnungen vorgenommen werden. Der Kompromisstext des Rates vom 1. Juli 2025[60] sieht u. a. ein modifiziertes Verfahren bei Ende-zu-Ende verschlüsselten Nachrichten vor[61]

---

58 Sowohl der JD als auch der EPRS haben Zweifel geäußert, ob es sich bei den Bestimmungen über die einzusetzende Technologie um eine hinreichend klare, präzise und vollständige gesetzliche Grundlage i. S. v. Art. 52 Abs. 1 GRCh handele. Vgl. JD-Gutachten, Rn. 21; EPRS-Folgenabschätzung, S. 52 f. Vgl. dagegen KOM-Non-Paper, Rn. 20 ff.

59 Der VO-Vorschlag ist hierauf ausgelegt (vgl. nur Art. 44 Abs. 2 Buchst. c VO-Vorschlag) und wird auch so interpretiert (vgl. nur EPRS-Folgenabschätzung, S. 54 f., 59, 62). Soweit im Sachstand der Wissenschaftlichen Dienste (WD 10 - 3000 - 021/22) auf eine Diskussion verwiesen wird, nach der eine Aufdeckung ggf. anhand von Metadaten erfolgen könnte, findet sich dieser Ansatz nicht ausdrücklich im VO-Vorschlag (vgl. Deutscher Bundestag, Wissenschaftliche Dienste, Sachstand, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 - 3000 - 021/22, 21. Mai 2022, S. 19).

60 Ratspräsidentschaft, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Presidency compromise texts, Dok.-Nr. 10131/25, 1. Juli 2025.

61 Siehe zum insofern erforderlichen Client-Side-Scanning und der Kritik hieran etwa: Deutscher Bundestag, Wissenschaftliche Dienste, Sachstand, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle“, WD 10 - 3000 - 021/22, 21. Mai 2022, S. 18 f., 22; EPRS-Folgenabschätzung, S. 55, 58 f. (Verletzung des Wesensgehalts von Art. 8 GRCh, jedenfalls aber Verletzung des Verhältnismäßigkeitsgrundsatzes).

und nimmt bestimmte Inhalte (Ton, Text) sowie dem Berufsgeheimnis[62] unterliegende Kommunikation und – vorerst – Grooming von Aufdeckungsanordnungen aus. Zudem sollen Meldungen an das EU-Zentrum in einem ersten Schritt pseudonymisiert erfolgen, um negative Auswirkungen von „False Positives“ zu begrenzen[63]. Auch soll der Umfang der an das EU-Zentrum zu übermittelnden Metadaten eingegrenzt werden. Das Konzept der auf Inhaltsdaten gerichteten Aufdeckungspflichten hinsichtlich bekannten und neuen Materials bleibt aber auch nach dem Kompromisstext vom 1. Juli 2025 bestehen.

Hinsichtlich der Durchführung einer Aufdeckungsanordnung durch den Einsatz von Technologien soll die Behörde nach Art. 7 Abs. 8 VO-Vorschlag dafür Sorge tragen, dass Aufdeckungsmaßnahmen möglichst auf einen **konkret risikobehafteten Teil** oder **Aspekt des jeweiligen Dienstes** beschränkt bleiben (s. Ziff. 3.1.1.). Der Wissenschaftliche Dienst des Europäischen Parlaments (European Parliamentary Research Service – EPRS) hat in seiner Folgenabschätzung aus April 2023 zur technischen Machbarkeit eines begrenzten Screenings Folgendes ausgeführt: Hinsichtlich bereits bekannten, als sexueller Missbrauch bestätigten Materials sei es möglich, Aufdeckungstechnologien zu programmieren, die die Überwachung auf bestimmte Personengruppen beschränken (bspw. auf Foren oder Chatgruppen, in denen zuvor Material über sexuellen Kindesmissbrauch ausgetauscht wurde).[64] Hinsichtlich **neuen Materials**, das noch nicht als sexueller Kindermissbrauch bestätigt wurde, sei es nach dem zum Erstellungszeitpunkt der Folgenabschätzung verfügbaren Technologie hingegen nicht möglich, die Klassifikatoren zur Aufdeckung hinreichend spezifisch auszugestalten. Daher könnten die Technologien nur **unterschiedslos auf alle Nutzer des jeweiligen interpersonellen Kommunikationsdienstes** angewendet werden.[65] Auch hinsichtlich des Groomings könne weder der Inhalt noch die betroffene Nutzergruppe angesichts der Komplexität des Phänomens eingegrenzt werden, sodass sich das Screening auf sämtliche Kommunikationsinhalte und alle Nutzer eines betroffenen Dienstes erstrecken müsste.[66]

