75 Jahre
Demokratie
lebendig

Deutscher Bundestag
Unterabteilung Europa
Fachbereich Europa

Ausarbeitung

EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen

Einordnung in die bisherige Rechtsprechung

EuGH-Urteil in der Rs. C-470/21 zur Vorratsdatenspeicherung von IP-Adressen
Einordnung in die bisherige Rechtsprechung

Aktenzeichen:	EU 6 - 3000 - 027/24
Abschluss der Arbeit:	8. August 2024
Fachbereich:	EU 6: Fachbereich Europa

Inhaltsverzeichnis

1. Einleitung und Fragestellung

Der Fachbereich Europa wurde mit der Prüfung beauftragt, ob das Urteil des Europäischen Gerichtshofs (EuGH) vom 30. April 2024 in der Rechtssache (Rs.) C-470/21 hinsichtlich der **Vorratsspeicherung von IP-Adressen zur Verfolgung von Straftaten** eine Bestätigung der bisherigen Rechtsprechung darstellt oder eine neue Rechtslage schafft.

Hierzu wird nachfolgend zunächst ein Überblick über den Inhalt des EuGH-Urteils und über im Schrifttum erfolgte Einordnungen in die bisherige Rechtsprechung gegeben (Ziff. 2.). Unter Ziff. 3 werden die vom EuGH bisher entwickelten unionsrechtlichen Anforderungen an nationale Regelungen zur Vorratsdatenspeicherung zusammengefasst. Ziff. 4 geht näher auf die Urteilsbegründung in der Rs. C-470/21 ein. Auf dieser Grundlage wird in Ziff. 5 bewertet, ob das EuGH-Urteil in der Rs. C-470/21 eine Bestätigung der bisherigen Rechtsprechung darstellt oder eine neue Rechtslage schafft.

Der Auftraggeber hat darüber hinaus die Frage aufgeworfen, **zur Verfolgung welcher Straftaten** in Deutschland eine Pflicht zur Vorratsspeicherung von IP-Adressen zulässig wäre. Unter Ziff. 6 wird analysiert, ob unionsrechtliche Anforderungen an Straftaten bestehen, zu deren Verfolgung IP-Adressen auf Vorrat gespeichert werden dürfen.

2. Überblick: Inhalt Urteils in der Rs. C-470/21 und Einordnungen im Schrifttum

Der EuGH entschied in der Rs. C-470/21, dass eine im nationalen Recht verankerte **allgemeine und unterschiedslose**[1] **Vorratsdatenspeicherung von IP-Adressen** einer Kommunikationsquelle[2], unter näher definierten Voraussetzungen „gegebenenfalls durch das Ziel der **Bekämpfung von Straftaten im Allgemeinen** gerechtfertigt sein kann“. Dies gelte, sofern eine solche Vorratsdatenspeicherung keinen schweren Grundrechtseingriff darstelle. Dafür müsse tatsächlich ausgeschlossen sein, „dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen.“[3]

---

1 Eine allgemeine und unterschiedslose Vorratsdatenspeicherung kann fast die gesamte Bevölkerung betreffen, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme vorgenommen wird, 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. 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, 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. 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, 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.

2 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.

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

Demgegenüber hatte der EuGH in **vorherigen Urteilen** entschieden, 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.[4] Diese Entscheidungen begründete der EuGH im Wesentlichen mit der **Schwere der Grundrechtseingriffe**. Diese resultierten nach Ansicht des EuGH daraus, dass die IP-Adressen aufgrund der jeweiligen nationalen Regelungen 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. Die in Rede stehenden nationalen Regelungen ließen nach Einschätzung des EuGH also „sehr genaue Schlüsse auf das Privatleben der Betroffenen" zu.[5]

Im **Schrifttum** wurde der Umstand, dass der EuGH in der Rs. C-470/21 – anders als in den vorhergehenden Urteilen – davon ausging, die Vorratsdatenspeicherung von IP-Adressen könne zur Ermittlung und Verfolgung *jeglicher* Straftaten mit dem EU-Recht vereinbar sein, teils als „**Wende"**[6] oder **„Abweichung"** von bzw. „**Lockerung"**[7] der bisherigen Rechtsprechung eingestuft. Andere Stimmen bewerten die Entscheidung demgegenüber als „**Erweiterung und Konkretisierung**"[8] oder nur als „**Konkretisierung**"[9] bzw. „**Präzisierung**"[10] Der Gerichtshof habe lediglich klargestellt, dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen zwangsläufig einen schwerwiegenden Grundrechtseingriff darstelle, weshalb auch das weniger gewichtige Gemeinwohlziel der Verhütung und Bekämpfung von Straftaten „im Allgemeinen" als Rechtfertigung der mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe in Betracht komme.[11]

---

4 Wobei solche Regelungen auf den absolut notwendigen Zeitraum begrenzt sein und durch klare und präzise Regeln die Einhaltung der geltenden materiellen und prozeduralen Voraussetzungen sowie den Schutz vor Missbrauchsrisiken sicherstellen müssen, vgl. EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 75, 97; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 70; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 155 f. und Ls. 1, 3. Spiegelstrich.

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

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

7 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.

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

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

10 *Bär*, in: BeckOK StPO, 52. Edition Juli 2024, § 100g StPO, Rn. 69a.

11 Vgl. in diesem Sinne: *Bär*, in: Beck, BeckOK StPO, 52. Edition Juli 2024, § 100g StPO, Rn. 69a.

3. Bisherige EuGH-Rechtsprechung zu mitgliedstaatlicher Vorratsdatenspeicherung

3.1. Art. 15 E-Privacy-Richtlinie i.V.m. den EU-Grundrechten als Rechtmäßigkeitsmaßstab

Der EuGH beurteilt die Unionsrechtskonformität nationaler Regelungen zur Vorratsdatenspeicherung in ständiger Rechtsprechung im Wesentlichen anhand von **Art. 15 E-Privacy-Richtlinie**[12] im Einklang mit den Vorgaben und **Garantien aus der Charta der Grundrechte der Europäischen Union** (**GRCh**).[13]

Die E-Privacy-Richtlinie konkretisiert die Grundrechte auf Achtung des Familienlebens aus Art. 7 GRCh und den Schutz personenbezogener Daten gemäß Art. 8 GRCh, indem sie den **Grundsatz** aufstellt, dass die Mitgliedstaaten die Vertraulichkeit elektronischer Nachrichten und der damit verbundenen Verkehrsdaten[14] sicherzustellen haben. Aus diesem Grund dürfen Daten grundsätzlich **nicht ohne die Einwilligung der Betroffenen auf Vorrat gespeichert** werden.[15]

Art. 15 Abs. 1 Satz 1 E-Privacy-Richtlinie normiert eine eng auszulegende[16] **Ausnahme** von diesem u. a. in Art. 5, 6, 9 E-Privacy-RL[17] normierten Grundsatz, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die **Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten** oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft **notwendig, angemessen und verhältnismäßig ist**. Zu diesem Zweck können die Mitgliedstaaten gemäß Art. 15 Abs. 1 Satz 2 E-Privacy-RL u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe **für begrenzte Zeit gespeichert** werden. Aus Art. 15 Abs. 1 Satz 3 E-Privacy-RL ergibt

---

12 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).

