Quelle: http://curia.europa.eu/

URTEIL DES GERICHTSHOFS (Plenum)

30. April 2024(*)

Inhaltsverzeichnis

Rechtlicher Rahmen
- Unionsrecht
  - Allgemeine Regelung zum Schutz personenbezogener Daten
    - – Richtlinie 95/46/EG
    - – DSGVO
  - Sektorielle Regelung zum Schutz personenbezogener Daten
    - – Richtlinie 2002/58
    - – Richtlinie (EU) 2016/680
  - Regelung zum Schutz der Rechte des geistigen Eigentums
- Französisches Recht
  - CPI
  - Dekret Nr. 2010-236
  - Gesetzbuch für Post und elektronische Kommunikation

Ausgangsverfahren und Vorlagefragen

Zu den Vorlagefragen
- Vorbemerkungen
- Zum Vorliegen einer Rechtfertigung des Zugangs einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind und von den Betreibern elektronischer Kommunikationsdienste zur Bekämpfung der online begangenen Nachahmung auf Vorrat gespeichert werden, gemäß Art. 15 Abs. 1 der Richtlinie 2002/58
  - Zu den Anforderungen an die Vorratsspeicherung von Identitätsdaten und der ihnen zuzuordnenden IP-Adressen durch die Betreiber elektronischer Kommunikationsdienste
  - Zu den Anforderungen an den Zugang zu den einer IP-Adresse zuzuordnenden Identitätsdaten, die von den Betreibern elektronischer Kommunikationsdienste gespeichert werden
  - Zum Erfordernis einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vor dem Zugang einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind
  - Zu den Anforderungen an den Zugang einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind, hinsichtlich der materiellen und prozeduralen Voraussetzungen sowie der Garantien in Bezug auf Missbrauchsgefahren, jeden unbe rechtigten Zugang zu den Daten und jede unberechtigte Nutzung

Kosten

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation – Richtlinie 2002/58/EG – Vertraulichkeit der elektronischen Kommunikation – Schutz – Art. 5 und Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7, 8 und 11 sowie Art. 52 Abs. 1 – Nationale Rechtsvorschriften,

mit denen im Internet begangene Nachahmungen durch Maßnahmen einer Behörde bekämpft werden sollen – Verfahren der ‚abgestuften Reaktion' – Vorgelagerte Erfassung von IP-Adressen, die für Aktivitäten genutzt werden, die Urheberrechte oder verwandte Schutzrechte verletzen, durch Einrichtungen der Rechteinhaber – Nachgelagerter Zugang der mit dem Schutz der Urheberrechte und verwandten Schutzrechte betrauten Behörde zu Identitätsdaten, die diesen von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten IP-Adressen zuzuordnen sind – Automatisierte Verarbeitung – Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle – Materielle und prozedurale Voraussetzungen – Garantien zum Schutz vor Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung"

In der Rechtssache C-470/21

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Conseil d'État (Staatsrat, Frankreich) mit Entscheidung vom 5. Juli 2021, beim Gerichtshof eingegangen am 30. Juli 2021, in dem Verfahren

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

gegen

Premier ministre,

Ministre de la Culture

erlässt

DER GERICHTSHOF (Plenum)

unter Mitwirkung des Präsidenten K. Lenaerts, des Vizepräsidenten L. Bay Larsen, des Kammerpräsidenten A. Arabadjiev, der Kammerpräsidentinnen A. Prechal (Berichterstatterin) und K. Jürimäe, der Kammerpräsidenten C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra und Z. Csehi, der Richter M. Ilešič, J.-C. Bonichot, S. Rodin und P. G. Xuereb, der Richterin L. S. Rossi, der Richter I. Jarukaitis, A. Kumin, N. Jääskinen und N. Wahl, der Richterin I. Ziemele, der Richter J. Passer und D. Gratsias, der Richterin M. L. Arastey Sahún und des Richters M. Gavalec,

Generalanwalt: M. Szpunar,

Kanzler: V. Giacobbo und M. Krausenböck, Verwaltungsrätinnen,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 5. Juli 2022,

unter Berücksichtigung der Erklärungen

– von La Quadrature du Net, der Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net und des French Data Network, vertreten durch A. Fitzjean Ó Cobhthaigh, Avocat,

– der französischen Regierung, vertreten durch A. Daniel, A.-L. Desjonquères und J. Illouz als Bevollmächtigte,

– der dänischen Regierung, vertreten durch J. F. Kronborg und V. Pasternak Jørgensen als Bevollmächtigte,

– der estnischen Regierung, vertreten durch M. Kriisa als Bevollmächtigte,

– der finnischen Regierung, vertreten durch H. Leppo als Bevollmächtigte,

– der schwedischen Regierung, vertreten durch H. Shev als Bevollmächtigte,

– der norwegischen Regierung, vertreten durch F. Bergsjø, S.-E. Dahl, J. T. Kaasin und P. Wennerås als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal und F. Wilman als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 27. Oktober 2022,

aufgrund des Beschlusses vom 23. März 2023 über die Wiedereröffnung der mündlichen Verhandlung und auf die mündliche Verhandlung vom 15. Mai 2023,

unter Berücksichtigung der Erklärungen

– von La Quadrature du Net, der Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net und des French Data Network, vertreten durch A. Fitzjean Ó Cobhthaigh, Avocat,

– der französischen Regierung, vertreten durch R. Bénard, J. Illouz und T. Stéhelin als Bevollmächtigte,

– der tschechischen Regierung, vertreten durch T. Suchá und J. Vláčil als Bevollmächtigte,

– der dänischen Regierung, vertreten durch J. F. Kronborg und C. A.-S. Maertens als Bevollmächtigte,

– der estnischen Regierung, vertreten durch M. Kriisa als Bevollmächtigte,

– Irlands, vertreten durch M. Browne, Chief State Solicitor, A. Joyce und D. O'Reilly als Bevollmächtigte im Beistand von D. Fenelly, BL,

– der spanischen Regierung, vertreten durch A. Gavela Llopis als Bevollmächtigte,

– der zyprischen Regierung, vertreten durch I. Neophytou als Bevollmächtigte,

– der lettischen Regierung, vertreten durch J. Davidoviča und K. Pommere als Bevollmächtigte,

– der niederländischen Regierung, vertreten durch E. M. M. Besselink, M. K. Bultermann und A. Hanje als Bevollmächtigte,

– der finnischen Regierung, vertreten durch A. Laine und H. Leppo als Bevollmächtigte,

– der schwedischen Regierung, vertreten durch F.-D. Göransson und H. Shev als Bevollmächtigte,

– der norwegischen Regierung, vertreten durch S.-E. Dahl und P. Wennerås als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal und F. Wilman als Bevollmächtigte,

– des Europäischen Datenschutzbeauftragten, vertreten durch V. Bernardo, C.-A. Marnier, D. Nardi und M. Pollmann als Bevollmächtigte,

– der Agentur der Europäischen Union für Cybersicherheit, vertreten durch A. Bourka als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 28. September 2023

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung 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) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

2 Es ergeht im Rahmen eines Rechtsstreits zwischen den Verbänden La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net und French Data Network einerseits sowie dem Premier ministre (Premierminister, Frankreich) und dem Ministre de la Culture (Minister für Kultur, Frankreich) andererseits über die Rechtmäßigkeit des Décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé „Système de gestion des mesures pour la protection des œuvres sur Internet" (Dekret Nr. 2010-236 vom 5. März 2010 über die nach Art. L. 331-29 des Gesetzbuchs über das geistige Eigentum gestattete automatisierte Verarbeitung personenbezogener Daten mit der Bezeichnung „System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet") (JORF Nr. 56 vom 7. März 2010, Text Nr. 19) in der durch das Décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Dekret Nr. 2017-924 vom 6. Mai 2017 über die Verwaltung von Urheberrechten und verwandten Schutzrechten durch eine Verwertungsgesellschaft und zur Änderung des Gesetzbuchs über das geistige Eigentum) (JORF Nr. 109 vom 10. Mai 2017, Text Nr. 176) geänderten Fassung (im Folgenden: Dekret Nr. 2010-236).

Rechtlicher Rahmen

Unionsrecht

Allgemeine Regelung zum Schutz personenbezogener Daten

– *Richtlinie 95/46/EG*

3 Der in Abschnitt II („Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten") von Kapitel II der Richtlinie 95/46/EG 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, berichtigt in ABl. 2017, L 40, S. 78) zu findende Art. 7 dieser Richtlinie bestimmte:

„Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

…

f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen."

4 In Art. 13 Abs. 1 der Richtlinie 95/46 hieß es:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

…

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen."

– *DSGVO*

5 Art. 2 („Sachlicher Anwendungsbereich") der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1, im Folgenden: DSGVO) bestimmt in den Abs. 1 und 2:

„(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

…

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit."

6 Art. 4 („Begriffsbestimmungen“) DSGVO sieht vor:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. ‚personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen; …

2. ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

…“

7 Art. 6 („Rechtmäßigkeit der Verarbeitung“) DSGVO sieht in Abs. 1 vor:

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

…

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen …

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.“

8 Art. 9 („Verarbeitung besonderer Kategorien personenbezogener Daten“) DSGVO sieht in Abs. 2 Buchst. e und f vor, dass das Verbot der Verarbeitung bestimmter Arten personenbezogener Daten, u. a. von Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person, keine Anwendung findet, wenn sich die Verarbeitung auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat, oder wenn die Verarbeitung u. a. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

9 Art. 23 („Beschränkungen“) DSGVO bestimmt in Abs. 1:

„Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5,

insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

…

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche."

Sektorielle Regelung zum Schutz personenbezogener Daten

– *Richtlinie 2002/58*

10 In den Erwägungsgründen 2, 6, 7, 11, 26 und 30 der Richtlinie 2002/58 heißt es:

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

…

(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. …“

11 Art. 2 („Begriffsbestimmungen“) der Richtlinie 2002/58 sieht vor:

„…

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;

…“

12 Art. 3 („Betroffene Dienste“) der Richtlinie 2002/58 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.“

13 Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie 2002/58 sieht vor:

„(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. …“

14 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.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

…

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.“

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

„(1) 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 Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.

…

(2) Die Bestimmungen des Kapitels III der Richtlinie [95/46] über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

…“

– *Richtlinie (EU) 2016/680*

16 Art. 1 („Gegenstand und Ziele“) der 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. 2016, L 119, S. 89) sieht in Abs. 1 vor:

„Diese Richtlinie enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“

17 In Art. 3 („Begriffsbestimmungen“) der Richtlinie 2016/680 heißt es:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

…

7. ‚zuständige Behörde‘

a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

…“

Regelung zum Schutz der Rechte des geistigen Eigentums

18 Art. 8 („Recht auf Auskunft“) der Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. 2004, L 157, S. 45, berichtigt in ABl. 2004, L 195, S. 16) bestimmt:

„(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer … erteilt werden …

(2) Die Auskünfte nach Absatz 1 erstrecken sich, soweit angebracht, auf

a) die Namen und Adressen der Hersteller, Erzeuger, Vertreiber, Lieferer und anderer Vorbesitzer der Waren oder Dienstleistungen sowie der gewerblichen Abnehmer und Verkaufsstellen, für die sie bestimmt waren;

…

(3) Die Absätze 1 und 2 gelten unbeschadet anderer gesetzlicher Bestimmungen, die

a) dem Rechtsinhaber weiter gehende Auskunftsrechte einräumen,

b) die Verwendung der gemäß diesem Artikel erteilten Auskünfte in straf- oder zivilrechtlichen Verfahren regeln,

c) die Haftung wegen Missbrauchs des Auskunftsrechts regeln,

d) die Verweigerung von Auskünften zulassen, mit denen die in Absatz 1 genannte Person gezwungen würde, ihre Beteiligung oder die Beteiligung enger Verwandter an einer Verletzung eines Rechts des geistigen Eigentums zuzugeben,

oder

e) den Schutz der Vertraulichkeit von Informationsquellen oder die Verarbeitung personenbezogener Daten regeln."

Französisches Recht

CPI

19 Art. L. 331-12 des Code de la propriété intellectuelle (Gesetzbuch über das geistige Eigentum) in der zum Zeitpunkt des Erlasses der von den Klägerinnen des Ausgangsverfahrens angefochtenen Entscheidung geltenden 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. …."

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

„Die [Hadopi] gewährleistet:

1° die Förderung der Entwicklung des rechtmäßigen Angebots und die Überwachung der rechtmäßigen und unrechtmäßigen Nutzung von Werken und Gegenständen, an denen ein Urheberrecht oder ein verwandtes Schutzrecht besteht, in elektronischen Kommunikationsnetzen, die zur Bereitstellung von Online-Kommunikationsdiensten für die Öffentlichkeit genutzt werden;

2° den Schutz dieser Werke und Gegenstände vor Verletzungen dieser Rechte in elektronischen Kommunikationsnetzen, die zur Bereitstellung von Online-Kommunikationsdiensten für die Öffentlichkeit genutzt werden;

…"

21 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 Weisungen von anderen Behörden.“

22 Art. L. 331-17 CPI bestimmt in Abs. 1:

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

23 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 Kommission für den Schutz von Rechten unter den in Art. L. 331-24 vorgesehenen Bedingungen mit einem Vorgang befasst, wird dieser Vorgang ihren Mitgliedern 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 Kommunikationsdienste 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 nº 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 sind.

