



# Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS  
HENRIK SAUGMANDSGAARD ØE  
vom 19. Juli 2016<sup>1</sup>

## Verbundene Rechtssachen C-203/15 und C-698/15

**Tele2 Sverige AB**  
**gegen**  
**Post- och telestyrelsen (C-203/15)**  
**und**  
**Secretary of State for the Home Department**  
**gegen**  
**Tom Watson,**  
**Peter Brice,**  
**Geoffrey Lewis,**  
**Beteiligte:**  
**Open Rights Group,**  
**Privacy International,**  
**Law Society of England and Wales (C-698/15)**

(Vorabentscheidungsersuchen des Kammarrätt i Stockholm [Verwaltungsgerichtshof Stockholm, Schweden] und des Court of Appeal [England & Wales] [Civil Division] [Berufungsgericht (England und Wales) (Abteilung für Zivilsachen), Vereinigtes Königreich])

„Vorlage zur Vorabentscheidung — Richtlinie 2002/58/EG — Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation — Innerstaatliche Rechtsvorschriften, die eine generelle Verpflichtung zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge vorschreiben — Art. 15 Abs. 1 — Charta der Grundrechte der Europäischen Union — Art. 7 — Recht auf Achtung der Privatsphäre — Art. 8 — Recht auf Schutz der personenbezogenen Daten — Schwerer Eingriff — Rechtfertigung — Art. 52 Abs. 1 — Voraussetzungen — Legitimes Ziel der Bekämpfung schwerer Kriminalität — Erfordernis einer gesetzlichen Grundlage im innerstaatlichen Recht — Erfordernis des absolut Notwendigen — Erfordernis der Verhältnismäßigkeit in einer demokratischen Gesellschaft“

## Inhaltsverzeichnis

I – Einleitung .....	3
II – Rechtlicher Rahmen .....	5

<sup>1</sup> — Originalsprache: Französisch.

A – Richtlinie 2002/58 .....	5
B – Schwedisches Recht .....	5
1. Umfang der Vorratsspeicherungspflicht .....	6
2. Zugang zu den auf Vorrat gespeicherten Daten .....	6
a) LEK .....	6
b) RB .....	6
c) Gesetz Nr. 2012:278 .....	7
3. Dauer der Vorratsspeicherung .....	7
4. Schutz und Sicherheit der auf Vorrat gespeicherten Daten.....	8
C – Recht des Vereinigten Königreichs .....	8
1. Umfang der Vorratsspeicherungspflicht .....	8
2. Zugang zu den auf Vorrat gespeicherten Daten .....	9
3. Dauer der Vorratsspeicherung .....	10
4. Schutz und Sicherheit der auf Vorrat gespeicherten Daten.....	10
III – Ausgangsverfahren und Vorlagefragen .....	11
A – Rechtssache C-203/15 .....	11
B – Rechtssache C-698/15 .....	12
IV – Verfahren vor dem Gerichtshof .....	12
V – Würdigung der Vorlagefragen.....	13
A – Zur Zulässigkeit der zweiten Frage in der Rechtssache C-698/15 .....	14
B – Zur Vereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung .....	15
1. Zur Geltung einer generellen Verpflichtung zur Vorratsspeicherung im Anwendungsbereich der Richtlinie 2002/58 .....	16
2. Zur Möglichkeit, durch die Einführung einer generellen Verpflichtung zur Vorratsspeicherung von der durch die Richtlinie 2002/58 geschaffenen Regelung abzuweichen .....	17
C – Zur Anwendbarkeit der Charta auf eine generelle Verpflichtung zur Vorratsspeicherung.....	20
D – Zur Vereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit den Anforderungen des Art. 15 Abs. 1 der Richtlinie 2002/58 und der Art. 7, 8 und 52 Abs. 1 der Charta .....	21
1. Zum Erfordernis einer gesetzlichen Grundlage im innerstaatlichen Recht.....	23

2. Zur Wahrung des Wesensgehalts der durch die Art. 7 und 8 der Charta anerkannten Rechte .....	26
3. Zum Bestehen einer dem Gemeinwohl dienenden Zielsetzung, die von der Union anerkannt wird und die eine generelle Verpflichtung zur Vorratsspeicherung rechtfertigen kann.....	26
4. Zur Geeignetheit einer generellen Verpflichtung zur Vorratsspeicherung im Hinblick auf die Bekämpfung schwerer Kriminalität .....	28
5. Zur Erforderlichkeit einer generellen Verpflichtung zur Vorratsspeicherung für die Bekämpfung schwerer Kriminalität .....	30
a) Zur Voraussetzung der absoluten Notwendigkeit einer generellen Verpflichtung zur Vorratsspeicherung .....	31
b) Zum zwingenden Charakter der vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien im Hinblick auf das Erfordernis des absolut Notwendigen .....	35
6. Zur Verhältnismäßigkeit einer generellen Verpflichtung zur Vorratsspeicherung in einer demokratischen Gesellschaft unter Berücksichtigung des Ziels der Bekämpfung schwerer Kriminalität .....	40
VI – Ergebnis .....	43

## I – Einleitung

1. 1788 schrieb James Madison, einer der Autoren der Verfassung der Vereinigten Staaten: „If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.“<sup>2</sup>

2. Die vorliegenden Rechtssachen stellen uns genau vor diese von Madison angeführte „große Schwierigkeit“. Sie betreffen die Vereinbarkeit innerstaatlicher Regelungen mit dem Unionsrecht, die zulasten der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes (im Folgenden: Betreiber) eine Pflicht zur Vorratsspeicherung von Daten elektronischer Kommunikationsvorgänge (im Folgenden: Kommunikationsdaten) begründen, die alle Kommunikationsmittel und alle Benutzer erfasst (im Folgenden: generelle Verpflichtung zur Vorratsspeicherung).