13 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 64 ff.; Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 48 ff.; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 31 ff.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 81 ff.

14 Art. 2 Buchst. b E-Privacy-RL definiert Verkehrsdaten als „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“.

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

16 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 57; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 40.

17 Vgl. näher zu Art. 5 ff. E-Privacy-RL: EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 35 ff.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 107 f.

sich, dass die von den Mitgliedstaaten nach dieser Vorschrift erlassenen Maßnahmen die allgemeinen Grundsätze des EU-Rechts, zu denen der Verhältnismäßigkeitsgrundsatz gehört, und die Achtung der GRCh gewährleisten müssen.[18]

3.2. Grundrechtsrelevanz der Vorratsdatenspeicherung

Nach ständiger Rechtsprechung des EuGH stellt die **Vorratsdatenspeicherung als solche** eine Abweichung von Art. 5 E-Privacy-RL und einen **Eingriff in Art. 7 und 8 GRCh** dar. Dies gilt unabhängig von der Sensibilität der Daten, von ihrer späteren Nutzung und davon, ob dem Betroffenen konkrete Nachteile entstehen.[19] Zudem könne das Gefühl des „Überwachtseins“ bzw. die Möglichkeit, aus den gespeicherten Daten detaillierte Profile der jeweiligen Nutzer zu erstellen, abschreckende Wirkung auf die Ausübung der in **Art. 11 GRCh** verankerten Meinungsäußerungsfreiheit haben.[20] Die Annahme solcher Grundrechtseingriffe ist nach ständiger EuGH-Rechtsprechung „umso gerechtfertigter“ als Verkehrsdaten und Standortdaten[21] eine Vielzahl von Aspekten des Privatlebens des Betroffenen enthalten könnten. Aus ihrer Gesamtheit seien daher „**sehr genaue Schlüsse auf das Privatleben der Betroffenen**“ möglich. Die (negativen) Wirkungen fielen **umso stärker** aus, je **größer die Menge und Vielfalt** der auf Vorrat gespeicherten Daten sei.[22]

3.3. Rechtfertigung von Grundrechtseingriffen

Sowohl aus Art. 15 Abs. 1 E-Privacy-RL selbst als auch aus Art. 52 Abs. 1 GRCh folgt, dass die in Art. 7, 8 und 11 GRCh verankerten Rechte keine uneingeschränkte Geltung beanspruchen können. Nach **Art. 52 Abs. 1 GRCh** können **Einschränkungen** der Grundrechte unter Achtung ihres Wesensgehalts und Wahrung des **Grundsatzes der Verhältnismäßigkeit** gerechtfertigt sein. Dies setzt nach Art. 52 Abs. 1 Satz 2 GRCh voraus, dass die jeweiligen Einschränkungen erforderlich sind und den von der EU anerkannten Gemeinwohlzielen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Als „Rechte und Freiheiten anderer“ kommen im Zusammenhang mit der Vorratsdatenspeicherung insbesondere das Recht auf Sicherheit aus Art. 6 GRCh sowie – im Zusammenhang mit dem Opferschutz bei der Kriminalitätsbekämpfung – staatliche Schutzverpflichtungen aus Art. 7

---

18 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 59.

19 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 69; Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 60; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 44; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn.115 ff.

20 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 78; *Ferner*, BeckOK StPO, 52. Edition 2024, § 174 TKG, Rn. 28 f.

21 Art. 2 Buchst. c E-Privacy-RL definiert Standortdaten-Daten als 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“.

22 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 61 f.; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 45 f.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 117 f.

GRCh sowie aus Art. 3, 4 GRCh hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit in Betracht.[23] Was die von der EU anerkannten Gemeinwohlziele anbelangt, betont der EuGH in ständiger Rechtsprechung, dass auf Art. 15 Abs. 1 E-Privacy-RL gestützte Maßnahmen den in dieser Norm **abschließend aufgezählten Zwecken** – nationale Sicherheit, Landesverteidigung, öffentliche Sicherheit oder Kriminalitätsverhütung bzw. -bekämpfung – **tatsächlich strikt dienen** müssen.[24] Nationale 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.[25]

3.4. Insbesondere: Verhältnis zwischen Eingriffsschwere und Gewichtigkeit des Gemeinwohlziels

Im Rahmen der vom EuGH durchgeführten Verhältnismäßigkeitsprüfung ist insbesondere relevant, wie schwer der Grundrechtseingriff wiegt und das **verfolgte Gemeinwohlziel** in **angemessenem Verhältnis zur Schwere des Eingriffs** steht („Zweck-Mittel-Relation“).[26]

Der EuGH geht dabei von einer **Hierarchie** der in Art. 15 Abs. 1 Satz 1 E-Privacy-RL normierten **Gemeinwohlziele entsprechend ihrer jeweiligen Bedeutung** aus.[27] Der Schutz der nationalen Sicherheit sei der gewichtigste Zweck, weshalb hiermit die im Vergleich zu den anderen Zwecken schwersten Grundrechtseingriffe gerechtfertigt werden könnten.[28] Auf dieser Grundlage hat der EuGH differenzierte Vorgaben dazu entwickelt, welche Gemeinwohlziele welche Formen der

---

23 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.

24 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.

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

26 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 68; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 53; Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 32; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 131 m.w.N.

27 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 71; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u.a., Rn. 57; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 135 f.

28 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 72; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 56 ff. m.w.N.