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

Sie können insbesondere von den Betreibern elektronischer Kommunikationsdienste die Identität, die Postanschrift, die E-Mail-Adresse und die Telefondaten des Teilnehmers erhalten, dessen Zugang zu Online-Kommunikationsdiensten für die Öffentlichkeit 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.“

24 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 für den 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."

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

„Wird die Kommission für den 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 rechtmäßige 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 diesem Verstoß 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 von Rechten eine Stellungnahme übermitteln und, wenn er dies ausdrücklich beantragt, nähere Angaben zum Inhalt der geschützten Werke oder Schutzgegenstände erhalten kann, die von dem ihm vorgeworfenen Verstoß betroffen sind."

26 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 Online-Kommunikationsdiensten für die Öffentlichkeit anzubieten;

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

27 Art. L. 335-2 Abs. 1 und 2 CPI sieht vor:

„Jede unter Missachtung der Gesetze und Verordnungen über das Urheberrecht ganz oder teilweise gedruckte oder eingravierte Ausgabe von Schriften, Musikkompositionen, Zeichnungen, Gemälden oder anderen Erzeugnissen ist eine Nachahmung, und jede Nachahmung stellt ein Delikt dar.

Die Nachahmung in Frankreich von Werken, die in Frankreich oder im Ausland veröffentlicht wurden, wird mit Freiheitsstrafe bis zu drei Jahren und mit Geldstrafe bis zu 300 000 Euro bestraft."

28 Art. L. 335-4 Abs. 1 CPI lautet:

„Jede Aufzeichnung, Vervielfältigung, entgeltliche oder unentgeltliche Wiedergabe oder öffentliche Zugänglichmachung oder jede Fernsehübertragung einer Darbietung, eines Ton- oder Bildträgers, eines Programms oder einer Presseveröffentlichung, die ohne die erforderliche Zustimmung des ausübenden Künstlers, des Produzenten von Ton- oder Bildträgern, des Unternehmens für audiovisuelle Kommunikation, des Verlegers oder der Presseagentur vorgenommen wird, wird mit Freiheitsstrafe bis zu drei Jahren und mit Geldstrafe bis zu 300 000 Euro bestraft."

29 Art. L. 335-7 CPI enthält Vorschriften über die Verhängung der Zusatzstrafe einer Aussetzung des Zugangs zu einem Online-Kommunikationsdienst für die Öffentlichkeit für bis zu einem Jahr u. a. gegen Personen, die Straftaten im Sinne der Art. L. 335-2 und L. 335-4 CPI begangen haben.

30 Art. L. 335-7-1 Abs. 1 CPI lautet:

„Für Übertretungen der fünften Kategorie im Sinne dieses Gesetzbuchs kann, sofern die Verordnung dies vorsieht, die in Art. L. 335-7 festgelegte Zusatzstrafe in gleicher Weise bei grober Fahrlässigkeit gegen den Inhaber des Zugangs zu einem Online-Kommunikationsdienst für die Öffentlichkeit verhängt werden, an den die Kommission für den Schutz von Rechten gemäß Art. L. 331-25 zuvor durch ein gegen Unterschrift zugestelltes Schreiben oder in anderer zum Nachweis des Datums der Zustellung geeigneter Weise eine Empfehlung gerichtet hat, mit der er aufgefordert wurde, eine Maßnahme zur Sicherung seines Internetzugangs zu ergreifen."

31 In Art. L. 336-3 CPI heißt es:

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

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

32 Art. R. 331-37 Abs. 1 CPI sieht vor:

„Die … Betreiber elektronischer Kommunikationsdienste 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 ihre Integrität und ihre Sicherheit gewährleistet, die personenbezogenen Daten und die in Nr. 2 des Anhangs des Dekrets [Nr. 2010-236] 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 Zugang zu Online-Kommunikationsdiensten für die Öffentlichkeit zu Zwecken der Vervielfältigung, der Darstellung, der öffentlichen Zugänglichmachung oder der öffentlichen Wiedergabe von geschützten Werken oder Gegenständen ohne die erforderliche Zustimmung der Inhaber der … Rechte genutzt wurde."

33 In Art. R. 331-40 CPI heißt es:

„Werden der Kommission für den Schutz von Rechten innerhalb eines Jahres, nachdem die in Art. L. 335-7-1 genannte Empfehlung ergangen ist, neue Sachverhalte unterbreitet, die eine grobe Fahrlässigkeit im Sinne von Art. R. 335-5 darstellen können, informiert sie den Teilnehmer durch ein gegen Unterschrift zugestelltes Schreiben darüber, dass diese Sachverhalte strafrechtlich verfolgt werden können. In diesem Schreiben wird der Betroffene aufgefordert, innerhalb von 15 Tagen Stellung zu nehmen. Es wird hinzugefügt, dass er innerhalb derselben Frist eine Anhörung gemäß Art. L. 331-21-1 beantragen kann und dass er das Recht auf Hinzuziehung eines Beistands hat. Ferner wird er aufgefordert, seine familiären Lasten und seine Mittel anzugeben.

Die Kommission kann den Betroffenen von sich aus zu einer Anhörung laden. In dem Ladungsschreiben ist anzugeben, dass er das Recht auf Hinzuziehung eines Beistands hat."

34 Art. R. 335-5 CPI bestimmt:

„I. – Sofern die in Abschnitt II genannten Bedingungen erfüllt sind, stellt es eine grobe Fahrlässigkeit des Inhabers eines Zugangs zu Online-Kommunikationsdiensten für die Öffentlichkeit dar, die mit der für Übertretungen der fünften Kategorie vorgesehenen Geldbuße geahndet wird, wenn er ohne legitimen Grund

1° entweder keine Maßnahme zur Sicherung dieses Zugangs getroffen hat

2° oder bei der Durchführung dieser Maßnahme mangelnde Sorgfalt gezeigt hat.

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

1° Die Kommission für den Schutz von Rechten hat dem Inhaber des Zugangs nach Art. L. 331-25 in den in diesem Artikel vorgesehenen Formen 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 erforderliche Zustimmung der Inhaber der … Rechte genutzt wird.

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

35 Zum 1. Januar 2022 fusionierte die Hadopi in Anwendung der Loi nº 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (Gesetz Nr. 2021-1382 vom 25. Oktober 2021 über die Regulierung und den Schutz des Zugangs zu kulturellen Werken im digitalen Zeitalter) (JORF Nr. 250 vom 26. Oktober 2021, Text Nr. 2) mit dem Conseil supérieur de l'audiovisuel (Aufsichtsbehörde für die audiovisuellen Medien, CSA), einer anderen unabhängigen Behörde, zur Autorité de régulation de la communication audiovisuelle et numérique (Regulierungsbehörde für die audiovisuelle und digitale Kommunikation, ARCOM).

36 Das oben in Rn. 25 erwähnte Verfahren der abgestuften Reaktion blieb jedoch im Wesentlichen unverändert, auch wenn es künftig nicht mehr von der Kommission für den Schutz von Rechten der Hadopi durchgeführt wird, die aus drei vom Conseil d'État (Staatsrat), von der Cour des Comptes (Rechnungshof) und von der Cour de cassation (Kassationshof) benannten Mitgliedern bestand, sondern von zwei Mitgliedern des Kollegiums der ARCOM, von denen eines vom Conseil d'État und das andere von der Cour de cassation benannt wird.

Dekret Nr. 2010-236

37 Das Dekret Nr. 2010-236, das u. a. auf der Grundlage von Art. L. 331-29 CPI erlassen wurde, sieht in Art. 1 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 den Artikeln L. 335-2, L. 335-3, L. 335-4 und R. 335-5 [CPI] darstellen könnten, sowie die Unterrichtung der Berufsorganisationen und der Verwertungsgesellschaften über diese Befassung;

…"

38 Art. 4 des Dekrets Nr. 2010-236 bestimmt:

„I. – Direkten Zugang zu den im Anhang dieses Dekrets 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 für den Schutz von Rechten.

II. – Die Betreiber elektronischer Kommunikationsdienste und die in Nr. 2 des Anhangs dieses Dekrets genannten Anbieter sind Adressaten

– der zur Identifizierung des Teilnehmers erforderlichen technischen Daten;

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

– der für die Umsetzung der Zusatzstrafen einer Sperrung des Zugangs zu einem Online-Kommunikationsdienst für die Öffentlichkeit erforderlichen Angaben, die der Kommission für den Schutz von Rechten 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 im Sinne der 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 Zugangssperre informiert.“

39 Der Anhang dieses Dekrets 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° Personenbezogene Daten und Informationen, die von ordnungsgemäß errichteten Berufsorganisationen, Verwertungsgesellschaften, dem Centre national du cinéma et de l’image animée sowie der Staatsanwaltschaft stammen:

Bezüglich der Tatbestände, die einen Verstoß gegen die in Artikel L. 336-3 [CPI] definierte Verpflichtung darstellen können:

Datum und Uhrzeit der Tatbestände;

IP-Adresse des betreffenden Teilnehmers;

verwendetes Peer-to-Peer-Protokoll;

vom Teilnehmer verwendetes Pseudonym;

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

(gegebenenfalls) Name der auf dem Rechner des Teilnehmers vorhandenen Datei;

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 Online-Kommunikationsdienst für die Öffentlichkeit.

…“

Gesetzbuch für Post und elektronische Kommunikation

40 Art. L. 34-1, II*bis*, des Code des postes et des communications électroniques (Gesetzbuch für Post und elektronische Kommunikation) bestimmt:

„Die Betreiber elektronischer Kommunikationsdienste sind verpflichtet, Folgendes 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 Laufzeit seines Vertrags;

2° für die in II*bis* Nr. 1 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 seines Vertrags bzw. dem Zeitpunkt, zu dem sein Konto geschlossen wird;

3° für die Zwecke der Bekämpfung schwerer Kriminalität und Delinquenz, der Abwehr schwerer Gefahren für die öffentliche Sicherheit und des Schutzes der nationalen Sicherheit die technischen Daten, anhand deren 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 Nutzung der Endgeräte."

Ausgangsverfahren und Vorlagefragen

41 Nachdem der französische Premierminister den Antrag der Klägerinnen des Ausgangsverfahrens auf Aufhebung des Dekrets Nr. 2010-236 implizit abgelehnt hatte, erhoben sie mit Klageschrift vom 12. August 2019 beim Conseil d'État (Staatsrat, Frankreich) Klage auf Nichtigerklärung dieser impliziten ablehnenden Entscheidung. Sie machten im Wesentlichen geltend, Art. L. 331-21 Abs. 3 bis 5 CPI, der zur Rechtsgrundlage dieses Dekrets gehöre, verstoße zum einen gegen das in der französischen Verfassung verankerte Recht auf Achtung des Privatlebens und zum anderen gegen das Unionsrecht, insbesondere Art. 15 der Richtlinie 2002/58 sowie die Art. 7, 8, 11 und 52 der Charta.

42 Zu dem die gerügte Verletzung der Verfassung betreffenden Aspekt der Klage hat der Conseil d'État (Staatsrat) dem Conseil constitutionnel (Verfassungsrat, Frankreich) eine vorrangige Frage der Verfassungsmäßigkeit vorgelegt.

43 Mit seiner Entscheidung Nr. 2020-841 QPC vom 20. Mai 2020, La Quadrature du Net u. a. (Recht der Übermittlung an die Hadopi), erklärte der Conseil constitutionnel (Verfassungsrat) die Abs. 3 und 4 von Art. L. 331-21 CPI für verfassungswidrig, Abs. 5 dieses Artikels hingegen mit Ausnahme des darin enthaltenen Wortes „insbesondere" für verfassungsgemäß.

44 Zu dem den gerügten Verstoß gegen das Unionsrecht betreffenden Aspekt der Klage machen die Klägerinnen des Ausgangsverfahrens insbesondere geltend, das Dekret Nr. 2010-236 und die Bestimmungen, die dessen Rechtsgrundlage bildeten, gestatteten in unverhältnismäßiger Weise den Zugang zu Verbindungsdaten für im Internet begangene Urheberrechtsverstöße von mangelnder Schwere, ohne vorherige Kontrolle durch einen Richter oder eine Stelle, die Garantien für Unabhängigkeit und Unparteilichkeit biete.

Insbesondere handele es sich bei den Verstößen nicht um „schwere Straftaten“ im Sinne des Urteils vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970).

45 Insoweit weist das vorlegende Gericht zum einen darauf hin, dass der Gerichtshof im Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), u. a. entschieden habe, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegenstehe, die zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Identitätsdaten der Nutzer elektronischer Kommunikationsmittel vorsähen. Bei den Identitätsdaten der Nutzer elektronischer Kommunikationsmittel sei eine solche Speicherung mithin ohne besondere Frist für Zwecke der Ermittlung, Feststellung und Verfolgung allgemeiner Straftaten möglich. Auch die Richtlinie 2002/58 stehe einem Datenzugang zu solchen Zwecken nicht entgegen.