2 — „Wenn Menschen Engel wären, brauchte es keine Regierung. Wenn Engel Menschen regieren würden, gäbe es keinen Bedarf für externe oder interne Kontrollen der Regierung. Wenn man aber eine Regierung bilden will, die von Menschen über Menschen ausgeübt werden soll, dann besteht die große Schwierigkeit in Folgendem: Zuerst muss man der Regierung die Macht verleihen, die Regierten zu kontrollieren, dann aber muss man sie zwingen, sich selbst zu kontrollieren“, Madison, J., „Federalist No. 51“, in Hamilton, A., Madison, J., und Jay, J., Hrsg. Genovese, M. A., *The Federalist Papers*, Palsgrave Macmillan, New York, 2009, S. 120 (freie Übersetzung). Madison war einer der Hauptautoren und einer der 39 Unterzeichner der Verfassung der Vereinigten Staaten (1787). Er wurde später der vierte Präsident der Vereinigten Staaten (von 1809 bis 1817).

3. Zum einen ist die Regierung durch die Vorratsspeicherung von Kommunikationsdaten in der Lage, die „Regierten zu kontrollieren“, indem sie den zuständigen Behörden ein Ermittlungswerkzeug an die Hand gibt, das bei der Bekämpfung schwerer Kriminalität, vor allem bei der Terrorismusbekämpfung, ausgesprochen nützlich sein kann. Die Vorratsspeicherung dieser Daten verleiht den Behörden im Wesentlichen die begrenzte Fähigkeit, durch Zugriff auf die Kommunikationsdaten einer Person, die entstanden, bevor diese überhaupt einer Beziehung zur schweren Kriminalität verdächtigt wurde, „die Vergangenheit zu entschlüsseln“<sup>3</sup>.

4. Zum anderen jedoch ist es dringend geboten, angesichts der schwerwiegenden Gefahren, die mit der Existenz dieser sämtliche Kommunikationsvorgänge im nationalen Staatsgebiet erfassenden Datenbanken verbunden sind, sowohl im Hinblick auf die Vorratsspeicherung als auch auf den Zugang zu den gespeicherten Daten die Regierung zu „zwingen, sich selbst zu kontrollieren“. Diese sehr umfangreichen Datenbanken ermöglichen es nämlich jedem, der Zugang zu ihnen hat, die gesamte Bevölkerung sofort zu katalogisieren<sup>4</sup>. Diese Gefahren müssen genauestens erfasst werden, indem u. a. geprüft wird, ob generelle Verpflichtungen zur Vorratsspeicherung wie die in den Ausgangsverfahren fraglichen absolut erforderlich und verhältnismäßig sind.

5. Im Rahmen der vorliegenden Rechtssachen sind daher der Gerichtshof und die vorlegenden Gerichte aufgerufen, ein Gleichgewicht herzustellen zwischen einerseits der Pflicht der Mitgliedstaaten, die Sicherheit der sich in ihrem Hoheitsgebiet aufhaltenden Personen zu gewährleisten, und andererseits der Wahrung der in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten.

6. Vor dem Hintergrund dieser „großen Schwierigkeit“ werde ich die Fragen prüfen, die dem Gerichtshof in den vorliegenden Rechtssachen vorgelegt worden sind. Diese betreffen konkret die Vereinbarkeit nationaler Rechtsvorschriften, die eine generelle Verpflichtung zur Vorratsspeicherung begründen, mit der Richtlinie 2002/58/EG<sup>5</sup> und den Art. 7 und 8 der Charta. Um diese Fragen zu beantworten, wird der Gerichtshof insbesondere klarzustellen haben, wie das Urteil Digital Rights Ireland u. a. (im Folgenden: DRI-Urteil)<sup>6</sup>, mit dem die Große Kammer des Gerichtshofs die Richtlinie 2006/24/EG<sup>7</sup> für ungültig erklärte, in einem nationalen Kontext auszulegen ist.

7. Aus den nachfolgend darzulegenden Gründen bin ich der Meinung, dass die von einem Mitgliedstaat eingeführte generelle Verpflichtung zur Vorratsspeicherung mit den im Unionsrecht verankerten Grundrechten vereinbar sein kann, sofern sie durch eine Reihe von Garantien, die ich im Zuge meiner Ausführungen benennen werde, eng eingegrenzt ist.

3 — Diese begrenzte Möglichkeit, „die Vergangenheit zu entschlüsseln“, kann vor allem bei der Identifizierung möglicher Komplizen von großem Nutzen sein, siehe Nrn. 178 bis 184 dieser Schlussanträge.

4 — Siehe Nrn. 252 bis 261 dieser Schlussanträge.

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) in der Fassung der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11).

6 — Urteil vom 8. April 2014 (C-293/12 und C-594/12, EU:C:2014:238).

7 — 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).

## II – Rechtlicher Rahmen

### A – Richtlinie 2002/58

8. Art. 1 („Geltungsbereich und Zielsetzung“) der Richtlinie 2002/58 lautet:

„(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 [Europäischen Union] zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46 ... im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des [AEUV] fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI [EUV], 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.“

9. In Abs. 1 von Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie 2002/58 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 ... für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.“

### B – Schwedisches Recht

10. Die – inzwischen für ungültig erklärte – Richtlinie 2006/24 wurde in schwedisches Recht umgesetzt durch Änderungen des Lag (2003:389) om elektronisk kommunikation (schwedisches Gesetz Nr. 2003:389 über die elektronische Kommunikation, im Folgenden: LEK) sowie der Förordning (2003:396) om elektronisk kommunikation (Verordnung Nr. 2003:396 über die elektronische Kommunikation, im Folgenden: FEK), die beide am 1. Mai 2012 in Kraft traten.

## 1. Umfang der Vorratsspeicherungspflicht

11. Nach Kapitel 6 § 16a LEK ist ein Betreiber zur Vorratsspeicherung der Kommunikationsdaten verpflichtet, die zur Identifizierung einer Nachricht, des Adressaten der Nachricht, zur Bestimmung von Datum, Uhrzeit und Dauer der Nachrichtenübermittlung, der Art einer Nachrichtenübermittlung sowie der Endeinrichtung und des Standorts mobiler Geräte bei Beginn und Ende der Nachrichtenübermittlung notwendig sind. Die Art der zu speichernden Daten ist im Einzelnen in den §§ 38 bis 43 FEK geregelt.

12. Diese Verpflichtung zur Vorratsspeicherung erstreckt sich auf Daten, die von einem Telefoniedienst, bei der Mobilfunktelefonie, bei der elektronischen Nachrichtenübermittlung, beim Internetzugang und bei der Bereitstellung von Kapazität für den Internetzugang verarbeitet werden.

