Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
MANUEL CAMPOS SÁNCHEZ-BORDONA
vom 15. Januar 2020[1]

Verbundene Rechtssachen C-511/18 und C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
gegen
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

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

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten und Schutz des Privatlebens im Bereich der elektronischen Kommunikation – Schutz der nationalen Sicherheit und Terrorismusbekämpfung – Richtlinie 2002/58/EG – Anwendungsbereich – Art. 1 Abs. 3 – Art. 15 Abs. 3 – Art. 4 Abs. 2 EUV – Charta der Grundrechte der Europäischen Union – Art. 6, 7, 8, 11, 47 und Art. 52 Abs. 1 – Allgemeine und unterschiedslose Speicherung von Verbindungsdaten und von Daten, mit denen Personen, die zur Schaffung von Inhalten beigetragen haben, identifiziert werden können – Sammlung von Verkehrs- und Standortdaten – Zugang zu den Daten"

1. Der Gerichtshof hat in den letzten Jahren seine ständige Rechtsprechung zur Speicherung und zum Zugang zu personenbezogenen Daten beibehalten, von der insbesondere folgende Urteile zu nennen sind:

– das Urteil vom 8. April 2014, Digital Rights Ireland u. a.[2], in dem der Gerichtshof die Richtlinie 2006/24/EG[3] für ungültig erklärt hat, weil sie einen unverhältnismäßigen Eingriff in die in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Rechte zuließ;

– das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a.[4], in dem er Art. 15 Abs. 1 der Richtlinie 2002/58/EG[5] ausgelegt hat;

1 Originalsprache: Spanisch.

2 Rechtssachen C-293/12 und C-594/12, im Folgenden: Urteil Digital Rights, EU:C:2014:238.

3 Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54).

4 Rechtssachen C-203/15 und C-698/15, im Folgenden: Urteil Tele2 Sverige und Watson, EU:C:2016:970.

5 Richtlinie des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37).

– das Urteil vom 2. Oktober 2018, Ministerio Fiscal [6], in dem die Auslegung dieser Bestimmung der Richtlinie 2002/58/EG bestätigt wurde.

2. Diese Urteile (insbesondere das zweite Urteil) geben den Behörden einiger Mitgliedstaaten Anlass zur Besorgnis, da ihnen ihrer Ansicht nach ein Instrument vorenthalten wird, das sie als für den Schutz der nationalen Sicherheit und für die Bekämpfung von Kriminalität und Terrorismus notwendig erachten. Aus diesem Grund fordern einige dieser Mitgliedstaaten, diese Rechtsprechung aufzugeben oder anzupassen.

3. Drei Gerichte der Mitgliedstaaten haben in vier Vorabentscheidungsersuchen [7], zu denen ich heute meine Schlussanträge vorlege, auf diese Besorgnis hingewiesen.

4. Die vier Rechtssachen beziehen sich insbesondere auf das Problem der Anwendung der Richtlinie 2002/58 auf Tätigkeiten im Zusammenhang mit der nationalen Sicherheit und der Terrorismusbekämpfung. Sollte die Richtlinie insoweit anwendbar sein, müsste im Anschluss geklärt werden, inwieweit die Mitgliedstaaten die von ihr geschützten Datenschutzrechte einschränken können. Schließlich ist zu prüfen, inwieweit die verschiedenen nationalen Regelungen (die britische [8], die belgische [9] und die französische [10]) auf diesem Gebiet mit dem Unionsrecht in seiner Auslegung durch den Gerichtshof vereinbar sind.

I. Rechtlicher Rahmen

A. Unionsrecht

1. Richtlinie 2002/58

5. Art. 1 („Geltungsbereich und Zielsetzung“) bestimmt:

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

…

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“

6 Rechtssache C-207/16, im Folgenden: Urteil Ministerio Fiscal, EU:C:2018:788.

7 Neben den zwei vorliegenden Rechtssachen (Rechtssache C-511/18 und C-512/18) sind dies die Rechtssachen C-623/17, Privacy International, und C-520/18, Ordre des barreaux francophones et germanophone u. a.

8 Rechtssache Privacy International, C-623/17.

9 Rechtssache Ordre des barreaux francophones et germanophone u. a., C-520/18.

10 Rechtssachen La Quadrature du Net u. a., C-511/18 und C-512/18.

6. In Art. 3 („Betroffene Dienste“) heißt es:

„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.“

7. Art. 5 („Vertraulichkeit der Kommunikation“) Abs. 1 bestimmt:

„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.“

8. Art. 6 („Verkehrsdaten“) sieht vor:

„(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.“

9. In Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG[11]“) Abs. 1 heißt es:

„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/EG 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 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

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

2. Richtlinie 2000/31/EG[12]

10. Art. 14 sieht vor:

„(1) Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen verantwortlich ist, sofern folgende Voraussetzungen erfüllt sind:

…

(3) Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen."

11. Art. 15 lautet:

„(1) Die Mitgliedstaaten erlegen Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

(2) Die Mitgliedstaaten können Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können."

3. Verordnung (EU) 2016/679[13]

12. Art. 2 („Sachlicher Anwendungsbereich") bestimmt:

„(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

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

12 Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr) (ABl. 2000, L 178, S. 1).

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

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.

…“

13. In Art. 23 Abs. 1 („Beschränkungen“) heißt es:

„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:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

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

j) die Durchsetzung zivilrechtlicher Ansprüche.“

14. Art. 95 („Verhältnis zur Richtlinie 2002/58/EG“) lautet:

„Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.“

B. Nationales Recht

1. Code de la sécurité intérieure (Gesetzbuch über innere Sicherheit)

15. In Art. L. 851-1 heißt es:

„Unter den in Kapitel 1 von Titel II dieses Buchs vorgesehenen Voraussetzungen kann gestattet werden, bei den Betreibern elektronischer Kommunikationsdienste und den in Art. L. 34-1 des Code des postes et des communications électroniques [Gesetzbuch für Post und elektronische Kommunikation] genannten Personen sowie den in den Nrn. 1 und 2 des Abschnitts I von Art. 6 der Loi n° 2004-575 … pour la confiance dans l'économie numérique [Gesetz Nr. 2004-575 … über das Vertrauen in die digitale Wirtschaft] genannten Personen Informationen oder Dokumente zu sammeln, die von ihren Netzen oder elektronischen Kommunikationsdiensten verarbeitet oder gespeichert werden, einschließlich technischer Daten in Bezug auf die Ermittlung von Teilnehmer- oder Verbindungsnummern elektronischer Kommunikationsdienste, die Erfassung aller Teilnehmer- oder Verbindungsnummern einer bestimmten Person, die Standorte der verwendeten Endgeräte sowie die Kommunikationen eines Teilnehmers, bestehend in der Liste der Nummern ein- und ausgehender Anrufe, der Dauer und des Datums der Kommunikationen …"

16. Die Art. L. 851-2 und L. 851-4 regeln, zu verschiedenen Zwecken und mittels verschiedener Modalitäten, den Echtzeit-Zugang der Behörden zu den gespeicherten Verbindungsdaten.

17. Art. L. 851-2 gestattet ausschließlich zum Zweck der Terrorismusverhütung die Sammlung von Informationen oder Dokumenten im Sinne von Art. L. 851-1 von den dort genannten Personen. Diese Sammlung darf nur eine oder mehrere Personen betreffen, bei denen zuvor festgestellt wurde, dass sie eventuell Verbindungen zu einer terroristischen Bedrohung aufweisen, und erfolgt in Echtzeit. Das Gleiche gilt für Art. L. 851-4, der erlaubt, dass die Betreiber ausschließlich die technischen Daten über den Standort der Endgeräte in Echtzeit übermitteln [14].

18. Nach Art. L. 851-3 können Anbieter elektronischer Kommunikationsdienste und technische Dienstleister verpflichtet werden, „in ihren Netzen automatisierte Verarbeitungen einzusetzen, die dazu dienen, anhand der in der Genehmigung aufgeführten Parameter Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen können" [15].

19. Art. L. 851-5 legt fest, dass unter bestimmten Bedingungen, „die Verwendung einer technischen Vorrichtung, die die Bestimmung des Standorts einer Person, eines Fahrzeugs oder eines Gegenstands in Echtzeit ermöglicht, genehmigt werden" kann.

20. Nach Art. L. 851-6 Abs. I ist es unter bestimmten Bedingungen möglich, „unmittelbar mit Hilfe eines Geräts oder einer technischen Vorrichtung im Sinne von Art. 226-3 Abs. 1 des Code pénal (Strafgesetzbuch) die technischen Verbindungsdaten, die die Identifizierung eines Endgeräts oder der Teilnehmernummer seines Nutzers ermöglichen, sowie Daten über den Standort der verwendeten Endgeräte zu sammeln".

14 Das vorlegende Gericht ist der Überzeugung, dass diese Techniken die Anbieter nicht mit einem zusätzlichen Speicherungserfordernis belasteten, das über das hinausgehe, was zur Inrechnungstellung ihrer Dienste, deren Vermarktung und der Erbringung von Mehrwertdiensten erforderlich sei.

15 Nach Ansicht des vorlegenden Gerichts zielt diese Technik nicht auf eine allgemeine und unterschiedslose Vorratsspeicherung, sondern ausschließlich darauf ab, für begrenzte Zeit unter allen von diesen Personen verarbeiteten Verbindungsdaten diejenigen zu sammeln, die einen Zusammenhang mit einer solchen schweren Zuwiderhandlung aufweisen könnten.

2. Code des postes et des communications électroniques (Gesetzbuch für Post und elektronische Kommunikation)

21. Art. L. 34-1 des Gesetzbuchs für Post und elektronische Kommunikation in seiner auf den Sachverhalt anwendbaren Fassung bestimmt:

„I. Der vorliegende Artikel gilt für die Verarbeitung personenbezogener Daten im Rahmen des öffentlichen Angebots elektronischer Kommunikationsdienste; er gilt insbesondere für Netze, die Instrumente zur Sammlung von Daten und zur Identifizierung unterstützen.

II. Die Betreiber elektronischer Kommunikationsdienste und insbesondere die Personen, deren Tätigkeit darin besteht, der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anzubieten, löschen oder anonymisieren alle Verkehrsdaten, vorbehaltlich der Bestimmungen unter III, IV, V und VI.

Personen, die der Öffentlichkeit elektronische Kommunikationsdienste anbieten, führen unter Beachtung der Bestimmungen des vorstehenden Absatzes interne Verfahren ein, die es gestatten, Ersuchen der zuständigen Behörden nachzukommen.

Personen, die im Rahmen einer haupt- oder nebenberuflichen Tätigkeit der Öffentlichkeit eine Verbindung anbieten, die über einen Zugang zum Netz eine Online-Kommunikation ermöglicht, müssen, auch wenn ihr Angebot kostenlos ist, die nach dem vorliegenden Artikel für die Betreiber elektronischer Kommunikationsdienste geltenden Bestimmungen beachten.

III. Für die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten oder eines Verstoßes gegen die in Art. L. 336-3 des Code de la propriété intellectuelle (Gesetzbuch über geistiges Eigentum) aufgestellte Verpflichtung oder für die Zwecke der Verhinderung von Beeinträchtigungen der Systeme zur automatisierten Verarbeitung von Daten, mit deren Regelung und Ahndung sich die Art. 323-1 bis 323-3-1 des Code pénal (Strafgesetzbuch) befassen, und allein zum Zweck der Bereitstellung, im erforderlichen Maß, für die Justizbehörde oder die in Art. L. 331-12 des Gesetzbuchs über geistiges Eigentum genannte Hohe Behörde oder die in Art. L. 2321-1 des Code de la défense (Verteidigungsgesetzbuch) genannte Nationale Behörde für die Sicherheit der Informationssysteme können die zur Löschung oder Anonymisierung bestimmter Kategorien technischer Daten dienenden Vorgänge für eine Höchstdauer von einem Jahr aufgeschoben werden. In einem Dekret, das nach Anhörung des Conseil d'État (Staatsrat) und nach Stellungnahme der Commission nationale de l'informatique et des libertés (Nationale Kommission für Informatik und Freiheiten) erlassen wird, werden innerhalb der unter VI aufgestellten Grenzen diese Kategorien von Daten und die Dauer ihrer Speicherung festgelegt, je nach der Tätigkeit der Betreiber und der Art der Kommunikationen, sowie die Modalitäten des etwaigen Ausgleichs der ermittelbaren und spezifischen Mehrkosten der Leistungen, die von den Betreibern insoweit auf Ersuchen des Staates erbracht werden.