3.2. Zur Relevanz der Entscheidung zur Rs. C-470/21 für die Chatkontrolle

Die rechtlichen Rahmenbedingungen für die Chatkontrolle nach der CSA-Verordnung könnten sich durch die Entscheidung zur Rs. C-470/21 nur dann in relevanter Weise geändert haben, wenn die **EuGH-Rechtsprechung zur Vorratsdatenspeicherung überhaupt übertragbar** wäre (Ziff. 3.2.1.). Darüber hinaus würde eine Anwendung der (vergleichsweise niedrigen) Rechtfertigungsanforderungen aus dieser Entscheidung auf die Aufdeckungspflichten voraussetzen, dass

---

62 Vgl. zur hohen Eingriffsintensität, wenn auch diese Bereiche erfasst sind: EPRS-Folgenabschätzung, S. 61.

63 Vgl. zu dieser Gefahr nur: *Flamme*, EU-Kommission: Gesetzesentwurf zur Chatkontrolle weckt verfassungsrechtliche Bedenken, MMR-Aktuell 2022, 448870.

64 EPRS-Folgenabschätzung, S. 59.

65 EPRS-Folgenabschätzung, S. 60 f. Vgl. in diesem Sinne auch: *Tuchtfeld*, „Vielen Dank, Ihre Post ist unbedenklich“: Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte, VerfBlog vom 25. Mai 2022; *Zurawski*, EU-Kommission: Vorschlag „Chatkontrolle“ – Verhältnisse der Überwachung, ZD-Aktuell 2022, 01240 „[Die Aufdeckungsanordnungen] lassen sich in Anbetracht der Anforderungen und schieren Mengen an Inhalten absehbar nur in Gestalt der vollständigen Kenntnisnahme und automatisierten Scannung aller Inhalte eines Dienstes realisieren“.

66 EPRS-Folgenabschätzung, S. 62.

die **Grundrechtseingriffe das gleiche Gewicht** haben (Ziff. 3.2.2.). Wäre dies der Fall, dann könnten die Aufdeckungsanordnungen, auch wenn sie als allgemeine und unterschiedslose Maßnahmen einzustufen wären, ohne weiteres mit dem Ziel der Bekämpfung des Kindesmissbrauchs, welcher als schwere Kriminalität einzustufen ist[67], gerechtfertigt werden. Ziff. 3.3.3. geht darauf ein, dass der juristische Dienst des Rates (JD) und der EPRS die Rechtfertigungsanforderungen für die Vorratsdatenspeicherung bzw. automatisierte Analyse von Verkehrs- und Standortdaten für maßgeblich halten.

3.2.1. Übertragbarkeit der Rechtsprechung zur Vorratsdatenspeicherung

Die Vorratsdatenspeicherung zeichnet sich dadurch aus, dass Diensteanbieter gesetzlich verpflichtet werden, bestimmte von ihnen erzeugte oder verarbeitete Daten für eine vorgegebene Zeit auf Vorrat zu speichern.[68] Das Konzept der Aufdeckungspflichten unterscheidet sich hiervon, weil sie durch behördliche Anordnung entstehen und darin bestehen, Kommunikationsinhalte zu scannen, statt sie auf Vorrat zu speichern.

Der EuGH hat in den verb. Rs. C-511/18, C-512/18 und C-520/18 auch zu einer von den Diensteanbietern vorzunehmenden **automatisierten Analyse** von Verkehrs- und Standortdaten anhand behördlich festgelegter Kriterien (mit dem Ziel der Terrorismusbekämpfung) und einer Erhebung dieser Daten für die menschlichen Kontrolle geurteilt. Er stufte die automatisierte Analyse der Verkehrs- und Standortdaten als allgemeine und unterschiedslose Datenverarbeitung ein, an die er die **gleichen Rechtfertigungsanforderungen** stellte wie an deren Vorratsdatenspeicherung.[69]

Der **JD** begründet die Übertragbarkeit der Entscheidung zu den verb. Rs. C-511/18, C-512/18 und C-520/18 damit, dass es auch dort um ein behördlich aufgegebenes Screening von Daten elektronischer Kommunikationsdienste unter Verwendung behördlich vorgegebener Indikatoren ging.[70] Er verweist in seinem Gutachten zum VO-Vorschlag aus April 2023 aber auch wiederholt auf die verb. Rs. C-793/19 und C-794/19 (SpaceNet), in der es ausschließlich um die Vorratsdatenspeicherung ging. Der **EPRS** prüft den Vorschlag der CSA-Verordnung anhand der Rechtsprechung

---

67 Vgl. EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19, Ligue des droits humains, Rn. 149.

68 Vgl. nur: EuGH, Urteil vom 8. April 2014, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland, Rn. 16 ff. zur Richtlinie über die Vorratsdatenspeicherung.