13. Die auf Vorrat zu speichernden Daten umfassen nicht nur alle Daten, die im Rahmen der Richtlinie 2006/24 zu speichern waren, sondern auch Daten über erfolglose Anrufe und Daten über den Standort, an dem ein mittels Mobilfunk getätigter Anruf endet. Nach den Vorstellungen, die dieser Richtlinie zugrunde lagen, umfassen die zu speichernden Daten nicht den Inhalt einer Kommunikation.

## 2. Zugang zu den auf Vorrat gespeicherten Daten

14. Für den Zugang zu den auf Vorrat gespeicherten Daten gelten drei Gesetze, nämlich das LEK, die Rättegångsbalk (Gerichtsverfahrensordnung, im Folgenden: RB) und das Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (schwedisches Gesetz Nr. 2012:278 über die Erfassung von Daten über die elektronische Kommunikation bei den Ermittlungstätigkeiten der Strafverfolgungsbehörde).

### a) LEK

15. Gemäß Kapitel 6 § 22 Abs. 1 Nr. 2 LEK hat der Betreiber einer Strafverfolgungsbehörde, der Polizeibehörde, der Säkerhetspolis (schwedische Sicherheitspolizei, im Folgenden: Säpo) oder einer sonstigen mit der Kriminalitätsbekämpfung betrauten Behörde auf Verlangen Teilnehmeranschlussdaten zu übergeben, falls sich die Daten auf eine mutmaßliche Straftat beziehen. Nach der genannten Vorschrift braucht es sich nicht um eine schwere Straftat zu handeln.

16. Der Begriff „Teilnehmeranschlussdaten“ bezeichnet in erster Linie Daten über Name, Anrede, Anschrift, Telefonnummer und IP-Adresse (Internetprotokolladresse).

17. Die Übergabe der Teilnehmeranschlussdaten nach Maßgabe des LEK setzt keine vorherige Kontrolle voraus, kann jedoch im Nachhinein von der Verwaltung überprüft werden. Das Recht staatlicher Bediensteter auf Zugang zu den Daten unterliegt im Übrigen keinen Einschränkungen.

### b) RB

18. Die RB regelt die Überwachung elektronischer Kommunikationsvorgänge im Rahmen von Voruntersuchungen.

19. Die Überwachung elektronischer Kommunikationsvorgänge ist im Wesentlichen nur zulässig, wenn der begründete Verdacht besteht, dass jemand eine Straftat, die mit Freiheitsstrafe von mindestens sechs Monaten bedroht ist, oder eine andere besonders aufgeführte Straftat begangen hat, und wenn diese Maßnahme für die Ermittlungen von besonderer Bedeutung ist.

20. Darüber hinaus ist diese Überwachung zulässig zum Zweck der Durchführung von Ermittlungen wegen einer Straftat, die mit einer Freiheitsstrafe von mindestens zwei Jahren bedroht ist, um festzustellen, wer dieser Straftat hinreichend verdächtig ist, wenn diese Maßnahme für die Ermittlungen von besonderer Bedeutung ist.

21. Nach Kapitel 27 § 21 der RB hat die Strafverfolgungsbehörde in der Regel vor Beginn der Überwachung der elektronischen Kommunikationsvorgänge die Genehmigung des zuständigen Gerichts einzuholen.

22. Ist die Befassung des zuständigen Gerichts noch vor der Einleitung der für die Ermittlungen zwingend erforderlichen Überwachung elektronischer Kommunikationsvorgänge offensichtlich unvereinbar mit der Dringlichkeit ihrer Durchführung oder käme es hierdurch zu Behinderungen, wird die Genehmigung gleichwohl bis zur Entscheidung des Gerichts von der Staatsanwaltschaft erteilt. Die Staatsanwaltschaft hat das Gericht hiervon unverzüglich schriftlich zu unterrichten. Das Gericht prüft umgehend, ob die Maßnahme begründet ist.

c) Gesetz Nr. 2012:278

23. Bei der Beschaffung von Informationen können nach § 1 des Gesetzes Nr. 2012:278 die Polizeibehörde, die Säpo und die Tullverk (schwedische Zollbehörde) unter den in diesem Gesetz festgelegten Voraussetzungen bei einem Betreiber ohne dessen Wissen Kommunikationsdaten erfassen.

24. Nach den §§ 2 und 3 des Gesetzes Nr. 2012:278 dürfen die Daten erfasst werden, wenn die Maßnahme nach den Umständen für die Verhütung, Abwendung oder Feststellung krimineller Handlungen von Bedeutung ist und diese kriminellen Handlungen Straftaten umfassen, die mit einer Freiheitsstrafe von mindestens zwei Jahren bedroht oder in § 3 aufgeführt sind (einschließlich verschiedener Formen der Sabotage und Spionage).

25. Die Entscheidung über die Vornahme dieser Maßnahme wird vom Leiter der betreffenden Behörde oder von einer hierfür bevollmächtigten Person getroffen.

26. In der Entscheidung müssen die von ihr erfasste kriminelle Handlung und der von ihr erfasste Zeitraum sowie die Telefonnummer, jede sonstige Adresse, das elektronische Kommunikationsgerät oder das geografische Gebiet angegeben werden. Der von der Genehmigung erfasste Zeitraum darf nicht länger als erforderlich sein und darf – soweit es sich um einen nach der Genehmigung liegenden Zeitraum handelt – einen Monat nicht überschreiten.

27. Die Datenerfassung bedarf keiner vorherigen Kontrolle. Allerdings ist nach § 6 des Gesetzes Nr. 2012:278 der Säkerhets- och integritetsskyddsnämnd (Ausschuss für Sicherheits- und Integritätsschutz, Schweden) über jede Entscheidung zur Erfassung von Daten in Kenntnis zu setzen. Nach § 1 des Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Gesetz Nr. 2007:980 über die Beaufsichtigung bestimmter Strafverfolgungshandlungen) hat der Ausschuss für Sicherheits- und Integritätsschutz die Anwendung des Gesetzes durch die Strafverfolgungsbehörden zu beaufsichtigen.