Vorratsdatenspeicherung, die sämtlich als schwerwiegende Grundrechtseingriffe eingestuft wurden, rechtfertigen können.[29]

Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, hat der EuGH entschieden, dass mit einer Speicherung von Verkehrs- und Standortdaten verbundene **schwere Grundrechtseingriffe** nur mit der **Bekämpfung schwerer Kriminalität** und der **Verhütung ernster Bedrohungen der öffentlichen Sicherheit** gerechtfertigt werden können. Von schwerwiegenden Grundrechtseingriffen ist auszugehen, wenn aus den auf Vorrat gespeicherten Daten(-Kategorien) sehr **genaue Schlüsse auf das Privatleben** des Betroffenen gezogen werden können (siehe schon Ziff. 2).[30]

Demgegenüber können **nicht schwerwiegende Grundrechtseingriffe** durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein.[31] Dies bejahte der EuGH bezüglich nationaler Rechtsvorschriften über die Vorratsdatenspeicherung von und den Zugang zu **Identitätsdaten einer Person**,[32] die nicht mit Informationen über die erfolgten Kommunikationen in Verbindung gebracht werden können.[33]

Hinsichtlich nationaler Regelungen, die u. a. die allgemeine und unterschiedslos **Vorratsdatenspeicherung von IP-Adressen vorsahen**, hat der EuGH in den vergangenen Jahren wiederholt entschieden, dass sie zu schweren Grundrechtseingriffen führten. Solche Eingriffe seien daher nur mit den **besonders gewichtigen Zwecken der Bekämpfung schwerer Kriminalität**, der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit oder mit dem Schutz der nationalen Sicherheit zu rechtfertigen.[34] Dies begründete der Gerichtshof damit, dass IP-Adressen als solche zwar einen geringeren Sensibilitätsgrad als sonstige Verkehrsdaten aufwiesen, sofern sie lediglich zur

---

29 „Formen der Vorratsdatenspeicherung“ sind insbesondere die allgemeine und unterschiedslose bzw. die gezielte Vorratsdatenspeicherung und die umgehende Sicherung, vgl. EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 132 sowie Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 129; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., Rn. 168 und den Überblick bei *Ferner*, in: BeckOK StPO, 52. Edition Juli 2024, § 174 TKG, Rn. 32.

30 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 78; Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 33 ff. m.w.N.

31 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 Quadratur du Net u. a., Rn. 140 ff. m.w.N.; GA *Szpunar*, Schlussanträge vom 28. September 2023 zu EuGH, Rs. C-470/21, La Quadrature du Net u. a. & & lutte contre la contrefaçon, Rn. 46.

32 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.

33 EuGH, Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 34; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., La Quadrature du Net u. a., Rn. 157 ff.; Urteil vom 2. Oktober 2018, Rs. C-207/16, Ministerio Fiscal, Rn. 57 ff.

34 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 79, Rn. 100; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 73 f.; Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 35 ff.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 156.

Identifikation der Kommunikationsquelle, nicht aber zur Identifikation des Kommunikationsadressaten dienten.[35] Allerdings gelangte der EuGH zu der Einschätzung, dass die jeweils in Rede stehenden nationalen Regelungen die Nutzung der IP-Adressen „zur **umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten** und infolgedessen seiner **Online-Aktivität**“ ermöglichten. Sie erlaubten nach Ansicht des EuGH die „**Erstellung eines detaillierten Profils**“ und stellten daher schwerwiegende Eingriffe in Art. 7, 8, 11 GRCh dar.[36]

3.5. Erfordernis klarer und präziser Regelungen

Schließlich ergibt sich aus der ständigen EuGH-Rechtsprechung, dass nationale Rechtsvorschriften über die Vorratsdatenspeicherung – um dem Grundsatz der Verhältnismäßigkeit zu genügen – „durch **klare und präzise Regeln** sicherstellen müssen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen“.[37] Insofern reichen nationale Garantien im Bereich allein des Daten*zugangs* nicht aus. Denn die Speicherung auf Vorrat stellt als solche einen vom Zugang zu diesen Daten zu unterscheidenden, eigenständigen und rechtfertigungsbedürftigen Grundrechtseingriff dar (vgl. Ziff. 3.2.).[38]

35 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 152.

36 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 79, 100, 102; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 73 f.; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 156.

37 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 75, 132; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u. a., Rn. 67; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, Rn. 168. Weitere Anforderungen an die Ausgestaltung nationaler Rechtsvorschriften ergeben sich aus: EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána u. a., Rn. 54; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a, Rn. 132.

38 EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 91; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 47.

4. Analyse des EuGH-Urteils in der Rs. C-470/21

Das Vorabentscheidungsverfahren in der Rs. C-470/27 bezog sich auf eine französische Regelung,[39] die es der mit der Aufdeckung von Urheberrechtsverletzungen im Internet betrauten Behörde („Hadopi“[40]) ermöglicht, Inhaber von IP-Adressen zu identifizieren, welche möglichweise für Urheber- oder sonstige Schutzrechtsverletzungen genutzt wurden.[41]

Das im gerichtlichen Ausgangsverfahren in Frankreich zur Prüfung stehende Prozedere lief so ab, dass in einem ersten Schritt Einrichtungen der Rechteinhaber IP-Adressen sammelten, die möglicherweise für Urheber- oder sonstige Schutzrechtsverletzungen genutzt wurden. Diese Adressen und eine nähere Beschreibung des möglichen Rechtsverstoßes (Datum, Uhrzeit, verwendetes Pseudonym etc.) wurden dann der Hadopi zur Verfügung gestellt („vorlagerte Verarbeitung“).[42] In einem zweiten Schritt („nachgelagerte Verarbeitung“) glichen die Internetzugangsanbieter auf Ersuchen der Hadopi die übermittelten IP-Adressen mit den Inhabern dieser Adressen ab und übermittelten Hadopi personenbezogene Daten der Inhaber (Name, Anschrift, telefonische Erreichbarkeit, E-Mailadresse).[43] Gegenüber den so identifizierten Personen konnte Hadopi dann im Rahmen eines sog. „Verfahrens der abgestuften Reaktion“ zunächst Empfehlungen bzw. Warnungen aussprechen und im Wiederholungsfall gegebenenfalls auch die Staatsanwaltschaft einschalten.[44]

Der EuGH stellt in seinem Urteil vom 30. April 2024 zunächst fest, dass sich das Vorabentscheidungsersuchen ausschließlich auf die nachgelagerte Verarbeitung beziehe.[45] Hinsichtlich der vorgelagerten Verarbeitung weist der Gerichtshof nur abstrakt darauf hin, dass eine etwaige Unionsrechtswidrigkeit der Sammlung von IP-Adressen durch die Rechteinhaber auch den anschließenden Abgleich dieser Adressen mit den Identitätsdaten durch die Betreiber elektronischer Kommunikationsdienste unionsrechtswidrig machen würde. Maßgeblich seien insofern die in Art. 6

