Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
MACIEJ SZPUNAR
vom 27. Oktober 2022[1]

Rechtssache C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
gegen
Premier ministre,
Ministère de la Culture

(Vorabentscheidungsersuchen des Conseil d'État [Staatsrat, Frankreich])

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Befugnis der Mitgliedstaaten, den Umfang bestimmter Rechte und Pflichten zu beschränken – Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist – Identitätsdaten, die einer IP-Adresse zugeordnet sind"

I. Einleitung

1. Die Frage der Vorratsspeicherung bestimmter Daten von Internetnutzern und des Zugangs zu ihnen ist eine Frage von ständiger Aktualität und Gegenstand einer noch jungen, aber bereits umfangreichen Rechtsprechung des Gerichtshofs.

2. Die vorliegende Rechtssache bietet dem Gerichtshof die Gelegenheit, sich erneut mit dieser Frage zu befassen, und zwar im neuen Kontext der Bekämpfung von Verletzungen der Rechte des geistigen Eigentums, die ausschließlich im Internet begangen werden.

[1] Originalsprache: Französisch.

II. Rechtlicher Rahmen

A. Unionsrecht

3. In den Erwägungsgründen 2, 6, 7, 11, 22, 26 und 30 der Richtlinie 2002/58/EG[2] heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union [(im Folgenden: Charta)] anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden.

…

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

(7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

…

(11) Wie die Richtlinie [95/46/EG[3]] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen

[2] Richtlinie 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. 2002, L 201, S. 37).

[3] Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31).

Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

…

(22) Mit dem Verbot der Speicherung von Nachrichten und zugehörigen Verkehrsdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung soll die automatische, einstweilige und vorübergehende Speicherung dieser Informationen insoweit nicht untersagt werden, als diese Speicherung einzig und allein zum Zwecke der Durchführung der Übertragung in dem elektronischen Kommunikationsnetz erfolgt und als die Information nicht länger gespeichert wird, als dies für die Übertragung und zum Zwecke der Verkehrsabwicklung erforderlich ist, und die Vertraulichkeit der Nachrichten gewahrt bleibt. …

…

(26) Teilnehmerdaten, die in elektronischen Kommunikationsnetzen zum Verbindungsaufbau und zur Nachrichtenübertragung verarbeitet werden, enthalten Informationen über das Privatleben natürlicher Personen und betreffen ihr Recht auf Achtung ihrer Kommunikationsfreiheit, oder sie betreffen berechtigte Interessen juristischer Personen. Diese Daten dürfen nur für einen begrenzten Zeitraum und nur insoweit gespeichert werden, wie dies für die Erbringung des Dienstes, für die Gebührenabrechnung und für Zusammenschaltungszahlungen erforderlich ist. Jede weitere Verarbeitung solcher Daten … darf nur unter der Bedingung gestattet werden, dass der Teilnehmer dieser Verarbeitung auf der Grundlage genauer, vollständiger Angaben des Betreibers des öffentlich zugänglichen elektronischen Kommunikationsdienstes über die Formen der von ihm beabsichtigten weiteren Verarbeitung und über das Recht des Teilnehmers, seine Einwilligung zu dieser Verarbeitung nicht zu erteilen oder zurückzuziehen, zugestimmt hat. …

…

(30) Die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und -dienste sollten so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. …“

4. In Art. 2 („Begriffsbestimmungen“) dieser Richtlinie heißt es:

„…

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) ‚Nutzer‘ eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

b) ‚Verkehrsdaten‘ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) ‚Standortdaten' 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;

d) ‚Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

…"

5. Art. 3 („Betroffene Dienste") dieser Richtlinie bestimmt:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen."

6. Art. 5 („Vertraulichkeit der Kommunikation") dieser Richtlinie bestimmt:

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

…

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie [95/46] u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."

7. In Art. 6 („Verkehrsdaten") der Richtlinie 2002/58 heißt es:

„(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen

Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

…“

8. Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) Abs. 1 der Richtlinie 2002/58 bestimmt:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie [95/46] für die nationale Sicherheit … (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des [Unionsrechts] einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.“

B. Französisches Recht

1. Code de la propriété intellectuelle (Gesetzbuch über geistiges Eigentum)

9. Art. L. 331-12 des Code de la propriété intellectuelle in seiner auf das Ausgangsverfahren anwendbaren Fassung (im Folgenden: CPI) bestimmt:

„Die Haute autorité pour la diffusion des œuvres et la protection des droits sur internet [(Hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet, im Folgenden: Hadopi)] ist eine unabhängige Behörde.“

10. Art. L. 331-13 CPI sieht vor:

„Die [Hadopi] gewährleistet:

…

2° Einen Schutz [von Werken und Gegenständen, an denen ein Urheberrecht oder ein verwandtes Schutzrecht in elektronischen Kommunikationsnetzen besteht,] vor Verletzungen dieser Rechte in den elektronischen Kommunikationsnetzwerken, die zur Bereitstellung von Online-Kommunikationsdiensten für die Öffentlichkeit benutzt werden; …“

11. In Art. L. 331-15 CPI heißt es:

„Die [Hadopi] besteht aus einem Kollegium und einer Kommission für den Schutz von Rechten. …

…

Bei der Erfüllung ihrer Aufgaben erhalten die Mitglieder des Kollegiums und der Kommission für den Schutz von Rechten keine Anweisungen von anderen Behörden."

12. Art. L. 331-17 CPI bestimmt:

„Die Kommission zum Schutz von Rechten wird beauftragt, die in Artikel L. 331-25 vorgesehenen Maßnahmen zu ergreifen."

13. In Art. L. 331-21 CPI heißt es:

„Die [Hadopi] verfügt zur Wahrnehmung der Aufgaben der Kommission für den Schutz von Rechten über vereidigte öffentliche Bedienstete, die [von ihrem] Präsidenten … nach Maßgabe eines Dekrets, das nach Anhörung des Conseil d'État [(Staatsrat)] erlassen wird, ermächtigt worden sind. …

Wird die genannte Kommission unter den in Art. L. 331-24 vorgesehenen Bedingungen mit einem Vorgang befasst, wird dieser Vorgang den Mitgliedern der Kommission für den Schutz von Rechten und den in Abs. 1 genannten öffentlichen Bediensteten vorgelegt. Sie prüfen den Sachverhalt.

Sie können für die Erfordernisse des Verfahrens alle Dokumente unabhängig von dem Medium, auf dem sie gespeichert sind, erhalten, einschließlich der Daten, die von den Betreibern elektronischer Kommunikation gemäß Art. L. 34-1 des Code des postes et des communications électroniques [(Gesetzbuch für Post und elektronische Kommunikation)] und von den Dienstleistern gespeichert und verarbeitet werden, die in den Nrn. 1 und 2 des Abschnitts I von Art. 6 der Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(Gesetz Nr. 2004-575 vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft)] genannt werden.

Sie können auch Kopien der Dokumente, die im vorstehenden Absatz genannt werden, erhalten.

Sie können u. a. von den Betreibern elektronischer Kommunikation die Identität, die Postanschrift, die elektronische Adresse und die Telefondaten des Teilnehmers erhalten, dessen Online-Zugang zu öffentlichen Kommunikationsdiensten zu Zwecken der Vervielfältigung, der Darstellung, der öffentlichen Zugänglichmachung oder der öffentlichen Wiedergabe von geschützten Werken bzw. Leistungen ohne Zustimmung – sofern sie erforderlich ist – der Inhaber der … Rechte genutzt wurde."

14. Art. L. 331-24 CPI bestimmt:

„Die Kommission für den Schutz von Rechten wird auf Befassung durch … vereidigte und zugelassene Bedienstete tätig, die von folgenden Stellen ernannt werden:

– ordnungsgemäß errichteten Berufsorganisationen;

– Verwertungsgesellschaften;

– dem Centre national du cinéma et de l'image animée [(staatliche Filmförderungsbehörde)].

Die Kommission zum Schutz von Rechten kann auch auf der Grundlage von Informationen tätig werden, die ihr von der Staatsanwaltschaft übermittelt werden.

Sie kann nicht mit Sachverhalten befasst werden, die länger als sechs Monate zurückliegen."

15. In Art. L. 331-25 dieses Gesetzbuchs, der das Verfahren der sogenannten „abgestuften Reaktion" regelt, heißt es:

„Wird die Kommission zum Schutz von Rechten mit Sachverhalten befasst, die einen Verstoß gegen die in Artikel L. 336-3 [CPI] festgelegte Verpflichtung darstellen könnten, kann sie dem Teilnehmer … eine Empfehlung übermitteln, in der sie ihn auf die Bestimmungen von Artikel L. 336-3 hinweist, ihn auffordert, die darin festgelegte Verpflichtung einzuhalten, und ihn auf die in den Artikeln L. 335-7 und L. 335-7-1 angedrohten Sanktionen aufmerksam macht. Diese Empfehlung enthält auch Informationen, die den Teilnehmer auf das legale Angebot an kulturellen Online-Inhalten, auf bestehende Sicherungsvorkehrungen, mit denen Verstöße gegen die in Artikel L. 336-3 festgelegte Verpflichtung verhindert werden können, sowie auf die Gefahren für die Erneuerung des künstlerischen Schaffens und für die Wirtschaft des Kultursektors hinweisen, die von Praktiken ausgehen, die das Urheberrecht und die verwandten Schutzrechte nicht beachten.

Ergeben sich innerhalb von sechs Monaten nach Versand der in Absatz 1 genannten Empfehlung erneut Tatsachen, die einen Verstoß gegen die in Artikel L. 336-3 festgelegte Verpflichtung darstellen könnten, kann die Kommission … eine neue Empfehlung versenden, die die gleichen Informationen wie die zuvor auf elektronischem Weg übermittelte enthält. Dieser Empfehlung ist ein gegen Unterschrift zugestelltes Schreiben oder ein anderes Mittel beizufügen, das geeignet ist, das Datum der Vorlage dieser Empfehlung nachzuweisen.