3. Dauer der Vorratsspeicherung

28. Gemäß Kapitel 6 § 16d LEK müssen die in Kapitel 6 § 16a LEK bezeichneten Daten für einen Zeitraum von sechs Monaten ab dem Tag der Beendigung der Kommunikation auf Vorrat gespeichert werden. Danach sind die Daten unverzüglich zu vernichten, es sei denn, in Kapitel 6 § 16d Abs. 2 LEK ist etwas anderes bestimmt. Nach dieser Vorschrift sind Daten, die vor Ablauf der Speicherungsfrist angefordert, aber noch nicht übergeben wurden, unverzüglich nach der Übergabe zu vernichten.

#### 4. Schutz und Sicherheit der auf Vorrat gespeicherten Daten

29. Nach Kapitel 6 § 20 Abs. 1 LEK ist es einer Person untersagt, die Kommunikationsdaten unbefugt weiterzugeben oder zu verwerten.

30. Nach Kapitel 6 § 3a LEK haben die Betreiber die besonderen technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der Daten während der Verarbeitung erforderlich sind. Aus den Gesetzesmaterialien zu dieser Vorschrift ergibt sich, dass bei der Festlegung des Schutzniveaus eine Abwägung zwischen Technik und Kosten einerseits und der Gefahr von Piraterie und Eingriffen andererseits nicht stattfinden darf.

31. Weitere Regeln über den Schutz der Daten finden sich in § 37 FEK sowie in den Verwaltungsvorschriften und allgemeinen Leitlinien der Post- och telestyrelse (schwedische Überwachungsbehörde für Post und Telekom, im Folgenden: PTS) über Schutzvorkehrungen bei der Vorratsspeicherung und Verarbeitung von Daten für Zwecke der Strafverfolgung (PTSFS 2012:4). In diesen Vorschriften heißt es u. a., dass die Betreiber verpflichtet sind, Maßnahmen zum Schutz der Daten vor unbeabsichtigter oder rechtswidriger Vernichtung, rechtswidriger Speicherung und Verarbeitung und rechtswidrigem Zugriff sowie rechtswidriger Preisgabe zu treffen. Die Betreiber haben außerdem fortlaufend und systematisch Sicherheitsarbeiten unter Berücksichtigung der mit der Vorratsspeicherungspflicht verbundenen besonderen Gefahren durchzuführen.

32. Im schwedischen Recht gibt es keine Bestimmungen zur Regelung der Frage, wo die auf Vorrat gespeicherten Daten aufbewahrt werden müssen.

33. Nach Kapitel 7 LEK kann die Aufsichtsbehörde, wenn der Betreiber seinen Verpflichtungen nicht nachkommt, Anordnungen und Verbote erlassen, die gegebenenfalls mit Zwangsgeldern bewehrt sind, sowie die vollständige oder teilweise Einstellung des Betriebs anordnen.

#### *C – Recht des Vereinigten Königreichs*

34. Die Vorschriften über die Vorratsspeicherung finden sich im Data Retention and Investigatory Powers Act 2014 (Gesetz von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen, im Folgenden: DRIPA), in den Data Retention Regulations 2014 (SI 2014/2042) (Verordnung zur Vorratsspeicherung von 2014, im Folgenden: Verordnung von 2014) sowie im Retention of Communications Data Code of Practice (Verhaltenskodex zur Speicherung von Kommunikationsdaten).

35. Die Vorschriften über den Datenzugang befinden sich in Teil I Kapitel II des Regulation of Investigatory Powers Act 2000 (Gesetz von 2000 über die Regelung von Ermittlungsbefugnissen, im Folgenden: RIPA), in der Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) (Dekret zur Regelung von Ermittlungsbefugnissen [Kommunikationsdaten] von 2010 in der durch die Regulation of Investigatory Powers [Communications Data] [Amendment] Order 2015 [SI 2015/228] geänderten Fassung) sowie im Acquisition and Disclosure of Communications Data Code of Practice (Verhaltenskodex zur Beschaffung und Offenlegung von Kommunikationsdaten, im Folgenden: Verhaltenskodex Datenbeschaffung).

#### 1. Umfang der Vorratsspeicherungspflicht

36. Nach Section 1 DRIPA kann der Secretary of State for the Home Department (Innenminister, Vereinigtes Königreich, im Folgenden: Minister) einen Betreiber zur Vorratsspeicherung aller Kommunikationsdaten verpflichten. Im Wesentlichen kann diese Verpflichtung alle Daten – mit Ausnahme des Inhalts der Nachricht – betreffen, die im Zusammenhang mit einer durch eine

Postdienstleistung oder ein Telekommunikationssystem weitergeleiteten Nachricht generiert werden. Diese Daten umfassen insbesondere den Ort, an dem sich der Dienstleistungsnutzer befindet, sowie die Daten, aufgrund deren die IP-Adresse oder eine andere Kennung, die zum Sender oder Empfänger einer Nachricht gehört, identifiziert werden kann.

37. Zu den Zwecken, die eine solche Speicherungsmaßnahme rechtfertigen können, gehören die Interessen der nationalen Sicherheit, die Vorbeugung oder Aufdeckung von Straftaten oder die Verhütung von Unruhen, die Interessen des wirtschaftlichen Wohls des Vereinigten Königreichs, soweit diese Interessen auch für die Interessen der nationalen Sicherheit relevant sind, das Interesse der öffentlichen Sicherheit, der Schutz der öffentlichen Gesundheit, die Zwecke der Festsetzung oder Erhebung von Steuern, Beiträgen oder sonstigen Beträgen, die an eine Regierungsbehörde zu entrichten sind, im Notfall die Verhinderung einer Schädigung der physischen oder psychischen Gesundheit, die Unterstützung von Untersuchungen möglicher Justizirrtümer, die Identifizierung einer Person, die gestorben ist oder die wegen eines Zustands, der nicht auf einer Straftat beruht (wie eine Naturkatastrophe oder ein Unfall), nicht in der Lage ist, sich zu identifizieren, die Ausübung von Funktionen mit Bezug zur Regulierung von Finanzdienstleistungen und -märkten oder zu finanzieller Stabilität sowie jeder durch Dekret des Ministers nach Section 22(2) DRIPA bezeichnete Zweck.