---

39 Insofern ist zu berücksichtigen, dass der EuGH im Rahmen von Vorabentscheidungsverfahren nach Art. 267 AEUV weder zur Auslegung innerstaatlicher Rechts- oder Verwaltungsvorschriften noch zu Äußerungen über deren Vereinbarkeit mit dem Unionsrecht befugt ist. Nach ständiger Rechtsprechung kann der EuGH nach Art. 267 AEUV nur das Unionsrecht in den Grenzen der der Union übertragenen Zuständigkeiten auslegen, weshalb es stets um die abstrakt formulierte Frage geht, ob das Unionsrecht einer auf bestimmte Weise ausgestalteten nationalen Regelungen entgegensteht, vgl. nur: EuGH, Urteil vom 30. April 2024, Rs. C-178/22, Procura della Repubblica il Tribunale di Bolzano, Rn. 31; Urteil vom 14. Dezember 2023, Rs. C 28/22, Getin Noble Bank, Rn. 53 m.w.N.

40 „Hadopi“ steht für „haute autorité pour la diffusion des œuvres et la protection des droits sur internet“, also hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet.

41 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 52.

42 Ebenda, Rn. 54.

43 Ebenda, Rn. 55.

44 Ebenda, Rn. 57.

45 Ebenda, Rn. 58.

Abs. 1 Buchst. f der EU-Datenschutzgrundverordnung (DSGVO)[46] normierten Vorgaben für die Verarbeitung personenbezogener Daten.[47]

Entsprechend der aufgeworfenen Vorlagefragen geht der Gerichtshof dann auf die unionsrechtlichen Anforderungen an die Speicherung von IP-Adressen und Identitätsdaten (Ziff. 4.1.), die unionsrechtlichen Vorgaben für den behördlichen Zugang zu diesen Daten (Ziff. 4.2.), das Erfordernis einer dem Zugang vorgeschalteten unabhängigen Kontrolle (Ziff. 4.3.) und die Gewährleistung materieller und prozeduraler Vorgaben sowie Missbrauchsschutz (Ziff. 4.4.) ein.[48]

4.1. Vorratsdatenspeicherung von Identitätsdaten und der ihnen zuzuordnenden IP-Adressen

Der EuGH prüft zunächst, ob eine nationale Regelung, die eine Pflicht zur **allgemeinen und unterschiedslosen Vorratsdatenspeicherung von IP-Adressen** zur **Bekämpfung von Straftaten im Allgemeinen** aufstellt, mit Art. 15 Abs. 1 E-Privacy-EL, Art. 7, 8, 11 GRC vereinbar ist.[49]

Hierzu stellt er im Wesentlichen auf die im Rahmen der Verhältnismäßigkeitsprüfung relevante **Zweck-Mittel-Relation** ab (siehe dazu Ziff. 3.4.). Der Gerichtshof prüft also, ob die Schwere des aus der Vorratsdatenspeicherung der IP-Adressen resultierenden Grundrechtseingriffs in einem angemessenen Verhältnis zur Gewichtigkeit des hiermit verfolgten Gemeinwohlziels steht.[50] Hierzu verweist der EuGH auf seine bereits in der verb. Rs. C-511/18, C-512/18 und C-520/18 getroffene Feststellung, dass zur Identifikation der Kommunikationsquelle gespeicherte **IP-Adressen als solche** einen **geringeren Sensibilitätsgrad** aufweisen als sonstige Kategorien von Verkehrsdaten (siehe schon Ziff. 3.4.).[51] Zwar könne sich eine besondere Eingriffsintensität ergeben, wenn sich die Pflicht zur Vorratsdatenspeicherung auf weitere Datenkategorien erstrecke und Verknüpfungsmöglichkeiten bestünden, die eine Erstellung detaillierter Profile bzw. genaue

---

46 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, 4. Mai 2016, S. 1 (korrigierte Fassung v. 23. Mai 2018).

47 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 59. Demgegenüber sei die E-Privacy-RL nicht anwendbar, da die Daten nicht „in Verbindung mit der Bereitstellung […] elektronischer Kommunikationsdienste“ i. S. v. Art. 3 E-Privacy-RL verarbeitet würden. Vgl. zudem zu der Frage, wann eine IP-Adresse ein personenbezogenes Datum darstellt, das anhängige Rechtsmittelverfahren in der Rs. C-413/23 P, welches auf dem Urteil des Europäischen Gerichts vom 26. April 2023, Rs. T-557/20 beruht. Siehe zudem EuGH, Urteil vom 19. Oktober 2016, Rs. C-582/14, Breyer.

48 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 64 ff.

49 Diese Frage stellte sich, weil der Hadopi gewährte Zugang zu den einer IP-Adresse zuzuordnenden Identitätsdaten notwendig einen Abgleich von Identitätsdaten und IP-Adressen und damit die Vorratsdatenspeicherung solcher IP-Adressen durch die Betreiber elektronischer Kommunikationsdienste voraussetzte, vgl. EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 71 ff.

50 Ebenda, Rn. 74.

51 Ebenda, Rn. 76 unter Verweis auf 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.

Schlüsse auf das Privatleben der jeweiligen Person zuließen (siehe schon Ziff. 3.4.).[52] Allerdings stelle „**nicht jede allgemeine und unterschiedslose Vorratsspeicherung** eines unter Umständen umfangreichen Bestands der von einer Person innerhalb eines bestimmten Zeitraums genutzten statischen und dynamischen **IP-Adressen** zwangsläufig **einen schweren Eingriff** in die durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte“ dar.[53] Vielmehr könne eine nationale Rechtsvorschrift, die entsprechende Speicherpflichten auferlege,

> „gegebenenfalls durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein, wenn tatsächlich **ausgeschlossen ist**, dass diese Speicherung **schwere Eingriffe in das Privatleben des Betroffenen** zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen“.[54]

Entsprechende mitgliedstaatliche Regelungen müssen also eine **wirksame strikte Trennung** verschiedener auf Vorrat gespeicherter Datenkategorien gewährleisten, wenn eine IP-Adressenspeicherung auf Vorrat zur Bekämpfung von Straftaten im Allgemeinen erfolgen soll.[55] Zu den insoweit von den Mitgliedstaaten vorzusehenden „**klare[n] und präzise[n] Regeln für die Modalitäten**“ der Vorratsdatenspeicherung erläutert der EuGH, dass

- diese sicherstellen müssen, „dass jede Kategorie von Daten, einschließlich der Identitätsdaten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird“;