46 Folglich sei in Bezug auf den Zugang zu Identitätsdaten der Nutzer elektronischer Kommunikationsmittel der Klagegrund der Klägerinnen des Ausgangsverfahrens, wonach das Dekret Nr. 2010-236 rechtswidrig sei, weil es im Rahmen der Bekämpfung nicht schwerwiegender Zuwiderhandlungen erlassen worden sei, zurückzuweisen.

47 Zum anderen habe der Gerichtshof im Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), u. a. entschieden, dass 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 sei, dass er einer nationalen Regelung entgegenstehe, 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 habe, ohne den Zugang zu ihnen einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle zu unterwerfen.

48 Insbesondere habe der Gerichtshof es in Rn. 120 dieses Urteils für unabdingbar erachtet, dass ein solcher Zugang zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder durch eine unabhängige Verwaltungsstelle unterworfen werde und dass deren Entscheidung auf einen mit Gründen versehenen, von den zuständigen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag ergehe.

49 Der Gerichtshof habe auf dieses Erfordernis im Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), in Bezug auf die Erhebung von Verbindungsdaten durch die

Nachrichtendienste in Echtzeit sowie im Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), hinsichtlich des Zugangs der nationalen Behörden zu Verbindungsdaten hingewiesen.

50 Ferner habe die Hadopi seit ihrer Errichtung im Jahr 2009 im Rahmen des in Art. L. 331-25 CPI vorgesehenen Verfahrens der abgestuften Reaktion mehr als 12,7 Millionen Empfehlungen an Teilnehmer ausgesprochen, davon 827 791 allein im Jahr 2019. Dies impliziere, dass die Bediensteten der Kommission für den Schutz von Rechten der Hadopi jedes Jahr zwangsläufig eine beträchtliche Zahl von Identitätsdaten der betreffenden Nutzer hätten erheben müssen. Würde deren Erhebung einer vorherigen Kontrolle unterworfen, brächte dies angesichts des Umfangs der Empfehlungen die Gefahr mit sich, dass ihre Umsetzung unmöglich gemacht würde.

51 Unter diesen Umständen 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?

3. Falls die zweite Frage bejaht wird und berücksichtigt wird, dass die Identitätsdaten 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 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?

Zu den Vorlagefragen

52 Mit seinen drei Vorlagefragen, die 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, wonach die mit dem Schutz von Urheberrechten und verwandten Schutzrechten vor im Internet begangenen Verstößen betraute Behörde Zugang zu den von den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste auf Vorrat gespeicherten Identitätsdaten, die den zuvor von Einrichtungen der Rechteinhaber gesammelten IP-Adressen zuzuordnen sind, erhält, damit die Behörde die Inhaber dieser für Aktivitäten, die möglicherweise solche Verstöße darstellen, genutzten Adressen identifizieren und gegebenenfalls ihnen gegenüber Maßnahmen ergreifen kann, ohne dass dieser Zugang vom Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängt.

Vorbemerkungen

53 Im Ausgangsverfahren geht es um zwei gesonderte und aufeinanderfolgende Verarbeitungen personenbezogener Daten im Rahmen der Tätigkeiten der Hadopi, einer unabhängigen Behörde, zu deren Aufgaben es gemäß Art. L. 331-13 CPI gehört, Werke und Gegenstände, an denen ein Urheberrecht oder ein verwandtes Schutzrecht besteht, vor Verletzungen dieser Rechte in elektronischen Kommunikationsnetzen zu schützen, die zur Bereitstellung von Online-Kommunikationsdiensten für die Öffentlichkeit genutzt werden.

54 Die erste, vorgelagerte Verarbeitung, die durch vereidigte und zugelassene Vertreter von Einrichtungen der Rechteinhaber vorgenommen wird, findet in zwei Schritten statt. Im ersten Schritt werden in Peer-to-Peer-Netzen IP-Adressen gesammelt, die für Aktivitäten genutzt worden zu sein scheinen, durch die ein Urheberrecht oder ein verwandtes Schutzrecht verletzt worden sein könnte. Im zweiten Schritt werden der Hadopi eine Reihe personenbezogener Daten und Informationen in Form von Protokollen zur Verfügung gestellt. Dabei handelt es sich nach der Liste in Nr. 1 des Anhangs des Dekrets 2010/236 um Datum und Uhrzeit der Tatbestände, die IP-Adresse der betreffenden Teilnehmer, das verwendete Peer-to-Peer-Protokoll, das vom Teilnehmer verwendete Pseudonym, Angaben zu den von den Tatbeständen betroffenen Werken oder Schutzgegenständen, (gegebenenfalls) den Namen der auf dem Rechner des Teilnehmers vorhandenen Datei und den Internetzugangsanbieter, bei dem der Zugang abonniert wurde oder der die technische Ressource IP zur Verfügung gestellt hat.

55 Die zweite, nachgelagerte Verarbeitung, die durch die Internetzugangsanbieter auf Ersuchen der Hadopi vorgenommen wird, findet ebenfalls in zwei Schritten statt. Im ersten Schritt werden die bei der vorgelagerten Verarbeitung gesammelten IP-Adressen mit den Inhabern dieser Adressen abgeglichen. Im zweiten Schritt werden der Hadopi eine Reihe personenbezogener Daten und Informationen über die Inhaber, die im Wesentlichen ihre Identität betreffen, zur Verfügung gestellt. Dabei handelt es sich nach der Liste in Nr. 2 des Anhangs des Dekrets 2010/236 im Wesentlichen um Nachnamen und Vornamen, Postanschrift und E-Mail-Adresse, telefonische Kontaktdaten sowie die Adresse der Telefonanlage des Teilnehmers.

56 Zu Letzterem sieht Art. L. 331-21 Abs. 5 CPI in der Fassung, die er durch die oben in Rn. 43 erwähnte Entscheidung des Conseil constitutionnel (Verfassungsrat) erhalten hat, vor, dass die Mitglieder der Kommission für den Schutz von Rechten der Hadopi und die von deren Präsidenten ermächtigten vereidigten öffentlichen Bediensteten von den Betreibern elektronischer Kommunikationsdienste die Identität, die Postanschrift, die E-Mail-Adresse und die Telefondaten des Teilnehmers erhalten können, dessen Zugang zu Online-Kommunikationsdiensten für die Öffentlichkeit zu Zwecken der Vervielfältigung, Darstellung, öffentlichen Zugänglichmachung oder öffentlichen Wiedergabe von geschützten Werken oder Gegenständen ohne Zustimmung – sofern erforderlich – der Rechteinhaber genutzt wurde.

57 Diese verschiedenen Verarbeitungen personenbezogener Daten sollen es der Hadopi ermöglichen, gegenüber den auf diese Weise identifizierten Inhabern von IP-Adressen die im Rahmen des in Art. L. 331-25 CPI geregelten Verwaltungsverfahrens der „abgestuften Reaktion“ vorgesehenen Maßnahmen zu ergreifen. Dabei handelt es sich zunächst um die Übersendung von „Empfehlungen“, die Warnungen gleichkommen. Sodann wird der Teilnehmer, falls die Kommission für den Schutz von Rechten der Hadopi innerhalb eines Jahres nach der Übersendung einer zweiten Empfehlung mit Tatbeständen befasst wird, die eine Wiederholung des festgestellten Verstoßes darstellen können, in der in Art. R. 331-40 CPI geregelten Weise darüber unterrichtet, dass bei den Tatbeständen „grobe Fahrlässigkeit“ im Sinne von Art. R. 335-5 CPI vorliegen könnte, die mit einer Geldbuße von bis zu 1 500 Euro bzw. 3 000 Euro im Wiederholungsfall geahndet wird. Schließlich wird nach Beratung die Staatsanwaltschaft mit Tatbeständen befasst, die eine solche Übertretung oder gegebenenfalls das Delikt der Nachahmung im Sinne von Art. L. 335-2 CPI oder Art. L. 335-4 CPI darstellen können, das mit Freiheitsstrafe von drei Jahren und mit Geldstrafe von 300 000 Euro bedroht ist.

58 Die Fragen des vorlegenden Gerichts betreffen aber nur die oben in Rn. 55 beschriebene nachgelagerte Verarbeitung und nicht die vorgelagerte Verarbeitung, deren wesentliche Merkmale oben in Rn. 54 dargelegt worden sind.

59 Falls die vorherige Sammlung von IP-Adressen durch die betreffenden Einrichtungen der Rechteinhaber mit dem Unionsrecht unvereinbar wäre, stünde das Unionsrecht jedoch auch der Nutzung dieser Daten im Rahmen der anschließenden Verarbeitung durch die Betreiber elektronischer Kommunikationsdienste entgegen, die im Abgleich der IP-Adressen mit den Identitätsdaten ihrer Inhaber besteht.

60 In diesem Kontext ist vorab darauf hinzuweisen, dass IP-Adressen nach der Rechtsprechung des Gerichtshofs sowohl Verkehrsdaten im Sinne der Richtlinie 2002/58 als auch personenbezogene Daten im Sinne der DSGVO darstellen (vgl. in diesem Sinne Urteil vom 17. Juni 2021, M.I.C.M., C-597/19, EU:C:2021:492, Rn. 102 und 113 sowie die dort angeführte Rechtsprechung).

61 Die Sammlung öffentlicher und für alle sichtbarer IP-Adressen durch Vertreter von Einrichtungen der Rechteinhaber fällt jedoch nicht in den Geltungsbereich der Richtlinie 2002/58, da eine solche Verarbeitung offenkundig nicht „in Verbindung mit der Bereitstellung … elektronischer Kommunikationsdienste“ im Sinne ihres Art. 3 stattfindet.

62 Dagegen stellt eine solche Sammlung von IP-Adressen – die, wie sich aus den dem Gerichtshof vorgelegten Akten ergibt, innerhalb bestimmter quantitativer Grenzen und unter bestimmten Voraussetzungen von der Commission nationale de l’informatique et des libertés (Nationale Kommission für Informatik und Freiheiten, CNIL, Frankreich) zwecks Übermittlung an die Hadopi zur etwaigen Nutzung in späteren Verwaltungs- oder Gerichtsverfahren im Rahmen der Bekämpfung von Aktivitäten, die gegen Urheberrechte und verwandte Schutzrechte verstoßen, genehmigt wird – eine „Verarbeitung“ im Sinne von Art. 4 Nr. 2 DSGVO dar, deren Rechtmäßigkeit von den in Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO aufgestellten Voraussetzungen abhängt, im Licht der insbesondere in den Urteilen vom 17. Juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492, Rn. 102 und 103), und vom 4. Juli 2023, Meta Platforms u. a. (Allgemeine Nutzungsbedingungen eines sozialen Netzwerks) (C-252/21, EU:C:2023:537, Rn. 106 bis 112 und die dort angeführte Rechtsprechung), herausgearbeiteten Rechtsprechung des Gerichtshofs.

63 Die oben in Rn. 55 beschriebene nachgelagerte Verarbeitung fällt in den Geltungsbereich der Richtlinie 2002/58, da sie „in Verbindung mit der Bereitstellung … elektronischer Kommunikationsdienste“ im Sinne ihres Art. 3 stattfindet, sofern die fraglichen Daten bei den Betreibern elektronischer Kommunikationsdienste im Einklang mit Art. L. 331-21 CPI erhoben werden.

Zum Vorliegen einer Rechtfertigung des Zugangs einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind und von den Betreibern elektronischer Kommunikationsdienste zur Bekämpfung der online begangenen Nachahmung auf Vorrat gespeichert werden, gemäß Art. 15 Abs. 1 der Richtlinie 2002/58

64 In Anbetracht der vorstehenden Vorbemerkungen stellt sich die vom vorlegenden Gericht aufgeworfene Frage, ob die mit dem Zugang einer Behörde wie der Hadopi zu Identitätsdaten, die einer IP-Adresse, über die sie bereits verfügt, zuzuordnen sind, verbundene Einschränkung der in den Art. 7, 8 und 11 der Charta verankerten Grundrechte gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 gerechtfertigt sein kann.

65 Der Zugang zu solchen personenbezogenen Daten kann nur gewährt werden, sofern sie im Einklang mit der Richtlinie 2002/58 auf Vorrat gespeichert wurden (vgl. in diesem Sinne Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 29).

Zu den Anforderungen an die Vorratsspeicherung von Identitätsdaten und der ihnen zuzuordnenden IP-Adressen durch die Betreiber elektronischer Kommunikationsdienste

66 Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet es den Mitgliedstaaten, Ausnahmen von der in ihrem Art. 5 Abs. 1 aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten zu schaffen, 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 u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit gespeichert werden. Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 der Richtlinie 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikation und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 110 und 111).

67 Eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift muss daher tatsächlich strikt einem der in der vorstehenden Randnummer genannten Ziele dienen, da deren Aufzählung in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 abschließenden Charakter hat, und muss die allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und die durch die Charta garantierten Grundrechte beachten. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen

nationalen Behörden zugänglich zu machen, Fragen aufwirft, die die Einhaltung nicht nur der den Schutz des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta, sondern auch des die Freiheit der Meinungsäußerung gewährleistenden Art. 11 der Charta betreffen (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 112 und 113).