38. Die nationalen Rechtsvorschriften enthalten kein Erfordernis dahin, dass der Erlass einer Vorratsspeicherungsanordnung Gegenstand einer vorherigen gerichtlichen oder unabhängigen Genehmigung sein muss. Der Minister muss prüfen, ob die Vorratsspeicherungspflicht für einen oder mehrere Zwecke, für die relevante Kommunikationsdaten auf Vorrat gespeichert werden dürfen, „erforderlich und verhältnismäßig“ ist.

## 2. Zugang zu den auf Vorrat gespeicherten Daten

39. Nach Section 22(4) RIPA können öffentliche Behörden den Betreiber durch eine Anordnung verpflichten, ihnen gegenüber Kommunikationsdaten offenzulegen. Form und Inhalt solcher Anordnungen sind in Section 23(2) RIPA geregelt. Eine solche Anordnung ist durch Vorschriften über die Aufhebung und Verlängerung zeitlich begrenzt.

40. Die Beschaffung von Kommunikationsdaten muss in Bezug auf einen oder mehrere der in Section 22 RIPA genannten Zwecke – die den vorstehend in Nr. 37 dieser Schlussanträge bezeichneten Zwecken, zu denen Kommunikationsdaten auf Vorrat gespeichert werden können, entsprechen – erforderlich und verhältnismäßig sein.

41. Nach dem Verhaltenskodex Datenbeschaffung ist eine gerichtliche Anordnung erforderlich im Fall eines Antrags auf Zugang, der zur Identifizierung der Quelle eines Journalisten gestellt wird, sowie im Fall eines Antrags auf Zugang, der von den lokalen Behörden vorgelegt wird.

42. In allen anderen Fällen hängt der Zugang der Behörden davon ab, dass eine Genehmigung von einer in der betreffenden Behörde bezeichneten Person erteilt wird. Eine bezeichnete Person ist jemand, der ein bestimmtes Büro, einen bestimmten Dienstgrad oder eine bestimmte Position in der maßgeblichen öffentlichen Behörde innehat und der durch das Dekret zur Regelung von Ermittlungsbefugnissen (Kommunikationsdaten) von 2015 für den Zweck ernannt wurde, Kommunikationsdaten zu beschaffen.

43. Für den Zugang zu Kommunikationsdaten, die Gegenstand des Berufsgeheimnisses sind, oder zu Kommunikationsdaten, die sich auf Ärzte, Mitglieder des Parlaments oder Geistliche beziehen, ist keine besondere gerichtliche oder unabhängige Genehmigung erforderlich. Der Verhaltenskodex Datenbeschaffung stellt nur klar, dass bei einem Antrag auf Zugang zu diesen Daten eine besondere Prüfung der Erforderlichkeit und der Verhältnismäßigkeit durchgeführt werden muss.

### 3. Dauer der Vorratsspeicherung

44. Section 1(5) DRIPA und Regulation 4(2) der Verordnung von 2014 bestimmen eine Höchstdauer von zwölf Monaten für die Vorratsspeicherung. Nach dem Verhaltenskodex zur Speicherung von Kommunikationsdaten darf der Zeitraum nur so lang sein, wie es erforderlich und verhältnismäßig ist. Regulation 6 der Verordnung von 2014 verpflichtet den Minister zur fortlaufenden Überprüfung einer Vorratsspeicherungsanordnung.

### 4. Schutz und Sicherheit der auf Vorrat gespeicherten Daten

45. Nach Section 1 DRIPA dürfen Betreiber die auf Vorrat gespeicherten Daten nicht offenlegen, es sei denn, die Offenlegung erfolgt gemäß Teil I Kapitel 2 RIPA, gemäß einem gerichtlichen Beschluss oder einer anderen gerichtlichen Erlaubnis oder Maßnahme oder gemäß einer Verordnung des Ministers nach Section 1 DRIPA.

46. Gemäß Regulation 7 und Regulation 8 der Verordnung von 2014 müssen die Betreiber die Integrität und Sicherheit der auf Vorrat gespeicherten Daten gewährleisten, die Daten vor versehentlicher oder rechtswidriger Zerstörung, vor Verlust oder versehentlicher Veränderung und vor ungenehmigter oder rechtswidriger Vorratsspeicherung, Verarbeitung, Zugänglichmachung oder Offenlegung schützen, die Daten vernichten, um einen Zugang nach Ablauf der Genehmigung zur Vorratsspeicherung unmöglich zu machen, sowie angemessene Sicherheitssysteme einrichten. Regulation 9 der Verordnung von 2014 verpflichtet den Information Commissioner (Informationskommissar), die Einhaltung dieser Verpflichtungen durch die Betreiber zu überprüfen.

47. Die Behörden, denen die Betreiber die Kommunikationsdaten übergeben, müssen diese Daten sowie alle Kopien, Auszüge und Zusammenfassungen davon gesichert verarbeiten und speichern. Gemäß dem Verhaltenskodex Datenbeschaffung müssen die Anforderungen des Data Protection Act (Datenschutzgesetz, im Folgenden: DPA), mit dem die Richtlinie 95/46 umgesetzt wurde, beachtet werden.

48. Mit dem RIPA wurde ein Interception of Communications Commissioner (Kommissar für das Abfangen von Kommunikation, im Folgenden: Abfangkommissar) eingesetzt, dessen Aufgabe die unabhängige Aufsicht über die Ausübung und Nutzung der in Teil I Kapitel II des RIPA enthaltenen Befugnisse und Pflichten ist. Der Abfangkommissar führt keine Aufsicht über die Anwendung von Section 1 des DRIPA. Er hat regelmäßig öffentliche Berichte und Berichte an das Parlament zu erstellen (Section 57[2] und Section 58 RIPA) und die Aufbewahrung von Aufzeichnungen und die Erstattung von Berichten durch öffentliche Behörden zu dokumentieren (Verhaltenskodex Datenbeschaffung, Paragraphen 6.1 bis 6.8). Eine Beschwerde kann beim Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) erhoben werden, wenn Grund zur Vermutung besteht, dass Daten auf unangemessene Weise beschafft wurden (Section 65 RIPA).