69 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 172 ff. Der EuGH stellte zur automatisierten Analyse fest: „Eine solche Regelung greift auch, unabhängig davon, wie diese Daten später genutzt werden, in die Grundrechte ein, die in den Art. 7 und 8 der Charta verankert sind. Schließlich kann sie im Sinne der in Rn. 118 des vorliegenden Urteils angeführten Rechtsprechung abschreckende Wirkungen in Bezug auf die Ausübung der durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung entfalten.“ (ebenda, Rn. 173).

70 Vgl. JD-Gutachten, Rn. 37 f.

des EuGH sowohl zum Verbot der generellen Überwachung als auch zur Vorratsdatenspeicherung.[71] Im Schrifttum wird die Rechtsprechung des EuGH zur Vorratsdatenspeicherung teils ohne weitere Begründung herangezogen.[72]

Die **Kommissionsdienststellen** haben in ihrem Non-Paper zur Abwägung der Rechte des Kindes mit denen der Dienstenutzer vom 16. Mai 2023 vertreten, dass **keine unbesehene Übertragung** der Rechtsprechung zu den Verarbeitungsformen „Vorratsdatenspeicherung" und „automatisierte Analyse" erfolgen sollte. Die in der CSA-Verordnung vorgeschlagene „Aufdeckung" unterscheide sich von diesen Verarbeitungsformen. Die Verhältnismäßigkeit müsse anhand der spezifischen Maßnahme der Aufdeckungsanordnung beurteilt werden.[73]

Abschließend könnte nur der EuGH entscheiden, ob und inwieweit die zur Vorratsdatenspeicherung entwickelten Maßstäbe auf die CSA-Verordnung anwendbar wären.

3.2.2. Zur Eingriffsintensivität der geplanten CSA-Verordnung, insbesondere zur Sensibilität von Inhaltsdaten

Die Übertragbarkeit der Rechtsprechung zur Vorratsdatenspeicherung unterstellt, käme es für die Übertragbarkeit der Rechtfertigungsanforderungen aus der Entscheidung zur Rs. C-470/21 darauf an, dass die mit den Aufdeckungspflichten einhergehenden Grundrechtseingriffe mit der Vorratsdatenspeicherung von IP-Adressen der Kommunikationsquelle vergleichbar sind.

Für die Meldung an das EU-Zentrum, die nach dem Kompromisstext des Rates in einem ersten Schritt pseudonymisiert erfolgen soll, müssten Metadaten und Identitätsdaten erfasst werden (Ziff. 3.1.1., Ziff. 3.1.3.). Zu diesen Daten zählen auch Angaben zum geographischen Standort bspw. in Form der **IP-Adresse**. Insofern gilt, dass die IP-Adresse hier als Verkehrsdatum (Standortdatum) und nicht als Identitätsdatum in Bezug genommen wird. Eine unmittelbare Anwendung der Entscheidung zur Rs. C-470/21 scheidet daher aus. Hinzukommt, dass die IP-Adresse mit weiteren Metadaten verknüpft ist (s. Ziff. 3.1., 3.1.3.), was – hinsichtlich der Meldung an das EU-Zentrum – ebenfalls gegen eine Übertragung der Entscheidung zur Rs. C-470/21 spricht. Insbesondere sieht der Kommissionsvorschlag aber vor, dass sich die Aufdeckungsanordnungen auf den **Inhalt** von Kommunikation beziehen.

Hinsichtlich des Scannens von Inhalten gilt, dass der EuGH – soweit ersichtlich – noch nicht ausdrücklich zur Verhältnismäßigkeit einer verpflichtenden Überprüfung der Inhalte interpersoneller Kommunikation zu Strafverfolgungszwecken geurteilt hat.[74] Aus Urteilen zur Vorratsdatenspeicherung – ihre Übertragbarkeit unterstellt – ergibt sich aber, dass bestimmte Eingriffe in den

---

71 EPRS-Folgenabschätzung, S. 42 ff., 48 ff.

72 Vgl. etwa *Flamme*, EU-Kommission: Gesetzesentwurf zur Chatkontrolle weckt verfassungsrechtliche Bedenken, MMR-Aktuell 2022, 448870; *Zurawski*, EU-Kommission: Vorschlag „Chatkontrolle" – Verhältnisse der Überwachung, ZD-Aktuell 2022, 01240. Vgl. auch: Deutscher Bundestag, Wissenschaftliche Dienste, Ausarbeitung, „Chatkontrolle" – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission, WD 10 - 3000 - 026/22, 7. Oktober 2022, S. 19.