68 Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt, sowie des in Art. 11 der Charta gewährleisteten Grundrechts auf freie Meinungsäußerung berücksichtigt werden, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 114 und die dort angeführte Rechtsprechung).

69 Insoweit ist hervorzuheben, dass die Vorratsspeicherung von Verkehrs- und Standortdaten als solche zum einen eine Abweichung von dem nach Art. 5 Abs. 1 der Richtlinie 2002/58 für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten darstellt und zum anderen einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Art. 7 und 8 der Charta verankert sind; dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben. Irrelevant ist auch, ob die gespeicherten Daten in der Folge genutzt werden, da der Zugriff auf solche Daten, unabhängig von ihrer späteren Nutzung, einen gesonderten Eingriff in die in der vorstehenden Randnummer genannten Grundrechte darstellt (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 115 und 116).

70 In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, bestimmte abweichende Maßnahmen vorzusehen (siehe oben, Rn. 66), 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, den Wesensgehalt der Rechte achten, unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Urteil vom

6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 120 und 121).

71 Im vorliegenden Fall wird der Hadopi zwar formal nur Zugang zu den einer IP-Adresse zuzuordnenden Identitätsdaten gewährt, doch weist dieser Zugang die Besonderheit auf, dass er zuvor einen Abgleich der IP-Adresse mit den Identitätsdaten ihres Inhabers durch die betreffenden Betreiber elektronischer Kommunikationsdienste erfordert. Der Zugang setzt somit notwendigerweise voraus, dass die Betreiber über die IP-Adressen sowie die Identitätsdaten ihrer Inhaber verfügen.

72 Außerdem begehrt die Hadopi Zugang zu diesen Daten allein zu dem Zweck, den Inhaber einer IP-Adresse zu identifizieren, die für Aktivitäten genutzt wurde, durch die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzt wurden, da er geschützte Werke rechtswidrig im Internet bereitgestellt hat, damit andere Personen sie herunterladen können. Unter diesen Umständen ist davon auszugehen, dass die Identitätsdaten in engem Zusammenhang sowohl mit der IP-Adresse als auch mit Informationen zu dem im Internet bereitgestellten Werk stehen, über die die Hadopi verfügt.

73 Ein solcher besonderer Kontext kann aber im Rahmen der Prüfung der etwaigen Rechtfertigung einer Maßnahme zur Vorratsspeicherung personenbezogener Daten gemäß Art. 15 Abs. 1 der Richtlinie 2002/58, ausgelegt im Licht der Art. 7, 8 und 11 der Charta, nicht außer Acht gelassen werden (vgl. entsprechend EGMR, 24. April 2018, Benedik/Slowenien, CE:ECHR:2018:0424JUD006235714, § 109).

74 Daher ist anhand der Anforderungen, die sich für die Speicherung von IP-Adressen aus Art. 15 Abs. 1 der Richtlinie 2002/58, ausgelegt im Licht der Art. 7, 8 und 11 der Charta, ergeben, eine etwaige Rechtfertigung des Eingriffs in die in diesen Artikeln der Charta verankerten Grundrechte zu prüfen, der mit der Vorratsspeicherung der Daten, zu denen die Hadopi zugangsbefugt ist, durch die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste einhergeht.

75 In diesem Kontext ist festzustellen, dass nach der Rechtsprechung des Gerichtshofs IP-Adressen zwar, wie oben in Rn. 60 dargelegt, Verkehrsdaten im Sinne der Richtlinie 2002/58 darstellen, sich aber von den anderen Kategorien von Verkehrs- und Standortdaten unterscheiden.

76 Hierzu hat der Gerichtshof ausgeführt, dass IP-Adressen ohne Anknüpfung an eine bestimmte Kommunikation erzeugt werden und in erster Linie dazu dienen, über die Betreiber elektronischer Kommunikationsdienste den Besitzer eines Endgeräts zu ermitteln, von dem aus eine Kommunikation über das Internet stattfindet. Sofern im Bereich von E-Mail und Internettelefonie nur die IP-Adressen der Kommunikationsquelle gespeichert werden und nicht die des

Adressaten einer Kommunikation, lässt sich diesen Adressen als solchen somit keine Information über die Dritten entnehmen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand. Diese Datenkategorie weist daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 152).

77 Zwar hat der Gerichtshof in Rn. 156 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58 trotz des geringeren Sensibilitätsgrads, den IP-Adressen haben, wenn sie ausschließlich zur Identifizierung des Nutzers eines elektronischen Kommunikationsdiensts dienen, einer allgemeinen und unterschiedslosen Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung für andere Zwecke als denen der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit oder des Schutzes der nationalen Sicherheit entgegensteht. Er hat sich bei dieser Schlussfolgerung jedoch ausdrücklich auf die Schwere des Eingriffs in die in den Art. 7, 8 und 11 der Charta verankerten Grundrechte gestützt, der mit einer solchen Speicherung der IP-Adressen verbunden sein kann.

78 Der Gerichtshof hat nämlich in Rn. 153 dieses Urteils ausgeführt, dass die IP-Adressen, da sie insbesondere zur „umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten“ und infolgedessen seiner Online-Aktivität genutzt werden können, die Erstellung eines „detaillierten Profils“ dieses Nutzers ermöglichen, so dass ihre für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse schwere Eingriffe in die Grundrechte des Betroffenen aus den Art. 7 und 8 der Charta darstellen, was auch abschreckende Wirkungen auf die Ausübung der durch Art. 11 der Charta garantierten Freiheit der Meinungsäußerung durch die Nutzer elektronischer Kommunikationsmittel entfalten kann.

79 Hervorzuheben ist jedoch, 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.

80 Insoweit betrafen zunächst die Rechtssachen, in denen das Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergangen ist, nationale Regelungen, die eine Pflicht zur Vorratsspeicherung eines Datensatzes vorsahen, der benötigt wurde, um Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren sowie den Ort der Endgeräte und der Kommunikation zu bestimmen; dazu gehörten u. a. Name und Adresse des Nutzers, die Telefonnummern des Anrufers und des

Angerufenen sowie die IP-Adresse für die Internetdienste. Überdies erfassten die in zwei dieser Rechtssachen in Rede stehenden nationalen Regelungen Daten in Bezug auf die Weiterleitung der elektronischen Kommunikation durch die Netze, die es ermöglichten, auch die Art online konsultierter Informationen zu identifizieren (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 82 und 83).

81 Die im Rahmen solcher nationaler Regelungen erfolgte Vorratsspeicherung der IP-Adressen war daher angesichts der übrigen Daten, deren Vorratsspeicherung sie vorschrieben, und der Möglichkeit, diese verschiedenen Daten zu kombinieren, geeignet, genaue Schlüsse auf das Privatleben der Personen zu ermöglichen, deren Daten betroffen waren, und konnte damit zu einem schweren Eingriff in ihre in den Art. 7 und 8 der Charta verankerten, den Schutz ihres Privatlebens und ihrer personenbezogenen Daten betreffenden Grundrechte sowie in ihre in Art. 11 der Charta verankerte Freiheit der Meinungsäußerung führen.

82 Dagegen kann die den Betreibern elektronischer Kommunikationsdienste durch eine Rechtsvorschrift im Sinne von Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht, die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen sicherzustellen, 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.

83 Daher muss sich ein Mitgliedstaat, der den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen auferlegen möchte, um ein mit der Bekämpfung von Straftaten im Allgemeinen verbundenes Ziel zu erreichen, vergewissern, dass die Modalitäten der Vorratsspeicherung dieser Daten zu gewährleisten vermögen, dass jede Kombination der IP-Adressen mit anderen unter Beachtung der Richtlinie 2002/58 auf Vorrat gespeicherten Daten ausgeschlossen ist, die es ermöglichen würde, genaue Schlüsse auf das Privatleben der Personen zu ziehen, deren Daten in dieser Weise gespeichert wurden.

84 Um sicherzustellen, dass eine solche, genaue Schlüsse auf das Privatleben der betreffenden Person ermöglichende Kombination von Daten ausgeschlossen ist, müssen die Modalitäten der Vorratsspeicherung die Struktur der Speicherung als solche betreffen, die im Wesentlichen so gestaltet sein muss, dass eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleistet ist.

85 Insoweit ist es zwar Sache des Mitgliedstaats, der den Betreibern elektronischer Kommunikationsdienste zur Erreichung eines mit der Bekämpfung von Straftaten im Allgemeinen verbundenen Ziels eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung der IP-Adressen auferlegen will, in seinen Rechtsvorschriften klare und präzise Regeln für die Modalitäten der Speicherung vorzusehen, die strengen Anforderungen genügen müssen. Der Gerichtshof kann jedoch Erläuterungen zu diesen Modalitäten geben.

86 Erstens müssen die in der vorstehenden Randnummer genannten nationalen Regeln sicherstellen, dass jede Kategorie von Daten, einschließlich der Identitätsdaten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird.

87 Zweitens müssen diese Regeln gewährleisten, 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.

88 Drittens dürfen die Regeln, soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, unter Beachtung der Anforderungen, die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta ergeben, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt.

89 Viertens muss die Zuverlässigkeit dieser strikten Trennung regelmäßig Gegenstand einer Kontrolle durch eine andere Behörde als die sein, die Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten personenbezogenen Daten begehrt.

90 Soweit im anwendbaren nationalen Recht solche strengen Anforderungen an die Modalitäten der allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen und anderen von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten vorgesehen sind, kann der Eingriff, der sich aus dieser Speicherung der IP-Adressen ergibt, schon aufgrund der Struktur ihrer Speicherung nicht als „schwer“ eingestuft werden.

91 Falls eine solche gesetzliche Regelung geschaffen wird, schließen die durch sie vorgeschriebenen Modalitäten der Speicherung der IP-Adressen nämlich eine Kombination dieser Daten mit anderen unter Beachtung der Richtlinie 2002/58 gespeicherten Daten aus, die es ermöglichen würde, genaue Schlüsse auf das Privatleben des Betroffenen zu ziehen.

92 Folglich hindert, sofern es eine den oben in den Rn. 86 bis 89 dargelegten Anforderungen entsprechende gesetzliche Regelung gibt, die gewährleistet, dass keine Kombination von Daten genaue Schlüsse auf das Privatleben der fraglichen Person zulassen wird, Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta den betreffenden Mitgliedstaat nicht daran, mit dem Ziel der Bekämpfung von Straftaten im Allgemeinen eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen aufzustellen.

93 Schließlich muss eine solche gesetzliche Regelung, wie sich aus Rn. 168 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergibt, eine auf das absolut Notwendige begrenzte Dauer der Speicherung vorsehen und durch klare und präzise Regeln sicherstellen, 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 Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügen.

94 Es ist Sache des vorlegenden Gerichts, zu prüfen, ob die im Ausgangsverfahren in Rede stehende nationale Regelung die in den Rn. 85 bis 93 des vorliegenden Urteils wiedergegebenen Voraussetzungen erfüllt.

Zu den Anforderungen an den Zugang zu den einer IP-Adresse zuzuordnenden Identitätsdaten, die von den Betreibern elektronischer Kommunikationsdienste gespeichert werden

95 Nach der Rechtsprechung des Gerichtshofs können im Bereich der Bekämpfung von Straftaten nur die Ziele der Bekämpfung schwerer Kriminalität oder der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit den schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte rechtfertigen, der mit dem Zugang der Behörden zu einem Satz von Verkehrs- oder Standortdaten verbunden ist, die geeignet sind, Informationen über die Kommunikation eines Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von ihm verwendeten Endgeräte zu liefern, aus denen genaue Schlüsse auf das Privatleben der Betroffenen gezogen werden können, ohne dass andere die Verhältnismäßigkeit eines Zugangsantrags betreffende Faktoren wie die Länge des Zeitraums, für den der Zugang zu solchen Daten begehrt wird, dazu führen können, dass das Ziel, Straftaten im Allgemeinen zu verhüten, zu ermitteln, festzustellen und zu verfolgen, einen solchen Zugang zu rechtfertigen vermag (Urteil vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 35).

96 Ist mit dem Zugang von Behörden zu den von den Betreibern elektronischer Kommunikationsdienste gespeicherten Identitätsdaten, die nicht mit

Informationen über die erfolgte Kommunikation verknüpft werden können, hingegen kein schwerer Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte verbunden, da diese Daten in ihrer Gesamtheit keine genauen Schlüsse auf das Privatleben der Personen zulassen, deren Daten betroffen sind, kann dieser Zugang durch ein Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 54, 57 und 60).

97 Hinzuzufügen ist, dass nach einem Grundsatz, der zur ständigen Rechtsprechung des Gerichtshofs gehört, der Zugang zu Verkehrs- und Standortdaten gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 nur mit dem im Allgemeininteresse liegenden Ziel gerechtfertigt werden kann, aufgrund dessen ihre Vorratsspeicherung den Betreibern elektronischer Kommunikationsdienste auferlegt wurde, es sei denn, dieser Zugang ist durch ein wichtigeres dem Gemeinwohl dienendes Ziel gerechtfertigt. Daraus ergibt sich insbesondere, dass ein solcher Zugang zur Bekämpfung von Straftaten im Allgemeinen keinesfalls gewährt werden kann, wenn ihre Speicherung mit dem Ziel der Bekämpfung schwerer Kriminalität oder gar des Schutzes der nationalen Sicherheit gerechtfertigt wurde (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 166).