- sie gewährleisten müssen, „dass in technischer Hinsicht eine wirksame strikte Trennung zwischen den verschiedenen Kategorien auf Vorrat gespeicherter Daten, u. a. den Identitätsdaten, den IP-Adressen, den verschiedenen Verkehrsdaten außer den IP-Adressen und den verschiedenen Standortdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung stattfindet“;

- sie, „soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt“ und

---

52 Ebenda, Rn. 77 ff. ebenfalls unter Verweis auf Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a.

53 Ebenda, Rn. 79 (Hervorhebungen hinzugefügt).

54 Ebenda, Rn. 82 (Hervorhebungen hinzugefügt), vgl. auch ebenda, Rn. 90 f.

55 Ebenda, Rn. 84

– „die Zuverlässigkeit dieser strikten Trennung regelmäßig Gegenstand einer Kontrolle durch eine andere Behörde als die sein [muss], die Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten personenbezogenen Daten begehrt“.[56]

Schließlich müsse eine solche gesetzliche Regelung der Mitgliedstaaten die **Dauer** der Speicherung auf das **absolut Notwendige** begrenzen sowie durch **klare und präzise Regeln** die Einhaltung der einschlägigen materiellen und prozeduralen Voraussetzungen sicherstellen und wirksamen Schutz vor Missbrauchsgefahren, unberechtigtem Datenzugang und unberechtigter Datennutzung gewährleisten (siehe zu diesem Erfordernis schon Ziff. 3.5.).[57]

4.2. Zugang zu den einer IP-Adresse zuzuordnenden Identitätsdaten

Auch hinsichtlich des behördlichen Zugangs zu den einer IP-Adresse zuzuordnenden Identitätsdaten stellt der EuGH im Wesentlichen darauf ab, ob es sich um einen nicht schwerwiegenden Eingriff handelt, der daher mit der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt werden kann.[58] Zu beachten sei zudem, dass ein behördlicher Zugang nur zu dem Zweck in Betracht komme, zu dem zuvor Daten auf Vorrat gespeichert wurden, oder aber zu einem gewichtigeren Zweck.[59]

Auf dieser Grundlage stellt der EuGH in einem **ersten Schritt** fest, dass den Behörden aufgrund der im Ausgangsverfahren in Rede stehende Regelung **grundsätzlich keine genauen Rückschlüsse** auf das Privatleben der Betroffenen möglich seien. Sofern das nationale Recht durch entsprechende klare und präzise Regeln sicherstelle, dass keine Überwachung der Online-Aktivität mittels IP-Adressen erfolgen könne und der Zugang nur zu ihrer Identifizierung für das Verfahren der abgestuften Reaktion geschehe, betreffe der Zugang die **IP-Adresse** als **Identitätsdatum** und nicht als Verkehrsdatum.[60] Sofern darüber hinaus die zugrundeliegende Speicherpflicht auch der Bekämpfung von Straftaten im Allgemeinen diene und den vom EuGH formulierten Modalitäten genüge (siehe Ziff. 4.1.), könne der Zugang ebenfalls durch die Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein.[61] Der EuGH weist ergänzend darauf hin, dass es im Einklang mit seiner Rechtsprechung zum „Recht auf Auskunft“ aus Art. 8 der Richtlinie 2004/48/EG[62] zur Durchsetzung der Rechte des geistigen Eigentums stehe, wenn eine mit der Bekämpfung von Urheberrechtsverletzungen betraute Behörde Zugang zu den Daten habe, die der

---

56 Ebenda, Rn. 85-89.

57 Ebenda, Rn. 93 unter Verweis auf EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 168.

58 Ebenda, Rn. 95 f. unter Verweis auf Urteil vom 2. März 2021, Rs. C-746/18, Prokuratuur, Rn. 35; Urteil vom 2. Oktober 2018, Rs. C-207/16, Ministerio Fiscal, Rn. 54 ff.

59 Ebenda, Rn. 97 f. m.w.N.

60 Ebenda, Rn. 99-101.

61 Ebenda, Rn. 103 f.

62 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. L 157, 30. April 2004, S. 45 (berichtigte Fassung v. 2. Juni 2004).

Identifizierung mutmaßlicher Täter dienen. Aus dieser Rechtsprechung ergebe sich, dass es den Mitgliedstaaten nach dem Unionsrecht freistehe, die Betreiber elektronischer Kommunikationsdienste zu verpflichten, personenbezogene Daten an Privatpersonen weiterzugeben, um die Verfolgung von Urheberrechtsverletzungen vor den Zivilgerichten zu ermöglichen.[63]

In einem **zweiten Schritt** betont der EuGH, dass die Schwere des Eingriffs aber nicht allein anhand der durch die jeweilige Rechtsvorschrift eröffneten Zugangsmöglichkeiten zu beurteilen sei. Vielmehr komme es auf die **Gesamtheit der der jeweiligen Behörde zur Verfügung stehenden Daten und Informationen** an.[64] Im zugrundeliegenden Fall seien daher die von den Einrichtungen der Rechteinhaber übermittelten Informationen (bspw. Titel des von der mutmaßlichen Rechtsverletzung betroffenen Werks) mit zu berücksichtigen. Nach Einschätzung des EuGH seien **atypische Situationen** denkbar, in denen die Behörde aus der Gesamtheit der Informationen doch genaue Schlüsse auf das Privatleben des Betroffenen ziehen könne; etwa, wenn sich anhand des Werktitels auf (sensible) Aspekte des Privatlebens schließen lasse.[65] Gleichwohl kann nach Ansicht des EuGH mit Blick auf die in Rede stehende nationale Regelung „nicht zwangsläufig“ von einem hohen Schweregrad ausgegangen werden. Insofern sei zu berücksichtigen, dass die zugangsberechtigte Behörde unabhängig sei. Außerdem sei relevant, dass innerhalb der Behörde nur ein begrenzter und vereidigter Personenkreis Zugang habe, der zudem – mit Ausnahme der Einbeziehung der Staatsanwaltschaft – zur Vertraulichkeit verpflichtet sei. Schließlich diene die nationale Regelung ausschließlich dazu, der Verletzung von Urheberrechten verdächtige Personen zu identifizieren, wobei der Umfang des Datenzugangs auf das erforderliche Maß beschränkt sei. Damit bleibt es nach Ansicht des EuGH dabei, dass eine nationale Regelung, wie die im Ausgangsverfahren in Rede stehende, keinen schwerwiegenden Grundrechtseingriff darstellt.[66]