…

VI. Die gemäß den Abs. III, IV und V gespeicherten und verarbeiteten Daten beziehen sich ausschließlich auf die Identifizierung der Nutzer der von den Betreibern angebotenen Dienste, die technischen Merkmale der von den Betreibern bereitgestellten Kommunikationsdienste und den Standort der Endgeräte.

Auf keinen Fall dürfen sie sich auf den Inhalt der ausgetauschten Nachrichten oder auf die Informationen, die in jeglicher Form im Rahmen dieser Kommunikation abgerufen wurden, beziehen.

Die Speicherung und Verarbeitung erfolgt gemäß den Bestimmungen des Gesetzes Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten.

Die Betreiber ergreifen alle erforderlichen Maßnahmen, um die Verwendung dieser Daten zu anderen als den in diesem Artikel vorgesehenen Zwecken zu verhindern."

22. Gemäß Art. R. 10-13 Abs. I sind die Betreiber verpflichtet, zum Zweck der Ermittlung, Aufdeckung und Verfolgung von Straftaten folgende Daten zu speichern:

„a) Angaben, die es erlauben, die Identität des Nutzers festzustellen;

b) Daten über die verwendeten Kommunikationsendgeräte;

c) Technische Merkmale sowie Datum, Uhrzeit und Dauer der Kommunikation;

d) Daten über beantragte oder in Anspruch genommene Zusatzleistungen und deren Anbieter;

e) Daten, die es erlauben, die Identität des Adressaten der Nachrichtenübermittlung festzustellen."

23. Nach Art. R. 10-13 Abs. II muss der Betreiber bei Telefonaktivitäten außerdem die Daten speichern, die die Feststellung des Ursprungs und des Standorts der Nachrichtenübermittlung ermöglichen.

24. Gemäß Abs. III sind die oben genannten Daten ab dem Tag der Speicherung für ein Jahr aufzubewahren.

3. Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Gesetz Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft)

25. Art. 6 Abschnitt II Abs. 1 des Gesetzes Nr. 2004-575 sieht vor, dass Personen, deren Tätigkeit darin besteht, der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anzubieten, und natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten, „die Daten in einer Weise erheben und speichern, die die Identifikation jeder Person ermöglicht, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat".

26. Nach Abs. 3 des Abschnitts II kann die Justizbehörde von diesen Personen die Übermittlung der in Abs. 1 genannten Daten verlangen.

27. Der letzte Absatz des Abschnitts II bestimmt, dass durch ein Dekret des Conseil d'État (Staatsrat) „die in Abs. 1 genannten Daten definiert sowie die Dauer und die Modalitäten ihrer Speicherung festgelegt werden" [16].

16 Die Definition erfolgte durch das Décret nº 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Dekret Nr. 2011-219 vom 25. Februar 2011 über die Speicherung von Daten, die die Feststellung der Identität von Personen ermöglichen, die zur Schaffung von Online-Inhalten beigetragen haben). Aus diesem Dekret sind insbesondere zu nennen: a) Art. 1 Abs. 1, wonach Personen, die Zugang zu Online-Kommunikationsdiensten gewähren, zur Speicherung folgender Daten verpflichtet sind: die Verbindungskennung, die dem Teilnehmer zugeordnete Kennung, die Kennung des für die Verbindung verwendeten Endgeräts, das Datum und die Uhrzeit des Verbindungsbeginns und -endes, die Eigenschaften der Leitung des Teilnehmers; b) Art. 1 Abs. 2, wonach Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten, für jede Transaktion zur Speicherung folgender Daten verpflichtet sind: die Verbindungskennung am Ursprung der Kommunikation, die dem betreffenden Inhalt zugeordnete Kennung, die Art der für die Verbindung mit dem Dienst und für die Übertragung von Inhalten verwendeten Protokolle, die Art der Transaktion, das Datum und die Uhrzeit der Transaktion, die vom Urheber der Transaktion verwendete Kennung, und c) Art. 1 Abs. 3, wonach die in den beiden vorstehenden Absätzen genannten Personen zur Speicherung folgender vom Nutzer bei Vertragsschluss oder bei der Kontoeinrichtung angegebenen Informationen verpflichtet sind: Verbindungskennung bei der Kontoerstellung; Vorname, Nachname oder Firmenname; zugehörige Postanschriften, verwendete Pseudonyme, zugehörige E-Mail-Adressen oder Konten, Telefonnummern, aktuelle Passwörter und Angaben zur Überprüfung oder Änderung der Passwörter.

II. Sachverhalt und Vorlagefragen

A. Rechtssache C-511/18

28. La Quadrature du Net, das French Data Network, Igwan.net und die Fédération des fournisseurs d'accès à internet associatifs (im Folgenden: Kläger) haben beim Conseil d'État (Staatsrat) Klage auf Nichtigerklärung verschiedener Dekrete zur Durchführung einiger Bestimmungen des Gesetzbuchs über innere Sicherheit [17] erhoben.

29. Die Kläger machen im Wesentlichen geltend, dass sowohl die angefochtenen Dekrete als auch diese Bestimmungen des Gesetzbuchs über innere Sicherheit nicht mit den in den Art. 7, 8 und 47 der Charta verankerten Rechten auf Achtung des Privatlebens, auf Schutz personenbezogener Daten und auf einen wirksamen Rechtsbehelf vereinbar seien.

30. Unter diesen Umständen legt der Conseil d'État (Staatsrat) dem Gerichtshof die folgenden Fragen zur Vorabentscheidung vor:

1. Ist die den Anbietern auf der Grundlage der permissiven Bestimmungen in Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht zur allgemeinen und unterschiedslosen Speicherung in einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere durch die Gefahr des Terrorismus, gekennzeichneten Kontext als ein Eingriff anzusehen, der durch das in Art. 6 der Charta garantierte Recht auf Sicherheit und die Erfordernisse der nach Art. 4 EUV in die alleinige Verantwortung der Mitgliedstaaten fallenden nationalen Sicherheit gerechtfertigt ist?

2. Ist die Richtlinie 2002/58 im Licht der Charta dahin auszulegen, dass sie gesetzgeberische Maßnahmen wie die Maßnahmen zur Sammlung von Verkehrs- und Standortdaten bestimmter Personen gestattet, die zwar die Rechte und Pflichten der Anbieter elektronischer Kommunikationsdienste berühren, ihnen aber keine spezielle Pflicht zur Speicherung ihrer Daten auferlegen?

3. Ist die Richtlinie 2002/58 im Licht der Charta dahin auszulegen, dass sie die Rechtmäßigkeit der Verfahren zur Sammlung von Verbindungsdaten stets von dem Erfordernis abhängig macht, dass die betroffenen Personen unterrichtet werden, wenn ihre Unterrichtung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann, oder können solche Verfahren in Anbetracht aller übrigen bestehenden Verfahrensgarantien als rechtmäßig angesehen werden, wenn diese Garantien die Wirksamkeit des Rechts auf Einlegung eines Rechtsbehelfs gewährleisten?

B. Rechtssache C-512/18

31. Die Kläger des Ausgangsverfahrens in der Rechtssache C-511/18, mit Ausnahme von Igwan.net, beantragen beim Conseil d'État (Staatsrat) außerdem die Nichtigerklärung der (stillschweigenden) Ablehnung ihres Antrags auf Aufhebung von Art. R. 10-13 des Code des postes et des communications électroniques sowie des Dekrets Nr. 2011-219 vom 25. Februar 2011.

17 Folgende Dekrete wurden angefochten: a) Décret nº 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Dekret Nr. 2015-1885 vom 28. September 2015 zur Benennung der spezialisierten Nachrichtendienste); b) Décret nº 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Dekret Nr. 2015-1211 vom 1. Oktober 2015 zu Rechtsstreitigkeiten über die Umsetzung der genehmigungspflichtigen nachrichtendienstlichen Techniken und über die Sicherheit des Staates betreffende Dateien); c) Décret nº 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (Dekret Nr. 2015-1639 vom 11. Dezember 2015 zur Benennung anderer Dienste als der spezialisierten Nachrichtendienste, die auf die in Titel V des VIII. Buchs des Gesetzbuchs über innere Sicherheit genannten Techniken zurückgreifen dürfen); und d) Décret nº 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Dekret Nr. 2016-67 vom 29. Januar 2016 über Techniken zur Gewinnung nachrichtendienstlicher Erkenntnisse).

32. Nach Ansicht der Kläger beinhalten die angefochtenen Vorschriften eine Verpflichtung zur Speicherung von Verkehrs-, Standort- und Verbindungsdaten, die aufgrund ihres allgemeinen Charakters eine unverhältnismäßige Beeinträchtigung der in den Art. 7, 8 und 11 der Charta verankerten Rechte auf Achtung des Privat- und Familienlebens, auf den Schutz personenbezogener Daten und auf Meinungsfreiheit darstelle und gegen Art. 15 Abs. 1 der Richtlinie 2002/58 verstoße.

33. Im Rahmen dieses Verfahrens hat der Conseil d'État (Staatsrat) die folgenden Fragen zur Vorabentscheidung vorgelegt:

1. Ist die den Anbietern auf der Grundlage der permissiven Bestimmungen in Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht zur allgemeinen und unterschiedslosen Speicherung, insbesondere angesichts der Garantien und Kontrollen, die anschließend in Bezug auf die Sammlung und Nutzung dieser Verbindungsdaten bestehen, als ein Eingriff anzusehen, der durch das in Art. 6 der Charta garantierte Recht auf Sicherheit und die Erfordernisse der nach Art. 4 EUV in die alleinige Verantwortung der Mitgliedstaaten fallenden nationalen Sicherheit gerechtfertigt ist?

2. Sind die Bestimmungen der Richtlinie 2000/31 im Licht der Art. 6, 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen, dass sie es einem Staat gestatten, eine nationale Regelung einzuführen, mit der Personen, deren Tätigkeit darin besteht, der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anzubieten, und natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten, verpflichtet werden, Daten so zu speichern, dass jede Person, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat, identifiziert werden kann, damit die Justizbehörde gegebenenfalls ihre Übermittlung verlangen kann, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen?

III. Verfahren vor dem Gerichtshof und Standpunkte der Parteien

34. Die Vorabentscheidungsersuchen sind am 3. August 2018 beim Gerichtshof eingegangen.

35. La Quadrature du Net, die Fédération des fournisseurs d'accès à Internet associatifs, das French Data Network, die deutsche, die belgische, die britische, die tschechische, die zyprische, die dänische, die spanische, die estnische, die französische, die ungarische, die irische, die polnische und die schwedische Regierung sowie die Kommission haben schriftliche Erklärungen eingereicht.

36. An der mündlichen Verhandlung vom 9. September 2019, die gemeinsam mit der in den Rechtssachen C-623/17, Privacy International, und C-520/18, Ordre des barreaux francophones et germanophone u. a., durchgeführt wurde, haben die Parteien der vier Vorabentscheidungsverfahren, die oben genannten Regierungen, die niederländische und die norwegische Regierung sowie die Kommission und der Europäische Datenschutzbeauftragte teilgenommen.

IV. Würdigung

37. Die Fragen des Conseil d'État (Staatsrat) lassen sich in drei Gruppen einteilen:

– Erstens geht es um die Frage, ob nationale Vorschriften, die den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verbindungsdaten (erste Frage in den Rechtssachen C-511/18 und C-512/18) und insbesondere der

Daten, mit denen die an der Schaffung der Inhalte der von ihnen erbrachten Dienste beteiligten Personen identifiziert werden können (zweite Frage in der Rechtssache C-512/18), auferlegt, mit dem Unionsrecht vereinbar sind.

– Zweitens ist zu klären, ob die Rechtmäßigkeit der Verfahren zur Sammlung von Verbindungsdaten stets von dem Erfordernis abhängig ist, dass die betroffenen Personen unterrichtet werden, wenn ihre Unterrichtung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann (dritte Frage in der Rechtssache C-511/18).

– Drittens stellt sich die Frage, ob die Sammlung von Verkehrs- und Standortdaten in Echtzeit ohne eine spezielle Pflicht zur Speicherung der Daten mit der Richtlinie 2002/58 vereinbar ist und, wenn ja, unter welchen Bedingungen (zweite Frage in der Rechtssache C-511/18).

38. Kurzum geht es darum, festzustellen, ob nationale Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste die folgenden zwei Arten von Pflichten auferlegen, mit dem Unionsrecht vereinbar sind: a) zum einen die Pflicht zur *Sammlung* bestimmter Daten, nicht aber zur Speicherung; b) zum anderen die Pflicht zur *Speicherung* der Verbindungsdaten und der Daten, die die Identifizierung der Personen erleichtern, die die Inhalte der von den Betreibern erbrachten Dienste schaffen.