49. Nach dem Verhaltenskodex Datenbeschaffung ist der Abfangkommissar nicht befugt, eine Rechtssache an dieses Gericht zu verweisen. Es ist ihm lediglich gestattet, eine Person über den vermuteten rechtswidrigen Einsatz von Befugnissen zu informieren, wenn er „nachweisen [kann], dass eine Person durch einen vorsätzlichen oder grob fahrlässigen Verstoß einen Nachteil erlitten hat“. Selbst wenn der Kommissar überzeugt ist, dass ein vorsätzlicher oder grob fahrlässiger Verstoß vorliegt, ist ihm dessen Offenlegung jedoch nicht gestattet, wenn die nationale Sicherheit durch die Offenlegung gefährdet würde.

### III – Ausgangsverfahren und Vorlagefragen

#### A – *Rechtssache C-203/15*

50. Am Tag nach der Verkündung des DRI-Urteils, d. h. am 9. April 2014, teilte Tele2 Sverige der PTS mit, dass das Unternehmen die in Kapitel 6 LEK vorgesehene Vorratsspeicherung von Daten einstellen werde. Außerdem werde Tele2 Sverige die bisher nach Kapitel 6 LEK auf Vorrat gespeicherten Daten löschen. Tele2 Sverige war der Ansicht, dass die schwedischen Rechtsvorschriften zur Umsetzung der Richtlinie 2006/24 nicht mit der Charta im Einklang stünden.

51. Am 15. April 2014 legte die Rikspolisstyrelse (Polizeidirektion, Schweden, im Folgenden: RPS) bei der PTS eine Beschwerde mit der Begründung ein, dass Tele2 Sverige die Übergabe von Daten bestimmter elektronischer Kommunikationsvorgänge an ihre Dienststellen eingestellt habe. In ihrer Beschwerde führte die RPS aus, dass die Weigerung von Tele2 Sverige erhebliche Konsequenzen für die Strafverfolgungstätigkeiten der Polizei nach sich ziehen werde.

52. Mit Bescheid vom 27. Juni 2014 gab die PTS Tele2 Sverige auf, die Vorratsspeicherung von Daten nach Kapitel 6 § 16a LEK und §§ 37 bis 43 FEK bis spätestens 25. Juli 2014 wieder aufzunehmen.

53. Gegen den PTS-Bescheid erhob Tele2 Sverige Klage beim Förvaltningsrätt i Stockholm (Verwaltungsgericht Stockholm, Schweden). Mit Urteil vom 13. Oktober 2014 wies dieses Gericht die Klage ab.

54. Tele2 Sverige legte gegen dieses Urteil beim vorlegenden Gericht Rechtsmittel ein mit dem Antrag, den angefochtenen Bescheid für nichtig zu erklären.

55. Nach Ansicht des Kammarrätt i Stockholm (Verwaltungsgerichtshof Stockholm) gibt es Gründe sowohl für als auch gegen die Auffassung, dass eine so umfassende Vorratsspeicherung, wie sie in Kapitel 6 § 16a LEK vorgesehen ist, mit Art. 15 Abs. 1 der Richtlinie 2002/58 und den Art. 7, 8 und 52 Abs. 1 der Charta vereinbar ist. Es hat daher das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist eine generelle Verpflichtung zur Vorratsspeicherung von Verkehrsdaten, die sich (wie in den Nrn. 13 bis 18 der Vorlageentscheidung beschrieben) auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung von Straftaten vorzusehen, mit Art. 15 Abs. 1 der Richtlinie 2002/58 unter Berücksichtigung der Art. 7, 8 und 52 Abs. 1 der Charta vereinbar?
2. Falls die erste Frage zu verneinen ist, kann die Vorratsspeicherung dennoch zulässig sein, wenn
  - a) der Zugang der nationalen Behörden zu den gespeicherten Daten wie in den Nrn. 19 bis 36 der Vorlageentscheidung beschrieben festgelegt ist und
  - b) die Sicherheitsanforderungen wie in den Nrn. 38 bis 43 der Vorlageentscheidung beschrieben geregelt sind und
  - c) sämtliche relevanten Daten wie in Nr. 37 der Vorlageentscheidung beschrieben für einen Zeitraum von sechs Monaten ab dem Tag, an dem die Kommunikation beendet wird, gespeichert und anschließend gelöscht werden müssen?

B – *Rechtssache C-698/15*

56. Herr Tom Watson, Herr Peter Brice und Herr Geoffrey Lewis haben vor dem High Court of Justice (England & Wales), Queen’s Bench Division (Administrative Court) (Gerichtshof [England und Wales], Abteilung Queen’s Bench [Verwaltungsgericht]), Anträge auf gerichtliche Überprüfung („judicial review“) der in Section 1 DRIPA enthaltenen Regelung der Vorratsspeicherung gestellt, die den Minister ermächtigt, die öffentlichen Telekommunikationsbetreiber zur Vorratsspeicherung aller Kommunikationsdaten für eine Dauer von höchstens zwölf Monaten zu verpflichten, wobei die Vorratsspeicherung des Inhalts der betreffenden Kommunikationsvorgänge ausgenommen ist.

57. Die Open Rights Group, Privacy International und die Law Society of England and Wales wurden als Streithelferinnen zu allen Antragsverfahren zugelassen.

58. Mit Urteil vom 17. Juli 2015 stellte dieses Gericht fest, dass die genannte Regelung dem Unionsrecht widerspreche, soweit sie die vom DRI-Urteil festgelegten Voraussetzungen, die auf die Vorschriften der Mitgliedstaaten zur Vorratsspeicherung von und zum Zugang zu Daten elektronischer Kommunikationsvorgänge Anwendung fänden, nicht erfülle. Gegen dieses Urteil legte der Minister Rechtsmittel beim vorlegenden Gericht ein.

59. In seinem Urteil vom 20. November 2015 nahm der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich) den vorläufigen Standpunkt ein, dass das DRI-Urteil keine verbindlichen unionsrechtlichen Voraussetzungen festgelegt habe, mit denen die nationalen Rechtsvorschriften im Einklang stehen müssten, sondern lediglich die Schutzregelungen identifiziert und beschrieben habe, die in der harmonisierten Unionsregelung fehlten.