73 KOM-Non-Paper, Rn. 17, 29-31, 49 f.

74 Vgl. JD-Gutachten, Rn. 62; KOM-Non-Paper, Rn. 15.

Inhalt interpersoneller Kommunikation den **Wesensgehalt** von Art. 7 GRCh beeinträchtigen können. Regelungen, die den Wesensgehalt eines Grundrechts nicht achten, sind gemäß Art. 52 Abs. 1 Hs. 2 GRCh **nicht rechtfertigungsfähig** und damit grundrechtswidrig. Im Urteil zu den verb. Rs. C-293/12 und C-594/12 (Digital Rights Ireland u. a.) stellte der EuGH zu einer Regelung über die allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten fest, dass diese deshalb nicht geeignet war, den Wesensgehalt von Art. 7 GRCh anzutasten, weil sie die „Kenntnisnahme des Inhalts elektronischer Kommunikation" nicht gestattete.[75] In der Rs. C-203/15 (Tele2 Sverige) stellte der EuGH fest, dass die dort in Rede stehende Regelung nicht den Wesensgehalt der Art. 7, 8 GRCh antaste, weil sie nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubte.[76] Der EuGH entschied in der Rs. C-362/14 (Schrems), dass

> „eine Regelung, die es den **Behörden** gestattet, **generell**[77] auf den **Inhalt elektronischer Kommunikation zuzugreifen**, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens [verletzt]".[78]

Der **JD** des Rates sieht auf dieser Grundlage eine ernste Gefahr, dass der EuGH – würde er mit dem VO-Vorschlag entsprechenden Regelungen befasst – eine Verletzung des Wesensgehalts von Art. 7 GRCh feststellen würde. Das begründet er damit, dass mit der Auferlegung von Aufdeckungspflichten der **generelle Zugriff auf die Inhalte interpersoneller elektronischer Kommunikation** des verpflichteten Dienstes sowie die generelle Weiterverarbeitung gestattet würden. Der Umstand, dass nach Art. 10 Abs. 3 Buchst. b VO-Vorschlag irrelevante Informationen nicht extrahiert werden sollen, schließe nicht aus, dass mit automatisierten Instrumenten zunächst einmal sämtliche Daten interpersoneller Kommunikation aller Nutzer des verpflichteten Kommunikationsdiensts zu scannen wären.[79] Der **EPRS** kommt zu dem Ergebnis, dass jedenfalls eine Anordnung zur Aufdeckung neuen Materials und Groomings (welches nach dem Ratskompromisstext vom 1. Juli 2025 nicht mehr Gegenstand der CSA-Verordnung sein soll), den Wesensgehalt verletze, weil es sich um eine **Form der allgemeinen und unterschiedslosen Überwachung handele**. Dies liege daran, dass zur Aufdeckung ein Scannen des Gesamtinhalts der über den jeweiligen Anbieter stattfindenden Kommunikation erforderlich sei.[80]

Die **Kommissionsdienststellen** haben in ihrem Non-Paper gegen die vorgenannten Ansichten argumentiert. Eine Anordnung zur Aufdeckung impliziere – anders als JD und EPRS meinen – **keine allgemeinen und unterschiedslosen Maßnahmen**, wie sie in der Rs. C-362/14 (Schrems) in Rede standen (s. noch Ziff. 3.2.3.). Es gehe auch nicht darum, privaten oder staatlichen Akteuren umfassenden Zugriff auf Inhaltsdaten zu geben. Der EuGH in den verb. Rs. C-293/12 und

---

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

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

77 „Generell" meinte hier den uneingeschränkten behördlichen Zugang zu sämtlichen personenbezogenen Daten aller Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, vgl. EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 93.

78 EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14, Schrems, Rn. 94 (Hervorhebungen hinzugefügt).

79 JD-Gutachten, Rn. 10, 56 ff.

80 EPRS-Folgenabschätzung, S. 54 f., 58.

C-594/12 (Digital Rights Ireland u. a.) nur die „Kenntnisnahme“ des Inhalts elektronischer Kommunikation für problematisch gehalten. Es komme daher – anders als insbesondere der JD vertreten hat – sehr wohl darauf an, dass nach dem VO-Vorschlag die Extraktion von Inhalten (als Ergebnis des Scannens des Gesamtinhalts) auf das unbedingt Notwendige beschränkt sei. Allein der Umstand, dass Inhaltsdaten verarbeitet würden, könne keine Verletzung des Wesensgehalts begründen, denn der EuGH habe in der Entscheidung zu den verb. Rs. C-511/18, 512/18 und C-520/18 festgestellt, dass aus Metadaten gewonnene Informationen genauso sensibel sein könnten wie Inhaltsdaten – und gleichwohl mit Blick auf die sensiblen Metadaten keine Wesensgehaltsbeeinträchtigung angenommen. Schließlich sei eine Verletzung des unionsgrundrechtlichen Wesensgehalts durch die geplante CSA-VO abzulehnen, weil sie **keinen vollständigen Überblick über das Privatleben der betroffenen Person ermögliche**.[81] Es sei zu beachten, dass der jeweils aufzudeckende Inhalt die Straftat selbst sei.[82]