98 Dagegen kann ein solches Ziel der Bekämpfung von Straftaten im Allgemeinen es rechtfertigen, den Zugang zu den gespeicherten Verkehrs- und Standortdaten in dem Umfang und für den Zeitraum zu gewähren, die für die Vermarktung der Dienste, die Rechnungsstellung und die Bereitstellung von Diensten mit Zusatznutzen erforderlich sind, wie es Art. 6 der Richtlinie 2002/58 gestattet (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 108 und 167).

99 Im vorliegenden Fall geht erstens aus der im Ausgangsverfahren in Rede stehenden nationalen Regelung hervor, dass die Hadopi keinen Zugang zu einem „Satz von Verkehrs- oder Standortdaten“ im Sinne der oben in Rn. 95 angeführten Rechtsprechung hat, so dass sie grundsätzlich keine genauen Schlüsse auf das Privatleben der betroffenen Personen ziehen kann. Ein Zugang, der es nicht erlaubt, solche Schlüsse zu ziehen, stellt jedoch keinen schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte dar.

100 Nach dieser Regelung und den Erläuterungen der französischen Regierung hierzu ist nämlich der Zugang, über den die Hadopi verfügt, strikt auf bestimmte Identitätsdaten des Inhabers einer IP-Adresse beschränkt und dient allein dazu, deren Inhaber identifizieren zu können, der im Verdacht steht, eine das Urheberrecht oder verwandte Schutzrechte beeinträchtigende Aktivität

entfaltet zu haben, indem er geschützte Werke rechtswidrig im Internet zum Herunterladen durch andere Personen bereitgestellt hat. Dieser Zugang zielt darauf ab, gegebenenfalls ihm gegenüber eine der im Rahmen des Verfahrens der abgestuften Reaktion vorgesehenen pädagogischen oder repressiven Maßnahmen zu erlassen, und zwar eine erste und eine zweite Empfehlung zu übersenden, gefolgt von einem Schreiben, mit dem ihm mitgeteilt wird, dass diese Aktivität eine grob fahrlässige Zuwiderhandlung darstellen könne, und schließlich von der Befassung der Staatsanwaltschaft zwecks Verfolgung dieser Übertretung oder des Delikts der Nachahmung.

101 Ferner muss die nationale Regelung klare und präzise Regeln vorsehen, mit denen sichergestellt werden kann, dass die unter Beachtung der Richtlinie 2002/58 auf Vorrat gespeicherten IP-Adressen nur zur Identifizierung der Person genutzt werden können, der eine bestimmte IP-Adresse zugewiesen wurde, während sie eine Nutzung ausschließen, die es ermöglicht, mittels einer oder mehrerer IP-Adressen die Online-Aktivität dieser Person zu überwachen. Wird eine IP-Adresse somit nur dazu genutzt, ihren Inhaber im Rahmen eines spezifischen Verwaltungsverfahrens, das zu seiner strafrechtlichen Verfolgung führen kann, zu identifizieren, und nicht zu Zwecken, die etwa darauf abzielen, seine Kontakte oder seinen Standort herauszufinden, so betrifft der allein zu diesem Zweck dienende Zugang zu der IP-Adresse diese als Identitätsdatum und nicht als Verkehrsdatum.

102 Außerdem ergibt sich aus dem oben in Rn. 97 angeführten, zur ständigen Rechtsprechung gehörenden Grundsatz, dass ein Zugang, wie er der Hadopi nach der im Ausgangsverfahren in Rede stehenden nationalen Regelung zusteht, da mit ihm das Ziel der Bekämpfung von Straftaten im Allgemeinen verfolgt wird, nur bei IP-Adressen gerechtfertigt sein kann, die von den Betreibern elektronischer Kommunikationsdienste für die Zwecke dieses Ziels und nicht für die Zwecke eines Ziels von größerer Bedeutung wie dem der Bekämpfung schwerer Kriminalität gespeichert werden müssen; dies gilt jedoch unbeschadet eines Zugangs, der durch ein solches Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt ist, wenn er IP-Adressen betrifft, die unter den Voraussetzungen von Art. 6 der Richtlinie 2002/58 auf Vorrat gespeichert werden.

103 Außerdem kann, wie sich aus den Rn. 85 bis 92 des vorliegenden Urteils ergibt, die auf einer Rechtsvorschrift im Sinne von Art. 15 Abs. 1 der Richtlinie 2002/58 beruhende Vorratsspeicherung von IP-Adressen für die Zwecke der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein, wenn die durch die betreffende gesetzliche Regelung eingeführten Modalitäten dieser Speicherung einer Reihe von Anforderungen genügen, die im Wesentlichen eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleisten sollen, so dass die Kombination von Daten verschiedener Kategorien effektiv ausgeschlossen ist. Falls den Betreibern elektronischer Kommunikationsdienste solche Modalitäten der

Vorratsspeicherung auferlegt werden, stellt eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen nämlich keinen schweren Eingriff in das Privatleben ihrer Inhaber dar, da diese Daten es nicht erlauben, genaue Schlüsse auf ihr Privatleben zu ziehen.

104 Falls eine solche gesetzliche Regelung geschaffen wird, kann daher in Anbetracht der oben in den Rn. 95 bis 97 angeführten Rechtsprechung der Zugang zu den für die Zwecke der Bekämpfung von Straftaten im Allgemeinen auf Vorrat gespeicherten IP-Adressen nach Art. 15 Abs. 1 der Richtlinie 2002/58 gerechtfertigt sein, wenn dieser Zugang allein dazu dient, die Person zu identifizieren, die im Verdacht steht, an solchen Taten beteiligt zu sein.

105 Überdies steht es im Einklang mit der Rechtsprechung des Gerichtshofs zum „Recht auf Auskunft“ im Kontext eines Verfahrens wegen Verletzung eines Rechts des geistigen Eigentums wie des in Art. 8 der Richtlinie 2004/48 vorgesehenen, wenn einer Behörde wie der Hadopi Zugang zu den einer öffentlichen IP-Adresse zuzuordnenden Identitätsdaten gewährt wird, die ihr von Einrichtungen der Rechteinhaber allein zu dem Zweck übermittelt wurde, den Inhaber dieser für Online-Aktivitäten, die Urheberrechte oder verwandte Schutzrechte verletzen können, genutzten Adresse zu identifizieren, um gegen ihn eine der im Rahmen des Verfahrens der abgestuften Reaktion vorgesehenen Maßnahmen zu verhängen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 47 ff.).

106 Im Rahmen dieser Rechtsprechung hat der Gerichtshof nämlich unter Hinweis darauf, dass die Anwendung der in der Richtlinie 2004/48 vorgesehenen Maßnahmen weder die DSGVO noch die Richtlinie 2002/58 berühren kann, entschieden, dass Art. 8 Abs. 3 der Richtlinie 2004/48 in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58 und Art. 7 Buchst. f der Richtlinie 95/46 es den Mitgliedstaaten nicht verwehrt, zur Ermöglichung der Verfolgung von Urheberrechtsverletzungen vor den Zivilgerichten die Betreiber elektronischer Kommunikationsdienste zu verpflichten, personenbezogene Daten an Privatpersonen weiterzugeben, ihnen aber auch nicht vorschreibt, eine solche Pflicht vorzusehen (vgl. in diesem Sinne Urteil vom 17. Juni 2021, M.I.C.M., C-597/19, EU:C:2021:492, Rn. 124 und 125 sowie die dort angeführte Rechtsprechung).

107 Zweitens dürfen bei der konkreten Beurteilung des Ausmaßes des mit dem Zugang einer Behörde zu personenbezogenen Daten verbundenen Eingriffs in das Privatleben allerdings die Besonderheiten des Kontexts dieses Zugangs und insbesondere die Gesamtheit der Daten und Informationen, die der Behörde nach der anwendbaren nationalen Regelung übermittelt wurden, einschließlich bereits vorhandener inhaltlich aussagekräftiger Daten und Informationen, nicht außer Acht gelassen werden (vgl. entsprechend EGMR, 24. April 2018, Benedik/Slowenien, CE:ECHR:2018:0424JUD006235714, § 109).

108 So ist im vorliegenden Fall bei dieser Beurteilung zu berücksichtigen, dass die Hadopi, bevor ihr Zugang zu den fraglichen Identitätsdaten gewährt wurde, von Einrichtungen der Rechteinhaber u. a. „Angaben zu den von den Tatbeständen betroffenen geschützten Werken oder Schutzgegenständen“ und „gegebenenfalls“ den „Namen der auf dem Rechner des Teilnehmers vorhandenen Datei“ im Sinne von Nr. 1 des Anhangs des Dekrets Nr. 2010-236 erhalten hatte.

109 Aus den dem Gerichtshof vorliegenden Akten geht – vorbehaltlich der Überprüfung durch das vorlegende Gericht – hervor, dass sich die Angaben zu dem betreffenden Werk, die in einem Protokoll enthalten sind, dessen Inhalt auf den Beratungen der CNIL vom 10. Juni 2010 beruht, im Wesentlichen auf dessen Titel und einen als „chunk“ bezeichneten Auszug beschränken, der die Form einer alphanumerischen Zeichenfolge und nicht einer Audio- oder Videoaufnahme des Werkes hat.

110 Insoweit kann zwar nicht generell ausgeschlossen werden, dass der Zugang einer Behörde zu einer begrenzten Zahl von Identitätsdaten des Inhabers einer IP-Adresse, die ihr von einem Betreiber elektronischer Kommunikationsdienste allein zu dem Zweck übermittelt wurden, den Inhaber in einem Fall zu identifizieren, in dem diese Adresse für Aktivitäten genutzt wurde, die Urheberrechte oder verwandte Schutzrechte verletzen können, sofern er mit der Analyse von – sei es auch begrenzten – Angaben zum Inhalt des rechtswidrig im Internet zur Verfügung gestellten Werkes, die ihr zuvor von Einrichtungen der Rechteinhaber übermittelt wurden, geeignet ist, die Behörde über bestimmte Aspekte des Privatlebens des Inhabers, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder sonstige Überzeugungen sowie Gesundheitszustand zu informieren, obwohl solche Daten ansonsten im Unionsrecht besonderen Schutz genießen.

111 Im vorliegenden Fall sind die der Hadopi zur Verfügung stehenden Daten und Informationen aufgrund ihrer Natur und ihres begrenzten Umfangs jedoch nur in atypischen Situationen geeignet, Informationen, unter Umständen sensibler Art, über Aspekte des Privatlebens der betreffenden Person zu offenbaren, die es dieser Behörde zusammen genommen ermöglichen könnten, genaue Schlüsse auf ihr Privatleben zu ziehen, z. B. durch die Erstellung ihres detaillierten Profils.

112 Dies könnte insbesondere bei einer Person der Fall sein, deren IP-Adresse in Peer-to-Peer-Netzen wiederholt oder in großem Umfang für Aktivitäten, die Urheberrechte oder verwandte Schutzrechte verletzen, im Zusammenhang mit geschützten Werken besonderer Arten genutzt wurde, die sich anhand von Worten ihres Titels eingruppieren lassen, durch die Informationen, unter Umständen sensibler Art, über Aspekte des Privatlebens dieser Person offenbar werden können.

113 Verschiedene Gesichtspunkte lassen allerdings den Schluss zu, dass im vorliegenden Fall der durch eine Regelung wie die im Ausgangsverfahren in Rede stehende gestattete Eingriff in das Privatleben einer Person, die im Verdacht steht, gegen Urheberrechte oder verwandte Schutzrechte verstoßende Aktivitäten ausgeübt zu haben, nicht zwangsläufig einen hohen Schweregrad aufweist. Zunächst ist nach einer solchen Regelung der Zugang der Hadopi zu den fraglichen personenbezogenen Daten einer begrenzten Zahl zugelassener und vereidigter Bediensteter dieser Behörde vorbehalten, bei der es sich im Übrigen gemäß Art. L. 331-12 CPI um eine unabhängige Behörde handelt. Sodann dient dieser Zugang allein dazu, eine Person zu identifizieren, die im Verdacht steht, gegen Urheberrechte oder verwandte Schutzrechte verstoßende Aktivitäten ausgeübt zu haben, wenn sich herausstellt, dass über ihren Internetzugang ein geschütztes Werk rechtswidrig zugänglich gemacht wurde. Schließlich ist der Zugang der Hadopi zu den fraglichen personenbezogenen Daten strikt auf die dafür erforderlichen Daten beschränkt (vgl. entsprechend EGMR, 17. Oktober 2019, López Ribalda u. a./Spanien, CE:ECHR:2019:1017JUD000187413, §§ 126 und 127).