In einem **dritten Schritt** weist der EuGH schließlich darauf hin, dass im Rahmen der Verhältnismäßigkeitsprüfung bei der Abwägung der in Rede stehenden Rechte und Interessen ausnahmsweise Allgemeininteressen wie die Verteidigung der öffentlichen Ordnung und die Verhütung von Straftaten schwerer wiegen könnten als die grundsätzlich vorrangigen Anliegen des Schutzes der Meinungsäußerungsäußerungsfreiheit und der Vertraulichkeit personenbezogener Daten. Dies komme insbesondere dann in Betracht, wenn andernfalls die **Wirksamkeit strafrechtlicher Ermittlungen** beeinträchtigt werden könne, etwa indem die tatsächliche Identifizierung des Täters oder die Verhängung von Sanktionen unmöglich gemacht bzw. übermäßig erschwert werde.[67]

Nach Auffassung des EuGH könne der **Zugang zu IP-Adressen** bei **online begangenen Straftaten** die einzige effektive – zumindest aber die im Vergleich zur Überprüfung aller Online-Aktivitäten

---

63 Vgl. im Einzelnen EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 105 f. und die dort in Bezug genommene Rechtsprechung: EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rn. 47 ff. und Urteil vom 17. Juni 2021, Rs. C-597/19, M.I.C.M., Rn. 124 f.

64 Ebenda, Rn. 107 unter Verweis auf EGMR, Urteil vom 24. April 2018, Beschw.-Nr. 62357/14, Benedik/Slowenien, Rn. 109.

65 Ebenda, Rn. 108-112.

66 Ebenda, Rn. 113-115.

67 Ebenda, Rn. 116 unter Verweis auf EGMR, Urteil vom 2. März 2009, Beschw.-Nr. 2872/02, K. U./Finnland, Rn. 49.

weniger einschneidende – Ermittlungsmaßnahme darstellen, um den IP-Adresseninhaber zu identifizieren. Dies spreche dafür, dass sowohl die **Speicherung** dieser Adressen als auch der **Zugang** zu ihnen zur Erreichung des verfolgten Ziels **zwingend erforderlich** und damit verhältnismäßig seien. Bei Nichtgewährung des Zugangs bestehe eine echte Gefahr der systematischen Straflosigkeit. Diese bestehe nicht nur bei Urheberrechtsverletzungen und verwandten Schutzrechten, sondern auch bei anderen **online begangenen** oder **„durch die Merkmale des Internets“** in der Vorbereitung oder Begehung **erleichterten Straftaten**. Das Bestehen einer solchen Gefahr sei ein bei der Abwägung verschiedener betroffener Rechte und Interessen im Rahmen der Verhältnismäßigkeitsprüfung relevanter Umstand.[68]

Auf dieser Grundlage kommt der EuGH zu dem Ergebnis, dass das Unionsrecht einer der französischen Regelung entsprechenden nationalen Vorschrift grundsätzlich nicht entgegenstehe, wobei diese es den zugangsberechtigten Bediensteten untersagen müsse,

- Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zum alleinigen Zweck der Anrufung der Staatsanwaltschaft, in welcher Form auch immer offenzulegen,

- die von diesen Personen besuchten Internetseiten nachzuverfolgen und

- die IP-Adressen zu anderen Zwecken als dem des Erlasses solcher Maßnahmen zu nutzen.[69]

4.3. Unabhängige (gerichtliche) Vorabkontrolle des Zugangs

Der EuGH stellt auch hinsichtlich des Erfordernisses einer dem Zugang vorgeschalteten Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde auf die Differenzierung zwischen einem schweren bzw. nicht schweren Grundrechtseingriff ab: Nach dem Verhältnismäßigkeitsgrundsatz sei davon auszugehen, dass eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle nur geboten sei, wenn der Zugang der nationalen Behörde die Gefahr eines schweren Grundrechtseingriffs berge, weil es möglich sein könnte, genaue Schlüsse auf sein Privatleben des Betroffenen zu ziehen und gegebenenfalls sein detailliertes Profil zu erstellen.[70]

Hinsichtlich einer Vorratsdatenspeicherung, die den unter Ziff. 4.1. dargestellten Anforderungen genüge, sei daher im Ausgangspunkt keine vorherige Kontrolle erforderlich.[71] Etwas anderes ergebe sich mit Blick auf das französische Verfahren aber bei Wiederholungstätern, da nicht ausgeschlossen werden könne, dass die betraute Behörde angesichts der nach und nach gesammelten Informationen doch ein Profil über den Betroffenen erstellen könne. Aus diesem Grund ist ab einem vom EuGH näher bestimmten Stadium des in Rede stehenden französischen Verwaltungs-

68 Ebenda, Rn. 117-121.

69 Ebenda, Rn. 122.

70 Ebenda, Rn. 128-133.

71 Ebenda, Rn. 134.

verfahrens eine vorherige Kontrolle erforderlich, die den vom EuGH entwickelten organisatorischen und kompetenziellen Anforderungen genügen muss.[72] Insbesondere müsse die vorab kontrollierende Stelle bei strafrechtlichen Ermittlungen in der Lage sein, einen gerechten Ausgleich zwischen Kriminalitätsbekämpfungsinteressen und Individualinteressen des Betroffenen zu gewährleisten und sicherstellen, dass der Zugang auf das absolut Notwendige beschränkt sei. Die Betroffenen müssten über wirksame Garantien vor Missbrauchsgefahren sowie vor unberechtigtem Datenzugang und unberechtigter Datennutzung verfügen. Deshalb sei eine vollautomatisierte Kontrolle nicht zulässig.[73]

4.4. Erfordernis klarer und präziser Regelungen zur Gewährleistung materieller und prozeduraler Vorgaben sowie Missbrauchsschutz

Der EuGH verweist schließlich auf seine bisherige Rechtsprechung, wonach der Zugang zu personenbezogenen Daten nur dann verhältnismäßig ist, wenn die jeweiligen Rechtsvorschriften klare und präzise Regeln enthalten, die gewährleisten, dass die materiellen und prozeduralen Voraussetzungen für den Zugang eingehalten werden und wirksame Garantien zum Schutz vor missbräuchlichem Zugang oder missbräuchlicher Nutzung bestehen. Solche Garantien seien besonders bedeutsam, wenn die personenbezogenen Daten – wie beim im Ausgangsverfahren in Rede stehenden Prozedere – automatisiert verarbeitet würden. Erforderlich sei insofern, dass das verwendete Datenverarbeitungssystem aufgrund einer Rechtsvorschrift regelmäßig von einer unabhängigen Stelle hinsichtlich seiner Integrität und wirksamen Garantien gegen Missbrauch überwacht werde.[74]

Schließlich müssten behördliche Datenverarbeitungen, wie sie die Hadopi durchführe, den Datenschutzvorschriften der Richtlinie 2016/680[75] genügen. Diese enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Zusammenhang mit der Bekämpfung von Kriminalität und Gefahren für die öffentliche Sicherheit (vgl. Art. 1 RL 2016/680). Dies liege daran, dass die getroffenen Maßnahmen einen „unmittelbar mit dem Gerichtsverfahren verbundenen vorstrafrechtlichen Charakter“ hätten, weshalb Hadopi eine Behörde i.S.v. Art. 3 RL 2016/680 sei.[76]

---

72 Vgl. im Einzelnen: ebenda, Rn. 135-146; zu den Anforderungen an die Ausgestaltung der Vorabkontrolle: ebenda, Rn. 125-127 sowie etwa: EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 104 ff. m.w.N.