Die auf der Grundlage dieses Artikels ausgesprochenen Empfehlungen enthalten das Datum und die Uhrzeit, zu denen die Tatsachen, die einen Verstoß gegen die in Artikel L. 336-3 festgelegte Verpflichtung darstellen können, festgestellt wurden. Der Inhalt der von dieser Verletzung betroffenen Werke oder Schutzgegenstände wird jedoch nicht bekannt gegeben. Sie geben die telefonischen, postalischen und elektronischen Kontaktdaten an, unter denen der Empfänger, wenn er dies wünscht, der Kommission für den Schutz der Rechte eine Stellungnahme übermitteln und, wenn er dies ausdrücklich beantragt, nähere Angaben zum Inhalt der geschützten Werke oder Schutzgegenstände erhalten kann, die von der ihm vorgeworfenen Pflichtverletzung betroffen sind."

16. Art. L. 331-29 CPI bestimmt:

„Die [Hadopi] wird ermächtigt, ein System zur automatisierten Verarbeitung personenbezogener Daten hinsichtlich der Personen, gegen die ein Verfahren im Rahmen dieses Unterabschnitts geführt wird, einzurichten.

Diese Verarbeitung dient der durch die Kommission für den Schutz von Rechten erfolgenden Durchführung der im vorliegenden Unterabschnitt vorgesehenen Maßnahmen, aller damit zusammenhängenden Verfahrenshandlungen sowie der Modalitäten zur Unterrichtung der Berufsorganisationen und der Verwertungsgesellschaften über etwaige Anrufungen der Justizbehörde sowie über Zustellungen gemäß Artikel L. 335-7 Abs. 5.

Ein Dekret … legt die Modalitäten zur Anwendung des vorliegenden Artikels fest. Es bestimmt insbesondere

– die Kategorien der gespeicherten Daten und ihre Aufbewahrungsfrist;

– die Empfänger, die zur Entgegennahme dieser Daten berechtigt sind, insbesondere die Personen, deren Tätigkeit darin besteht, einen Zugang zu öffentlichen Online-Kommunikationsdiensten anzubieten;

– die Bedingungen, unter denen die betroffenen Personen bei der [Hadopi] ihr Recht auf Zugang zu den sie betreffenden Daten … ausüben können."

17. Art. R. 331-37 CPI sieht vor:

„Die … Betreiber elektronischer Kommunikation und die … Dienstleister sind verpflichtet, durch eine Zusammenschaltung mit dem in Art. L. 331-29 genannten System für die automatisierte Verarbeitung personenbezogener Daten oder unter Verwendung eines Speichermediums, das Integrität und Sicherheit gewährleistet, die personenbezogenen Daten und die in Nr. 2 des Anhangs des Dekrets Nr. 2010-236 vom 5. März 2010 [über die automatisierte Verarbeitung personenbezogener Daten unter der Bezeichnung ‚System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet', die nach Artikel L. 331-29 (CPI) gestattet ist[4],] genannten Informationen innerhalb von acht Tagen mitzuteilen, nachdem die Kommission für den Schutz von Rechten die technischen Daten übermittelt hat, die zur Identifizierung des Teilnehmers erforderlich sind, dessen Online-Zugang zu öffentlichen Kommunikationsdaten zu Zwecken der Vervielfältigung, der Darstellung, der öffentlichen Zugänglichmachung oder der öffentlichen Wiedergabe von geschützten Werken bzw. Leistungen ohne Zustimmung – sofern sie erforderlich ist – der Inhaber der … Rechte genutzt wurde.

…"

18. Art. R. 335-5 CPI bestimmt:

„I.- Sofern die in Abschnitt II genannten Bedingungen erfüllt sind, stellt es eine qualifizierte Fahrlässigkeit des Inhabers eines Zugangs zu öffentlichen Online-Kommunikationsdiensten dar, die mit der für Übertretungen der fünften Kategorie vorgesehenen Geldstrafe geahndet wird, wenn dieser ohne rechtmäßigen Grund:

1° entweder keine Maßnahme zur Sicherung dieses Zugangs getroffen hat

2° oder bei der Durchführung dieser Maßnahme keine Sorgfalt hat walten lassen.

[4] JORF vom 7. März 2010, Text Nr. 19.

II.- Die Bestimmungen des Abschnitts I sind nur anwendbar, wenn die beiden folgenden Bedingungen erfüllt sind:

1° Die Kommission zum Schutz von Rechten hat dem Inhaber des Zugangs nach Art. L. 331-25 in der in diesem Artikel vorgesehenen Form empfohlen, eine Maßnahme zur Sicherung seines Zugangs zu treffen, mit der verhindert werden kann, dass der Zugang erneut zum Zweck der Vervielfältigung, der Darbietung, der öffentlichen Zugänglichmachung oder der öffentlichen Wiedergabe von Werken oder Gegenständen, die durch ein Urheberrecht oder ein verwandtes Schutzrecht geschützt sind, ohne die Zustimmung der Inhaber der … Rechte, sofern diese erforderlich ist, genutzt wird;

2° Innerhalb eines Jahres nach Zustellung dieser Empfehlung wird dieser Zugang erneut für die in Abschnitt II Nr. 1 genannten Zwecke genutzt."

19. Art. L. 336-3 dieses Gesetzbuchs bestimmt:

„Der Inhaber des Zugangs zu öffentlichen Online-Kommunikationsdiensten ist verpflichtet, sicherzustellen, dass dieser Zugang nicht ohne Zustimmung der Inhaber … – sofern sie erforderlich ist – zu Zwecken der Vervielfältigung, der Darstellung, der öffentlichen Zugänglichmachung oder der öffentlichen Wiedergabe von Werken oder Gegenständen genutzt wird, die durch ein Urheberrecht oder ein verwandtes Schutzrecht geschützt sind.

Der Verstoß des Inhabers des Zugangs gegen die in Absatz 1 definierte Verpflichtung hat … nicht zur Folge, dass der Inhaber strafrechtlich zur Verantwortung gezogen wird."

2. Dekret vom 5. März 2010

20. Art. 1 des Dekrets vom 5. März 2010 sieht in seiner auf den Sachverhalt des Ausgangsverfahrens anwendbaren Fassung vor:

„Die Verarbeitung personenbezogener Daten unter der Bezeichnung ‚System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet' dient der Umsetzung folgender Maßnahmen durch die Kommission für den Schutz von Rechten der [Hadopi]:

1° der im III. Buch des legislativen Teils des [CPI] (Titel III Kapitel I Abschnitt 3 Unterabschnitt 3) und im III. Buch des Verordnungsteils dieses Gesetzbuchs (Titel III Kapitel I Abschnitt 2 Unterabschnitt 2) vorgesehenen Maßnahmen;

2° der Befassung der Staatsanwaltschaft mit Sachverhalten, die Straftaten nach Artikel L. 335-2, L. 335-3, L. 335-4 und R. 335-5 desselben Gesetzbuchs darstellen könnten, sowie der Unterrichtung der Berufsorganisationen und der Verwertungsgesellschaften über diese Befassung;

…"

21. Art. 4 dieses Dekrets bestimmt:

„I. – Direkten Zugang zu den im Anhang zu diesem Dekret aufgeführten personenbezogenen Daten und Informationen haben die vereidigten öffentlichen Bediensteten, die vom Präsidenten der [Hadopi] gemäß Art. L. 331-21 [CPI] ermächtigt wurden, sowie die Mitglieder der in Art. 1 genannten Kommission zum Schutz von Rechten.

II – Die Betreiber elektronischer Kommunikation und die in Nr. 2 des Anhangs zu diesem Dekret genannten Anbieter sind Adressaten

– der technischen Daten, die zur Identifizierung des Teilnehmers erforderlich sind;

– der in Artikel L. 331-25 [CPI] vorgesehenen Empfehlungen im Hinblick auf deren elektronischen Versand an ihre Teilnehmer;

– der für die Umsetzung der Zusatzstrafen der Sperrung des Zugangs zu einem öffentlichen Online-Kommunikationsdienst erforderlichen Angaben, die der Kommission zum Schutz der Rechte durch die Staatsanwaltschaft zur Kenntnis gebracht werden.

III – Die Berufsorganisationen und die Verwertungsgesellschaften sind Adressaten einer Information über die Befassung der Staatsanwaltschaft.

IV – Die Justizbehörden sind Adressaten der Protokolle über die Feststellung von Tatsachen, die Verstöße nach Artikel L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 und R. 335-5 [CPI] darstellen können.

Das automatisierte Strafregister wird über die Vollstreckung der Strafe der Sperrung informiert.“

22. Der Anhang zum Dekret vom 5. März 2010 sieht vor:

„Bei der als ‚System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet‘ bezeichneten Verarbeitung werden folgende personenbezogene Daten und Informationen gespeichert:

1° Persönliche Daten und Informationen von ordnungsgemäß errichteten Berufsorganisationen, Verwertungsgesellschaften, dem Centre national du cinéma et de l'image animée sowie von der Staatsanwaltschaft:

[b]ezüglich der Tatsachen, die eine Verletzung der in Artikel L. 336-3 [CPI] definierten Verpflichtung darstellen können:

Datum und Uhrzeit der Tat;

IP-Adresse des betreffenden Teilnehmers;

verwendetes Peer-to-Peer-Protokoll;

vom Teilnehmer verwendetes Pseudonym;

Angaben zu den von den Taten betroffenen geschützten Werken oder Schutzgegenständen;

(gegebenenfalls) Name der Datei, wie sie auf dem Rechner des Teilnehmers vorhanden ist;

Internetzugangsanbieter, bei dem der Zugang abonniert wurde oder der die technische Ressource IP zur Verfügung gestellt hat.

…

2° Personenbezogene Daten und Informationen über den Teilnehmer, die von den Betreibern elektronischer Kommunikationsdienste … und den Anbietern … erhoben werden:

Nachname, Vornamen;

Postanschrift und E-Mail-Adressen;

telefonische Kontaktdaten;

Adresse der Telefonanlage des Teilnehmers;

Internetzugangsanbieter, der die technischen Ressourcen des in Nr. 1 genannten Zugangsanbieters nutzt und bei dem der Teilnehmer seinen Vertrag abgeschlossen hat; Aktenzeichen;

Datum des Beginns der Sperrung des Zugangs zu einem öffentlichen Online-Kommunikationsdienst.