Abschließend könnte nur der EuGH entscheiden, ob die Regelungen der CSA-Verordnung, in der Form, in der sie endgültig in Kraft treten, eine Verletzung des Wesensgehalts darstellen. Dabei könnte es u. a. darauf ankommen, ob

- auf das automatisierte Scannen, die Extraktion oder die Kenntnisnahme bzw. den Zugriff abzustellen ist,

- es sich um eine generelle bzw. allgemeine und unterschiedslose Maßnahme handelt (s. sogleich Ziff. 3.2.3.),

- ob es – wie die Kommissionsdienststellen meinen – auch bei Inhaltsdaten für die Eingriffsschwere darauf ankommt, dass sie einen vollständigen Überblick über das Privatleben der betroffenen Person ermöglichen,[83] und wenn ja, ob dies hinsichtlich der CSA-Verordnung zu bejahen wäre. Die von den Kommissionsdienststellen in Bezug genommene Entscheidung zu den verb. Rs. C-511/18, C-512/18 und C-520/18 ist insofern nicht eindeutig. Denn der EuGH entschied dort lediglich, dass Verkehrs- und Standortdaten, wenn aus ihnen genaue Rückschlüsse auf das Privatleben gezogen werden können, genauso sensibel seien, wie der Inhalt der Kommunikation selbst.[84] Damit ist aber nicht gesagt, dass Inhaltsdaten nur dann besonders sensibel sind, wenn auch sie die Erstellung eines Profils der Betroffenen zulassen.

Unabhängig von der Frage der Wesensgehaltsbeeinträchtigung dürfte gleichwohl von einer **besonderen Eingriffsschwere** auszugehen sein. Denn selbst die Kommissiondienststellen halten

---

81 KOM-Non-Paper, Rn. 38 ff.

82 KOM-Non-Paper, Rn. 11, 43.

83 Dagegen offenbar: EPRS-Folgenabschätzung, S. 60.

84 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 117, 184. Ebenso EuGH, Urteil vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige, Rn. 99.

Eingriffe in die Kommunikationsinhalte für „sensibel“ („sensitive“), sodass sie eine **starke Rechtfertigung** erforderten.[85] Zudem begründete der EuGH die besondere Eingriffsschwere in den verb. Rs. C-511/18, C-512/18 und C-520/18 ausdrücklich damit, dass es möglich war, die Art der online konsultierten Information zu identifizieren.[86] Er ging davon aus, dass **Verkehrs- und Standortdaten**, die die **Erstellung eines Profils** des Betroffenen ermöglichen, eine **ebenso sensible Information** darstelle, wie der **Kommunikationsinhalt**.[87] Der JD vertrat in seinem Gutachten die Einschätzung, dass die Rechtsprechung des EuGH zur allgemeinen Vorratsdatenspeicherung von IP-Adressen und Identitätsdaten nicht übertragbar sei, da es bei den Aufdeckungsanordnungen um deutlich sensiblere Daten gehe.[88]

Vor diesem Hintergrund **liegt es nicht nahe**, dass der EuGH – würde er mit den im VO-Vorschlag vorgesehenen Regelungen befasst – **die in der Rs. C-470/21 entwickelten Rechtfertigungsanforderungen** für nicht schwerwiegende Grundrechtseingriffe (IP-Adressen der Informationsquelle als Identitätsdaten) **anwenden würde**.

3.2.3. Übertragung der Rechtfertigungsanforderungen der allgemeinen und unterschiedslosen oder der gezielten Vorratsdatenspeicherung von Verkehrs- und Standortdaten

JD[89] und EPRS[90] sind der Ansicht, dass die Verhältnismäßigkeit der Aufdeckungsanordnung unter Berücksichtigung der EuGH-Rechtsprechung zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu beurteilen sei.[91] Danach ist die allgemeine und unterschiedslose Vorratsdatenspeicherung von Verkehrs- und Standortdaten nur zum Schutz der nationalen Sicherheit zulässig

85 KOM-Non-Paper, Rn. 45.

86 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 83, 174.