39. Zuvor ist jedoch zu klären, ob in dem Kontext [18], in dem diese nationalen Rechtsvorschriften erlassen wurden (d. h. bei einer möglichen Gefährdung der nationalen Sicherheit), die Richtlinie 2002/58 zur Anwendung kommt.

A. Zur Anwendbarkeit der Richtlinie 2002/58

40. Das vorlegende Gericht geht davon aus, dass die im Ausgangsverfahren streitigen Rechtsvorschriften in den Anwendungsbereich der Richtlinie 2002/58 fallen. Dies ergebe sich aus der Rechtsprechung, die mit dem Urteil Tele2 Sverige und Watson begründet und mit dem Urteil Ministerio Fiscal bestätigt worden sei.

41. Einige der an dem Verfahren beteiligten Regierungen vertreten demgegenüber die Ansicht, die streitigen Rechtsvorschriften seien nicht von dieser Richtlinie erfasst, und begründen dies u. a. mit dem Urteil vom 30. Mai 2006, Parlament/Rat und Kommission [19].

42. Ich stimme mit dem Conseil d'État (Staatsrat) darin überein, dass dieser Teil der Debatte mit dem Urteil Tele2 Sverige und Watson abschließend geklärt wurde. Der Gerichtshof hat bestätigt, dass die Richtlinie 2002/58 grundsätzlich zur Anwendung kommt, wenn die Betreiber elektronischer Kommunikationsdienste gesetzlich verpflichtet sind, die Daten ihrer Teilnehmer zu speichern und den Behörden Zugang zu gewähren. Dass diese Pflichten den Betreibern aus Gründen der nationalen Sicherheit auferlegt werden, ändert daran nichts.

43. Ich muss bereits an dieser Stelle anmerken, dass das Urteil Tele2 Sverige und Watson, sollte es einen Widerspruch zu älteren Urteilen geben, diesen vorgehen würde, da es später ergangen und durch das Urteil Ministerio Fiscal bestätigt worden ist. Ich bin jedoch der Ansicht, dass, wie ich noch erläutern werde, kein Widerspruch besteht.

18 „[E]inem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere durch die Gefahr des Terrorismus, gekennzeichneten Kontext", wie es in der ersten Frage in der Rechtssache C-511/18 heißt.

19 Rechtssachen C-317/04 und C-318/04, im Folgenden: Urteil Parlament/Rat und Kommission, EU:C:2006:346.

1. Urteil Parlament/Rat und Kommission

44. Die Rechtssachen, in denen das Urteil Parlament/Rat und Kommission ergangen ist, betrafen

– das Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von PNR-Daten [Passenger Name Records (Fluggastdatensätze)] und deren Übermittlung durch die Fluggesellschaften an die Behörden der Vereinigten Staaten [20];

– die Angemessenheit des Schutzes der personenbezogenen Daten, die in den an diese Behörden zu übermittelnden Passenger Name Records enthalten sind [21].

45. Der Gerichtshof hat im Ergebnis entschieden, dass die Übermittlung der Daten eine Verarbeitung zum Zweck der öffentlichen Sicherheit und der Unterstützung der Tätigkeiten des Staates im strafrechtlichen Bereich darstellt. Nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 fallen die streitigen Beschlüsse bzw. Entscheidungen nicht in den Anwendungsbereich dieser Richtlinie.

46. Die Daten wurden von den Fluggesellschaften ursprünglich im Rahmen einer unter das Unionsrecht fallenden Tätigkeit – des Verkaufs eines Flugscheins – erhoben. Die Datenverarbeitung war hingegen gemäß der streitigen Entscheidung „nicht für die Erbringung einer Dienstleistung erforderlich …, sondern [wurde] zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen“ [22].

47. Der Gerichtshof hat einen teleologischen Ansatz gewählt, der dem Zweck der Datenverarbeitung Rechnung trägt: Wenn mit der Datenverarbeitung der Schutz der öffentlichen Sicherheit bezweckt wird, fällt dies nicht in den Anwendungsbereich der Richtlinie 95/46. Dieser Zweck war jedoch nicht das einzige entscheidende Kriterium [23], und so wird in dem Urteil betont: „Die Übermittlung findet nämlich in einem von staatlichen Stellen geschaffenen Rahmen statt und dient der öffentlichen Sicherheit.“ [24]

20 Beschluss 2004/496/EG des Rates vom 17. Mai 2004 über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (ABl. 2004, L 183, S. 83, berichtigt im ABl. 2005, L 255, S. 168) (Rechtssache C-317/04).

21 Entscheidung 2004/535/EG der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden (ABl. 2004, L 235, S. 11) (Rechtssache C-318/04).

22 Urteil Parlament/Rat und Kommission, Rn. 57. In Rn. 58 heißt es jedoch, dass die „Tatsache, dass es private Wirtschaftsteilnehmer sind, die die [Daten] zu gewerblichen Zwecken erhoben haben und in einen Drittstaat übermitteln“, nicht bedeutet, dass diese Übermittlung nicht gemäß Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 in deren Anwendungsbereich fällt, da „die Übermittlung in einem von staatlichen Stellen geschaffenen Rahmen statt[findet] und … der öffentlichen Sicherheit“ dient.

23 Dies hob später der verstorbene Generalanwalt Bot in seinen Schlussanträgen in der Rechtssache Irland/Parlament und Rat (C-301/06, EU:C:2008:558) hervor. Nach seiner Ansicht kann das Urteil Parlament/Rat und Kommission „nicht bedeuten, dass allein die Prüfung des mit der Verarbeitung von personenbezogenen Daten verfolgten Ziels dafür maßgeblich ist, ob eine solche Verarbeitung in den Anwendungsbereich des durch die Richtlinie 95/46 errichteten Datenschutzsystems fällt. Zu prüfen ist auch, im Rahmen welcher Art von Tätigkeiten eine Verarbeitung von Daten vorgenommen wird. Nur wenn eine solche Verarbeitung für Tätigkeiten genutzt wird, die den Staaten oder den staatlichen Stellen zugewiesen sind und mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben, ist die Verarbeitung nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 vom gemeinschaftlichen System zum Schutz personenbezogener Daten, das durch diese Richtlinie begründet wurde, ausgeschlossen“ (Nr. 122).

24 Urteil Parlament/Rat und Kommission, Rn. 58. Ziel des Abkommens war es im Wesentlichen, die Fluggesellschaften, die Passagierflüge zwischen der Europäischen Union und den Vereinigten Staaten durchführten, zu verpflichten, den US-Behörden elektronischen Zugang zu PNR-Daten in ihren computergestützten Reservierungs-/Abfertigungssystemen zu gewähren. Mit dem Abkommen wurde somit eine Form der internationalen Zusammenarbeit zwischen der Union und den Vereinigten Staaten zur Bekämpfung des Terrorismus und anderer schwerer Straftaten geschaffen und gleichzeitig versucht, dieses Ziel mit dem des Schutzes der personenbezogenen Daten der Fluggäste in Einklang zu bringen. In diesem Zusammenhang unterschied sich die den Fluggesellschaften auferlegte Verpflichtung nicht wesentlich von einem direkten Datenaustausch zwischen Behörden.

48. Anhand des Urteils Parlament/Rat und Kommission wird somit der Unterschied zwischen der Ausschlussklausel und den Beschränkungs- oder Begrenzungsklauseln der Richtlinie 95/46 (analog zu den Klauseln der Richtlinie 2002/58) deutlich. Der Umstand, dass in beiden Arten von Klauseln ähnliche im Allgemeininteresse liegende Ziele genannt werden, verstärkt jedoch, wie Generalanwalt Bot ausgeführt hat [25], die Verwirrung hinsichtlich ihrer jeweiligen Reichweite.

49. Diese Verwirrung ist wahrscheinlich der Grund für die Auffassung der Mitgliedstaaten, die sich für die Nichtanwendbarkeit der Richtlinie 2002/58 auf diesen Kontext aussprechen. Sie vertreten den Standpunkt, das Interesse der nationalen Sicherheit werde nur durch die Ausschlussklausel in Art. 1 Abs. 3 der Richtlinie 2002/58 geschützt. Jedoch dienen auch die in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Beschränkungen, darunter u. a. die Beschränkung aus Gründen der nationalen Sicherheit, diesem Interesse. Diese Bestimmung wäre überflüssig, wenn die Richtlinie 2002/58 immer dann, wenn mit der nationalen Sicherheit argumentiert wird, nicht anwendbar wäre.

2. Urteil Tele2 Sverige und Watson

50. Im Urteil Tele2 Sverige und Watson ging es um die Frage, ob bestimmte nationale Rechtsvorschriften, die den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste eine generelle Verpflichtung zur Vorratsspeicherung der Daten über diese Kommunikation auferlegen, mit dem Unionsrecht vereinbar sind. Der Sachverhalt entsprach daher im Wesentlichen dem den vorliegenden Vorabentscheidungsersuchen zugrunde liegenden Sachverhalt.

51. Erneut nach der Anwendbarkeit des Unionsrechts – nun in Form der Richtlinie 2002/58 – befragt, hat der Gerichtshof zunächst darauf hingewiesen, „dass für die Bestimmung der Reichweite des Geltungsbereichs der Richtlinie 2002/58 insbesondere deren Systematik zu berücksichtigen ist“ [26].

52. In diesem Zusammenhang hat der Gerichtshof Folgendes ausgeführt: „Zwar beziehen sich die Rechtsvorschriften, um die es in Art. 15 Abs. 1 der Richtlinie 2002/58 geht, auf spezifische Tätigkeiten der Staaten oder der staatlichen Stellen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben. … Zudem decken sich die Zweckbestimmungen, denen die Rechtsvorschriften nach dieser Bestimmung entsprechen müssen – Schutz der nationalen Sicherheit … –, im Wesentlichen mit den Zielen, die mit den in Art. 1 Abs. 3 der Richtlinie genannten Tätigkeiten verfolgt werden.“ [27]

53. Somit deckt sich der Zweck der Maßnahmen, mit denen die Mitgliedstaaten gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 den Schutz der Privatsphäre beschränken können, (an dieser Stelle) mit dem Zweck, der die Befreiung bestimmter staatlicher Tätigkeiten von den Bestimmungen der Richtlinie nach Art. 1 Abs. 3 rechtfertigt.

54. Nach Überzeugung des Gerichtshofs erlaubt dieser Gesichtspunkt „[i]n Anbetracht der Systematik der Richtlinie 2002/58“ jedoch „nicht den Schluss, dass die Rechtsvorschriften im Sinne des Art. 15 Abs. 1 dieser Richtlinie von deren Geltungsbereich ausgeschlossen sind, da dieser Bestimmung damit jede praktische Wirksamkeit genommen würde. Art. 15 Abs. 1 der Richtlinie 2002/58 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden“ [28].

25 Schlussanträge von Generalanwalt Bot in der Rechtssache Irland/Parlament und Rat (C-301/06, EU:C:2008:558, Nr. 127).

26 Urteil Tele2 Sverige und Watson, Rn. 67.

27 Ebd., Rn. 72.

28 Ebd., Rn. 73.

55. Hinzu kommt, dass die in Art. 15 Abs. 1 der Richtlinie 2002/58 zugelassenen Beschränkungen „– zu den in dieser Bestimmung genannten Zwecken – die Tätigkeit der Betreiber elektronischer Kommunikationsdienste“ regeln. Demnach ist diese Bestimmung in Verbindung mit Art. 3 der Richtlinie „dahin auszulegen, dass diese Rechtsvorschriften in den Geltungsbereich dieser Richtlinie fallen“ [29].

56. Folglich umfasst nach Ansicht des Gerichtshofs der Anwendungsbereich der Richtlinie 2002/58 sowohl eine Rechtsvorschrift, die den Betreibern „vorschreibt, die Verkehrs- und Standortdaten auf Vorrat zu speichern, da damit zwangsläufig eine Verarbeitung personenbezogener Daten durch die Betreiber verbunden ist [30]“, als auch eine Rechtsvorschrift, die den Zugang der Behörden zu den von den Betreibern auf Vorrat gespeicherten Daten betrifft [31].

57. Die Auslegung der Richtlinie 2002/58, die der Gerichtshof im Urteil Tele2 Sverige und Watson vorgenommen hat, wird im Urteil Ministerio Fiscal bestätigt.