114 Ein weiterer Gesichtspunkt, der nach den Angaben in den dem Gerichtshof vorliegenden Akten, die aber der Überprüfung durch das vorlegende Gericht bedürfen, geeignet ist, den Grad des mit dem Zugang der Hadopi verbundenen Eingriffs in die das Privatleben und personenbezogene Daten schützenden Grundrechte noch mehr zu verringern, betrifft den Umstand, dass nach der anwendbaren nationalen Regelung die Bediensteten der Hadopi, die Zugang zu den betreffenden Daten und Informationen haben, zur Wahrung der Vertraulichkeit verpflichtet sind, so dass es ihnen untersagt ist, diese Daten und Informationen in irgendeiner Form – außer zur Anrufung der Staatsanwaltschaft – offenzulegen und sie zu anderen Zwecken zu nutzen als dazu, den Inhaber einer IP-Adresse, der im Verdacht steht, gegen Urheberrechte oder verwandte Schutzrechte verstoßende Aktivitäten ausgeübt zu haben, zu identifizieren, um gegen ihn eine der im Rahmen des Verfahrens der abgestuften Reaktion vorgesehenen Maßnahmen zu verhängen (vgl. entsprechend EGMR, 17. Dezember 2009, Gardel/Frankreich, CE:ECHR:2009:1217JUD001642805, § 70).

115 Sofern eine nationale Regelung die oben in Rn. 101 genannten Voraussetzungen erfüllt, ermöglichen die einer Behörde wie der Hadopi übermittelten IP-Adressen somit keine Nachverfolgung der von ihrem Inhaber besuchten Internetseiten; dies spricht dafür, dass der mit dem Zugang dieser Behörde zu den im Ausgangsverfahren in Rede stehenden Identifizierungsdaten verbundene Eingriff nicht als schwerwiegend eingestuft werden kann.

116 Drittens ist darauf hinzuweisen, dass für die Zwecke des aufgrund des Erfordernisses der Verhältnismäßigkeit in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vorzunehmenden Ausgleichs der in Rede stehenden Rechte und Interessen, auch wenn die Freiheit der Meinungsäußerung und die

Vertraulichkeit personenbezogener Daten vorrangige Anliegen sind und die Nutzer von Telekommunikations- und Internetdiensten die Garantie haben müssen, dass ihre Intimität und ihr Recht auf freie Meinungsäußerung gewahrt werden, diese Grundrechte nicht absolut sind. Im Rahmen einer Abwägung der in Rede stehenden Rechte und Interessen müssen sie nämlich bisweilen hinter anderen Grundrechten und Erfordernissen des Allgemeininteresses wie der Verteidigung der öffentlichen Ordnung und der Verhütung von Straftaten oder dem Schutz der Rechte und Freiheiten anderer zurücktreten. Dies ist insbesondere dann der Fall, wenn die diesen vorrangigen Anliegen beigemessene Priorität geeignet ist, die Wirksamkeit strafrechtlicher Ermittlungen zu beeinträchtigen, etwa indem die tatsächliche Identifizierung eines Straftäters und die Verhängung einer Sanktion gegen ihn unmöglich gemacht oder übermäßig erschwert werden (vgl. entsprechend EGMR, 2. März 2009, K. U./Finnland, CE:ECHR:2008:1202JUD000287202, § 49).

117 In diesem Kontext ist, wie der Gerichtshof bereits entschieden hat, gebührend zu berücksichtigen, dass bei online begangenen Straftaten der Zugang zu IP-Adressen die einzige Ermittlungsmaßnahme darstellen kann, die eine effektive Identifizierung der Person ermöglicht, der diese Adresse zugewiesen war, als die Tat begangen wurde (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 154).

118 Dieser Umstand spricht, wie auch der Generalanwalt in Nr. 59 seiner Schlussanträge vom 28. September 2023 im Wesentlichen ausgeführt hat, dafür, dass die Vorratsspeicherung dieser Adressen und der Zugang zu ihnen zur Bekämpfung von Straftaten wie online begangenen Verletzungen von Urheberrechten oder verwandten Schutzrechten zur Erreichung des verfolgten Ziels zwingend erforderlich sind und daher dem durch Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht ihres elften Erwägungsgrundes und von Art. 52 Abs. 2 der Charta vorgeschriebenen Erfordernis der Verhältnismäßigkeit entsprechen.

119 Würde ein solcher Zugang nicht gestattet, bestünde im Übrigen, wie der Generalanwalt im Wesentlichen in den Nrn. 78 bis 80 seiner Schlussanträge vom 27. Oktober 2022 sowie in den Nrn. 80 und 81 seiner Schlussanträge vom 28. September 2023 hervorgehoben hat, eine echte Gefahr der systemischen Straflosigkeit nicht nur von Straftaten in Form der Verletzung der Urheberrechte oder verwandter Schutzrechte, sondern auch von anderen Arten von Straftaten, die online begangen werden oder deren Begehung oder Vorbereitung durch die Merkmale des Internets erleichtert wird. Das Bestehen einer solchen Gefahr ist ein relevanter Umstand, wenn im Rahmen einer Abwägung der verschiedenen betroffenen Rechte und Interessen beurteilt wird, ob ein Eingriff in die Rechte, die durch die Art. 7, 8 und 11 der Charta garantiert werden, eine gemessen am Ziel der Bekämpfung von Straftaten verhältnismäßige Maßnahme ist.

120 Zwar ist der Zugang einer Behörde wie der Hadopi zu Identitätsdaten, die der IP-Adresse zuzuordnen sind, von der aus die Straftat online begangen wurde, nicht zwangsläufig die einzige mögliche Maßnahme zur Identifizierung der Person, der diese Adresse zum Zeitpunkt der Begehung der Straftat zugewiesen war. Sie könnte nämlich *a priori* auch dadurch identifiziert werden, dass alle Online-Aktivitäten der betreffenden Person geprüft werden, insbesondere indem etwaige von ihr in den sozialen Netzwerken hinterlassene „Spuren“ wie die in diesen Netzwerken benutzte Kennung oder ihre Kontaktdaten analysiert werden.

121 Wie der Generalanwalt in Nr. 83 seiner Schlussanträge vom 28. September 2023 ausgeführt hat, wäre eine solche Ermittlungsmaßnahme jedoch besonders einschneidend, da sie genaue Informationen über das Privatleben der Betroffenen offenbaren könnte. Sie würde somit für diese Personen einen schwereren Eingriff in ihre durch die Art. 7, 8 und 11 der Charta garantierten Rechte bedeuten als den, der mit einer Regelung wie der im Ausgangsverfahren in Rede stehenden verbunden ist.

122 Aus dem Vorstehenden ergibt sich, dass 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 grundsätzlich einer nationalen Regelung nicht entgegensteht, mit der einer mit dem Schutz von Urheberrechten und verwandten Schutzrechten vor online begangenen Verletzungen dieser Rechte betrauten Behörde Zugang zu Identitätsdaten, die IP-Adressen zuzuordnen sind, die zuvor von Einrichtungen der Rechteinhaber gesammelt und von den Betreibern elektronischer Kommunikationsdienste wirksam strikt getrennt auf Vorrat gespeichert wurden, allein deshalb gewährt wird, damit die Behörde die Inhaber dieser Adressen identifizieren kann, die im Verdacht stehen, für die begangenen Verletzungen verantwortlich zu sein, und gegebenenfalls Maßnahmen gegen sie ergreifen kann. In einem solchen Fall muss die anwendbare nationale Regelung es den Bediensteten, die über einen solchen Zugang verfügen, untersagen, 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, zweitens die von diesen Personen besuchten Internetseiten nachzuverfolgen und drittens die IP-Adressen zu anderen Zwecken als dem des Erlasses solcher Maßnahmen zu nutzen.

Zum Erfordernis einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vor dem Zugang einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind

123 Es stellt sich jedoch die Frage, ob der Zugang der Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind, zudem von einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht werden muss.

124 Um in der Praxis die vollständige Einhaltung der Voraussetzungen zu gewährleisten, die die Mitgliedstaaten vorsehen müssen, um sicherzustellen, dass der Zugang auf das absolut Notwendige beschränkt wird, hat der Gerichtshof es für „unabdingbar“ erachtet, dass der Zugang der zuständigen nationalen Behörden zu Verkehrs- und Standortdaten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 120, vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 189, vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 51, und vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 106).

125 Diese vorherige Kontrolle setzt erstens voraus, dass das mit ihr betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle über alle Befugnisse verfügt und alle Garantien aufweist, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden berechtigten Interessen und Rechte in Einklang gebracht werden. Speziell im Fall strafrechtlicher Ermittlungen verlangt eine solche Kontrolle, dass das Gericht oder die Stelle in der Lage ist, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 107 und die dort angeführte Rechtsprechung).

126 Zweitens muss, wenn die Kontrolle nicht von einem Gericht, sondern von einer unabhängigen Verwaltungsstelle wahrgenommen wird, diese über eine Stellung verfügen, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorzugehen, ohne jede Einflussnahme von außen. Das Erfordernis, wonach die mit der Wahrnehmung der vorherigen Kontrolle betraute Stelle unabhängig sein muss, gebietet somit, dass es sich bei ihr um eine andere Stelle als die den Zugang zu den Daten begehrende Behörde handelt, damit diese Stelle in der Lage ist, ihre Kontrolle objektiv und unparteiisch, geschützt vor jeder Einflussnahme von außen, auszuüben. Im strafrechtlichen Bereich impliziert das Erfordernis der Unabhängigkeit insbesondere, dass die mit der vorherigen Kontrolle betraute Behörde zum einen nicht an der Durchführung des fraglichen Ermittlungsverfahrens beteiligt ist und zum anderen eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren hat (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 108 und die dort angeführte Rechtsprechung).

127 Drittens muss die nach Art. 15 Abs. 1 der Richtlinie 2002/58 erforderliche unabhängige Kontrolle vor jedem Zugang zu den betreffenden Daten erfolgen, außer in hinreichend begründeten Eilfällen, in denen die Kontrolle kurzfristig erfolgen muss. Eine spätere Kontrolle würde es nämlich nicht ermöglichen, dem Ziel der vorherigen Kontrolle zu entsprechen, das darin besteht, zu verhindern, dass ein über das absolut Notwendige hinausgehender Zugang zu den fraglichen Daten gewährt wird (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 110).

128 Der Gerichtshof hat es zwar, wie sich aus der oben in Rn. 124 angeführten Rechtsprechung ergibt, für „unabdingbar“ erachtet, dass der Zugang der zuständigen nationalen Behörden zu Verkehrs- und Standortdaten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird, doch ist diese Rechtsprechung im Kontext nationaler Maßnahmen entwickelt worden, die für die Zwecke eines mit der Bekämpfung schwerer Kriminalität zusammenhängenden Ziels einen allgemeinen Zugang zu allen gespeicherten Verkehrs- und Standortdaten ermöglichten, unabhängig von jedem – sei es auch nur mittelbaren – Zusammenhang mit dem verfolgten Ziel, und die somit schwere oder „besonders schwere“ Eingriffe in die betreffenden Grundrechte umfassten.

129 Als es um die Voraussetzungen für die mögliche Rechtfertigung eines Zugangs zu Identitätsdaten nach Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta ging, hat der Gerichtshof das Erfordernis einer solchen vorherigen Kontrolle hingegen nicht ausdrücklich erwähnt (vgl. in diesem Sinne Urteile vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 59, 60 und 62, vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 157 und 158, sowie vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 34).

130 Aus der Rechtsprechung des Gerichtshofs zu dem nach Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 zu beachtenden Grundsatz der Verhältnismäßigkeit und insbesondere aus der Rechtsprechung, wonach die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der u. a. in den Art. 5, 6 und 9 dieser Richtlinie vorgesehenen Rechte und Pflichten zu rechtfertigen, in der Weise zu beurteilen ist, dass die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs in die in den Art. 7, 8 und 11 der Charta verankerten Grundrechte bestimmt und geprüft wird, ob die mit dieser Beschränkung verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht (Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 131), ergibt sich, dass der Umfang des Eingriffs in die betreffenden Grundrechte, den der Zugang zu den fraglichen personenbezogenen Daten mit sich bringt, und der Grad der Sensibilität dieser Daten auch Einfluss auf die materiellen und

prozeduralen Garantien haben müssen, die dieser Zugang voraussetzt und zu denen das Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle gehört.

131 Daher ist in Anbetracht des Grundsatzes der Verhältnismäßigkeit davon auszugehen, dass eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle geboten ist, wenn im Kontext einer nationalen Regelung, die den Zugang einer Behörde zu personenbezogenen Daten vorsieht, dieser Zugang die Gefahr eines schweren Eingriffs in die Grundrechte des Betroffenen in dem Sinne birgt, dass er es der Behörde ermöglichen könnte, genaue Schlüsse auf sein Privatleben zu ziehen und gegebenenfalls sein detailliertes Profil zu erstellen.

132 Umgekehrt besteht dieses Erfordernis einer vorherigen Kontrolle nicht, wenn der mit dem Zugang einer Behörde zu personenbezogenen Daten verbundene Eingriff in die betreffenden Grundrechte nicht als schwerwiegend eingestuft werden kann.

133 Dies ist der Fall, wenn der Zugang zu Identitätsdaten der Nutzer elektronischer Kommunikationsmittel allein zur Ermittlung des betreffenden Nutzers dient, ohne dass diese Daten mit Informationen über die erfolgte Kommunikation in Verbindung gebracht werden können, da nach der Rechtsprechung des Gerichtshofs der mit einer solchen Verarbeitung dieser Daten verbundene Eingriff grundsätzlich nicht als schwerwiegend eingestuft werden kann (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 157 und 158).