87 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 117, 184. Ebenso EuGH, Urteil vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige, Rn. 99.

88 Siehe im Einzelnen: JD-Gutachten, Rn. 70 f.

89 Vgl. im Einzelnen: JD-Gutachten, Rn. 36 ff., 63 ff., 72 ff.

90 EPRS-Folgenabschätzung, S. 58 ff.

91 Wobei der JD davon ausgeht, dass das Screening von Kommunikationsinhalten einen schwerwiegenderen Eingriff darstellt als vergleichbare Verarbeitungen von Verkehrs- und Standortdaten, vgl. JD-Gutachten, Rn. 49.

ist.[92] Die gezielte Vorratsdatenspeicherung von Verkehrs- und Standortdaten kann auch mit der Bekämpfung schwerer Kriminalität gerechtfertigt werden (vgl. Ziff. 2.3., Spstr. 1, 2).[93]

JD und EPRS gehen davon aus, dass die im VO-Vorschlag vorgesehenen Aufdeckungsanordnungen zu **allgemeinen und unterschiedslosen Maßnahmen** führen würden, die allein mit dem Schutz der nationalen Sicherheit, **wohl aber nicht mit dem Ziel der Bekämpfung sexuellen Kindesmissbrauchs zu rechtfertigen** wären.[94] Dieser Ansatz findet sich auch im Schrifttum. Soweit dort aber die Einschätzung vertreten wird, dass eine „allgemeine Überwachung sämtlicher [digitaler] Kommunikation"[95] bzw. eine „bevölkerungsweite, anlasslose Überwachung von Individualkommunikation"[96] geplant sei, die zudem das Gefühl ständiger Überwachung hervorrufe[97], scheint dies die geplanten Regelungen der CSA-Verordnung nicht vollständig zu berücksichtigen. Denn anders als bei der allgemeinen und unterschiedslosen Vorratsdatenspeicherung, die fast die gesamte Bevölkerung betreffen kann, weil sämtliche Betreiber elektronischer Kommunikationsdienste verpflichtet sind,[98] sind Aufdeckungsanordnungen von einem zuvor identifizierten Risiko und einer behördlichen Abwägungsentscheidung abhängig. Sie richten sich jeweils an nur einen Anbieter interpersoneller Kommunikationsdienste (der allerdings viele Nutzer haben kann). Der adressierte Anbieter muss die Nutzer nach Art. 10 Abs. 5 Buchst. a VO-Vorschlag zudem informieren, dass und wie er die an ihn gerichtete Aufdeckungsanordnung durchführt. Nach

92 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 1. Siegelstrich; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor 1, 1. Spiegelstrich.

93 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Tenor 1, 2. Siegelstrich; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Tenor 1, 1. Spiegelstrich; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Tenor 1, 2. Spiegelstrich.

94 Vgl. EPRS-Folgenabschätzung, S. 62; JD-Gutachten, Rn. 72 ff.

95 Vgl. *Tuchtfeld*, „Vielen Dank, Ihre Post ist unbedenklich": Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte, VerfBlog vom 25. Mai 2022, in Bezug genommen in: Deutscher Bundestag, Fachbereich Europa, Sachstand, Überblick zum Stand der rechtswissenschaftlichen Diskussion zum Vorschlag der Kommission vom 11. Mai 2022, COM(2022), 209 final, PE 6 - 3000 - 032/22, 20. Juni 2022. S. 5.

96 Deutschlandfunk. EU-Gesetz gegen Kindesmissbrauchsinhalte. Chatkontrolle „nicht mit Menschenrechten vereinbar". Gespräch zwischen Sören Brinkmann und dem Medienrecht nach Stephan Dreyer vom 11. Mai 2022, abrufbar unter: https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html, zitiert in: Deutscher Bundestag, Wissenschaftliche Dienste, Sachstand, Genese und Inhalt des Vorschlags der EU-Kommission zur „Chatkontrolle", WD 10 - 3000 - 021/22, 21. Mai 2022.

97 Vgl. Deutscher Bundestag, Wissenschaftliche Dienste, Ausarbeitung, „Chatkontrolle" – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission, WD 10 - 3000 - 026/22, 7. Oktober 2022, S. 19.

98 Vgl. EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 66; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 143.