73 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 147-151.

74 Ebenda, Rn. 152 f.

75 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119, 4. Mai 2016, S. 89 (korrigierte Fassung v. 23. Mai 2018).

76 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 157 ff., auch dazu, dass die DSGVO auf derartige Maßnahmen der Gefahrenabwehr, Strafverfolgung und -vollstreckung keine Anwendung finde.

5. Einordnung des Urteils in der Rs. C-470/21 in die bisherige Rechtsprechung zur Vorratsdatenspeicherung

Die vom Auftraggeber aufgeworfene Frage, ob das EuGH-Urteil in der Rs. C-470/21 hinsichtlich der Vorratsspeicherung von IP-Adressen zur Verfolgung von Straftaten eine Bestätigung der bisherigen Rechtsprechung darstellt oder eine neue Rechtslage schafft, lässt sich anhand der Zusammenfassung der bisherigen EuGH-Rechtsprechung (Ziff. 3) und der Analyse des Urteils in der Rs. C-470/21 (Ziff. 4) wie folgt beantworten:

Der EuGH hat in der Rs. C-470/21 **erstmals entschieden**, dass eine **allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen** auch durch das Gemeinwohlziel der Verhütung und Bekämpfung von **Straftaten im Allgemeinen** gerechtfertigt sein kann.[77] In vorhergehenden Urteilen hatte der Gerichtshof insoweit nur das gewichtigere Ziel der Verhütung bzw. Bekämpfung „schwerer Kriminalität“ als Rechtfertigungsgrund anerkannt. Gleichwohl ist die Entscheidung in der Rs. C-470/21 **nicht als Aufgabe der bisherigen Auslegung des Unionsrechts** im Bereich der Vorratsdatenspeicherung von IP-Adressen einzustufen. Der EuGH bestätigt vielmehr seine Rechtsauffassung, dass schwere Eingriffe in Art. 7, 8, 11 GRCh im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur durch den Zweck der Bekämpfung schwerer Kriminalität gerechtfertigt sein können, während bei nicht schwerwiegenden Eingriffen auch die Bekämpfung von Straftaten im Allgemeinen als Rechtfertigungsgrund in Betracht komme (vgl. Ziff. 3.4. und 4.1.).

Nach Einschätzung des EuGH stellten die den bisherigen Vorabentscheidungsverfahren zugrunde liegenden nationalen Regelungen zur Vorratsdatenspeicherung von IP-Adressen schwerwiegende Grundrechtseingriffe mit entsprechend hohen Rechtfertigungsanforderungen dar, da sie genaue Rückschlüsse auf das Privatleben der Betroffenen zuließen.[78] Nach Bewertung des Gerichtshofs war dies im der Rs. C-470/21 zugrundeliegenden Sachverhalt aber nicht der Fall.[79] Der EuGH stellt deshalb klar, „dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung eines unter Umständen umfangreichen Bestands der von einer Person innerhalb eines bestimmten Zeitraums genutzten statischen und dynamischen IP-Adressen zwangsläufig einen schweren Eingriff in die durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte darstellt“. Zudem formuliert er Modalitäten, die erfüllt sein müssen, um sicherzustellen, dass eine solche, genaue

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

78 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 77 ff. unter Verweis auf Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 153 f. sowie Vgl. zudem EuGH, Urteil vom 20. September 2022, verb. Rs. C-793/19 und C-794/19, SpaceNet, Rn. 79, Rn. 100; Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 73 f.

79 So auch: Generalanwalt *Szpunar*, Schlussanträge vom 28. September 2023 zu EuGH, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 54-56.

Schlüsse auf das Privatleben der Betroffenen ermöglichende Kombination von Daten ausgeschlossen ist.[80]

Die Entscheidung in der Rs. C-470/21 schafft damit keine völlig neue Rechtslage.[81] Die im Vergleich zu vorhergehenden Entscheidungen abweichende Tatsachgrundlage gab dem EuGH aber Gelegenheit, klarzustellen, dass und unter welchen Voraussetzungen eine allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen keinen schweren Grundrechtseingriff darstellt und daher mit der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt werden kann.[82] Dies spricht dafür, im Urteil zur Rs. C-470/21 eine **Erweiterung und Konkretisierung der bisherigen Rechtsprechung** zu sehen, die die differenzierten Vorgaben zur Rechtfertigung schwerwiegender Grundrechtseingriffe ergänzt.

Es sei noch darauf hingewiesen, dass der EuGH auch hinsichtlich der von den Mitgliedstaaten zu beachtenden Vorgaben bei der Ausgestaltung des Zugangs und dessen Vorabkontrolle auf die Abgrenzung zwischen schwerwiegenden und nicht schwerwiegenden Grundrechtseingriffen abstellt. Sofern die IP-Adresse letztlich nur die Funktion eines Identitätsdatums erfüllt und eine Nachverfolgung bzw. Überwachung der Online-Aktivitäten des Betroffenen ausgeschlossen ist, kann die Zugangseröffnung durch die Bekämpfung von Straftaten im Allgemeinen in Betracht kommen, sofern die vom EuGH formulierten Modalitäten beachtet werden (vgl. im Einzelnen Ziff. 4.2.). Eine unabhängige Vorabkontrolle des Zugangs ist nur bei schwerwiegenden Grundrechtseingriffen erforderlich (Ziff. 4.3.).

6. Unionsrechtliche Vorgaben zu Straftaten, auf die sich die IP-Adressen-Vorratsdatenspeicherung beziehen darf

Der Auftraggeber möchte zudem wissen, **zur Verfolgung welcher Straftaten** eine Pflicht zur Vorratsdatenspeicherung von IP-Adressen zulässig wäre. Nachfolgend wird darauf eingegangen, ob und welche Anforderungen sich insoweit aus dem Unionsrecht ergeben.