134 Wird eine Vorratsspeicherung wie die oben in den Rn. 86 bis 89 beschriebene eingeführt, hängt folglich der Zugang der Behörde zu den Identitätsdaten, die den dabei gespeicherten IP-Adressen zuzuordnen sind, im Prinzip nicht vom Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle ab.

135 Allerdings kann, wie bereits oben in den Rn. 110 und 111 ausgeführt, nicht ausgeschlossen werden, dass in atypischen Situationen die Daten und begrenzten Informationen, die einer Behörde im Rahmen eines Verfahrens wie des im Ausgangsverfahren in Rede stehenden Verfahrens der abgestuften Reaktion zur Verfügung gestellt werden, Informationen, unter Umständen sensibler Art, über Aspekte des Privatlebens der betreffenden Person offenbaren können, die es dieser Behörde zusammen genommen ermöglichen könnten, genaue Schlüsse auf ihr Privatleben zu ziehen und gegebenenfalls ihr detailliertes Profil zu erstellen.

136 Wie sich aus Rn. 112 des vorliegenden Urteils ergibt, kann eine solche Gefahr für das Privatleben insbesondere dann eintreten, wenn eine Person in Peer-to-Peer-Netzen wiederholt oder in großem Umfang Aktivitäten, die Urheberrechte

oder verwandte Schutzrechte verletzen, im Zusammenhang mit geschützten Werken besonderer Arten entfaltet, die sich anhand von Worten ihres Titels eingruppieren lassen, durch die Informationen, unter Umständen sensibler Art, über Aspekte des Privatlebens dieser Person offenbar werden können.

137 So kann im vorliegenden Fall im Rahmen des Verwaltungsverfahrens der abgestuften Reaktion ein Inhaber einer IP-Adresse in besonderem Maß einer solchen Gefahr für sein Privatleben ausgesetzt sein, wenn dieses Verfahren das Stadium erreicht, in dem die Hadopi darüber zu entscheiden hat, ob sie die Staatsanwaltschaft mit Handlungen befasst, die als grob fahrlässige Übertretung oder als Delikt der Nachahmung eingestuft werden können.

138 Ihre Befassung setzt nämlich voraus, dass an den Inhaber einer IP-Adresse bereits zwei Empfehlungen und ein Notifizierungsschreiben mit der Mitteilung gerichtet worden waren, dass seine Aktivitäten strafrechtlich verfolgt werden können; diese Maßnahmen implizieren, dass die Hadopi jeweils Zugang zu den Identitätsdaten des Inhabers der für Aktivitäten, die gegen Urheberrechte oder verwandte Schutzrechte verstießen, genutzten IP-Adresse sowie zu einer Datei über das betreffende Werk hatte, die im Wesentlichen dessen Titel enthielt.

139 Es kann aber nicht ausgeschlossen werden, dass die damit während der verschiedenen Phasen des Verwaltungsverfahrens der abgestuften Reaktion nach und nach gelieferten Daten zusammen genommen übereinstimmende und unter Umständen sensible Informationen über Aspekte des Privatlebens des Betroffenen offenbaren könnten, die es gegebenenfalls ermöglichen, sein Profil zu erstellen.

140 Somit kann die Intensität der Beeinträchtigung des Rechts auf Achtung des Privatlebens allmählich zunehmen, während das Verfahren der abgestuften Reaktion, das als sequenzieller Prozess abläuft, die verschiedenen Stufen durchläuft, aus denen es besteht.

141 Im vorliegenden Fall kann der Zugang der Hadopi zu allen im Lauf der verschiedenen Stufen dieses Verfahrens zusammengetragenen Daten über die betreffende Person es durch die Verknüpfung dieser Daten ermöglichen, genaue Schlüsse auf ihr Privatleben zu ziehen. Deshalb muss die nationale Regelung im Rahmen eines Verfahrens wie des Verfahrens der abgestuften Reaktion, um das es im Ausgangsverfahren geht, in einem bestimmten Stadium dieses Verfahrens auch eine den oben in den Rn. 125 bis 127 genannten Voraussetzungen genügende vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle vorsehen, um die Gefahr unverhältnismäßiger Eingriffe in die das Privatleben und die personenbezogenen Daten des Betroffenen schützenden Grundrechte auszuschließen. Dies bedeutet, dass in der Praxis eine solche Kontrolle erfolgen muss, bevor die Hadopi die ihr von einem Betreiber elektronischer Kommunikationsdienste zur Verfügung gestellten, einer IP-Adresse zuzuordnenden Identitätsdaten einer Person, die

bereits Gegenstand von zwei Empfehlungen war, mit der Datei über das Werk verknüpfen kann, das im Internet für andere Personen zum Herunterladen bereitgestellt wurde. Somit muss diese Kontrolle vor der etwaigen Versendung des in Art. R. 331-40 CPI erwähnten Notifizierungsschreibens erfolgen, mit dem festgestellt wird, dass diese Person Handlungen vorgenommen hat, die einen grob fahrlässigen Verstoß darstellen können. Erst im Anschluss an eine solche vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle und die von ihm oder ihr erteilte Zustimmung darf die Hadopi ein solches Schreiben versenden und anschließend gegebenenfalls die Staatsanwaltschaft befassen, damit sie diese Tat verfolgt.

142 Der Hadopi sollte gestattet werden, die Fälle zu identifizieren, in denen der Inhaber der betreffenden IP-Adresse diese dritte Stufe eines solchen Verfahrens der abgestuften Reaktion erreicht. Daher muss das Verfahren so organisiert und strukturiert sein, dass die bei den Betreibern elektronischer Kommunikationsdienste erhobenen Identitätsdaten einer Person, der die zuvor im Internet gesammelten IP-Adressen zuzuordnen sind, von den bei der Hadopi für die Prüfung des Sachverhalts zuständigen Personen nicht automatisch mit Dateien verknüpft werden können, die Elemente enthalten, denen sich die Titel der geschützten Werke entnehmen lassen, deren Bereitstellung im Internet die Sammlung der IP-Adressen gerechtfertigt hat.

143 Somit muss diese Verknüpfung für die Zwecke der dritten Stufe der abgestuften Reaktion ausgesetzt werden, wenn die Erhebung der genannten Identitätsdaten in einem Fall der möglichen zweiten Wiederholung einer gegen Urheberrechte oder verwandte Schutzrechte verstoßenden Aktivität das oben in Rn. 141 beschriebene Erfordernis einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle auslöst.

144 Überdies kann dadurch, dass sich das oben in den Rn. 141 bis 143 dargelegte Erfordernis der vorherigen Kontrolle auf die dritte Stufe des Verfahrens der abgestuften Reaktion beschränkt und nicht für dessen frühere Stufen gilt, auch dem Argument Rechnung getragen werden, dass die Praktikabilität dieses Verfahrens gewahrt bleiben muss, das vor allem in seinen Stufen vor der etwaigen Versendung des Notifizierungsschreibens und gegebenenfalls einer Befassung der Staatsanwaltschaft durch eine Vielzahl von Zugangsanträgen der Behörde gekennzeichnet ist, die sich aus der ebenso großen Zahl der ihr von den Einrichtungen der Rechteinhaber übermittelten Protokollen ergibt.

145 Zum Gegenstand der oben in den Rn. 141 bis 143 behandelten vorherigen Kontrolle ergibt sich ferner aus der oben in den Rn. 95 und 96 angeführten Rechtsprechung, dass in Fällen, in denen die betreffende Person im Verdacht steht, bei allgemeinen Straftaten „grob fahrlässig“ im Sinne von Art. R. 335-5 CPI gehandelt zu haben, das mit dieser Kontrolle betraute Gericht oder die mit ihr betraute unabhängige Verwaltungsstelle den Zugang verweigern muss,

wenn er es der Behörde, die ihn beantragt hat, erlauben würde, genaue Schlüsse auf das Privatleben der betreffenden Person zu ziehen.

146 Dagegen sollte in Fällen, in denen die dem Gericht oder der unabhängigen Verwaltungsstelle zur Kenntnis gebrachten Anhaltspunkte den Verdacht begründen, dass die betreffende Person das Delikt der Nachahmung im Sinne von Art. L. 335-2 CPI oder Art. L. 335-4 CPI begangen hat, auch dann ein Zugang gewährt werden, wenn er es erlaubt, solche genauen Schlüsse zu ziehen, da es einem Mitgliedstaat freisteht, in einem derartigen Delikt die Beeinträchtigung eines Grundinteresses der Gesellschaft zu sehen und es der schweren Kriminalität zuzurechnen.

147 Was schließlich die Modalitäten dieser vorherigen Kontrolle angeht, ist die französische Regierung der Ansicht, dass es angesichts der besonderen Merkmale des Zugangs der Hadopi zu den fraglichen Daten, insbesondere ihres großen Umfangs, angebracht wäre, wenn eine etwa erforderliche vorherige Kontrolle vollständig automatisiert würde. Mit einer solchen Kontrolle, die rein objektiven Charakter habe, solle nämlich im Wesentlichen überprüft werden, ob das Protokoll, mit dem die Hadopi befasst werde, alle nötigen Informationen und Daten enthalte, ohne dass die Hadopi diese zu würdigen habe.

148 Eine vorherige Kontrolle kann jedoch in keinem Fall vollständig automatisiert sein, da eine solche Kontrolle, wie aus der oben in Rn. 125 angeführten Rechtsprechung hervorgeht, bei strafrechtlichen Ermittlungen jedenfalls verlangt, dass das betreffende Gericht oder die betreffende unabhängige Verwaltungsstelle in der Lage ist, für einen gerechten Ausgleich zwischen den berechtigten Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen.

149 Eine solche Abwägung der verschiedenen berechtigten Interessen und der betreffenden Rechte erfordert nämlich das Tätigwerden einer natürlichen Person, das umso notwendiger ist, als der automatisierte Ablauf und der große Umfang der in Rede stehenden Datenverarbeitung Gefahren für das Privatleben mit sich bringen.

150 Außerdem vermag eine vollständig automatisierte Kontrolle grundsätzlich nicht sicherzustellen, dass der Zugang nicht über das absolut Notwendige hinausgeht und dass die Personen, deren personenbezogene Daten betroffen sind, über wirksame Garantien vor Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügen.

151 Daher können automatisierte Kontrollen es zwar ermöglichen, bestimmte in den Protokollen der Einrichtungen der Rechteinhaber enthaltene Informationen

zu überprüfen, doch müssen mit ihnen jedenfalls Kontrollen durch natürliche Personen einhergehen, die in vollem Umfang den oben in den Rn. 125 bis 127 aufgeführten Anforderungen genügen.

Zu den Anforderungen an den Zugang einer Behörde zu Identitätsdaten, die einer IP-Adresse zuzuordnen sind, hinsichtlich der materiellen und prozeduralen Voraussetzungen sowie der Garantien in Bezug auf Missbrauchsgefahren, jeden unberechtigten Zugang zu diesen Daten und jede unberechtigte Nutzung

152 Aus der Rechtsprechung des Gerichtshofs ergibt sich, dass der Zugang zu personenbezogenen Daten nur dann mit dem in Art. 15 Abs. 1 der Richtlinie 2002/58 aufgestellten Erfordernis der Verhältnismäßigkeit vereinbar sein kann, wenn die Rechtsvorschriften, die ihn gestatten, klare und präzise Regeln enthalten, die vorsehen, dass die für den Zugang geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung verfügen (vgl. in diesem Sinne Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 132 und 173, sowie vom 2. März 2021, Prokuratuur [Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 49 und die dort angeführte Rechtsprechung).

153 Wie der Gerichtshof hervorgehoben hat, ist das Erfordernis, über solche Garantien zu verfügen, umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden (Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 176 und die dort angeführte Rechtsprechung).

154 Insoweit hat die französische Regierung in Beantwortung einer vom Gerichtshof im Hinblick auf die mündliche Verhandlung am 5. Juli 2022 gestellten Frage bestätigt, dass der Zugang der Hadopi zu den Identitätsdaten im Rahmen des Verfahrens der abgestuften Reaktion, wie im Übrigen Art. L. 331-29 CPI zu entnehmen ist, auf einer im Wesentlichen automatisierten Datenverarbeitung beruht, die mit der Vielzahl der von den Einrichtungen der Rechteinhaber in den Peer-to-Peer-Netzen festgestellten und der Hadopi in Form von Protokollen übermittelten Nachahmungen zu erklären ist.

155 Aus den dem Gerichtshof vorliegenden Akten geht insbesondere hervor, dass die Bediensteten der Hadopi bei dieser Datenverarbeitung im Wesentlichen automatisiert und ohne Würdigung der betreffenden Tatsachen als solche prüfen, ob die Protokolle, mit denen sie befasst wird, alle in Nr. 1 des Anhangs des Dekrets Nr. 2010-236 genannten Informationen und Daten enthalten, insbesondere zu den betreffenden rechtswidrigen Bereitstellungen im Internet

und den dabei genutzten IP-Adressen. Solche Verarbeitungen müssen aber mit Kontrollen durch natürliche Personen einhergehen.