Art. 10 Abs. 6 VO-Vorschlag sollen Nutzer informiert werden, bei denen potenzieller Kindesmissbrauch festgestellt wurde, sofern die Aufdeckungsmaßnahme dadurch nicht beeinträchtigt wird.[99]

JD und EPRS begründen ihre Einschätzung, dass es sich um eine allgemeine und unterschiedslose Maßnahme handele, indem sie darlegen, dass die Aufdeckungsanordnung **keine gezielte Maßnahme** i. S. d. Rechtsprechung des EuGH sei. Eine gezielte Maßnahme setze nach der Rechtsprechung des EuGH voraus, dass eine Beschränkung auf ein geografischen Gebiet und/oder einen Personenkreis gegeben ist, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, oder auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung schwerer Kriminalität beitragen könnten.[100] Der JD argumentiert, dass sich die Aufdeckungsanordnungen auf sämtliche Nutzer eines Dienstes beziehen, ohne dass es darauf ankäme, ob die **jeweiligen Personen** eine auch nur **mittelbare Verbindung zu Straftaten** im Zusammenhang mit sexuellem Kindesmissbrauch hätten.[101] Angesichts des schwerwiegenden Eingriffs, der aus dem Bezug auf Inhaltsdaten resultiere, reiche eine Verbindung zwischen jeweiligen Dienst und Straftaten im Zusammenhang mit dem sexuellen Kindesmissbrauch nicht aus.[102] Der EPRS betont, dass das Instrument der Aufdeckungsanordnung nur dann mit der Bekämpfung von Kindesmissbrauch als schwerem Verbrechen gerechtfertigt werden könnten, wenn sie auf Personen beschränkt werden könne, bei denen objektive Anhaltspunkte für eine zumindest mittelbare Verbindung zu strafbarem sexuellen Kindesmissbrauch vorliege. Der EPRS geht davon aus, dass eine solche Begrenzung hinsichtlich der Aufdeckung neuen Materials und des Groomings (im Ratskompromisstext vom 1. Juli 2025 ausgeklammert) technisch gar nicht möglich sei.[103]

Demgegenüber halten Kommissionsdienststellen die Rechtsprechung zur Vorratsdatenspeicherung und automatischen Analyse von Verkehrs- und Standortdaten für nicht übertragbar. Die Eingriffsintensität sei in diesen Fällen eine andere gewesen, weil es um große Datenpools gegangen sei, aus denen Schlüsse auf das Privatleben der Betroffenen gezogen werden konnten. Demgegenüber gehe mit dem in der CSA-Verordnung vorgeschlagenen „Treffer/kein Treffer"-Modell aufgrund von Indikatoren keine Gefahr einher, dass genaue Schlüsse auf das Privatleben Einzelner gezogen werden (s. schon Ziff. 3.2.1.).[104] Jedenfalls sprächen aber gute Gründe für die Einstufung als gezielte Maßnahme. Angeführt wird:

---

99 Der EuGH hatte das allgemeine Gefühl der Überwachung hingegen damit begründet, dass die Vorratsspeicherung der Daten vorgenommen wurde, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert wurden, vgl. EuGH, Urteil vom 21. Dezember 2016, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige, Rn. 100.

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

101 Vgl. JD-Gutachten, Rn. 39 ff., 78 Buchst. c.

102 JD-Gutachten, Rn. 41, 43, 49.

103 EPRS-Folgenabschätzung, S. 58 ff.

104 KOM-Non-Paper, Rn. 29, 31.

- Die Aufdeckungsanordnung wäre an einen bestimmten Diensteanbieter bzw. einzelne Aspekte oder Teile dieses Dienstes, nicht aber an alle elektronischen Kommunikationsdienste gerichtet.

- Die Aufdeckungspflichten würden nicht unmittelbar durch Gesetz, sondern aufgrund einer Einzelfallentscheidung unter Berücksichtigung der Auswirkungen auf die Grundrechte, die verfügbaren Technologien und notwendige Schutzmaßnahmen ergehen.

- Aufdeckungsanordnungen würden als letztes Mittel nur erlassen, wenn dies aufgrund des bestehenden Risikos trotz der ergriffenen Risikobewertungs- und Risikominderungsmaßnahmen gerechtfertigt sei.

- Es bestünden strikte Fristvorgaben für die Dauer der Aufdeckungspflichten.