Anhaltspunkte ergeben sich aus dem Urteil des EuGH vom 30. April 2024 in der Rs. C-178/22. Dieses Vorabentscheidungsersuchen betraf u. a. die Frage, welche Straftaten als „schwer“ einzustufen und daher geeignet sind, schwere Grundrechtseingriffe im Zusammenhang mit dem Zugang zu Vorratsdaten zu rechtfertigen.[83] Der EuGH stellte klar, dass das **Strafrecht und die Regeln des Strafverfahrens**, soweit die EU in diesem Bereich keine Rechtsvorschriften erlassen habe, in

80 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 79, 84 ff.

81 In diesem Sinne auch: *Marquard*, EuGH: Vorratsdatenspeicherung auch bei allgemeinen Straftaten zulässig, ZD-Aktuell 2024, 01714.

82 Vgl. auch: *Ferner*, in: BeckOK StPO, 52. Edition Juli 2024, § 174 TKG, Rn. 35.2.

83 Vgl. EuGH, Urteil vom 30. April 2024, Rs. C-178/22, Procura della Repubblica il Tribunale di Bolzano, Rn. 34 ff.

die **Zuständigkeit der Mitgliedstaaten** fielen. Die Mitgliedstaaten müssten von dieser Zuständigkeit jedoch unter **Wahrung des Unionsrechts** Gebrauch machen.[84] Daraus leitete der EuGH ab, dass die Definition schwerer Straftaten in die Zuständigkeit der Mitgliedstaaten falle, die hierbei aber das Gebot der engen Auslegung von Art. 15 Abs. 1 E-Privacy-RL und die sich aus Art. 7, 8, 11, 52 Abs. 1 GRC ergebenden Anforderungen an die Verhältnismäßigkeit beachten müssten.[85] Daraus folge, dass Mitgliedstaaten den Begriff „schwere Straftat" und im weiteren Sinne den Begriff „schwere Kriminalität" nicht dadurch verfälschen dürften, dass sie Straftaten einbeziehen, bei denen es sich angesichts der vorherrschenden gesellschaftlichen Bedingungen in dem betreffenden Mitgliedstaat offensichtlich nicht um schwere Straftaten handele.[86]

Aus der Entscheidung in der Rs. C-178/22 folgt, dass die Definition von Straftatbeständen für die Anwendung von Art. 15 Abs. 1 E-Privacy-RL in die Zuständigkeit der Mitgliedstaaten fällt. Die Mitgliedstaaten müssen von dieser Zuständigkeit aber unter Wahrung des Unionsrechts Gebrauch machen. Relevant dürfte insofern insbesondere die **Wahrung des Verhältnismäßigkeitsgrundsatzes** aus Art. 52 Abs. 1 GRCh sein. Es kommt also darauf an, ob die im nationalen Rechtvorgesehene Vorratsdatenspeicherung von IP-Adressen zur Bekämpfung der jeweiligen Straftaten geeignet, erforderlich und – in Abwägung mit den betroffenen Rechten und Pflichten – angemessen ist (vgl. Ziff. 3.3., 3.4.).

Wie unter Ziff. 4.2. bereits dargestellt, geht der EuGH in der Rs. C-470/21 davon aus, dass die Speicherung von und der Zugang zu IP-Adressen bei **online begangenen Straftaten** oder bei **„durch die Merkmale des Internets"** in der Vorbereitung oder Begehung **erleichterten Straftaten** („internetbezogenen Straftaten")[87] die einzige effektive, zumindest aber die am wenigsten einschneidende Ermittlungsmaßnahme sei. Sie könne daher zwingend notwendig und verhältnismäßig sein. Das Bestehen einer echten Gefahr der systematischen Straflosigkeit ist nach Ansicht des EuGH ein bei der Abwägung der betroffenen Rechte und Interessen relevanter Umstand.[88] In diesem Sinne hatte der EuGH auch schon in den verb. Rs. C-511/18, C-512/18 und C-520/18 – dort hinsichtlich der Bekämpfung schwerer Kriminalität – festgestellt, dass bei der Abwägung der widerstreitenden Interessen und Rechte im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen sei, dass im Fall einer im Internet begangenen Straftat die IP-Adresse der einzige Anhaltspunkt sein könne, der es ermögliche, den Inhaber der IP-Adresse zum Tatzeitpunkt zu ermitteln. Hinzu komme, dass die Vorratsspeicherung der IP-Adressen durch die Betreiber elektroni-

84 EuGH, Urteil vom 30. April 2024, Rs. C-178/22, Procura della Repubblica il Tribunale di Bolzano, Rn. 44 mit-Verweis auf EuGH, Urteil vom 26. Februar 2019, verb. Rs. C-202/18 und C-238/18, Rimšēvičs und EZB/Lettland, Rn. 57 m.w.N.

85 EuGH, Urteil vom 30. April 2024, Rs. C-178/22, Procura della Repubblica il Tribunale di Bolzano, Rn. 46 ff.

86 Vgl. im Einzelnen: ebenda, Rn. 50 ff.

87 So der von *Hartl/Vogel*, Lockerungen der Voraussetzungen zur Vorratsdatenspeicherung, NJW 2024, S. 2099 (2107), verwendete Begriff.

88 EuGH, Urteil vom 30. April 2024, Rs. C-470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 117-121 unter Bezugnahme auf GA *Szpunar*, Schlussanträge vom 27. Oktober 2022 zu EuGH, Rs. 470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 78 ff; GA *Szpunar*, Schlussanträge vom 28. September 2023 zu EuGH, Rs. 470/21, La Quadrature du Net u. a. & lutte contre la contrefaçon, Rn. 80 ff.

scher Kommunikationsdienste über die Dauer ihrer Zuweisung hinaus im Prinzip nicht erforderlich erscheine, um eine Rechnung für die fraglichen Dienste zu erstellen, so dass sich die Feststellung von im Internet begangenen Straftaten, ohne Rückgriff auf eine nationale Vorschrift zur Vorratsdatenspeicherung als unmöglich erweisen könne.[89] Aus unionsrechtlicher Sicht dürfte eine Vorratsdatenspeicherung von IP-Adressen also insbesondere zur Verfolgung internetbezogener Straftaten in Betracht kommen.

Fachbereich Europa

89 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadratur du Net u. a., Rn. 154.