…“

3. Post- und Telekommunikationsgesetzbuch

23. Art. L. 34-1 des Code des postes et des communications électroniques (Gesetzbuch für Post und elektronische Kommunikation) in der durch Art. 17 des Gesetzes Nr. 2021-998 vom 30. Juli 2021 geänderten Fassung [5] (im Folgenden: CPCE) sieht in seinem Abs. IIa vor, dass „die Anbieter von Diensten der elektronischen Kommunikation … verpflichtet [sind], auf Vorrat zu speichern:

1. für die Zwecke der Strafverfolgung, der Abwehr von Gefahren für die öffentliche Sicherheit und des Schutzes der nationalen Sicherheit die Informationen über die Identität des Nutzers bis zum Ablauf von fünf Jahren ab dem Ende der Gültigkeit des Vertrags;

[5] JORF vom 31. Juli 2021, Text Nr. 1. Diese Fassung von Art. L. 34-1 CPCE, die seit dem 31. Juli 2021 in Kraft ist, wurde nach der Entscheidung des Conseil d'État (Staatsrat, Frankreich) vom 21. April 2021, Nr. 393099 (JORF vom 25. April 2021) verabschiedet, die die vorherige Fassung dieser Bestimmung verworfen hatte, die eine Verpflichtung zur Vorratsspeicherung personenbezogener Daten „zum Zweck der Ermittlung, Feststellung und Verfolgung von Straftaten oder eines Verstoßes gegen die Verpflichtung gemäß Art. L. 336-3 [CPI]“ zu dem alleinigen Zweck vorsah, bei Bedarf die Bereitstellung insbesondere für die Hadopi zu ermöglichen. Mit Entscheidung Nr. 2021-976-977 QPC vom 25. Februar 2022 (Habib A. u. a.) hat der Conseil constitutionnel (Verfassungsrat, Frankreich) diese frühere Fassung von Art. L. 34-1 CPCE im Wesentlichen mit der Begründung für verfassungswidrig erklärt, dass „die angefochtenen Bestimmungen, indem sie die allgemeine und undifferenzierte Vorratsspeicherung von Verbindungsdaten zulassen, einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens darstellen“ (Rn. 13). Dieses Gericht hat nämlich festgestellt, dass die Verbindungsdaten, die nach diesen Bestimmungen auf Vorrat gespeichert werden müssen, nicht nur die Identifizierung der Nutzer elektronischer Kommunikationsdienste betreffen, sondern auch andere Daten, die „angesichts ihrer Art, ihrer Vielfalt und der Verarbeitungen, denen sie unterzogen werden können, … zahlreiche und genaue Informationen über diese Nutzer sowie gegebenenfalls über Dritte [liefern], die besonders stark in ihr Privatleben eingreifen“ (Rn. 11).

2. für die in Nr. 1 dieses Absatzes IIa genannten Zwecke die übrigen Angaben, die der Nutzer beim Abschluss eines Vertrags oder der Einrichtung eines Kontos macht, und die Informationen über die Zahlung bis zum Ablauf von einem Jahr ab dem Ende der Laufzeit des Vertrags bzw. dem Zeitpunkt, zu dem das Konto geschlossen wird;

3. für die Zwecke der Bekämpfung schwerer Kriminalität, der Abwehr schwerer Gefahren für die öffentliche Sicherheit und des Schutzes der nationalen Sicherheit die technischen Daten, anhand derer sich die Quelle der Verbindung feststellen lässt, oder die technischen Daten betreffend die verwendeten Endgeräte bis zum Ablauf von einem Jahr ab der Verbindung oder der Verwendung der Endgeräte."

III. Ausgangsverfahren, Vorlagefragen und Verfahren vor dem Gerichtshof

24. Mit Klageschrift vom 12. August 2019 und zwei ergänzenden Schriftsätzen vom 12. November 2019 und 6. Mai 2021 haben La Quadrature du Net, die Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net und das French Data Network beim Conseil d'État (Staatsrat, Frankreich) einen Antrag auf Nichtigerklärung der stillschweigenden Entscheidung gestellt, mit der der Premierminister ihren Antrag auf Aufhebung des Dekrets vom 5. März 2010 abgelehnt hat, obwohl dieses Dekret und die Bestimmungen, die seine Rechtsgrundlage bildeten, nach ihrer Auffassung nicht nur die von der französischen Verfassung garantierten Rechte übermäßig beeinträchtigten, sondern auch gegen Art. 15 der Richtlinie 2002/58 sowie gegen die Art. 7, 8, 11 und 52 der Charta verstießen.

25. Insbesondere machen die Kläger des Ausgangsverfahrens geltend, dass das Dekret vom 5. März 2010 und die Bestimmungen, die seine Rechtsgrundlage bilden, den Zugang zu Verbindungsdaten im Hinblick auf Urheberrechtsverletzungen, die im Internet begangen würden und nicht schwerwiegend seien, in unverhältnismäßiger Weise ohne vorherige Kontrolle durch einen Richter oder eine Behörde, die Garantien für Unabhängigkeit und Unparteilichkeit biete, erlaubten.

26. In diesem Zusammenhang weist das vorlegende Gericht zunächst darauf hin, dass der Gerichtshof in seinem jüngsten Urteil La Quadrature du Net u. a.[6] entschieden hat, dass der im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta zu lesende Art. 15 Abs. 1 der Richtlinie 2002/58 Rechtsvorschriften nicht entgegensteht, die zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der *die Identität* der Nutzer elektronischer Kommunikationsmittel *betreffenden Daten* vorsehen. Somit sei eine solche Vorratsspeicherung dieser Daten ohne besondere Frist zum Zweck der Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen möglich.

27. Das vorlegende Gericht leitet daraus ab, dass der von den Klägern des Ausgangsverfahrens vorgebrachte Klagegrund, mit dem diese geltend machten, dass das Dekret vom 5. März 2010 rechtswidrig sei, da es im Rahmen der Bekämpfung nicht schwerwiegender Verstöße erlassen worden sei, nur zurückgewiesen werden könne.

[6] Vgl. Urteil vom 6. Oktober 2020 (C-511/18, C-512/18 und C-520/18, im Folgenden: Urteil La Quadrature du Net u. a., EU:C:2020:791, Tenor).

28. Dieses Gericht weist sodann darauf hin, dass der Gerichtshof in seinem Urteil Tele2 Sverige und Watson [7] entschieden hat, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten, zum Gegenstand hat, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen.

29. Es stellt fest, dass der Gerichtshof im Urteil Tele2 [8] klargestellt hat, dass es, um in der Praxis die vollständige Einhaltung dieser Bedingungen zu gewährleisten, unabdingbar ist, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird.

30. Das vorlegende Gericht weist darauf hin, dass der Gerichtshof dieses Erfordernis im Urteil La Quadrature du Net u. a. [9] in Bezug auf die Erhebung von Verbindungsdaten in Echtzeit durch die Nachrichtendienste sowie im Urteil Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) [10] in Bezug auf den Zugang der nationalen Behörden zu den Verbindungsdaten aufgestellt hat.

31. Das vorlegende Gericht weist schließlich darauf hin, dass die Hadopi seit ihrer Gründung im Jahr 2009 im Rahmen des Verfahrens der abgestuften Reaktion gemäß Art. L 331-25 CPI mehr als 12,7 Millionen Empfehlungen an Inhaber von Abonnements ausgesprochen hat, davon 827 791 allein im Jahr 2019. Dazu müssten die Bediensteten der Kommission für den Schutz von Rechten der Hadopi jedes Jahr eine beträchtliche Anzahl von Daten über die Identität der betroffenen Nutzer erheben können. Diese Erhebung einer vorherigen Kontrolle zu unterwerfen bringe nach Ansicht des vorlegenden Gerichts angesichts des Umfangs dieser Empfehlungen die Gefahr mit sich, dass die Umsetzung der Empfehlungen unmöglich würde.

32. Vor diesem Hintergrund hat der Conseil d'État (Staatsrat) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Gehören die Identitätsdaten, die einer IP-Adresse zugeordnet sind, zu den Verkehrs- oder Standortdaten, die grundsätzlich einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist, unterliegen müssen?

2. Falls die erste Frage bejaht wird und berücksichtigt wird, dass die Daten hinsichtlich der Identität der Nutzer, einschließlich ihrer Kontaktdaten, wenig sensibel sind: Ist dann die Richtlinie 2002/58 im Licht der Charta dahin auszulegen, dass sie einer nationalen Regelung entgegensteht, wonach diese Daten, die einer IP-Adresse der Nutzer zugeordnet sind, von einer Behörde ohne vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist, erhoben werden?

7 Vgl. Urteil vom 21. Dezember 2016 (C-203/15 und C-698/15, im Folgenden: Urteil Tele2, EU:C:2016:970, Tenor).

8 Rn. 120 dieses Urteils.

9 Rn. 189 dieses Urteils.

10 Urteil vom 2. März 2021 (C-746/18, im Folgenden: Urteil Prokuratuur, EU:C:2021:152).

3. Falls die zweite Frage bejaht wird und berücksichtigt wird, dass die Daten hinsichtlich der Identität wenig sensibel sind, dass nur diese Daten erhoben werden dürfen, und das auch nur zu dem Zweck, Verstöße gegen Pflichten zu verhindern, die im nationalen Recht klar, abschließend und restriktiv festgelegt werden, und dass eine systematische Kontrolle des Zugangs zu den Daten jedes einzelnen Nutzers durch ein Gericht oder eine andere Verwaltungsstelle, deren Entscheidung bindend ist, die Erfüllung des öffentlichen Auftrags gefährden könnte, mit dem die fragliche Behörde betraut ist, die selbst unabhängig ist und die die Erhebung vornimmt: Steht dann die Richtlinie 2002/58 dem entgegen, dass diese Kontrolle mittels angepasster Verfahren wie einer automatisierten Kontrolle erfolgt, gegebenenfalls unter der Aufsicht einer Dienststelle innerhalb der Einrichtung, die Garantien für Unabhängigkeit und Unparteilichkeit gegenüber den mit der Erhebung beauftragten Bediensteten bietet?