58. Könnte argumentiert werden, dass das Urteil Tele2 Sverige und Watson eine mehr oder weniger implizite Abweichung von der mit dem Urteil Parlament/Rat und Kommission begründeten Rechtsprechung darstellt? Diese Auffassung wird z. B. von der irischen Regierung vertreten, die geltend macht, dass nur das Urteil Parlament/Rat und Kommission mit der Rechtsgrundlage der Richtlinie 2002/58 vereinbar sei und nicht gegen Art. 4 Abs. 2 EUV verstoße [32].

59. Die französische Regierung vertritt den Standpunkt, dass der Widerspruch überwunden werden könne, wenn berücksichtigt werde, dass sich das Urteil Tele2 Sverige und Watson auf Tätigkeiten der Mitgliedstaaten im Bereich des Strafrechts, das Urteil Parlament/Rat und Kommission hingegen auf die Sicherheit und Verteidigung des Staates beziehe. Für die vorliegende Rechtssache sei das Urteil Tele2 Sverige und Watson daher nicht einschlägig, und es müsse der im Urteil Parlament/Rat und Kommission getroffenen Entscheidung gefolgt werden [33].

60. Wie bereits erwähnt, bin ich der Ansicht, dass sich die beiden Urteile, anders als von der französischen Regierung vorgetragen, auf integrative Weise auslegen lassen. Die Auffassung der französischen Regierung teile ich nicht, da sich die Erwägungen im Urteil Tele2 Sverige und Watson, die sich ausdrücklich auf die Terrorismusbekämpfung [34] beziehen, meines Erachtens auf jede andere Bedrohung der nationalen Sicherheit (bei der der Terrorismus nur eine von vielen ist) ausdehnen lassen.

3. Möglichkeit einer integrativen Auslegung des Urteils Parlament/Rat und Kommission und des Urteils Tele2 Sverige und Watson

61. Nach meiner Überzeugung hat der Gerichtshof in den Urteilen Tele2 Sverige und Watson sowie Ministerio Fiscal den Grundgedanken der Ausschluss- und Beschränkungsklauseln sowie den systematischen Zusammenhang zwischen den beiden Arten von Klauseln berücksichtigt.

29 Ebd., Rn. 74.

30 Ebd., Rn. 75.

31 Ebd., Rn. 76.

32 Rn. 15 und 16 der schriftlichen Erklärungen der irischen Regierung.

33 Rn. 34 bis 50 der schriftlichen Erklärungen der französischen Regierung.

34 Urteil Tele2 Sverige und Watson, Rn. 103 und 119.

62. Wenn der Gerichtshof in der Rechtssache Parlament/Rat und Kommission festgestellt hat, dass die Datenverarbeitung nicht in den Anwendungsbereich der Richtlinie 95/46 fällt, so beruht dies, wie bereits erwähnt, darauf, dass bei der Zusammenarbeit zwischen der Europäischen Union und den Vereinigten Staaten in einem typischerweise internationalen Rahmen die staatliche Dimension der Tätigkeit gegenüber der Tatsache, dass die Verarbeitung auch eine gewerbliche oder private Dimension beinhaltet, überwiegt. Eine der zu jenem Zeitpunkt streitigen Fragen betraf die geeignete Rechtsgrundlage für die angefochtene Entscheidung.

63. Bei den in den Urteilen Tele2 Sverige und Watson und Ministerio Fiscal geprüften nationalen Maßnahmen hat der Gerichtshof hingegen auf den internen Umfang der Datenverarbeitung abgestellt: Der rechtliche Rahmen, in dem die Datenverarbeitung vorgenommen wurde, war ausschließlich national, und es fehlte somit die externe Dimension, die den Gegenstand des Urteils Parlament/Rat und Kommission kennzeichnete.

64. Die unterschiedliche Gewichtung der internationalen und der nationalen (gewerblichen und privaten) Dimension der Datenverarbeitung hatte zur Folge, dass in der ersten Rechtssache die Ausschlussklausel des Unionsrechts für den Schutz des in der nationalen Sicherheit liegenden Allgemeininteresses besser geeignet war. In der zweiten Rechtssache konnte dieses Interesse hingegen durch die in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehene Beschränkungsklausel wirksam geschützt werden.

65. Es gibt noch einen weiteren Unterschied, der an den unterschiedlichen Regelungszusammenhang anknüpft: Die Urteile konzentrieren sich jeweils auf die Auslegung einer von zwei Vorschriften, die zwar gleich aussehen, aber nicht gleich sind.

66. Im Urteil Parlament/Rat und Kommission wurde über die Auslegung von Art. 3 Abs. 2 der Richtlinie 95/46 entschieden, im Urteil Tele2 Sverige und Watson hingegen über Art. 1 Abs. 3 der Richtlinie 2002/58. Eine aufmerksame Lektüre dieser Artikel zeigt ausreichend Unterschiede, um die Urteile des Gerichtshofs in den beiden Rechtssachen zu untermauern.

67. Nach Art. 3 Abs. 2 der Richtlinie 95/46 findet „[d]iese Richtlinie … *keine Anwendung auf die Verarbeitung personenbezogener Daten*, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, … und auf keinen Fall auf *Verarbeitungen* betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die *Verarbeitung* die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich [35]“.

68. Nach Art. 1 Abs. 3 der Richtlinie 2002/58 gilt diese Richtlinie „*nicht für Tätigkeiten*, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, … und auf keinen Fall für *Tätigkeiten* betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die *Tätigkeit* die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich“ [36].

69. Während Art. 3 Abs. 2 der Richtlinie 95/46 die *Verarbeitung von Daten* für Zwecke der – soweit hier von Interesse – Sicherheit des Staates ausschließt, schließt Art. 1 Abs. 3 der Richtlinie 2002/58 *Tätigkeiten* zum Schutz der – ebenfalls soweit hier von Interesse – Sicherheit des Staates aus.

35 Hervorhebung nur hier.

36 Hervorhebung nur hier.

70. Dieser Unterschied ist nicht unerheblich. Die Richtlinie 95/46 nimmt von ihrem Anwendungsbereich eine Tätigkeit (die „Verarbeitung personenbezogener Daten"), die jeder ausüben kann, aus, wenn diese Verarbeitung u. a. die Sicherheit des Staates betrifft. Die Frage, *wer* die Verarbeitung der Daten vornimmt, ist hier irrelevant. Die Bestimmung der ausgeschlossenen Handlungen erfolgt somit teleologisch bzw. zweckbestimmt und ohne Unterscheidung nach der Art der handelnden Personen.

71. In der Rechtssache Parlament/Rat und Kommission ging es dem Gerichtshof somit in erster Linie um den Zweck, für den die Daten verarbeitet werden. Die „Tatsache, dass es private Wirtschaftsteilnehmer sind, die die … Daten zu gewerblichen Zwecken erhoben haben und in einen Drittstaat übermitteln", spielte keine Rolle, denn wesentlich war, dass „die Übermittlung in einem von staatlichen Stellen geschaffenen Rahmen statt[findet] und … der öffentlichen Sicherheit" dient [37].

72. Die „Tätigkeiten betreffend die Sicherheit des Staates" hingegen, die nicht in den im Urteil Tele2 Sverige und Watson analysierten Anwendungsbereich der Richtlinie 2002/58 fallen, können nicht von irgendeiner Person ausgehen, sondern nur vom Staat selbst. Außerdem umfassen sie nicht die gesetzgeberischen oder regulatorischen Funktionen des Staates, sondern ausschließlich die tatsächlichen Handlungen der staatlichen Stellen.

73. Tatsächlich handelt es sich bei den in Art. 1 Abs. 3 der Richtlinie 2002/58 aufgeführten *Tätigkeiten* durchgehend um „spezifische Tätigkeiten der Staaten oder der staatlichen Stellen, die mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben" [38]. Diese „Tätigkeiten" können jedoch nicht gesetzgeberischer Art sein. Ansonsten wären alle von den Mitgliedstaaten erlassenen Vorschriften über die Verarbeitung personenbezogener Daten vom Anwendungsbereich der Richtlinie 2002/58 ausgenommen, sobald der Versuch gemacht wird, sie als für den Schutz der Sicherheit des Staates erforderlich zu rechtfertigen.

74. Dies würde zum einen die Wirksamkeit der Richtlinie deutlich verringern, da die bloße Argumentation mit einem juristischen Begriff, der so unbestimmt ist wie der der nationalen Sicherheit, dazu führen würde, dass die vom Unionsgesetzgeber zum Schutz der personenbezogenen Daten der Bürger ausgearbeiteten Garantien gegenüber den Mitgliedstaaten nicht mehr gelten. Dieser Schutz, der ohne die Unterstützung der Mitgliedstaaten nicht durchführbar ist, wird für den Bürger auch gegenüber den nationalen Behörden gewährleistet.

75. Zum anderen würde eine Auslegung des Begriffs „staatliche Tätigkeiten", die auch den Erlass von Rechtsvorschriften umfasst, Art. 15 der Richtlinie 2002/58 aushöhlen, der die Mitgliedstaaten gerade dazu befugt, – im Interesse des Schutzes von u. a. der nationalen Sicherheit – „Rechtsvorschriften" zu erlassen, um bestimmte in der Richtlinie enthaltene Rechte und Pflichten zu beschränken" [39].

76. Der Gerichtshof hat in der Rechtssache Tele2 Sverige und Watson darauf hingewiesen, dass „für die Bestimmung der Reichweite des Geltungsbereichs der Richtlinie 2002/58 insbesondere deren Systematik zu berücksichtigen ist" [40]. Folglich sieht eine Auslegung von Art. 1 Abs. 3 und Art. 15 Abs. 1 der Richtlinie 2002/58, die diesen Vorschriften einen Sinn verleiht, ohne ihre Wirksamkeit zu beeinträchtigen, so aus, dass die erste der beiden Vorschriften einen materiellen Ausschluss der *Tätigkeiten* der Mitgliedstaaten im Bereich der nationalen Sicherheit (und vergleichbarer Bereiche)

37 Parlament/Rat und Kommission, Rn. 58.

38 Urteil Ministerio Fiscal, Rn. 32. In diesem Sinne auch Urteil Tele2 Sverige und Watson, Rn. 72.

39 Es ließe sich tatsächlich kaum vertreten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 eine Beschränkung der in ihr festgelegten Rechte und Pflichten in einem Bereich wie dem der nationalen Sicherheit zulässt, der nach Art. 1 Abs. 3 der Richtlinie selbst grundsätzlich nicht in deren Geltungsbereich fällt. Wie der Gerichtshof im Urteil Tele2 Sverige und Watson, Rn. 73, festgestellt hat, setzt Art. 15 Abs. 1 der Richtlinie 2002/58 „zwangsläufig voraus, dass die dort genannten nationalen Vorschriften … in den Geltungsbereich der Richtlinie fallen, da diese Richtlinie die Mitgliedstaaten zum Erlass solcher Vorschriften ausdrücklich nur dann ermächtigt, wenn die darin vorgesehenen Voraussetzungen eingehalten werden".

40 Urteil Tele2 Sverige und Watson, Rn. 67.

und die zweite Vorschrift eine Befugnis zum Erlass von *Rechtsvorschriften* (d. h. Vorschriften mit allgemeiner Geltung), die im Interesse der nationalen Sicherheit die Tätigkeiten von der Hoheitsgewalt der Mitgliedstaaten unterliegenden Personen betreffen, und somit zur Einschränkung der in der Richtlinie 2002/58 garantierten Rechte enthält.

4. Ausschluss der nationalen Sicherheit in der Richtlinie 2002/58

77. Die nationale Sicherheit (bzw. ihr in Art. 15 Abs. 1 genanntes Synonym „Sicherheit des Staates") wird in der Richtlinie 2002/58 in zweifacher Hinsicht berücksichtigt. Zum einen stellt sie einen Grund für den *Ausschluss* (vom Geltungsbereich dieser Richtlinie) aller Tätigkeiten der Mitgliedstaaten „betreffend" die Sicherheit des Staates dar. Zum anderen ist sie Grund für eine per Gesetz umzusetzende *Beschränkung* der in der Richtlinie 2002/58 festgelegten Rechte und Pflichten, d. h. von Tätigkeiten privater oder gewerblicher Art außerhalb des Bereichs der hoheitlichen Tätigkeiten [41].