60. Der Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen]) ist jedoch der Auffassung, dass die Antworten auf diese unionsrechtlichen Fragen nicht eindeutig seien und dass sie für den Erlass seines Urteils erforderlich seien. Er hat daher das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Legt das DRI-Urteil (einschließlich insbesondere seiner Rn. 60 bis 62) verbindliche, für die nationale Regelung eines Mitgliedstaats über den Zugang zu gemäß den nationalen Rechtsvorschriften auf Vorrat gespeicherten Daten geltende Voraussetzungen für die Vereinbarkeit mit den Art. 7 und 8 der Charta fest?
2. Erweitert das DRI-Urteil die Reichweite von Art. 7 und/oder Art. 8 der Charta über die von Art. 8 der Europäischen Menschenrechtskonvention (EMRK), wie er in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) festgestellt ist, hinaus?

**IV – Verfahren vor dem Gerichtshof**

61. Die Vorabentscheidungsersuchen sind am 4. Mai 2015 (Rechtssache C-203/15) und am 28. Dezember 2015 (Rechtssache C-698/15) in das Register der Kanzlei des Gerichtshofs eingetragen worden.

62. Mit Beschluss vom 1. Februar 2016 hat der Gerichtshof entschieden, die Rechtssache C-698/15 dem beschleunigten Verfahren gemäß Art. 105 Abs. 1 seiner Verfahrensordnung zu unterwerfen.

63. In der Rechtssache C-203/15 haben Tele2 Sverige, die belgische, die tschechische, die dänische, die deutsche, die estnische, die irische, die spanische, die französische, die ungarische, die niederländische und die schwedische Regierung, die Regierung des Vereinigten Königreichs sowie die Europäische Kommission schriftliche Erklärungen vorgelegt.

64. In der Rechtssache C-698/15 haben Herr Watson, Herr Brice und Herr Lewis, die Open Rights Group, Privacy International, die Law Society of England and Wales, die tschechische, die dänische, die deutsche, die estnische, die irische, die französische, die zyprische, die polnische und die finnische Regierung, die Regierung des Vereinigten Königreichs sowie die Kommission schriftliche Erklärungen vorgelegt.

65. Mit Beschluss des Gerichtshofs vom 10. März 2016 sind diese beiden Rechtssachen zu gemeinsamer mündlicher Verhandlung und gemeinsamer Entscheidung verbunden worden.

66. In der mündlichen Verhandlung vom 12. April 2016 sind die Vertreter von Tele2 Sverige, von Herrn Watson, Herrn Brice und Herrn Lewis, der Open Rights Group, von Privacy International und der Law Society of England and Wales, der tschechischen, der dänischen, der deutschen, der estnischen, der irischen, der spanischen, der französischen, der finnischen und der schwedischen Regierung, der Regierung des Vereinigten Königreichs und der Kommission erschienen, um Ausführungen zu machen.

## V – Würdigung der Vorlagefragen

67. Mit der ersten Frage in der Rechtssache C-203/15 möchte das vorlegende Gericht wissen, ob unter Berücksichtigung des DRI-Urteils Art. 15 Abs. 1 der Richtlinie 2002/58 sowie die Art. 7, 8 und 52 Abs. 1 der Charta dahin auszulegen sind, dass sie einen Mitgliedstaat daran hindern, den Betreibern eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren fragliche aufzuerlegen, und zwar unabhängig davon, ob etwaige Garantien mit dieser Verpflichtung einhergehen.

68. Für den Fall der Verneinung dieser Frage gehen die zweite Frage in der Rechtssache C-203/15 und die erste Frage in der Rechtssache C-698/15 dahin, ob die genannten Bestimmungen dahin auszulegen sind, dass sie einen Mitgliedstaat daran hindern, den Betreibern eine generelle Verpflichtung zur Vorratsspeicherung aufzuerlegen, wenn mit dieser Verpflichtung nicht alle vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils bezeichneten Garantien einhergehen, die den Zugang zu den Daten, die Dauer der Vorratsspeicherung sowie den Schutz und die Sicherheit der Daten betreffen.

69. Da diese drei Fragen eng zusammengehören, werde ich sie im Folgenden gemeinsam prüfen.

70. Dagegen erfordert die zweite Frage in der Rechtssache C-698/15 eine gesonderte Behandlung. Mit dieser Frage möchte das vorlegende Gericht wissen, ob das DRI-Urteil den Anwendungsbereich von Art. 7 und/oder 8 der Charta über den Anwendungsbereich von Art. 8 EMRK hinaus erweitert hat. Ich werde im folgenden Abschnitt darlegen, weshalb ich der Ansicht bin, dass diese Frage als unzulässig zurückzuweisen ist.

71. Bevor ich mit der Prüfung dieser Vorlagefragen beginne, halte ich es für hilfreich, kurz darzustellen, welche Arten von Daten von den in den Ausgangsverfahren in Rede stehenden Vorratsspeicherungspflichten betroffen sind. Nach den Feststellungen der vorlegenden Gerichte entspricht der Umfang der genannten Verpflichtungen im Wesentlichen dem Umfang der Verpflichtung, die in Art. 5 der Richtlinie 2006/24 vorgesehen war<sup>8</sup>. Schematisch gesehen können die Kommunikationsdaten, die Gegenstand dieser Vorratsspeicherungspflichten sind, in vier Kategorien unterteilt werden<sup>9</sup>:

— Daten, die die Identifizierung der Quelle und des Adressaten einer Nachricht ermöglichen;

8 — Diese Entsprechung ist verständlich, da die nationalen Regelungen die inzwischen ungültige Richtlinie umsetzen sollten.

9 — Vgl. die Darstellung der in den Ausgangsverfahren fraglichen nationalen Regelungen in den Nrn. 11 bis 13 und 36 dieser Schlussanträge.

- Daten, die die Bestimmung des Standorts der Quelle und des Adressaten einer Nachricht ermöglichen;
- Daten bezüglich Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung sowie
- Daten, die die Bestimmung der Art einer Nachrichtenübermittlung und der Art der benutzten Endeinrichtung ermöglichen.