33. Die Kläger des Ausgangsverfahrens, die französische, die estnische, die schwedische und die norwegische Regierung sowie die Europäische Kommission haben schriftliche Erklärungen eingereicht. Diese Beteiligten – mit Ausnahme der estnischen Regierung – sowie die dänische und die finnische Regierung waren in der mündlichen Verhandlung am 5. Juli 2022 vertreten.

IV. Würdigung

A. Erste und zweite Vorlagefrage

34. Mit seinen ersten beiden Vorlagefragen, die meines Erachtens zusammen zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die einer Verwaltungsbehörde, die mit dem Schutz von Urheberrechten und verwandten Schutzrechten gegen im Internet begangene Verletzungen dieser Rechte betraut ist, den Zugang zu Identitätsdaten, die IP-Adressen zugeordnet sind, gewährt, damit diese Behörde die Inhaber dieser Adressen, die im Verdacht stehen, für diese Rechtsverletzungen verantwortlich zu sein, ermitteln und gegebenenfalls Maßnahmen gegen sie ergreifen kann, ohne dass dieser Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt.

1. Abgrenzung der Vorlagefragen

a) Vorherige Erhebung von IP-Adressen durch Einrichtungen von Rechteinhabern

35. Aus dem Vorabentscheidungsersuchen geht hervor, dass der im Ausgangsverfahren in Rede stehende Mechanismus der abgestuften Reaktion zwei aufeinanderfolgende Datenverarbeitungen umfasst, deren erste in der vorherigen Erhebung der IP-Adressen von Urheberrechtsverletzern in Peer-to-Peer-Netzwerken durch die Einrichtungen von Rechteinhabern und deren zweite in der Verknüpfung dieser IP-Adressen mit der Identität der Personen durch die Hadopi besteht, nachdem diese befasst wurde, um Empfehlungen an Personen zu versenden, deren Zugang zu öffentlichen Online-Kommunikationsdiensten unter Verletzung der Vorschriften des Urheberrechts genutzt wurde.

36. Die erste und die zweite Vorlagefrage beziehen sich nur auf die zweite Verarbeitung, die von der Hadopi durchgeführt wird.

37. Die Kläger des Ausgangsverfahrens machen jedoch geltend, dass die erste Verarbeitung vom Gerichtshof überprüft werden sollte, weil die Nutzung dieser IP-Adressen, sollten sie unter Verletzung der Bestimmungen der Richtlinie 2002/58 erlangt worden sein, im Rahmen der zweiten Verarbeitung notwendigerweise gegen diese Bestimmungen verstoßen würde.

38. Dieses Vorbringen vermag nicht zu überzeugen. Art. 3 Abs. 1 der Richtlinie 2002/58 beschränkt ihren Anwendungsbereich auf die „Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste“. Wie die französische Regierung in der mündlichen Verhandlung klargestellt hat, erhalten die Einrichtungen von Rechteinhabern die fraglichen IP-Adressen jedoch nicht über die Anbieter elektronischer Kommunikationsdienste, sondern direkt online, indem sie öffentlich zugängliche Daten abfragen.

39. Es kann daher nur festgestellt werden, dass die vorherige Erhebung von IP-Adressen durch die Organisationen von Rechteinhabern nicht unter die Bestimmungen der Richtlinie 2002/58 fällt und daher, wie die Kommission ausführt, allenfalls im Licht der Bestimmungen der Verordnung (EU) 2016/679[11] zu prüfen sein könnte. Eine solche Prüfung würde meines Erachtens aber über den Rahmen der dem Gerichtshof zur Vorabentscheidung vorgelegten Fragen hinausgehen, zumal das vorlegende Gericht keine näheren Angaben zur vorhergehenden Erhebung macht, die es dem Gerichtshof ermöglichen würden, ihm eine nützliche Antwort zu geben.

40. Unter diesen Umständen werde ich meine Analyse auf die Frage des Zugangs der Hadopi zu den einer IP-Adresse zugeordneten Identitätsdaten konzentrieren.

b) Verknüpfung von IP-Adressen und Identitätsdaten

41. Die ersten beiden Vorlagefragen beziehen sich auf die „Identitätsdaten, die einer IP-Adresse zugeordnet sind“, die nach Ansicht des vorlegenden Gerichts von geringer Sensibilität sind. In seiner Vorlageentscheidung bezieht sich das vorlegende Gericht ausschließlich auf die Randnummern des Urteils La Quadrature du Net u. a., die sich auf die Vorratsspeicherung von Identitätsdaten beziehen.

42. Es trifft zwar zu, dass die Rechtsprechung des Gerichtshofs zwischen dem System der Vorratsspeicherung und des Zugangs zu IP-Adressen und dem System der Vorratsspeicherung und des Zugangs zu Identitätsdaten von Nutzern elektronischer Kommunikationsmittel unterscheidet, wobei das zweite System weniger streng ist als das erste[12].

43. Meines Erachtens geht es im vorliegenden Fall aber trotz der Formulierung dieser beiden Vorlagefragen nicht um die Frage des bloßen Zugangs zu den Identitätsdaten der Nutzer elektronischer Kommunikationsmittel, sondern um die Verknüpfung dieser Daten mit den IP-Adressen, die der Hadopi nach der Erhebung und Übermittlung dieser Adressen durch die Organisationen von Rechteinhabern zur Verfügung stehen. Wie die Kommission ausführt, zielt der Zugang der Hadopi zu den Identitätsdaten nämlich darauf ab, einen größeren Datensatz, insbesondere die IP-Adressen und die Auszüge aus abgerufenen Dateien, freizugeben und ihre Auswertung zu ermöglichen, weil die Identitätsdaten und die IP-Adressen unabhängig

[11] Verordnung des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1).

[12] Vgl. Urteil La Quadrature du Net u. a. (Rn. 155 und 159).

voneinander für die nationalen Behörden nutzlos sind, da sich weder aus der Identität noch aus der IP-Adresse an sich Informationen über die Online-Aktivitäten natürlicher Personen gewinnen lassen, wenn sie nicht miteinander in Verbindung gebracht werden.

44. Daraus folgt, dass die ersten beiden Vorlagefragen meines Erachtens dahin zu verstehen sind, dass sie nicht nur auf die Identitätsdaten der Nutzer eines elektronischen Kommunikationsmittels abzielen, sondern auch auf den Zugang zu den IP-Adressen, die es ermöglichen, die Quelle einer Verbindung zu identifizieren.

c) Vorratsspeicherung der IP-Adressen durch die Anbieter von Kommunikationsdiensten

45. Wie die französische Regierung und die Kommission zutreffend anmerken, zielen die dem Gerichtshof vorgelegten Vorabentscheidungsfragen formal nicht auf die Vorratsspeicherung von Daten durch die Anbieter elektronischer Kommunikationsdienste ab, sondern allein auf den Zugriff der Hadopi auf Identitätsdaten, die IP-Adressen zugeordnet sind.

46. Meines Erachtens ist die Frage des Zugangs der Hadopi zu diesen Daten jedoch in Wirklichkeit untrennbar mit der Vorfrage ihrer Vorratsspeicherung durch die Anbieter von Kommunikationsdiensten verbunden. Wie der Gerichtshof ausgeführt hat, werden die Daten allein zu dem Zweck aufbewahrt, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen [13]. Mit anderen Worten können die Vorratsspeicherung von Daten und der Zugang zu ihnen nicht isoliert voneinander betrachtet werden, obwohl Letzterer von der Ersteren abhängt.

47. Zwar hat der Gerichtshof die Vereinbarkeit einer allein den Zugang der zuständigen nationalen Behörden zu bestimmten personenbezogenen Daten betreffenden nationalen Regelung mit Art. 15 Abs. 1 der Richtlinie 2002/58 bereits unabhängig von der Frage geprüft, ob die Speicherung der betreffenden Daten mit dieser Bestimmung vereinbar war [14]. Die vorliegenden Vorabentscheidungsfragen könnten daher unabhängig davon beantwortet werden, ob die fraglichen Daten gemäß den Bestimmungen des Unionsrechts aufbewahrt wurden.

48. Ich stelle jedoch zunächst fest, dass der Gerichtshof im Urteil Ministerio Fiscal [15] bei der Prüfung, ob der Zugang der nationalen Behörden zu bestimmten personenbezogenen Daten mit dem Unionsrecht vereinbar ist, strikt denselben Grundsätzen gefolgt ist wie bei der Prüfung der Vereinbarkeit der Vorratsspeicherung dieser Daten mit dem Unionsrecht. Der Gerichtshof bezieht sich nämlich ausschließlich auf die zu letzterem Thema entwickelte Rechtsprechung, um sie auf die Frage des Zugangs zu personenbezogenen Daten zu übertragen. Mit anderen Worten: Wenn die Vereinbarkeit der Vorratsspeicherung bestimmter Daten mit dem Unionsrecht nicht geprüft wird, wird diese Prüfung auf die Stufe der Frage des Zugangs zu diesen Daten verschoben, so dass die Vereinbarkeit dieses Zugangs letztlich von der Vereinbarkeit der Vorratsspeicherung abhängt.

49. Sodann hat der Gerichtshof eindeutig zum Ausdruck gebracht, dass der Zugang zu personenbezogenen Daten nur gewährt werden darf, wenn diese Daten von den Anbietern elektronischer Kommunikationsdienste in einer Weise auf Vorrat gespeichert wurden, die mit

[13] Vgl. Urteil Tele2 (Rn. 79).

[14] Vgl. Urteil vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 49).

[15] Urteil vom 2. Oktober 2018 (C-207/16, EU:C:2018:788).