78. Auf welche Tätigkeiten bezieht sich Art. 1 Abs. 3 der Richtlinie 2002/58? Meiner Überzeugung nach führt der Conseil d'État (Staatsrat) selbst ein gutes Beispiel an, wenn er die Art. L. 851-5 und L. 851-6 des Gesetzbuchs über innere Sicherheit nennt und auf „unmittelbar vom Staat umgesetzte Techniken zur Sammlung von Informationen, ohne die Tätigkeiten der Anbieter elektronischer Kommunikationsdienste zu regeln und ihnen spezielle Pflichten aufzuerlegen" [42], verweist.

79. Meiner Ansicht nach ist dies der Schlüssel zur Bestimmung des Umfangs der Ausschlussklausel in Art. 1 Abs. 3 der Richtlinie 2002/58. *Tätigkeiten* zum Schutz der nationalen Sicherheit, die von den Behörden, ohne die Unterstützung durch Privatpersonen anzufordern und somit ohne ihnen Verpflichtungen bei der Unternehmensführung aufzuerlegen, auf eigene Rechnung durchgeführt werden, fallen nicht unter diese Richtlinie.

80. Die Liste der Tätigkeiten der Behörden, die von der allgemeinen Regelung für die Verarbeitung personenbezogener Daten ausgenommen sind, ist eng auszulegen. Konkret darf der Begriff der *nationalen Sicherheit*, für die nach Art. 4 Abs. 2 EUV jeder Mitgliedstaat allein verantwortlich ist, nicht auf andere, näher oder weiter entfernte Bereiche des öffentlichen Lebens ausgedehnt werden.

81. Da die Vorlagefragen auch Handlungen von Privatpersonen (d. h. derjenigen, die die elektronischen Kommunikationsdienste für die Nutzer bereitstellen) und nicht nur Maßnahmen der staatlichen Behörden betreffen, ist hier eine Abgrenzung des Begriffs der nationalen Sicherheit im engeren Sinne nicht erforderlich.

82. Meines Erachtens lässt sich jedoch das Kriterium des Rahmenbeschlusses 2006/960/JI [43] heranziehen, dessen Art. 2 Buchst. a zwischen Strafverfolgungsbehörden im weiteren Sinne („eine nationale Polizei-, Zoll- oder sonstige Behörde, die nach nationalem Recht befugt ist, Straftaten oder kriminelle Aktivitäten aufzudecken, zu verhüten und aufzuklären und in Verbindung mit diesen Tätigkeiten öffentliche Gewalt auszuüben und Zwangsmaßnahmen zu ergreifen") einerseits und den „Behörden oder Stellen, die sich speziell mit Fragen der nationalen Sicherheit befassen", andererseits unterscheidet [44].

41 Wie Generalanwalt Saugmandsgaard Øe in seinen Schlussanträgen in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nr. 47) beiläufig ausgeführt hat, dürfen „einerseits personenbezogene Daten, die *unmittelbar* im Rahmen der – hoheitlichen – Tätigkeiten des Staates in einem Bereich des Strafrechts verarbeitet werden, und andererseits solche Daten, die im Rahmen von – wirtschaftlichen – Tätigkeiten eines Anbieters von elektronischen Kommunikationsdiensten verarbeitet werden, und die *danach* von den zuständigen staatlichen Behörden verwendet werden, nicht verwechselt werden".

42 Rn. 18 und 21 des Vorlagebeschlusses in der Rechtssache C-511/18.

43 Rahmenbeschluss des Rates vom 18. Dezember 2016 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. 2006, L 386, S. 89).

44 Ebenso lässt der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. 2008, L 350, S. 60), nach seinem Art. 1 Abs. 4 „die wesentlichen nationalen Sicherheitsinteressen und spezifische nachrichtendienstliche Tätigkeiten, die die innere Sicherheit betreffen, unberührt".

83. Im elften Erwägungsgrund der Richtlinie 2002/58 heißt es, dass die Richtlinie „[w]ie die Richtlinie [95/46] … nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das [Unions]recht fallen“, gilt. Deshalb hat die Richtlinie 2002/58 „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 … Sicherheit des Staates … erforderlich sind“.

84. Zwischen der Richtlinie 95/46 und der Richtlinie 2002/58 besteht in Bezug auf die Zuständigkeiten der Mitgliedstaaten im Bereich der nationalen Sicherheit in der Tat eine Kontinuität. Keine der beiden Richtlinien bezweckt den Schutz der Grundrechte in diesem speziellen Bereich, in dem die Tätigkeiten der Mitgliedstaaten „nicht unter das [Unions]recht fallen“.

85. Das im elften Erwägungsgrund genannte „Gleichgewicht“ ergibt sich aus der Notwendigkeit, die Zuständigkeit der Mitgliedstaaten in Fragen der nationalen Sicherheit zu achten, wenn sie diese *unmittelbar und mit eigenen Mitteln* ausüben. Wenn es hingegen, auch aus den gleichen Gründen der nationalen Sicherheit, der Unterstützung durch Privatpersonen, denen bestimmte Verpflichtungen auferlegt werden, bedarf, dann ist ein Bereich (die Pflicht dieser Privatpersonen zum Schutz der Privatsphäre) betroffen, der dem Unionsrecht unterliegt.

86. Sowohl die Richtlinie 95/46 als auch die Richtlinie 2002/58 wollen dieses Gleichgewicht erzielen, indem sie in Art. 13 Abs. 1 bzw. Art. 15 Abs. 1 eine Einschränkung der Rechte von Einzelpersonen durch Rechtsvorschriften der Mitgliedstaaten zulassen. Insoweit gibt es keinen Unterschied zwischen den beiden Richtlinien.

87. Nach Art. 2 Abs. 2 der Verordnung 2016/679, die einen (neuen) allgemeinen Rahmen für den Schutz personenbezogener Daten festlegt, findet die Verordnung keine Anwendung auf die „Verarbeitung personenbezogener Daten“ durch die Mitgliedstaaten „im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen“.

88. Während in der Richtlinie 95/46 die Verarbeitung personenbezogener Daten nur durch ihren Zweck und nicht durch die Person, die sie durchführt, gekennzeichnet war, werden in der Verordnung 2016/679 die Verarbeitungen, die nicht in ihren Anwendungsbereich fallen, sowohl anhand ihres Zwecks als auch anhand derjenigen, die sie durchführen, bestimmt: Ausgeschlossen sind Verarbeitungen, die die Mitgliedstaaten im Rahmen einer *Tätigkeit* vornehmen, die nicht in den Anwendungsbereich des Unionsrechts fällt (Art. 2 Abs. 2 Buchst. a und b), sowie Verarbeitungen, die die Behörden *zum Zwecke der Bekämpfung von Straftaten und des Schutzes* vor Gefahren für die öffentliche Sicherheit vornehmen [45].

89. Die Bestimmung dieser Tätigkeiten der öffentlichen Gewalt muss zwangsläufig restriktiv erfolgen, da andernfalls den Unionsvorschriften zum Schutz der Privatsphäre die Wirksamkeit genommen würde. Art. 23 der Verordnung 2016/679 sieht – im Einklang mit Art. 15 Abs. 1 der Richtlinie 2002/58 – vor, dass die in der Verordnung festgelegten Pflichten und Rechte *im Wege von Gesetzgebungsmaßnahmen* beschränkt werden können, wenn dies u. a. zur Sicherstellung der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit erforderlich ist. Auch hier wäre, wenn der Schutz dieser Ziele für einen Ausschluss vom Anwendungsbereich der Verordnung 2016/679 ausreichen würde, die Berufung auf die nationale Sicherheit als Rechtfertigung für die Beschränkung der durch die Verordnung garantierten Rechte im Wege von Gesetzgebungsmaßnahmen überflüssig.

45 Die Verordnung 2016/679 schließt nämlich die Verarbeitung von Daten durch die Mitgliedstaaten im Rahmen einer *Tätigkeit*, die nicht in den Anwendungsbereich des Unionsrechts fällt, sowie die Verarbeitung durch die Behörden *zum Zwecke des Schutzes* der öffentlichen Sicherheit aus.

90. Wie bei der Richtlinie 2002/58 wäre es widersprüchlich, wenn die in Art. 23 der Verordnung 2016/679 vorgesehenen Gesetzgebungsmaßnahmen (die, wie ich noch einmal betonen möchte, staatliche Beschränkungen der Persönlichkeitsrechte der Bürger aus Gründen der nationalen Sicherheit zulassen) in den Anwendungsbereich der Verordnung fielen und gleichzeitig die Berufung auf die nationale Sicherheit dazu führen würde, dass die Verordnung ohne Weiteres unanwendbar wäre, was eine Nichtanerkennung jeglicher subjektiver Rechte bedeuten würde.

B. Bestätigung und Möglichkeiten der Weiterentwicklung des Urteils Tele2 Sverige und Watson

91. In meinen Schlussanträgen in der Rechtssache C-520/18 analysiere ich die einschlägige Rechtsprechung des Gerichtshofs im Detail [46] und schlage im Ergebnis ihre Bestätigung und gleichzeitig eine Auslegungsmöglichkeit zur Klärung ihres Inhalts vor.

92. Ich beziehe mich auf diese Analyse und halte es nicht für erforderlich, sie hier wiederzugeben. Bei meinen nachstehenden Ausführungen zu den vom Conseil d'État (Staatsrat) zur Vorabentscheidung vorgelegten Fragen sind folglich auch die entsprechenden Abschnitte der Schlussanträge in der Rechtssache C-520/18 zu berücksichtigen.

C. Antwort auf die Vorlagefragen

1. Pflicht zur Vorratsspeicherung (erste Vorlagefrage in den Rechtssachen C-511/18 und C-512/18 sowie zweite Vorlagefrage in der Rechtssache C-512/18)

93. In Bezug auf die den Betreibern elektronischer Kommunikationsdienste auferlegte Pflicht zur Vorratsspeicherung von Daten möchte das vorlegende Gericht insbesondere wissen,

– ob diese nach Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht einen Eingriff darstellt, der durch das in Art. 6 der Charta verankerte „Recht auf Sicherheit" sowie das Ziel der nationalen Sicherheit gerechtfertigt ist (erste Frage in den Rechtssachen C-511/18 und C-512/18 sowie dritte Frage in der Rechtssache C-511/18); und

– ob die Richtlinie 2000/31 die Speicherung von Daten zulässt, anhand deren Personen, die zur Schaffung öffentlich zugänglicher Online-Inhalte beigetragen haben, identifiziert werden können (zweite Frage in der Rechtssache C-512/18).

a) Vorbemerkung

94. Der Conseil d'État (Staatsrat) verweist auf die in den Art. 7 (Achtung des Privat- und Familienlebens), 8 (Schutz personenbezogener Daten) und 11 (Freiheit der Meinungsäußerung und Informationsfreiheit) der Charta geschützten Grundrechte. Auch nach Überzeugung des Gerichtshofs könnten diese Grundrechte durch die von den nationalen Behörden den Betreibern elektronischer Kommunikationsdienste auferlegte Verpflichtung zur Speicherung von Verkehrsdaten verletzt werden [47].

95. Das vorlegende Gericht verweist außerdem auf das in Art. 6 der Charta verankerte Recht auf Sicherheit. Dabei geht es weniger davon aus, dass dieses Recht verletzt worden sei, sondern nennt das Recht als Grund, der die Auferlegung dieser Pflicht rechtfertigen könne.

46 Nrn. 27 bis 68.

47 Urteil Tele2 Sverige und Watson, Rn. 92 mit entsprechendem Zitat des Urteils Digital Rights, Rn. 25 und 70.

96. Ich stimme mit der Kommission darin überein, dass der Verweis auf Art. 6 in dieser Hinsicht irreführend ist. Ebenso wie die Kommission bin ich der Ansicht, dass die Vorschrift nicht dahin auszulegen ist, dass sie „der Union eine positive Verpflichtung zur Ergreifung von Maßnahmen zum Schutz des Einzelnen vor Straftaten auferlegen“ [48] kann.

97. Die durch diesen Artikel der Charta geschützte Sicherheit ist nicht mit der öffentlichen Sicherheit gleichzusetzen. Oder anders ausgedrückt hat dieses Recht auf Sicherheit genauso viel mit der öffentlichen Sicherheit zu tun wie jedes andere Grundrecht, da die öffentliche Sicherheit eine unabdingbare Voraussetzung für die Wahrnehmung der Grundrechte und Grundfreiheiten darstellt.