156 Da eine solche automatisierte Verarbeitung eine Reihe falsch positiver Ergebnisse mit sich bringen kann sowie vor allem die Gefahr, dass eine potenziell sehr große Zahl personenbezogener Daten von Dritten zu missbräuchlichen oder unrechtmäßigen Zwecken missbraucht wird, ist es wichtig, dass das von einer Behörde verwendete Datenverarbeitungssystem aufgrund einer Rechtsvorschrift regelmäßig von einer unabhängigen Stelle überwacht wird, bei der es sich im Verhältnis zu dieser Behörde um einen Dritten handelt. Bei der Überwachung sind die Integrität des Systems, einschließlich der vom System zu gewährleistenden wirksamen Garantien in Bezug auf Missbrauchsgefahren, jeden unberechtigten Zugang zu diesen Daten und jede unberechtigte Nutzung, sowie seine Wirksamkeit und Zuverlässigkeit bei der Aufdeckung von Verstößen zu prüfen, die im Wiederholungsfall als grobe Fahrlässigkeit oder als Nachahmung eingestuft werden können.

157 Schließlich ist hinzuzufügen, dass bei einer Verarbeitung personenbezogener Daten durch eine Behörde, wie sie die Hadopi im Rahmen des Verfahrens der abgestuften Reaktion vornimmt, die besonderen Datenschutzvorschriften der Richtlinie 2016/680 eingehalten werden müssen, die nach ihrem Art. 1 Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, enthält.

158 Im vorliegenden Fall ist die Hadopi, auch wenn sie nach dem anwendbaren nationalen Recht nicht über eigene Entscheidungsbefugnisse verfügt, bei der Verarbeitung personenbezogener Daten im Rahmen des Verfahrens der abgestuften Reaktion und beim Erlass von Maßnahmen wie einer Empfehlung oder der Unterrichtung des Betroffenen darüber, dass die in Rede stehenden Tatbestände strafrechtlich verfolgt werden können, als eine an der Verhütung und Ermittlung von Straftaten in Form grob fahrlässig begangener Übertretungen oder des Delikts der Nachahmung beteiligte „Behörde“ im Sinne von Art. 3 der Richtlinie 2016/680 einzustufen und fällt daher in ihren in Art. 1 festgelegten Anwendungsbereich.

159 Hierzu hat die französische Regierung in Beantwortung einer vom Gerichtshof im Hinblick auf die mündliche Verhandlung am 5. Juli 2022 gestellten Frage ausgeführt, dass die von der Hadopi im Rahmen der Umsetzung des Verfahrens der abgestuften Reaktion getroffenen Maßnahmen „einen unmittelbar mit dem Gerichtsverfahren verbundenen vorstrafrechtlichen Charakter“ hätten, so dass das von der Hadopi geschaffene System zur Verwaltung von Maßnahmen zum Schutz von Werken im Internet, wie sich aus der Rechtsprechung des

vorlegenden Gerichts ergebe, den zur Umsetzung der Richtlinie 2016/680 dienenden Bestimmungen des nationalen Rechts unterliege.

160 Dagegen fällt eine solche Datenverarbeitung durch die Hadopi nicht in den Anwendungsbereich der DSGVO. Sie findet nach ihrem Art. 2 Abs. 2 Buchst. d nämlich keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

161 Wie der Generalanwalt in Nr. 104 seiner Schlussanträge vom 27. Oktober 2022 ausgeführt hat, ist die Richtlinie 2016/680 somit von der Hadopi im Rahmen des Verfahrens der abgestuften Reaktion zu beachten, so dass die an einem solchen Verfahren beteiligten Personen in den Genuss einer Reihe materieller und prozeduraler Garantien kommen müssen, zu denen ein Zugangs-, Berichtigungs- und Löschungsrecht in Bezug auf die von der Hadopi verarbeiteten personenbezogenen Daten gehört sowie die Möglichkeit, eine Beschwerde bei einer unabhängigen Aufsichtsbehörde einzulegen, an die sich gegebenenfalls ein unter den Bedingungen des allgemeinen Rechts in Anspruch zu nehmender gerichtlicher Rechtsbehelf anschließt.

162 In diesem Kontext geht aus den im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften hervor, dass im Rahmen des Verfahrens der abgestuften Reaktion, genauer gesagt bei der Absendung der zweiten Empfehlung und der anschließenden Notifizierung einer möglichen Einstufung der festgestellten Tatbestände als Straftat, der Empfänger dieser Mitteilungen über bestimmte prozedurale Garantien verfügt, wie das Recht, Erklärungen abzugeben, das Recht, nähere Angaben zu dem ihm zur Last gelegten Verstoß zu erhalten, sowie hinsichtlich der Notifizierung das Recht, eine Anhörung zu beantragen und sich von einem Beistand unterstützen zu lassen.

163 Jedenfalls ist es Sache des vorlegenden Gerichts, zu prüfen, ob diese nationalen Rechtsvorschriften alle durch die Richtlinie 2016/680 vorgeschriebenen materiellen und prozeduralen Garantien vorsehen.

164 Nach alledem ist auf die drei Vorlagefragen zu antworten, dass 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 nicht entgegensteht, die der mit dem Schutz von Urheberrechten und verwandten Schutzrechten vor Verletzungen dieser Rechte im Internet betrauten Behörde den Zugang zu den von den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste auf Vorrat gespeicherten Identitätsdaten, die IP-Adressen zuzuordnen sind, die zuvor von Einrichtungen der Rechteinhaber gesammelt wurden, gestattet, damit die Behörde die Inhaber dieser für Aktivitäten, die solche Rechtsverletzungen darstellen können, genutzten

Adressen identifizieren und gegebenenfalls Maßnahmen gegen sie ergreifen kann, unter der Voraussetzung, dass nach dieser Regelung

– diese Daten zu Bedingungen und unter technischen Modalitäten gespeichert werden, die gewährleisten, dass es ausgeschlossen ist, dass aus der Vorratsspeicherung genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen, z. B. durch Erstellung ihres detaillierten Profils, gezogen werden können, was insbesondere dadurch erreicht werden kann, dass den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur Vorratsspeicherung der verschiedenen Kategorien personenbezogener Daten wie Identitätsdaten, IP-Adressen sowie Verkehrs- und Standortdaten auferlegt wird, die eine wirksame strikte Trennung dieser verschiedenen Datenkategorien gewährleistet, mit der im Stadium der Speicherung jede kombinierte Nutzung dieser verschiedenen Datenkategorien verhindert wird, und die Dauer der Speicherung das absolut notwendige Maß nicht überschreitet;

– der Zugang dieser Behörde zu solchen wirksam strikt getrennt auf Vorrat gespeicherten Daten ausschließlich dazu dient, die Person zu identifizieren, die im Verdacht steht, eine Straftat begangen zu haben, und dieser Zugang mit den erforderlichen Garantien versehen ist, um auszuschließen, dass er, abgesehen von atypischen Situationen, genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen ermöglichen kann, z. B. durch die Erstellung ihres detaillierten Profils, was insbesondere impliziert, dass es den Bediensteten dieser Behörde, denen ein solcher Zugang gestattet worden ist, untersagt ist, Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zum alleinigen Zweck der Befassung der Staatsanwaltschaft, in welcher Form auch immer offenzulegen, die von diesen Personen besuchten Internetseiten nachzuverfolgen und allgemeiner die IP-Adressen zu anderen Zwecken als dem der Identifizierung ihrer Inhaber im Hinblick auf den Erlass etwaiger gegen sie gerichteter Maßnahmen zu nutzen;

– die Möglichkeit für die bei der betreffenden Behörde mit der Prüfung des Sachverhalts betrauten Personen, solche Daten mit Dateien zu verknüpfen, die Elemente enthalten, denen sich der Titel geschützter Werke entnehmen lässt, deren Bereitstellung im Internet die Sammlung der IP-Adressen durch Einrichtungen der Rechteinhaber gerechtfertigt hat, in Fällen der erneuten Entfaltung einer Aktivität, mit der dieselbe Person Urheberrechte oder verwandte Schutzrechte verletzt, von einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht wird, wobei die Kontrolle nicht vollständig automatisiert sein darf und vor einer solchen Verknüpfung erfolgen muss, da diese es in derartigen Fällen ermöglichen kann, genaue Schlüsse auf das Privatleben der Person zu

ziehen, deren IP-Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen;

– das von der Behörde verwendete Datenverarbeitungssystem in regelmäßigen Abständen einer zur Überprüfung der Integrität des Systems, einschließlich wirksamer Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung, sowie seiner Wirksamkeit und Zuverlässigkeit bei der Aufdeckung etwaiger Verstöße dienenden Kontrolle durch eine unabhängige Stelle unterliegt, bei der es sich im Verhältnis zu dieser Behörde um einen Dritten handelt.

Kosten

165 Für die Beteiligten des Ausgangsverfahrens ist das Verfahren Teil des beim vorlegenden Gericht anhängigen Verfahrens; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Plenum) für Recht erkannt:

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) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union

dahin auszulegen, dass

er einer nationalen Regelung nicht entgegensteht, die der mit dem Schutz von Urheberrechten und verwandten Schutzrechten vor Verletzungen dieser Rechte im Internet betrauten Behörde den Zugang zu den von den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste auf Vorrat gespeicherten Identitätsdaten, die IP-Adressen zuzuordnen sind, die zuvor von Einrichtungen der Rechteinhaber gesammelt wurden, gestattet, damit die Behörde die Inhaber dieser für Aktivitäten, die solche Rechtsverletzungen darstellen können, genutzten Adressen identifizieren und gegebenenfalls Maßnahmen gegen sie ergreifen kann, unter der Voraussetzung, dass nach dieser Regelung

– **diese Daten zu Bedingungen und unter technischen Modalitäten gespeichert werden, die gewährleisten, dass es ausgeschlossen ist, dass**

aus der Vorratsspeicherung genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen, z. B. durch Erstellung ihres detaillierten Profils, gezogen werden können, was insbesondere dadurch erreicht werden kann, dass den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur Vorratsspeicherung der verschiedenen Kategorien personenbezogener Daten wie Identitätsdaten, IP-Adressen sowie Verkehrs- und Standortdaten auferlegt wird, die eine wirksame strikte Trennung dieser verschiedenen Datenkategorien gewährleistet, mit der im Stadium der Speicherung jede kombinierte Nutzung dieser verschiedenen Datenkategorien verhindert wird, und die Dauer der Speicherung das absolut notwendige Maß nicht überschreitet;

– **der Zugang dieser Behörde zu solchen wirksam strikt getrennt auf Vorrat gespeicherten Daten ausschließlich dazu dient, die Person zu identifizieren, die im Verdacht steht, eine Straftat begangen zu haben, und dieser Zugang mit den erforderlichen Garantien versehen ist, um auszuschließen, dass er, abgesehen von atypischen Situationen, genaue Schlüsse auf das Privatleben der Inhaber der IP-Adressen ermöglichen kann, z. B. durch die Erstellung ihres detaillierten Profils, was insbesondere impliziert, dass es den Bediensteten dieser Behörde, denen ein solcher Zugang gestattet worden ist, untersagt ist, Informationen über den Inhalt der von den Inhabern der IP-Adressen konsultierten Dateien, außer zum alleinigen Zweck der Befassung der Staatsanwaltschaft, in welcher Form auch immer offenzulegen, die von diesen Personen besuchten Internetseiten nachzuverfolgen und allgemeiner die IP-Adressen zu anderen Zwecken als dem der Identifizierung ihrer Inhaber im Hinblick auf den Erlass etwaiger gegen sie gerichteter Maßnahmen zu nutzen;**

– **die Möglichkeit für die bei der betreffenden Behörde mit der Prüfung des Sachverhalts betrauten Personen, solche Daten mit Dateien zu verknüpfen, die Elemente enthalten, denen sich der Titel geschützter Werke entnehmen lässt, deren Bereitstellung im Internet die Sammlung der IP-Adressen durch Einrichtungen der Rechteinhaber gerechtfertigt hat, in Fällen der erneuten Entfaltung einer Aktivität, mit der dieselbe Person Urheberrechte oder verwandte Schutzrechte verletzt, von einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle abhängig gemacht wird, wobei die Kontrolle nicht vollständig automatisiert sein darf und vor einer solchen Verknüpfung erfolgen muss, da diese es in derartigen Fällen ermöglichen kann, genaue Schlüsse auf das Privatleben der Person zu ziehen, deren IP-Adresse für Aktivitäten genutzt wurde, die möglicherweise Urheberrechte oder verwandte Schutzrechte verletzen;**

– **das von der Behörde verwendete Datenverarbeitungssystem in regelmäßigen Abständen einer zur Überprüfung der Integrität des Systems, einschließlich wirksamer Garantien zum Schutz vor den Gefahren eines missbräuchlichen oder unberechtigten Zugangs zu den Daten und ihrer missbräuchlichen oder unberechtigten Nutzung, sowie seiner Wirksamkeit und Zuverlässigkeit bei der Aufdeckung etwaiger Verstöße dienenden Kontrolle durch eine unabhängige Stelle unterliegt, bei der es sich im Verhältnis zu dieser Behörde um einen Dritten handelt.**