Art. 15 Abs. 1 der Richtlinie 2002/58 im Einklang steht [16], und dass der Zugang von Privatpersonen zu personenbezogenen Daten, der dazu dient, die Verfolgung von Urheberrechtsverletzungen vor Zivilgerichten zu ermöglichen, mit dem Unionsrecht nur unter der Voraussetzung vereinbar ist, dass diese Daten in einer Weise auf Vorrat gespeichert wurden, die im Einklang mit dieser Bestimmung steht [17].

50. Schließlich entscheidet der Gerichtshof in ständiger Rechtsprechung, dass der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift gespeicherten Verkehrs- und Standortdaten, der unter vollständiger Beachtung der sich aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58 ergebenden Voraussetzungen zu erfolgen hat, grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung diesen Betreibern auferlegt wurde [18]. Mit anderen Worten hängt die Vereinbarkeit des Zugangs der nationalen Behörden zu bestimmten personenbezogenen Daten mit dem Unionsrecht vollständig von der Vereinbarkeit der Vorratsspeicherung dieser Daten mit dem Unionsrecht ab.

51. Daraus folgt meines Erachtens, dass die Prüfung der Vereinbarkeit einer nationalen Regelung, die den Zugang einer nationalen Behörde zu personenbezogenen Daten vorsieht, mit dem Unionsrecht voraussetzt, dass zuvor die Vereinbarkeit der Vorratsspeicherung dieser Daten mit dem Unionsrecht festgestellt wird.

52. Unter diesen Umständen werde ich meine Analyse mit einem Hinweis auf die Rechtsprechung des Gerichtshofs zur Vorratsspeicherung von IP-Adressen beginnen, die der Quelle einer Verbindung zugewiesen sind, um die Grenzen dieser Rechtsprechung aufzuzeigen und ein angepasstes Schema für die Prüfung der in Rede stehenden Regelung vorzuschlagen.

2. Die Rechtsprechung des Gerichtshofs zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 in Bezug auf Maßnahmen zur Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind

53. Art. 5 Abs. 1 der Richtlinie 2002/58 stellt den Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten auf, der u. a. das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert [19].

54. In Bezug auf die Verarbeitung und Speicherung von Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen, durch die Anbieter elektronischer Kommunikationsdienste sieht die Richtlinie 2002/58 in ihrem Art. 6 Abs. 1 vor, dass diese Daten zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr erforderlich sind, und präzisiert in ihrem Art. 6 Abs. 2, dass die Verkehrsdaten, die zum Zweck der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, nur bis zum Ablauf der Frist verarbeitet werden dürfen, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Andere Standortdaten als Verkehrsdaten

16 Vgl. Urteil Prokuratuur (Rn. 29).

17 Vgl. Urteil vom 17. Juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, Rn. 127 bis 130).

18 Vgl. Urteile La Quadrature du Net u. a. (Rn. 166), vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, im Folgenden: Urteil Commissioner of An Garda Síochána u. a., EU:C:2022:258, Rn. 98), und vom 20. September 2022, SpaceNet (C-793/19 und C-794/19, im Folgenden: Urteil SpaceNet, EU:C:2022:702, Rn. 131).

19 Vgl. Urteile La Quadrature du Net u. a. (Rn. 107), Commissioner of An Garda Síochána u. a. (Rn. 35) und SpaceNet (Rn. 52).

dürfen nach Art. 9 Abs. 1 dieser Richtlinie nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben [20].

55. Durch den Erlass der Richtlinie 2002/58 hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt [21]. Folglich beschränkt sich die Richtlinie 2002/58 nicht darauf, den Zugang zu solchen Daten durch Garantien zu regeln, die Missbrauch verhindern sollen, sondern sie regelt insbesondere auch den Grundsatz des Verbots der Speicherung dieser Daten durch Dritte.

56. Indem Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten gestattet, Rechtsvorschriften zu erlassen, die die Rechte und Pflichten gemäß u. a. den Art. 5, 6 und 9 dieser Richtlinie – wie sie sich aus den Grundsätzen der Vertraulichkeit der Kommunikation und dem Verbot der Speicherung der damit verbundenen Daten ergeben – „beschränken“, sieht diese Bestimmung unter diesen Umständen eine Ausnahme von der allgemeinen Regel vor, die u. a. in den Art. 5, 6 und 9 vorgesehen ist, und ist daher nach ständiger Rechtsprechung eng auszulegen. Eine solche Bestimmung vermag es daher nicht zu rechtfertigen, dass die Ausnahme von der grundsätzlichen Verpflichtung, die Vertraulichkeit der elektronischen Kommunikation und der damit verbundenen Daten sicherzustellen, und insbesondere von dem in Art. 5 dieser Richtlinie vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden [22].

57. Hinsichtlich der Zwecke, die eine Beschränkung der insbesondere in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten rechtfertigen können, hat der Gerichtshof bereits entschieden, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie genannten Zwecke abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss [23].

58. Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die nach dieser Vorschrift von den Mitgliedstaaten erlassenen Vorschriften die allgemeinen Grundsätze des Unionsrechts beachten müssen, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die Achtung der durch die Charta garantierten Grundrechte gewährleisten müssen. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch nationale Rechtsvorschriften auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta betreffen, sondern auch die in Art. 11 der Charta gewährleistete Freiheit der Meinungsäußerung, und dass diese Freiheit eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Europäische Union nach Art. 2 EUV gründet [24].

[20] Vgl. Urteile Tele2 (Rn. 86), La Quadrature du Net u. a. (Rn. 108), Commissioner of An Garda Síochána u. a. (Rn. 38) und SpaceNet (Rn. 55).

[21] Vgl. Urteile La Quadrature du Net u. a. (Rn. 109), Commissioner of An Garda Síochána u. a. (Rn. 37) und SpaceNet (Rn. 54).

[22] Vgl. Urteile La Quadrature du Net u. a. (Rn. 110 und 111), Commissioner of An Garda Síochána u. a. (Rn. 40) und SpaceNet (Rn. 57).

[23] Vgl. Urteile La Quadrature du Net u. a. (Rn. 112), Commissioner of An Garda Síochána u. a. (Rn. 41) und SpaceNet (Rn. 58).

[24] Vgl. Urteile La Quadrature du Net u. a. (Rn. 113 und 114), Commissioner of An Garda Síochána u. a. (Rn. 42) und SpaceNet (Rn. 60).

59. In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, die in den Art. 5, 6, und 9 dieser Richtlinie vorgesehenen Rechte und Pflichten zu beschränken, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen. Nach Art. 52 Abs. 1 der Charta sind nämlich Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer und der in den Art. 3, 4, 6 und 7 der Charta verankerten Rechte zukommt [25], aus denen sich positive Verpflichtungen der Behörden ergeben können [26].

60. Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen berechtigten Interessen und Rechte somit miteinander in Einklang gebracht werden. In diesem Rahmen ergibt sich bereits aus dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58, dass die Mitgliedstaaten eine Vorschrift erlassen können, die vom Grundsatz der Vertraulichkeit abweicht, wenn eine solche Vorschrift „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist, wobei es im elften Erwägungsgrund der Richtlinie heißt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss [27].

61. Insoweit geht aus der Rechtsprechung des Gerichtshofs hervor, dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der u. a. in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, zu beurteilen ist, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht [28].

62. Ich stelle außerdem fest, dass der Gerichtshof in seiner Rechtsprechung zwischen den Eingriffen unterscheidet, die sich aus dem Zugang zu Daten ergeben, die als solche genaue Informationen über die betreffende Kommunikation und damit über das Privatleben der Person liefern und für die strenge Aufbewahrungsvorschriften gelten, und den Eingriffen, die sich aus dem Zugang zu Daten ergeben, die solche Informationen nur liefern können, wenn sie mit anderen Daten, wie etwa IP-Adressen, verknüpft werden [29].

63. So hat der Gerichtshof insbesondere in Bezug auf IP-Adressen festgestellt, dass diese ohne Anknüpfung an eine bestimmte Kommunikation erzeugt werden und in erster Linie dazu dienen, über die Betreiber elektronischer Kommunikationsdienste die natürliche Person zu ermitteln, der ein Endgerät gehört, von dem aus eine Kommunikation über das Internet stattfindet. Sofern nur

[25] Vgl. Urteile La Quadrature du Net u. a. (Rn. 120 bis 122), Commissioner of An Garda Síochána u. a. (Rn. 48) und SpaceNet (Rn. 63).

[26] Vgl. Urteile La Quadrature du Net u. a. (Rn. 120 bis 122), Commissioner of An Garda Síochána u. a. (Rn. 49) und SpaceNet (Rn. 64).

[27] Vgl. Urteile La Quadrature du Net u. a. (Rn. 127 bis 129), Commissioner of An Garda Síochána u. a. (Rn. 50 und 51) und SpaceNet (Rn. 65 und 66).

[28] Vgl. Urteile La Quadrature du Net u. a. (Rn. 131), Commissioner of An Garda Síochána u. a. (Rn. 53), und SpaceNet (Rn. 68).

[29] Siehe Nrn. 41 ff. der vorliegenden Schlussanträge.

die IP-Adressen der Kommunikationsquelle gespeichert werden und nicht die des Adressaten dieser Kommunikation, weist diese Kategorie von Daten daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf [30].

64. Zugleich weist der Gerichtshof darauf hin, dass die IP-Adressen insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, so dass diese Daten die Erstellung eines detaillierten Profils dieses Nutzers und genaue Schlüsse auf sein Privatleben ermöglichen. Die Vorratsspeicherung und die Analyse der IP-Adressen stellen daher *schwere* Eingriffe in die in den Art. 7 und 8 der Charta verankerten Grundrechte dar und können abschreckende Wirkungen in Bezug auf die Ausübung der in Art. 11 der Charta garantierten Freiheit der Meinungsäußerung haben [31].

65. Um die widerstreitenden Rechte und berechtigten Interessen miteinander in Einklang zu bringen, wie es die Rechtsprechung verlangt, ist jedoch nach ständiger Rechtsprechung zu berücksichtigen, dass im Fall einer im Internet begangenen Straftat die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde [32].