98. Die Kommission weist darauf hin, dass Art. 6 der Charta mit Art. 5 der Europäischen Menschenrechtskonvention (im Folgenden: EMRK) übereinstimmt, wie aus den beigefügten Erläuterungen hervorgeht. Die Lektüre von Art. 5 EMRK zeigt, dass es sich bei der dort geschützten „Sicherheit“ ausschließlich um die persönliche Sicherheit handelt, d. h. um eine Garantie des Rechts auf physische Freiheit gegenüber willkürlicher Festnahme oder Freiheitsentziehung, kurz gesagt um die Sicherheit, dass niemand, außer in den gesetzlich vorgesehenen Fällen und unter Einhaltung der vorgesehenen Voraussetzungen und Verfahren, seiner Freiheit beraubt wird.

99. Es geht somit um die *persönliche Sicherheit* sowie die Bedingungen, unter denen die physische Freiheit der Menschen eingeschränkt werden darf[49], und nicht um die der Existenz des Staates innewohnende *öffentliche Sicherheit*, die in einer entwickelten Gesellschaft unerlässlich ist, um die Ausübung öffentlicher Befugnisse mit der Wahrnehmung individueller Rechte in Einklang zu bringen.

100. Einige Regierungen fordern jedoch, dass das Recht auf Sicherheit im Sinne der öffentlichen Sicherheit stärker zu berücksichtigen sei. Der Gerichtshof hat dies nicht ignoriert, sondern in seinen Urteilen [50] und Gutachten [51] ausdrücklich erwähnt. So hat er die Bedeutung der dem Gemeinwohl dienenden Ziele des Schutzes der nationalen Sicherheit und der öffentlichen Ordnung [52], der Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit sowie der Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit [53] nie bestritten, sondern diese zu Recht als „von größter Bedeutung“ bezeichnet [54]. Wie er betont, „trägt der Schutz der öffentlichen Sicherheit auch zum Schutz der Rechte und Freiheiten anderer bei“ [55].

101. Die sich mit den vorliegenden Vorabentscheidungsersuchen bietende Gelegenheit könnte genutzt werden, um noch deutlicher das Streben nach einem Gleichgewicht zwischen dem Recht auf Sicherheit auf der einen und dem Recht auf Privatsphäre und auf Schutz personenbezogener Daten auf der anderen Seite voranzutreiben. Auf diese Weise ließe sich die Kritik einer Bevorzugung der Rechte auf Privatsphäre und Datenschutz zum Nachteil des Rechts auf Sicherheit vermeiden.

102. Auf dieses Gleichgewicht beziehen sich meiner Ansicht nach der elfte Erwägungsgrund und Art. 15 Abs. 1 der Richtlinie 2002/58, wenn sie von der Erforderlichkeit und der Verhältnismäßigkeit der Maßnahmen in *einer demokratischen Gesellschaft* sprechen. Das Recht auf Sicherheit ist, wie ich hier noch einmal betonen möchte, für das Bestehen und Überleben einer Demokratie unabdingbar

48 Rn. 37 der schriftlichen Erklärungen der Kommission.

49 So die Auslegung des EGMR. Vgl. statt aller das Urteil vom 5. Juli 2016, Buzadji gegen Moldawien, CE:ECHR:2016:0705JUD002375507. Dort heißt es in § 84, dass der Hauptzweck des in Art. 5 EMRK verankerten Rechts die Verhinderung einer willkürlichen oder ungerechtfertigten Entziehung der individuellen Freiheit ist.

50 Urteil Digital Rights, Rn. 42.

51 Gutachten 1/15 (PNR-Abkommen EU–Kanada) vom 26. Juli 2017 (im Folgenden: Gutachten 1/15, EU:C:2017:592, Rn. 149 und die dort angeführte Rechtsprechung).

52 Urteil vom 15. Februar 2016, N. (C-601/15 PPU, EU:C:2016:84, Rn. 53).

53 Urteil Digital Rights, Rn. 42 und die dort angeführte Rechtsprechung.

54 Ebd., Rn. 51.

55 Gutachten 1/15, Rn. 149.

und muss daher im Rahmen der Bewertung dieser Verhältnismäßigkeit in vollem Umfang berücksichtigt werden. Anders ausgedrückt ist die Wahrung der Vertraulichkeit der Daten in einer demokratischen Gesellschaft zwar von wesentlicher Bedeutung, doch darf auch der Wert der Sicherheit nicht unterschätzt werden.

103. Der Kontext ernsthafter und anhaltender Bedrohungen der nationalen Sicherheit und insbesondere der Terrorismusgefahr darf somit nicht außer Betracht gelassen werden, wie es auch im letzten Satz von Rn. 119 des Urteils Tele2 Sverige und Watson heißt. Ein nationales System kann auf eine Art und Weise reagieren, die in einem zu Wesen und Intensität der existierenden Bedrohungen angemessenen Verhältnis steht, ohne dass diese Reaktion zwangsläufig die gleiche sein muss wie die anderer Mitgliedstaaten.

104. Ich muss abschließend hinzufügen, dass die vorstehenden Überlegungen nicht ausschließen, dass die nationalen Rechtsvorschriften in bestimmten *Ausnahmesituationen*, die sich durch eine unmittelbar bevorstehende Bedrohung oder eine außergewöhnliche Gefahr auszeichnen und in dem Mitgliedstaat eine offizielle Notstandserklärung rechtfertigen, für einen begrenzten Zeitraum eine so weitgehende und allgemeine Pflicht zur Vorratsspeicherung, wie es für erforderlich erachtet wird, auferlegen können [56].

105. Folglich sollte die erste Vorlagefrage der beiden Vorabentscheidungsersuchen umformuliert werden, so dass sie sich eher auf die Möglichkeit der Rechtfertigung eines Eingriffs mit Gründen der nationalen Sicherheit bezieht. Die Frage wäre daher, ob die den Betreibern elektronischer Kommunikationsdienste auferlegte Verpflichtung mit Art. 15 Abs. 1 der Richtlinie 2002/58 vereinbar ist.

b) Würdigung

1) Eigenschaften der internen Rechtsvorschriften gemäß den beiden Vorabentscheidungsersuchen im Licht der Rechtsprechung des Gerichtshofs

106. Gemäß den Vorlagebeschlüssen enthalten die in den Ausgangsverfahren streitigen Vorschriften eine Pflicht zur Vorratsspeicherung:

– für Betreiber elektronischer Kommunikationsdienste und insbesondere Personen, die der Öffentlichkeit einen Online-Zugang zu Kommunikationsdiensten anbieten, und

– für natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Töne, Bilder oder Botschaften jeder Art gewährleisten [57].

107. Die Betreiber sind verpflichtet, für ein Jahr ab dem Tag der Speicherung Angaben, die es erlauben, die Identität des Nutzers festzustellen, Daten über die verwendeten Kommunikationsendgeräte, technische Merkmale sowie Datum, Uhrzeit und Dauer des Telefonats, Daten über die beantragten oder ausgeführten Zusatzleistungen und deren Betreiber, Daten, die es erlauben, die Identität des Adressaten der Nachrichtenübermittlung festzustellen, sowie bei Telefonaktivitäten Angaben zu Ursprung und Standort der Nachrichtenübermittlung aufzubewahren [58].

56 Vgl. Nrn. 105 bis 107 meiner Schlussanträge in der Rechtssache C-520/18.

57 Dies ergibt sich aus Art. L. 851-1 des Gesetzbuches über innere Sicherheit, der auf Art. L. 34-1 des Gesetzbuchs für Post und elektronische Kommunikation und auf Art. 6 des Gesetzes Nr. 2004-575 über das Vertrauen in die digitale Wirtschaft verweist.

58 So festgelegt in Art. R. 10-13 des Gesetzbuchs für Post und elektronische Kommunikation.

108. Was speziell Internetzugangsdienste und Speicherdienste betrifft, verpflichten die nationalen Vorschriften zur Speicherung der IP-Adressen [59], der Passwörter, der Zahlungsart, falls ein Vertragsabschluss oder ein Zahlungskonto vorliegt, sowie der Referenz, des Betrags, des Datums und der Uhrzeit der Transaktion [60].

109. Diese Pflicht zur Speicherung besteht für die Ermittlung, Aufdeckung und Verfolgung von Straftaten [61]. Anders als – wie hier gezeigt werden wird – die Pflicht zur *Sammlung* von Verkehrs- und Standortdaten zielt die Pflicht zur *Speicherung* nicht nur auf die Verhütung von Terrorismus ab [62].

110. In Bezug auf die Voraussetzungen für den *Zugang* zu den gespeicherten Daten lässt sich den Vorlagebeschlüssen entnehmen, dass dieser Zugang entweder den allgemeinen Voraussetzungen (Eingreifen einer Justizbehörde) unterliegt oder auf einzeln ernannte und bevollmächtigte Beamte beschränkt ist, nachdem der Premierminister auf der Grundlage einer unverbindlichen Stellungnahme einer unabhängigen Verwaltungsbehörde [63] eine entsprechende Genehmigung erteilt hat.

111. Wie die Kommission anmerkt [64], fällt auf, dass die Daten, zu deren Speicherung die nationalen Vorschriften verpflichten, im Wesentlichen den Daten entsprechen, die der Gerichtshof in den Urteilen Digital Rights und Tele2 Sverige und Watson analysiert hat [65]. Wie bei jenen Rechtssachen unterliegen diese Daten einer „Pflicht zur allgemeinen und unterschiedslosen Speicherung“, was der Conseil d'État (Staatsrat) zu Beginn seiner Vorlagefragen ganz offen feststellt.

112. Sofern dies der Fall ist, was letztlich das vorlegende Gericht zu beurteilen hat, muss der Schluss gezogen werden, dass die streitigen Vorschriften einen „Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte … von großem Ausmaß [darstellen] und als besonders schwerwiegend anzusehen“ sind [66].

113. Keine der beteiligten Parteien hat in Frage gestellt, dass Vorschriften mit solchen Eigenschaften einen Eingriff in diese Rechte darstellen. Es ist daher nicht erforderlich, sich mit diesem Punkt zu befassen, und es muss auch nicht daran erinnert werden, dass die Verletzung dieser Rechte unweigerlich zu einer Beeinträchtigung der Grundfesten einer Gesellschaft führt, deren Ziel neben anderen Werten der Schutz der in der Charta verankerten Privatsphäre ist.

114. Aus der Rechtsprechung, die mit dem Urteil Tele2 Sverige und Watson begründet und mit dem Urteil Ministerio Fiscal bestätigt wurde, ergibt sich, dass Vorschriften wie die im Ausgangsverfahren in Rede stehenden „die Grenzen des absolut Notwendigen [überschreiten] und … nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden [können], wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt“ [67].

59 Für die Überprüfung dieses Punktes, der in der mündlichen Verhandlung streitig war, ist das vorlegende Gericht zuständig.

60 Art. 1 des Dekrets Nr. 2011-219.

61 Art. R. 10-13 des Gesetzbuchs für Post und elektronische Kommunikation.

62 Sowohl La Quadrature du Net als auch die Fédération des fournisseurs d'accès à Internet associatifs betonen die Vielzahl der Zwecke, denen die Speicherung dient, das den Behörden übertragene Ermessen, das Fehlen objektiver Kriterien bei der Definition und die Bedeutung, die nicht als schwerwiegend einzustufenden Formen der Kriminalität zugemessen wird.

63 Die Commission nationale de contrôle des techniques de renseignement (Nationale Kommission für die Kontrolle nachrichtendienstlicher Techniken). Vgl. hierzu Rn. 145 bis 148 der schriftlichen Erklärungen der französischen Regierung.

64 Rn. 60 der schriftlichen Erklärungen der Kommission.

65 Tatsächlich sind die Daten hier etwas umfangreicher, da für Internetzugangsdienste auch die Speicherung der IP-Adresse oder der Passwörter vorgesehen ist.

66 Urteil Tele2 Sverige und Watson, Rn. 100.

67 Ebd., Rn. 107.

115. Wie die im Urteil Tele2 Sverige und Watson geprüfte Regelung erstreckt sich auch die hier fragliche „allgemein auf alle Teilnehmer und registrierten Nutzer … und [erfasst] alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten [und sieht] keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor“ [68]. Sie gilt folglich „auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte“, und sieht keine Ausnahme vor, „so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen“ [69].

116. Die streitige Regelung verlangt auch keinen „Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten“ [70].

117. Daraus folgt, dass diese Regelung „die Grenzen des absolut Notwendigen [überschreitet] und … nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden [kann], wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt“ [71].

118. Die vorstehenden Erwägungen veranlassten den Gerichtshof, festzustellen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 den entsprechenden nationalen Vorschriften entgegensteht, „die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel“ vorsehen [72].