- Aufdeckungsanordnungen wären auf spezifische Inhalte beschränkt, die spezifische Straftaten beträfen. Es gehe nicht um breites Spektrum von Straftaten oder allgemeine Gefahren für die nationale Sicherheit.[105]

Zudem sei die JD und EPRS vorgenommene Abgrenzung zwischen allgemeinen und unterschiedslosen bzw. gezielten Maßnahmen **allein anhand der Frage**, ob die betroffenen **Nutzer eine Verbindung zu den relevanten Straftaten** hätten, **zu eng**. Vielmehr könne es nach der Rechtsprechung des EuGH auch eine Rolle spielen, ob die Dauer der Maßnahme beschränkt sei.[106] Und selbst wenn man eine indirekte Verbindung zwischen den betroffenen Nutzern und den etwaigen Straftaten verlangen würde, verweist das Non-Paper darauf, dass der EuGH eine solche (lose) Verbindung über das **geographische Kriterium** bereits bei stark frequentierten **physischen Orte** (bspw. Flughäfen) bestätigt habe, sodass hierauf gerichtete Datenverarbeitungen große Teile der Bevölkerung beträfen. Auf dieser Grundlage wird im KOM-Non-Paper dargelegt, dass von einer solchen Verbindung auch mit Blick auf „**digitale Orte**“ ausgegangen werden könne. Auf dieser Grundlage kommen die Kommissionsdienststellen zu der Einschätzung, dass der VO-Vorschlag objektive Kriterien normiere, die eine **hinreichende Verbindung** zwischen den verarbeiteten Daten und dem mit den vorgeschlagenen Regelungen verfolgten Ziel herstellten. Es gebe in der Rechtsprechung auch keine Anhaltspunkte dafür, dass die Anforderungen an eine „hinreichende Verbindung“ bei Inhaltsdaten anders auszulegen seien als bei Metadaten.[107] Es sei zu bedenken, dass es sich um online begangene und zudem besonders schwere Straftaten handele, die effektiv nur unter Einbindung der Diensteanbieter aufgedeckt werden könnten (s. Ziff. 2.1.1., 2.1.6.).[108] Die Behörden hätten gemäß Art. 3, 4, 7 GRCh[109] eine Schutzpflicht gegenüber Kindern.[110] Auf der

105 KOM-Non-Paper, Rn. 27.

106 Vgl. KOM-Non-Paper, Rn. 31 f.

107 KOM-Non-Paper, Rn. 32 ff.

108 KOM-Non-Paper, Rn. 9, 42, 52 ff.

109 Vgl. EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 126 ff.

110 KOM-Non-Paper, Rn. 51.

Grundlage der bestehenden Rechtsprechung ließen sich Aufdeckungsanordnungen daher mit der Bekämpfung sexuellen Kindesmissbrauchs als schwerem Verbrechen rechtfertigen.[111]

Sollten die Aufdeckungsanordnungen und damit das Scannen von Kommunikationsinhalten in Kraft treten, könnte **abschließend nur der EuGH entscheiden**, welche Rechtfertigungsanforderungen zu stellen bzw. entwickeln sind.

4. Ergebnis

Der EuGH hat in der Rs. C-470/21 klargestellt, dass die allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen der Kommunikationsquelle unter bestimmten Bedingungen eine mit der Vorratsdatenspeicherung von Identitätsdaten vergleichbare (geringe) Eingriffsintensität haben kann. Derartige Grundrechtseingriffe können durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt werden. Dies ändert aber nichts an den höheren Rechtfertigungsanforderungen für die Vorratsdatenspeicherung von Verkehrs- und Standortdaten, die genaue Rückschlüsse auf das Privatleben der Betroffenen zulässt (s. Ziff. 2.2., 2.3.).

Wesentliches Mittel der „Chatkontrolle“ ist nach dem Vorschlag der Kommission für eine CSA-Verordnung das durch Aufdeckungsanordnungen vorgegebene Scannen von Kommunikationsinhalten (Ziff. 3.1.3.). Die Rechtsprechung des EuGH zur Vorratsdatenspeicherung von Inhaltsdaten und zur Vorratsdatenspeicherung sowie zur automatischen Analyse von Verkehrs- und Standortdaten spricht dafür, dass der Gerichtshof hierin schwerwiegenden Grundrechtseingriff sehen könnte. Diese Konstellation wäre dann nicht mit der der Rs. C-470/21 zugrundeliegenden (geringen) Eingriffsintensität vergleichbar. Der JD und der EPRS haben Bedenken geäußert, dass das Scannen von Kommunikationsinhalten den Wesensgehalt von Art. 7 GRCh tangieren könnte. Sie gehen davon aus, dass es sich bei den Aufdeckungsanordnungen nach dem aktuellen Stand der Technik um allgemeine und unterschiedslose Maßnahmen handele, die nicht mit der Bekämpfung schwerer Kriminalität gerechtfertigt werden könnten. Die Kommissionsdienststellen sind der Ansicht, dass es sich um gezielte Maßnahmen handele, die mit dem Ziel der Bekämpfung schwerer Kriminalität (d. h. Kindesmissbrauch) gerechtfertigt werden können (s. Ziff. 3.2.2., Ziff. 3.2.3.).

Fachbereich Europa

111 KOM-Non-Paper, Rn. 57.