66. Daher hat der Gerichtshof entschieden, dass eine Rechtsvorschrift, die die allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta verstößt, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen, wobei angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs neben dem Schutz der nationalen Sicherheit nur die Bekämpfung *schwerer Kriminalität* und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet sind, diesen Eingriff zu rechtfertigen [33].

67. Außerdem hat der Gerichtshof klargestellt, dass die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten darf und dass eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten vorsehen muss [34].

3. Die Grenzen der Rechtsprechung zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 in Bezug auf Maßnahmen zur Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind

68. Die Lösung, zu der der Gerichtshof in Bezug auf nationale Maßnahmen zur Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, im Licht von Art. 15 Abs. 1 der Richtlinie 2002/58 gelangt ist, weist jedoch meines Erachtens zwei Hauptschwierigkeiten auf.

30 Vgl. Urteil La Quadrature du Net u. a. (Rn. 152)

31 Vgl. Urteile La Quadrature du Net u. a. (Rn. 153), Commissioner of An Garda Síochána u. a. (Rn. 73) und SpaceNet (Rn. 103). Hervorhebung nur hier.

32 Vgl. Urteile La Quadrature du Net u. a. (Rn. 154), Commissioner of An Garda Síochána u. a. (Rn. 73) und SpaceNet (Rn. 103).

33 Vgl. Urteile La Quadrature du Net u. a. (Rn. 155 und 156), Commissioner of An Garda Síochána u. a. (Rn. 74) und SpaceNet (Rn. 104 und 105). Hervorhebung nur hier.

34 Vgl. Urteile La Quadrature du Net u. a. (Rn. 156) und SpaceNet (Rn. 105).

a) Vereinbarkeit mit der Rechtsprechung zur Weitergabe von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, im Rahmen von Klagen zum Schutz der Rechte des geistigen Eigentums

69. Erstens: Wie ich bereits in meinen Schlussanträgen in der Rechtssache M.I.C.M. [35] erwähnt hatte, besteht eine gewisse Spannung zwischen dieser Rechtsprechungslinie und derjenigen zur Weitergabe von IP-Adressen an die Inhaber von Rechten des geistigen Eigentums im Rahmen von Klagen zum Schutz dieser Rechte, die die Verpflichtung der Mitgliedstaaten betont, den Inhabern der Rechte des geistigen Eigentums tatsächliche Möglichkeiten zu gewährleisten, einen Ersatz für die durch die Verletzung dieser Rechte entstandenen Schäden zu erlangen [36].

70. Was diese zweite Linie der Rechtsprechung betrifft, entscheidet der Gerichtshof nämlich in ständiger Rechtsprechung, dass das Unionsrecht die Mitgliedstaaten nicht daran hindert, eine Verpflichtung zur Weitergabe personenbezogener Daten an Privatpersonen zu schaffen, um die Verfolgung von Urheberrechtsverstößen vor den Zivilgerichten zu ermöglichen [37].

71. Der Gerichtshof stellt in diesem Zusammenhang fest, dass die Möglichkeit für die Mitgliedstaaten, die Verpflichtung zur Offenlegung personenbezogener Daten im Rahmen von Zivilverfahren vorzusehen, sich zunächst aus der Möglichkeit ergibt, eine solche Offenlegung im Rahmen der Verfolgung von Straftaten vorzusehen [38], die sodann auf die zivilrechtliche Verfolgung von Rechtsverletzungen ausgeweitet wurde.

72. Zugleich schreibt der Gerichtshof in Bezug auf IP-Adressen jedoch vor, dass diese Daten nur zur Bekämpfung schwerer Kriminalität und zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit auf Vorrat gespeichert werden dürfen [39].

73. Die Versuche, diese beiden Rechtsprechungslinien miteinander in Einklang zu bringen, führen meines Erachtens zu unangemessenen Ergebnissen und können nicht überzeugen.

74. Zum einen kann die Bekämpfung von Verletzungen der Rechte des geistigen Eigentums entgegen der von der französischen Regierung in der mündlichen Verhandlung vertretenen Auffassung nicht unter die Bekämpfung der schweren Kriminalität fallen. Der Begriff „schwere Kriminalität“ ist meines Erachtens autonom auszulegen. Er darf nicht von den Auffassungen der einzelnen Mitgliedstaaten abhängen, weil es andernfalls möglich wäre, die Anforderungen von Art. 15 Abs. 1 der Richtlinie 2002/58 zu umgehen, je nachdem, ob die Mitgliedstaaten ein weites Verständnis der Bekämpfung schwerer Kriminalität vertreten oder nicht. Wie ich bereits ausgeführt habe, decken sich die Interessen im Zusammenhang mit dem Schutz der Rechte des geistigen Eigentums nicht mit denen, die der Bekämpfung schwerer Kriminalität zugrunde liegen [40].

75. Zum anderen stünde die Erlaubnis, IP-Adressen an Inhaber von Rechten des geistigen Eigentums im Rahmen von Verfahren weiterzugeben, die den Schutz dieser Rechte zum Gegenstand haben, obwohl die Vorratsspeicherung dieser Adressen nur im Rahmen der

35 C-597/19, EU:C:2020:1063, Nr. 98.

36 Vgl. meine Schlussanträge in der Rechtssache M.I.C.M. (C-597/19, EU:C:2020:1063, Nr. 97).

37 Vgl. Urteile vom 19. April 2012, Bonnier Audio u. a. (C-461/10, EU:C:2012:219, Rn. 55), vom 4. Mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, Rn. 34), und vom 17. Juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, Rn. 47 bis 54).

38 Vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae (C-275/06, EU:C:2008:54, Rn. 50 bis 52).

39 Vgl. Nr. 65 der vorliegenden Schlussanträge.

40 Vgl. meine Schlussanträge in der Rechtssache M.I.C.M. (C-597/19, EU:C:2020:1063, Nr. 103).

Bekämpfung schwerer Kriminalität zulässig ist, eindeutig im Widerspruch zur Rechtsprechung des Gerichtshofs zur Vorratsspeicherung von Verbindungsdaten und liefe darauf hinaus, den Voraussetzungen für die Speicherung solcher Daten ihre praktische Wirkung zu nehmen, weil dann jedenfalls aus anderen Gründen auf sie zugegriffen werden könnte.

76. Daraus folgt meines Erachtens, dass die Vorratsspeicherung von IP-Adressen zum Zweck des Schutzes von Rechten des geistigen Eigentums sowie ihre Weitergabe an die Inhaber dieser Rechte im Rahmen von Verfahren, die diesen Schutz zum Gegenstand haben, gegen Art. 15 Abs. 1 der Richtlinie 2002/58 in der Auslegung durch die Rechtsprechung des Gerichtshofs verstoßen könnte. Obwohl die Verpflichtung zur Übermittlung personenbezogener Daten an Privatpersonen zum Zweck der Verfolgung von Urheberrechtsverletzungen vor den Zivilgerichten vom Gerichtshof selbst ermöglicht wurde, wird sie mithin gleichzeitig durch seine eigene Rechtsprechung zur Vorratsspeicherung von IP-Adressen durch die Anbieter elektronischer Kommunikationsdienste neutralisiert.

77. Eine solche Lösung ist jedoch unbefriedigend, weil sie das Gleichgewicht der verschiedenen auf dem Spiel stehenden Interessen, das der Gerichtshof herstellen wollte, in Frage stellen würde, indem sie den Inhabern von Rechten des geistigen Eigentums das wichtigste – wenn nicht einzige – Mittel entzöge, die Urheber der Verletzungen dieser Rechte im Internet zu identifizieren. Diese Überlegung veranlasst mich, die zweite Schwierigkeit darzulegen, die sich meines Erachtens aus der vom Gerichtshof im Licht von Art. 15 Abs. 1 der Richtlinie 2002/58 entwickelten Rechtsprechung zu nationalen Maßnahmen zur Vorratsspeicherung von IP-Adressen ergeben kann, die der Quelle einer Verbindung zugeordnet sind.

b) Gefahr einer systemischen Straflosigkeit für Straftaten, die ausschließlich im Internet begangen werden

78. Zweitens führt diese Lösung somit nach meiner Auffassung zu praktischen Schwierigkeiten. Wie der Gerichtshof selbst ausführt, kann im Fall einer ausschließlich im Internet begangenen Straftat die IP-Adresse der einzige Anhaltspunkt sein, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde.

79. Dennoch scheint mir dieser Gesichtspunkt bei der Abwägung der betroffenen Interessen nicht vollständig berücksichtigt zu werden. Da der Gerichtshof die Möglichkeit der Vorratsspeicherung von IP-Adressen gleichwohl auf den Rahmen der Bekämpfung schwerer Kriminalität beschränkt, schließt er zugleich aus, dass diese Daten zur Bekämpfung von Straftaten im Allgemeinen gespeichert werden können, obwohl einige dieser Straftaten nur mit Hilfe dieser Daten verhindert, aufgedeckt oder bestraft werden können.

80. Mit anderen Worten könnte die Rechtsprechung des Gerichtshofs dazu führen, dass den nationalen Behörden die einzige Möglichkeit genommen wird, die Täter solcher Straftaten im Internet zu identifizieren, die nicht zur schweren Kriminalität zählen, wie z. B. Verletzungen der Rechte des geistigen Eigentums. Dies würde *de facto* zu einer systemischen Straflosigkeit für ausschließlich im Internet begangene Straftaten führen, zu denen im Übrigen nicht nur die Verletzungen von Rechten des geistigen Eigentums zählen. Ich denke dabei insbesondere an Online-Verleumdungen. Das Unionsrecht sieht zwar Anordnungen gegen Vermittler vor, deren

Dienste zur Begehung solcher Straftaten genutzt werden [41], doch könnte die Rechtsprechung des Gerichtshofs dazu führen, dass die Urheber dieser Handlungen nie verfolgt werden könnten.