119. Es stellt sich nun die Frage, ob die Rechtsprechung des Gerichtshofs über die Vorratsspeicherung personenbezogener Daten wenn nicht erneuert, so doch zumindest angepasst werden sollte, wenn der Zweck dieser „allgemeinen und unterschiedslosen“ Speicherung die Terrorismusbekämpfung ist. Die erste Vorlagefrage in der Rechtssache C-511/18 stellt sich in „einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere durch die Gefahr des Terrorismus, gekennzeichneten Kontext“.

120. Wenn dies der *tatsächliche Zusammenhang* ist, in dem die Pflicht zur Vorratsspeicherung auferlegt wird, so bezweckt diese in ihrem *rechtlichen Zusammenhang* jedoch nicht nur die Terrorismusbekämpfung. Die vor dem Conseil d'État (Staatsrat) streitige Regelung über Datenspeicherung und Zugang zu den Daten knüpft diese Pflicht an Zwecke der allgemeinen Ermittlung, Aufdeckung und Verfolgung von Straftaten.

121. Ich möchte auf jeden Fall darauf hinweisen, dass die Terrorismusbekämpfung auch in den Ausführungen im Urteil Tele2 Sverige und Watson genannt wurde, der Gerichtshof jedoch nicht der Ansicht war, dass diese Art der Kriminalität eine Änderung seiner Rechtsprechung erfordern würde [73].

122. Daher bin ich grundsätzlich der Überzeugung, dass die Frage des vorlegenden Gerichts, die die Besonderheit der terroristischen Bedrohung in den Vordergrund stellt, in dem Sinne, in dem der Gerichtshof im Urteil Tele2 Sverige und Watson entschieden hat, beantwortet werden sollte.

68 Ebd., Rn. 105.

69 Ebd.

70 Urteil Tele2 Sverige und Watson, Rn. 106.

71 Ebd., Rn. 107.

72 Ebd., Rn. 112.

73 Ebd., Rn. 103.

123. Wie ich in den Schlussanträgen in der Rechtssache Stichting Brein festgestellt habe, zwingt „[d]ie Sicherheit der Rechtsanwendung … die Gerichte, wenn nicht zur starren Anwendung des *Stare-decisis* -Grundsatzes, so doch zu der Umsicht, sich an das zu halten, was sie nach reiflicher Überlegung zu einem juristischen Problem selbst entschieden haben“ [74].

2) Eingeschränkte Datenspeicherung bei Bedrohungen der Sicherheit des Staates, einschließlich einer terroristischen Bedrohung

124. Ist es dennoch möglich, diese Rechtsprechung in Anbetracht ihrer Auswirkungen auf den Kampf gegen den Terrorismus bzw. auf den Schutz des Staates vor ähnlichen Bedrohungen für die nationale Sicherheit anzupassen oder zu ergänzen?

125. Ich habe bereits darauf hingewiesen, dass die bloße Speicherung personenbezogener Daten einen Eingriff in die in den Art. 7, 8 und 11 der Charta garantierten Rechte darstellt [75]. Unabhängig davon, dass mit der Datenspeicherung letztlich ein gleichzeitiger oder rückwirkender *Zugang* zu den Daten zu einem bestimmten Zeitpunkt bezweckt wird [76], stellt eine Datenspeicherung, die über das für die Übermittlung einer Nachricht oder die Abrechnung der vom Betreiber erbrachten Dienste unbedingt erforderliche Maß hinausgeht, einen Verstoß gegen die in den Art. 5 und 6 der Richtlinie 2002/58 festgelegten Grenzen dar.

126. Die Nutzer dieser Dienste (d. h. in Wirklichkeit fast alle Bürger der entwickelten Gesellschaften) können mit Recht erwarten bzw. sollten mit Recht erwarten können, dass ohne ihre Zustimmung keine weiteren Daten gespeichert werden als die, die in Übereinstimmung mit diesen Rechtsvorschriften gespeichert werden dürfen. Die Ausnahmen des Art. 15 Abs. 1 der Richtlinie 2002/58 sind vor dem Hintergrund dieser Prämisse zu sehen.

127. Wie ich bereits erläutert habe, hat der Gerichtshof im Urteil Tele2 Sverige und Watson, auch in Bezug auf die Terrorismusbekämpfung, eine allgemeine und unterschiedslose Vorratsspeicherung personenbezogener Daten abgelehnt [77].

128. Entgegen der geäußerten Kritik bin ich nicht der Ansicht, dass in diesem Urteil die terroristische Bedrohung als besonders schwere Form der Kriminalität, die ausdrücklich auf einen Angriff auf die Staatsgewalt und die Destabilisierung und Zerstörung der staatlichen Institutionen abzielt, unterschätzt wird. Die Bekämpfung des Terrorismus ist für den Staat buchstäblich lebenswichtig, und ihr Erfolg stellt ein dem Gemeinwohl dienendes Ziel dar, auf das der Rechtsstaat nicht verzichten kann.

74 Rechtssache C-527/15, EU:C:2016:938, Nr. 41.

75 Wie der Gerichtshof im Gutachten 1/15, Rn. 124, erneut betont hat, „stellt die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht dar. Dasselbe gilt für die Speicherung personenbezogener Daten und den Zugang zu den Daten zu ihrer Verwendung durch die Behörden. Für die Feststellung eines solchen Eingriffs kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben“.

76 Wie Generalanwalt Cruz Villalón in den Schlussanträgen in der Rechtssache Digital Rights, C-293/12 und C-594/12 (EU:C:2013:845, Nr. 72), festgestellt hat, „stellen die Erhebung und vor allem die Vorratsspeicherung vielfältiger, im Rahmen des größten Teils der laufenden elektronischen Kommunikation der Unionsbürger erzeugter oder verarbeiteter Daten in gigantischen Datenbanken selbst dann einen qualifizierten Eingriff in das Privatleben dieser Bürger dar, wenn sie nur die Voraussetzungen dafür schaffen würden, dass ihre sowohl persönlichen als auch beruflichen Tätigkeiten nachträglich kontrolliert werden können. Die Erhebung dieser Daten schafft die Voraussetzungen für eine Überwachung, die, auch wenn sie nur vergangenheitsbezogen bei ihrer Auswertung erfolgt, das Recht der Unionsbürger auf das Geheimnis ihres Privatlebens gleichwohl während der gesamten Dauer der Vorratsspeicherung permanent bedroht. Aufgrund des erzeugten diffusen Gefühls des Überwachtwerdens stellt sich die Frage nach der Dauer der Vorratsdatenspeicherung in besonders eindringlicher Weise“.

77 Urteil Tele2 Sverige und Watson, Rn. 103: „[E]ine solche … Zielsetzung kann jedoch … für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen“.

129. Fast alle am Verfahren beteiligten Regierungen sowie die Kommission sind sich einig, dass – abgesehen von den technischen Schwierigkeiten – eine teilweise und differenzierte Speicherung personenbezogener Daten den nationalen Nachrichtendiensten die Möglichkeit des Zugangs zu Informationen nehmen würde, die für die Erkennung von Gefahren für die öffentliche Sicherheit und die Verteidigung des Staates sowie für die Verfolgung der Täter von Terroranschlägen unentbehrlich sind [78].

130. Dieser Auffassung möchte ich entgegensetzen, dass die Terrorismusbekämpfung nicht nur aus dem Blickwinkel der Wirksamkeit betrachtet werden sollte. Es zeigt die Schwierigkeit, aber auch die wahre Größe der Terrorismusbekämpfung, wenn ihre Mittel und Methoden den Erfordernissen des Rechtsstaats entsprechen, der in erster Linie bedeutet, dass Macht und Stärke den Grenzen des Gesetzes und insbesondere einer Rechtsordnung, deren Grund und Zweck die Verteidigung der Grundrechte ist, unterliegen.

131. Während der Terrorismus seine Mittel allein mit der bloßen (und größtmöglichen) Wirksamkeit seiner Angriffe auf die bestehende Ordnung rechtfertigt, wird die Wirksamkeit des Rechtsstaats in Begriffen gemessen, die nicht zulassen, dass zu seiner Verteidigung auf die Verfahren und Garantien, die ihn als rechtmäßige Ordnung qualifizieren, verzichtet wird. Wenn sich der Rechtsstaat allein auf die Wirksamkeit konzentriert, verliert er die Eigenschaft, die ihn auszeichnet, und kann im Extremfall selbst zu einer Bedrohung für den Bürger werden. Werden staatliche Stellen mit unangemessen weitreichenden Instrumenten zur Verbrechensbekämpfung, mit denen sie die Grundrechte ignorieren oder entkräften könnten, ausgestattet, lässt sich nicht mehr gewährleisten, dass sich ihr unkontrolliertes und uneingeschränktes Handeln nicht letztlich zum Nachteil der Freiheit aller wendet.

132. Für die Wirksamkeit der Handlungen der staatlichen Stellen besteht, wie ich hier noch einmal wiederholen möchte, eine unüberwindliche Barriere in Form der Grundrechte der Bürger, die nach Art. 52 Abs. 1 der Charta nur durch Gesetz und unter Wahrung ihres wesentlichen Inhalts eingeschränkt werden dürfen, sofern die Einschränkungen „erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“ [79].

133. Für die Bedingungen, unter denen nach dem Urteil Tele2 Sverige und Watson eine *gezielte* Vorratsspeicherung zulässig wäre, verweise ich auf meine Schlussanträge in der Rechtssache C-520/18 [80].

134. Umstände, unter denen die den Sicherheitsbehörden verfügbaren Informationen den begründeten Verdacht der Vorbereitung eines Terroranschlags zulassen, können einen rechtmäßigen Grund für eine Verpflichtung zur Speicherung bestimmter Daten darstellen. Dies gilt erst recht für die tatsächliche Begehung eines Anschlags. Während in letzterem Fall die Begehung der Straftat an sich ein

78 Diesen Standpunkt vertritt z. B. die französische Regierung, die dafür konkrete Beispiele der Nützlichkeit einer allgemeinen Vorratsspeicherung anführt, die es dem Staat ermöglicht hat, auf die in den letzten Jahren in Frankreich verübten schweren Terroranschläge zu reagieren (Rn. 107 und Rn. 122 bis 126 der schriftlichen Erklärungen der französischen Regierung).

79 Urteil vom 15. Februar 2016, N. (C-601/15 PPU, EU:C:2016:84, Rn. 50). Es handelt sich somit um ein schwer zu erzielendes Gleichgewicht zwischen öffentlicher Ordnung und Freiheit, auf das ich bereits hingewiesen habe und das grundsätzlich alle Rechtsvorschriften der Union zum Ziel haben. Als Beispiel soll hier die Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. 2017, L 88, S. 6) genannt werden. Während die Mitgliedstaaten nach Art. 20 Abs. 1 der Richtlinie sicherstellen müssen, dass den für die Ermittlung oder strafrechtliche Verfolgung der terroristischen Straftaten zuständigen Personen, Stellen oder Diensten „wirksame Ermittlungsinstrumente … zur Verfügung stehen“, heißt es im 21. Erwägungsgrund, dass der Einsatz dieser wirksamen Instrumente „gezielt erfolgen und dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragen und … das Recht auf den Schutz personenbezogener Daten achten“ sollte.

80 Nrn. 87 bis 95.

Rechtfertigungsgrund für die Datenspeicherung sein kann, wäre es bei einem bloßen Verdacht eines Anschlags erforderlich, dass die dem Verdacht zugrunde liegenden Umstände ein Mindestmaß an Plausibilität aufweisen, was eine wesentliche Voraussetzung für eine objektive Abwägung der rechtfertigenden Umstände ist.

135. Es ist zwar schwierig, aber nicht unmöglich, die Kategorien von Daten, deren Speicherung als erforderlich angesehen wird, und den Kreis der betroffenen Personen nach objektiven Kriterien präzise festzulegen. Am *praktischsten und effizientesten* wäre sicherlich die allgemeine und unterschiedslose Speicherung aller Daten, die von den Betreibern elektronischer Kommunikationsdienste erhoben werden können, doch habe ich bereits darauf hingewiesen, dass über diese Frage nicht anhand der *tatsächlichen Effizienz*, sondern anhand der *rechtlichen Effizienz* im Rahmen eines Rechtsstaats entschieden werden muss.

136. Für diese Feststellung ist – innerhalb der in der Rechtsprechung des Gerichtshofs vorgegebenen Grenzen – in der Regel der Gesetzgeber zuständig. Hierfür verweise ich erneut auf meine Schlussanträge in der Rechtssache C-520/18 [81].