81. Wenn man nicht hinzunehmen bereit ist, dass eine ganze Reihe von Straftaten niemals verfolgt werden könnte, sollte das Gleichgewicht zwischen den verschiedenen Interessen meines Erachtens erneut analysiert werden.

82. Diese verschiedenen Erwägungen veranlassen mich dazu, dem Gerichtshof eine gewisse Anpassung seiner im Licht von Art. 15 Abs. 1 der Richtlinie 2002/58 entwickelten Rechtsprechung zu nationalen Maßnahmen zur Vorratsspeicherung von IP-Adressen vorzuschlagen.

4. Vorschlag einer Anpassung der Rechtsprechung des Gerichtshofs zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 in Bezug auf Maßnahmen zur Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind

83. In Anbetracht der vorstehenden Erwägungen bin ich der Auffassung, dass Art. 15 Abs. 1 der Richtlinie 2002/58 dahin ausgelegt werden sollte, dass er Maßnahmen nicht entgegensteht, die eine allgemeine und unterschiedslose Speicherung von IP-Adressen, die der Quelle einer Verbindung zugeordnet sind, für einen Zeitraum, der zeitlich auf das absolut Notwendige beschränkt ist, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Internet vorsehen, bei denen die IP-Adresse der *einzige Anhaltspunkt* ist, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde.

84. In diesem Zusammenhang muss ich darauf hinweisen, dass ein solcher Vorschlag meines Erachtens nicht das Erfordernis der Verhältnismäßigkeit in Frage stellt, dem die Vorratsspeicherung von Daten angesichts der Schwere des mit ihr verbundenen Eingriffs in die in Art. 7 und 8 der Charta verankerten Grundrechte unterliegt [42]. Er erfüllt diese Anforderung im Gegenteil voll und ganz.

85. Zum einen verfolgt die mit der Vorratsspeicherung von IP-Adressen einhergehende Einschränkung der in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten eine dem Gemeinwohl dienende Zielsetzung, die in angemessenem Verhältnis zur Schwere dieses Eingriffs steht, nämlich die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, die in Vorschriften aufgeführt sind, die andernfalls wirkungslos bleiben würden.

86. Zum anderen hält sich diese Einschränkung im Rahmen des absolut Notwendigen. Eine solche Speicherung auf Vorrat ist nämlich auf bestimmte Fälle beschränkt, d. h. auf Straftaten, die im Internet begangen werden und bei denen die Identifizierung des Täters nur anhand der ihm zugewiesenen IP-Adresse erfolgen kann. Es geht mit anderen Worten nicht darum, eine allgemeine und unterschiedslose Vorratsdatenspeicherung ohne weitere Voraussetzungen zuzulassen, sondern lediglich darum, die Verfolgung ganz bestimmter Straftaten – und nicht von Straftaten im Allgemeinen – zu ermöglichen.

[41] Art. 15 Abs. 1 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. 2000, L 178, S. 1).

[42] Vgl. Nrn. 60 und 61 der vorliegenden Schlussanträge.

87. Auch wenn Art. 15 Abs. 1 der Richtlinie 2002/58 einer allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Internet, bei denen die IP-Adresse der einzige Anhaltspunkt ist, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde, nicht entgegensteht, ist jedoch klarzustellen, dass die Rechtsprechung diese Möglichkeit „von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig [macht], *die die Nutzung dieser Daten regeln müssen*“ [43]. Der Gerichtshof hat außerdem klargestellt, dass eine derartige Maßnahme „strenge Voraussetzungen und Garantien hinsichtlich der *Auswertung dieser Daten* … vorsehen [muss]“ [44].

88. Mit anderen Worten: Wie bereits ausgeführt, können die Vorratsspeicherung von Daten und der Zugang zu diesen Daten nicht isoliert voneinander betrachtet werden. Unter diesen Umständen verstößt die Möglichkeit der Hadopi, auf IP-Adressen zuzugreifen, zwar nicht von vornherein gegen Art. 15 Abs. 1 der Richtlinie 2002/58, sofern diese Daten im Einklang mit den Anforderungen dieser Bestimmung gespeichert wurden, aber zur Beantwortung der dem Gerichtshof zur Vorabentscheidung vorgelegten Fragen ist es noch erforderlich, zu prüfen, ob die Voraussetzungen für den Zugang der Hadopi zu den IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, als solche mit dieser Bestimmung vereinbar sind, insbesondere im Hinblick auf die Frage, ob eine vorherige Kontrolle eines solchen Zugangs durch ein Gericht oder eine unabhängige Verwaltungsbehörde erforderlich ist oder nicht.

89. Nachdem ich die Vorfrage der Vorratsspeicherung von IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, analysiert habe, werde ich den Zugang der Hadopi zu diesen Daten im Licht von Art. 15 Abs. 1 der Richtlinie 2002/58 untersuchen.

5. Zugang der Hadopi zu den einer IP-Adresse zugeordneten Identitätsdaten

90. Aus der Rechtsprechung des Gerichtshofs ergibt sich in Bezug auf die Zwecke, die eine nationale Maßnahme rechtfertigen können, die vom Grundsatz der Vertraulichkeit der elektronischen Kommunikation abweicht, dass der Zugang zu den Daten strikt und objektiv einem dieser Zwecke entsprechen muss und dass der mit dieser Maßnahme verfolgte Zweck in einem angemessenen Verhältnis zur Schwere des Eingriffs in die Grundrechte stehen muss, den dieser Zugang mit sich bringt [45].

91. Darüber hinaus kann, wie ich bereits dargelegt habe [46], der Zugang zu Daten, die von Anbietern in Anwendung einer nach Art. 15 Abs. 1 der Richtlinie 2002/58 ergriffenen Maßnahme auf Vorrat gespeichert werden, grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden, zu dem die Speicherung diesen Betreibern auferlegt wurde [47].

[43] Vgl. Urteil La Quadrature du Net u. a. (Rn. 155). Hervorhebung nur hier.

[44] Vgl. Urteil La Quadrature du Net u. a. (Rn. 156). Hervorhebung nur hier.

[45] Vgl. Urteile vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 55), und Prokuratuur (Rn. 32).

[46] Nr. 47 der vorliegenden Schlussanträge.

[47] Vgl. Urteile SpaceNet (Rn. 131), La Quadrature du Net u. a. (Rn. 166) und Commissioner of An Garda Síochána u. a. (Rn. 98).

92. So hat der Gerichtshof im Einklang mit dem Grundsatz der Verhältnismäßigkeit entschieden, dass ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur durch einen Zweck der Bekämpfung einer ebenfalls als schwer einzustufenden Kriminalität gerechtfertigt sein kann [48].

93. In diesem Zusammenhang weise ich darauf hin, dass der Zugang der Hadopi zu den Identitätsdaten, die einer IP-Adresse zugeordnet sind, entgegen dem Vorbringen der französischen Regierung und der Kommission sehr wohl einen schwerwiegenden Eingriff in die Grundrechte darstellt. Es geht nämlich nicht nur um den Zugriff auf die Identitätsdaten, die an sich von geringer Sensibilität sind, sondern darum, diese Daten mit einem umfassenderen Datensatz zu verknüpfen, nämlich mit der IP-Adresse, und auch, wie die Kläger des Ausgangsverfahrens betonen, mit einem Auszug aus der Datei, die urheberrechtswidrig heruntergeladen wurde. Es handelt sich somit um die Verknüpfung der Identität einer Person mit dem Inhalt der abgerufenen Datei und der IP-Adresse, über die der Abruf erfolgte.

94. Aber ebenso wie ich die Vorratsspeicherung von Daten, die einen schwerwiegenden Eingriff in die Grundrechte darstellt, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Internet, bei denen die IP-Adresse der einzige Anhaltspunkt ist, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zur Tatzeit zugewiesen war, für zulässig halte [49], bin ich der Auffassung, dass zur Verfolgung des gleichen Zwecks auch der Zugang zu diesen Daten ermöglicht werden sollte, weil andernfalls eine allgemeine Straflosigkeit für ausschließlich im Internet begangene Straftaten hingenommen werden müsste.

95. Der Zugang der Hadopi zu den mit einer IP-Adresse verknüpften Identitätsdaten ist daher meines Erachtens durch das dem Gemeinwohl dienende Ziel gerechtfertigt, zu dem die Vorratsspeicherung den Anbietern elektronischer Kommunikationsdienste auferlegt worden ist.

96. Die Rechtsprechung des Gerichtshofs stellt jedoch klar, dass sich eine nationale Regelung über den Zugang der zuständigen Behörden zu den auf Vorrat gespeicherten Verkehrs- und Standortdaten nicht darauf beschränken darf, dass der Zugang dem mit dieser Regelung verfolgten Zweck zu entsprechen hat, sondern auch die materiellen und prozeduralen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu diesen Daten festlegen muss [50].

97. Insbesondere hat der Gerichtshof entschieden, dass sich die nationale Regelung – weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten unabhängig davon, ob irgendein Zusammenhang mit dem verfolgten Ziel besteht, nicht als auf das absolut Notwendige beschränkt angesehen werden kann – bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten der Nutzer zu gewähren ist, auf objektive Kriterien stützen muss, so dass überprüft werden kann, ob der Zugang nur zu den Daten von Personen gewährt wird, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein [51].

48 Vgl. Urteile Tele2 (Rn. 115), vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 56), und Prokuratuur (Rn. 33).

49 Vgl. Nrn. 65 ff. der vorliegenden Schlussanträge.

50 Vgl. Urteile Tele2 (Rn. 118), Prokuratuur (Rn. 49) und Commissioner of An Garda Síochána u. a. (Rn. 104).

51 Vgl. Urteile Tele2 (Rn. 119), Prokuratuur (Rn. 50) und Commissioner of An Garda Síochána u. a. (Rn. 105).

98. Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, ist es nach der Rechtsprechung unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird [52].

99. Ich stelle jedoch fest, dass der Gerichtshof dieses Erfordernis einer vorherigen Kontrolle des Zugangs zu personenbezogenen Daten unter besonderen Umständen aufgestellt hat, die sich vom vorliegenden Fall unterscheiden und zu *besonders schwerwiegenden* Eingriffen in das Privatleben der Nutzer elektronischer Kommunikationsdienste führen.