3) Zugang zu den gespeicherten Daten

137. Unter der Voraussetzung, dass die Betreiber die Daten in einer der Richtlinie 2002/58 entsprechenden Art und Weise erhoben haben und dass die Speicherung gemäß Art. 15 Abs. 1 erfolgt ist [82], dürfen die zuständigen Behörden unter den Bedingungen, die der Gerichtshof genannt hat und die ich in meinen Schlussanträgen in der Rechtssache C-520/18, auf die ich mich beziehe, analysiere, auf diese Informationen zugreifen [83].

138. Auch im vorliegenden Fall muss die nationale Regelung die materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten festlegen [84]. Im Kontext dieser Vorabentscheidungsersuchen müssten diese Voraussetzungen den Zugang zu den Daten von Personen ermöglichen, die im Verdacht stehen, eine terroristische Straftat zu planen, zu begehen oder begangen zu haben oder in eine solche Straftat verwickelt zu sein [85].

139. Es ist also unabdingbar, dass der Zugang zu den entsprechenden Daten – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung auf einen mit Gründen versehenen Antrag der zuständigen Behörden ergeht, unterworfen wird [86]. Dort, wo eine abstrakte Überprüfung durch das Gesetz nicht ausreicht, wird somit eine *konkrete* Überprüfung durch eine unabhängige Behörde gewährleistet, die gleichermaßen an die Garantie der Sicherheit des Staates und an die Verteidigung der Grundrechte der Bürger gebunden ist.

81 Nrn. 100 bis 107.

82 Sofern die in Rn. 122 des Urteils Tele2 Sverige und Watson genannten Bedingungen erfüllt sind: Der Gerichtshof hat darauf hingewiesen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 es den Mitgliedstaaten nicht erlaubt, von Art. 4 Abs. 1 und Art. 4 Abs. 1a abzuweichen, nach denen die Betreiber Maßnahmen ergreifen müssen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor unberechtigtem Zugang geschützt sind. In diesem Sinne hat er festgestellt: „Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind."

83 Nrn. 52 bis 60.

84 Urteil Tele2 Sverige und Watson, Rn. 118.

85 Ebd., Rn. 119.

86 Ebd., Rn. 120.

4) Pflicht zur Speicherung von Daten, mit denen die Identität der Urheber von Inhalten festgestellt werden kann, im Licht der Richtlinie 2000/31 (zweite Vorlagefrage in der Rechtssache C-512/18)

140. Das vorlegende Gericht verweist auf die Richtlinie 2000/31 als Bezugspunkt für die Klärung der Frage, ob bestimmte Personen[87] und Betreiber öffentlich zugänglicher Kommunikationsdienste verpflichtet werden können, „Daten so zu speichern, dass jede Person, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat, identifiziert werden kann, damit die Justizbehörde gegebenenfalls ihre Übermittlung verlangen kann, um für die Beachtung der Vorschriften über die zivil- oder strafrechtliche Haftung zu sorgen".

141. Ich stimme mit der Kommission darin überein, dass nicht geprüft werden muss, ob diese Pflicht mit der Richtlinie 2000/31[88] vereinbar ist, da die Richtlinie nach ihrem Art. 1 Abs. 5 Buchst. b auf „Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien 95/46/EG und 97/66/EG erfasst werden", keine Anwendung findet. Diese Richtlinien entsprechen der Verordnung 2016/679 und der Richtlinie 2002/58[89], deren Art. 23 Abs. 1 bzw. Art. 15 Abs. 1 meiner Ansicht nach wie oben erläutert auszulegen sind.

2. Pflicht zur Sammlung von Verkehrs- und Standortdaten in Echtzeit (zweite Vorlagefrage in der Rechtssache C-511/18)

142. Dem vorlegenden Gericht zufolge gestattet Art. L. 851-2 des Gesetzbuchs über innere Sicherheit die Sammlung in Echtzeit von Informationen über Personen, bei denen zuvor festgestellt wurde, dass sie Verbindungen zu einer terroristischen Bedrohung haben könnten, ausschließlich für die Zwecke der Verhütung von Terrorismus. Ebenso gestattet Art. L. 851-4 dieses Gesetzbuchs, dass die Betreiber die technischen Daten über den Standort der Endgeräte in Echtzeit übermitteln.

143. Das vorlegende Gericht vertritt den Standpunkt, dass diese Techniken die betreffenden Anbieter nicht mit einem zusätzlichen Speicherungserfordernis belasteten, das über das hinausgehe, was zur Inrechnungstellung ihrer Dienste und deren Vermarktung erforderlich sei.

144. Nach Art. L. 851-3 des Gesetzbuchs über innere Sicherheit können Anbieter elektronischer Kommunikationsdienste und technische Dienstleister ferner verpflichtet werden, „in ihren Netzen automatisierte Verarbeitungen einzusetzen, die dazu dienen, anhand der in der Genehmigung aufgeführten Parameter Verbindungen aufzuspüren, die auf eine terroristische Bedrohung hinweisen können". Diese Technik, die keine allgemeine und unterschiedslose Vorratsspeicherung impliziert, zielt ausschließlich darauf ab, für begrenzte Zeit die Verbindungsdaten zu sammeln, die einen Zusammenhang mit einer terroristischen Straftat aufweisen könnten.

145. Meiner Auffassung nach müssen die Bedingungen für den Zugang zu gespeicherten personenbezogenen Daten auch für den Zugang zu den während der elektronischen Kommunikation erzeugten Daten in Echtzeit gelten. Ich beziehe mich insoweit auf meine entsprechenden Ausführungen. Es ist unerheblich, ob es sich um gespeicherte Daten oder um in Echtzeit gewonnene Daten handelt, da in beiden Fällen personenbezogene Daten, unabhängig davon, ob diese aus der Vergangenheit oder aus der Gegenwart stammen, offengelegt werden.

87 Personen, „die … zur Bereitstellung für die Öffentlichkeit durch öffentliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Botschaften jeder Art gewährleisten".

88 Diese Richtlinie wird vom vorlegenden Gericht in der zweiten Vorlagefrage der Rechtssache C-512/18 allgemein und ohne nähere Angabe einer konkreten Bestimmung genannt.

89 Rn. 112 und 113 der schriftlichen Erklärungen der Kommission.

146. Ist der Zugang in Echtzeit die Folge dessen, dass durch eine automatisierte Verarbeitung im Sinne von Art. L. 851-3 des Gesetzbuchs über innere Sicherheit Verbindungen aufgespürt wurden, müssen die für diese Verarbeitung im Voraus festgelegten Modelle und Kriterien spezifisch, zuverlässig und nicht diskriminierend sein, so dass sie die Identifizierung von Personen ermöglichen, gegen die ein begründeter Verdacht der Beteiligung an terroristischen Straftaten bestehen könnte [90].

3. Pflicht zur Unterrichtung der betroffenen Personen (dritte Vorlagefrage in der Rechtssache C-511/18)

147. Der Gerichtshof hat entschieden, dass die Behörden, denen Zugang zu den Daten gewährt wird, die betroffenen Personen davon in Kenntnis setzen müssen, sobald dies die laufenden Ermittlungen nicht mehr beeinträchtigen kann. Begründet wird diese Verpflichtung damit, dass diese Information erforderlich ist, damit die betroffenen Personen das Recht auf Einlegung eines Rechtsbehelfs ausüben können, das in Art. 15 Abs. 2 der Richtlinie 2002/58 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist [91].

148. Mit seiner dritten Vorlagefrage in der Rechtssache C-511/18 möchte der Conseil d'État (Staatsrat) wissen, ob diese Informationspflicht auf jeden Fall gilt oder ob sie, wenn andere Garantien wie die in seinem Vorlagebeschluss genannten vorgesehen sind, außer Acht gelassen werden kann.

149. Nach seinen Angaben [92] beschränken sich die genannten Garantien darauf, dass sich Personen, die prüfen lassen möchten, ob eine nachrichtendienstliche Technik in unzulässiger Weise eingesetzt wurde, an ihn wenden können. Er erklärt dann gegebenenfalls im Rahmen eines Verfahrens, das den in Gerichtsverfahren üblichen Grundsatz des kontradiktorischen Verfahrens nicht berücksichtigt, die Genehmigung der Maßnahme für nichtig und ordnet die Vernichtung der gesammelten Informationen an.

150. Das vorlegende Gericht ist der Ansicht, dass diese Rechtsvorschriften das Recht auf einen effektiven gerichtlichen Rechtsschutz nicht verletzten. Ich hingegen vertrete den Standpunkt, dass dies zwar theoretisch für diejenigen zutrifft, die prüfen wollen, ob sie Gegenstand nachrichtendienstlicher Tätigkeiten sind. Bei denjenigen, die Gegenstand eines solchen Verfahrens sind oder waren und nicht darüber unterrichtet wurden und sich daher nicht die Frage stellen können, ob ihre Rechte verletzt wurden, liegt jedoch ein Verstoß gegen das Recht auf einen effektiven gerichtlichen Rechtsschutz vor.

151. Die vom vorlegenden Gericht angeführten Rechtsschutzgarantien scheinen davon abhängig zu sein, ob derjenige, der den Verdacht hat, dass Informationen über seine Person gesammelt werden, selbst die Initiative ergreift. Das Recht auf Zugang zu einem Gericht zur Verteidigung seiner Rechte muss jedoch für alle wirksam sein, was bedeutet, dass derjenige, dessen personenbezogene Daten verarbeitet wurden, die Möglichkeit haben muss, diese Verarbeitung gerichtlich auf ihre Rechtmäßigkeit überprüfen zu lassen, und dass er folglich darüber unterrichtet werden muss.

152. Nach den Angaben des vorlegenden Gerichts kann das gerichtliche Verfahren zwar von Amts wegen oder aufgrund einer Verwaltungsbeschwerde eingeleitet werden. Jedoch muss der Betroffene auf jeden Fall die Möglichkeit haben, das Verfahren selbst einzuleiten, und hierfür ist es notwendig, dass er über die Verarbeitung seiner personenbezogenen Daten unterrichtet wird. Die Verteidigung seiner Rechte darf nicht davon abhängig gemacht werden, dass er durch Dritte oder mit eigenen Mitteln von der Datenverarbeitung erfährt.

90 Urteil Digital Rights, Rn. 59.

91 Urteil Tele2 Sverige und Watson, Rn. 121.

92 Rn. 8 bis 11 des Vorlagebeschlusses.

153. Sofern also die behördlichen Ermittlungen, für die Zugang zu den gespeicherten Daten gewährt wird, nicht mehr beeinträchtigt werden können, ist die betroffene Person über den Zugang zu informieren.

154. Eine andere Frage ist, dass das gerichtliche Verfahren, nachdem die betroffene Person über den Zugang zu ihren Daten informiert wurde und sie das Verfahren eingeleitet hat, den Erfordernissen der Vertraulichkeit und Geheimhaltung entsprechen muss, die mit der Prüfung der Tätigkeit von Behörden in sensiblen Bereichen wie der Sicherheit und Verteidigung des Staates verbunden sind. Diese Frage ist jedoch nicht Gegenstand dieser Vorabentscheidungsersuchen, und deshalb halte ich es nicht für erforderlich, dass der Gerichtshof darüber entscheidet.

V. Ergebnis

155. Nach alledem schlage ich dem Gerichtshof vor, dem Conseil d'État (Staatsrat, Frankreich) wie folgt zu antworten:

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 Verbindung mit den Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union ist dahin auszulegen, dass er

1. nationalen Vorschriften entgegensteht, die in einem durch ernste und anhaltende Bedrohungen der nationalen Sicherheit, insbesondere durch die Gefahr des Terrorismus, gekennzeichneten Kontext den Betreibern und Anbietern elektronischer Kommunikationsdienste eine Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten aller Teilnehmer sowie der Daten auferlegen, mit denen die Personen, die zur Schaffung der Inhalte der erbrachten Dienste beigetragen haben, identifiziert werden können;

2. nationalen Vorschriften entgegensteht, die nicht die Pflicht vorsehen, die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten durch die zuständigen Behörden zu unterrichten, wenn diese Unterrichtung die behördlichen Maßnahmen nicht mehr beeinträchtigen kann;

3. nationalen Vorschriften, die die Sammlung von Verkehrs- und Standortdaten von Einzelpersonen in Echtzeit ermöglichen, dann nicht entgegensteht, wenn diese Maßnahmen nach den für den Zugang zu rechtmäßig gespeicherten personenbezogenen Daten festgelegten Verfahren und mit denselben Garantien ergriffen werden.