100. In jedem der Urteile, in denen dieses Erfordernis hervorgehoben wurde, handelte es sich nämlich um nationale Maßnahmen, die den Zugang zu allen Verkehrs- und Standortdaten der Nutzer in Bezug auf alle elektronischen Kommunikationsmittel [53] oder zumindest auf die Festnetz- und Mobiltelefonie gestatteten [54]. Genauer gesagt ging es um den Zugang zu einem „Satz von [Daten], die geeignet sind, Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Kommunikationen oder über den Standort der von ihm verwendeten Endgeräte zu liefern und genaue Schlüsse auf sein Privatleben zuzulassen“ [55], so dass eine vorherige Kontrolle des Zugangs zu diesen Daten durch ein Gericht oder eine unabhängige Verwaltungsstelle meines Erachtens nur unter diesen Voraussetzungen erforderlich ist.

101. Zum einen bleibt der Zugang der Hadopi aber darauf beschränkt, die Identitätsdaten mit der verwendeten IP-Adresse und der zu einem bestimmten Zeitpunkt aufgerufenen Datei in Verbindung zu bringen, ohne dass dies dazu führt, dass die zuständigen Behörden die vom betroffenen Nutzer besuchten Internetseiten nachverfolgen können, so dass sie daher auch keine genauen Schlüsse auf sein Privatleben ziehen können, die über die Kenntnis der bestimmten Datei, die zum Zeitpunkt des Verstoßes aufgerufen wurde, hinausgehen. Es geht also nicht darum, die Nachverfolgung aller Online-Aktivitäten des betroffenen Nutzers zu ermöglichen.

102. Zum anderen betreffen diese Daten, wie in den von den Einrichtungen der Rechteinhaber erstellten Protokollen festgestellt wurde, nur die Daten von Personen, die Handlungen vorgenommen haben, die einen Verstoß gegen die in Art. L. 336-3 CPI festgelegte Verpflichtung darstellen können. Der Zugriff der Hadopi zu den mit den IP-Adressen verknüpften Identitätsdaten ist daher streng auf das beschränkt, was zur Erreichung des verfolgten Ziels notwendig ist, nämlich die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Internet zu ermöglichen, bei denen die IP-Adresse der einzige Anhaltspunkt ist, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde, ein Ziel, in das sich der Mechanismus der abgestuften Reaktion einfügt.

103. Unter diesen Umständen bin ich der Auffassung, dass Art. 15 Abs. 1 der Richtlinie 2002/58 nicht verlangt, den Zugang der Hadopi zu den mit den IP-Adressen der Nutzer verknüpften Identitätsdaten der vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle zu unterwerfen.

[52] Vgl. Urteile Tele2 (Rn. 120), Prokuratuur (Rn. 51) und Commissioner of An Garda Síochána u. a. (Rn. 106).

[53] Vgl. Urteile Tele2 und Commissioner of An Garda Síochána u. a.

[54] Vgl. Urteil Prokuratuur.

[55] Vgl. Urteil Prokuratuur (Rn. 45).

104. Im Übrigen stelle ich fest, dass der Zugang der Hadopi zu diesen Daten, wie die französische Regierung ausführt, zwar keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Stelle unterliegt, aber gleichwohl nicht jeglicher Kontrolle entzogen ist, weil die von der Hadopi an die Betreiber elektronischer Kommunikationsdienste übersandte Datei täglich von einem vereidigten Bediensteten anhand der eingegangenen Ersuchen zusammengestellt wird, die nach dem Zufallsprinzip anhand einer Stichprobe überprüft werden, bevor diese Daten in die Datei aufgenommen werden [56]. Vor allem ist zu beachten, dass das Verfahren der abgestuften Reaktion weiterhin den Bestimmungen der Richtlinie (EU) 2016/680 [57] unterliegt. Somit genießen die von der Hadopi erfassten natürlichen Personen eine Reihe von materiellen und prozeduralen Garantien, die in dieser Richtlinie vorgesehen sind. Diese umfassen das Recht auf Zugang, Berichtigung und Löschung der von der Hadopi verarbeiteten personenbezogenen Daten sowie die Möglichkeit, eine Beschwerde bei einer unabhängigen Aufsichtsbehörde einzureichen, an die sich gegebenenfalls ein nach den Bedingungen des allgemeinen Rechts einzulegender gerichtlicher Rechtsbehelf anschließt [58].

105. Daher schlage ich vor, auf die ersten beiden Vorlagefragen zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung nicht entgegensteht, die Anbietern elektronischer Kommunikationsdienste die Vorratsspeicherung von Identitätsdaten, die IP-Adressen zugeordnet sind, erlaubt und einer Verwaltungsbehörde, die für den Schutz von Urheberrechten und verwandten Schutzrechten gegen im Internet begangene Verletzungen dieser Rechte zuständig ist, Zugang zu diesen – und nur diesen – Daten gewährt, damit diese Behörde die Inhaber dieser Adressen, die im Verdacht stehen, für diese Rechtsverletzungen verantwortlich zu sein, ermitteln und gegebenenfalls Maßnahmen gegen sie ergreifen kann, ohne dass dieser Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, wenn diese Daten den einzigen Anhaltspunkt darstellen, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde.

B. Dritte Vorlagefrage

106. Für den Fall, dass die ersten beiden Fragen bejaht werden, möchte das vorlegende Gericht mit seiner dritten Vorlagefrage wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 in Anbetracht der geringen Sensibilität der Identitätsdaten, der strengen Kontrolle des Zugangs zu den Daten und des Gebots, den der in Rede stehenden Verwaltungsbehörde übertragenen öffentlichen Auftrag nicht zu gefährden, im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er dem entgegensteht, dass die vorherige Kontrolle des Zugangs

[56] Am Rande weise ich darauf hin, dass auch Machbarkeitsargumente gegen eine Verpflichtung zu einer systematischen Vorabkontrolle sprechen. Ein organisiertes System zur Bekämpfung im Internet begangener Urheberrechtsverletzungen wie das im Ausgangsverfahren in Rede stehende setzt die Notwendigkeit voraus, große Mengen personenbezogener Daten zu verarbeiten, die der Zahl der verfolgten Verstöße entsprechen, d. h. beispielsweise für das Jahr 2019 nach den schriftlichen Erklärungen der französischen Regierung 33 465 von der Hadopi bearbeiteten Anträgen auf Identifizierung von IP-Adressen pro Tag. In diesem Zusammenhang würde die Verpflichtung, den Zugang zu diesen Daten vorab zu kontrollieren, in der Praxis das Funktionieren der Mechanismen zur organisierten Bekämpfung von Urheberrechtverletzungen im Internet gefährden und das Gleichgewicht zwischen den Rechten der Nutzer und denen der Urheber in Frage stellen.

[57] Richtlinie 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. 2016, L 119, S. 89).

[58] Alle diese Garantien sind in den Bestimmungen von Kapitel III Titel III der Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 (Gesetz Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten) (JORF vom 7. Januar 1978) vorgesehen.

mittels angepasster Verfahren wie einer automatisierten Kontrolle erfolgt, gegebenenfalls unter der Aufsicht einer Dienststelle innerhalb der Einrichtung, die Garantien für Unabhängigkeit und Unparteilichkeit gegenüber den mit der Erhebung beauftragten Bediensteten bietet.

107. Aus dem Wortlaut der dritten Vorlagefrage sowie aus der schriftlichen Antwort der französischen Regierung auf die Fragen des Gerichtshofs geht hervor, dass die angepassten Kontrollverfahren, auf die in dieser Frage Bezug genommen wird, nicht auf ein im nationalen Recht bestehendes Kontrollsystem abzielen, sondern darauf, mögliche Wege zu erkunden, um die französische Regelung gegebenenfalls mit dem Unionsrecht in Einklang zu bringen.

108. Nach ständiger Rechtsprechung zielt ein Vorabentscheidungsersuchen jedoch nicht darauf ab, Gutachten zu allgemeinen oder hypothetischen Fragen abzugeben, sondern darauf, dem Bedürfnis nach einer tatsächlichen Entscheidung eines Rechtsstreits über das Unionsrecht Genüge zu tun [59].

109. Da die dritte Vorlagefrage daher meines Erachtens hypothetischen Charakter hat, ist sie als unzulässig anzusehen.

110. Jedenfalls ist in Anbetracht der von mir vorgeschlagenen Antwort auf die ersten beiden Vorlagefragen die dritte Frage nicht zu beantworten.

V. Ergebnis

111. Nach alledem schlage ich dem Gerichtshof vor, die vom Conseil d'État (Staatsrat, Frankreich) gestellten Vorlagefragen wie folgt zu beantworten:

Art. 15 Abs. 1 der 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) ist im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union

dahin auszulegen,

dass er einer nationalen Regelung nicht entgegensteht, die Anbietern elektronischer Kommunikationsdienste die Vorratsspeicherung von Identitätsdaten, die IP-Adressen zugeordnet sind, erlaubt und einer Verwaltungsbehörde, die für den Schutz von Urheberrechten und verwandten Schutzrechten gegen im Internet begangene Verletzungen dieser Rechte zuständig ist, Zugang zu diesen – und nur diesen – Daten gewährt, damit diese Behörde die Inhaber dieser Adressen, die im Verdacht stehen, für diese Rechtsverletzungen verantwortlich zu sein, ermitteln und gegebenenfalls Maßnahmen gegen sie ergreifen kann, ohne dass dieser Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, wenn diese Daten den einzigen Anhaltspunkt darstellen, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde.

[59] Vgl. Urteile vom 26. Oktober 2017, Balgarska energiyna borsa (C-347/16, EU:C:2017:816, Rn. 31), vom 31. Mai 2018, Confetra u. a. (C-259/16 und C-260/16, EU:C:2018:370, Rn. 63), und vom 17. Oktober 2019, Elektrorazpredelenie Yug (C-31/18, EU:C:2019:868, Rn. 32).