72. Der Inhalt der Nachrichten ist nach dem Vorbild der in Art. 5 Abs. 2 der Richtlinie 2006/24 vorgesehenen Regelung von den in den Ausgangsverfahren in Rede stehenden generellen Verpflichtungen zur Vorratsspeicherung von Verkehrsdaten ausgenommen.

*A – Zur Zulässigkeit der zweiten Frage in der Rechtssache C-698/15*

73. Mit der zweiten Frage in der Rechtssache C-698/15 wird der Gerichtshof ersucht, klarzustellen, ob das DRI-Urteil den Anwendungsbereich von Art. 7 und/oder 8 der Charta über den Anwendungsbereich von Art. 8 EMRK in seiner Auslegung durch den EGMR hinaus erweitert.

74. In dieser Frage kommt insbesondere ein vom Minister vor dem vorlegenden Gericht geltend gemachtes Argument zum Ausdruck, wonach die Rechtsprechung des EGMR nicht verlange, dass der Zugang zu den Daten von der vorherigen Genehmigung einer unabhängigen Stelle abhängt und dass die Vorratsspeicherung und der Zugang zu diesen Daten auf die Bekämpfung schwerer Straftaten beschränkt sei.

75. Meines Erachtens ist diese Frage aus folgenden Gründen als unzulässig zurückzuweisen. Zwar sind die Erwägungen des Gerichtshofs im DRI-Urteil und die dort von ihm gewählte Lösung offensichtlich von ausschlaggebender Bedeutung für die Entscheidung in den Ausgangsverfahren. Der Umstand jedoch, dass dieses Urteil möglicherweise den Anwendungsbereich von Art. 7 und/oder 8 der Charta über den Anwendungsbereich von Art. 8 EMRK hinaus erweitert hat, ist als solcher für diese Entscheidung unerheblich.

76. Insoweit ist darauf hinzuweisen, dass nach Art. 6 Abs. 3 EUV die Grundrechte, wie sie in der EMRK gewährleistet sind, als allgemeine Grundsätze Teil des Unionsrechts sind. Solange die Union der EMRK nicht beigetreten ist, stellt diese jedoch kein Rechtsinstrument dar, das förmlich in die Unionsrechtsordnung übernommen worden ist<sup>10</sup>.

77. Zwar wird mit Art. 52 Abs. 3 Satz 1 der Charta eine Auslegungsregel aufgestellt, wonach die Rechte der Charta, die den durch die EMRK garantierten Rechten entsprechen, „die gleiche Bedeutung und Tragweite [haben], wie sie ihnen in der genannten Konvention verliehen wird“.

78. Nach Art. 52 Abs. 3 Satz 2 der Charta steht jedoch „[d]iese Bestimmung ... dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt“. Meines Erachtens ergibt sich aus diesem Satz, dass es dem Gerichtshof freisteht, sofern er es im Rahmen des Unionsrechts für erforderlich hält, den Anwendungsbereich der Bestimmungen der Charta über den Anwendungsbereich der entsprechenden Bestimmungen der EMRK hinaus zu erweitern.

10 — Gutachten 2/13 vom 18. Dezember 2014 (EU:C:2014:2454, Rn. 179) und Urteil vom 15. Februar 2016, N. (C-601/15 PPU, EU:C:2016:84, Rn. 45 und die dort angeführte Rechtsprechung).

79. Hilfsweise füge ich hinzu, dass Art. 8 der Charta, wie er vom Gerichtshof im DRI-Urteil ausgelegt worden ist, ein Recht gewährt, das in keinem durch die EMRK garantierten Recht eine Entsprechung hat, nämlich das Recht auf Schutz der personenbezogenen Daten, was im Übrigen durch die Erläuterungen zu Art. 52 der Charta bestätigt wird<sup>11</sup>. Folglich gilt die Auslegungsregel des Art. 52 Abs. 3 Satz 1 der Charta auf keinen Fall für die Auslegung von Art. 8 der Charta, worauf Herr Brice und Herr Lewis, die Open Rights Group und Privacy International, die Law Society of England and Wales sowie die tschechische, die irische und die finnische Regierung hingewiesen haben.

80. Aus dem Vorstehenden ergibt sich, dass es das Unionsrecht zulässt, dass die Art. 7 und 8 der Charta einen weiter gehenden Schutz als die EMRK gewähren. Der Umstand, dass das DRI-Urteil möglicherweise den Anwendungsbereich dieser Bestimmungen der Charta über den Anwendungsbereich von Art. 8 EMRK hinaus erweitert hat, ist daher für sich genommen für die Entscheidung in den Ausgangsverfahren unerheblich. Die Entscheidung in diesen Verfahren hängt hauptsächlich von den Voraussetzungen ab, unter denen eine generelle Verpflichtung zur Vorratsspeicherung als mit Art. 15 Abs. 1 der Richtlinie 2002/58 sowie mit den Art. 7, 8 und 52 Abs. 1 der Charta, ausgelegt im Licht des DRI-Urteils, vereinbar angesehen werden kann, was Gegenstand der drei anderen in den vorliegenden Rechtssachen gestellten Fragen ist.

81. Nach ständiger Rechtsprechung kann das Ersuchen eines nationalen Gerichts nur zurückgewiesen werden, wenn die erbetene Auslegung des Unionsrechts offensichtlich in keinem Zusammenhang mit der Realität oder dem Gegenstand des Ausgangsrechtsstreits steht, wenn das Problem hypothetischer Natur ist oder wenn der Gerichtshof nicht über die tatsächlichen oder rechtlichen Angaben verfügt, die für eine sachdienliche Beantwortung der ihm vorgelegten Fragen erforderlich sind<sup>12</sup>.

82. Aus den vorstehend dargelegten Gründen ist die zweite Frage in der Rechtssache C-698/15 meines Erachtens nur von theoretischem Interesse, da eine etwaige Antwort auf diese Frage es nicht ermöglicht, Kriterien für die Auslegung des Unionsrechts aufzuzeigen, anhand deren das vorlegende Gericht über den bei ihm anhängigen Rechtsstreit in Anwendung dieses Rechts entscheiden könnte<sup>13</sup>.

83. Unter diesen Umständen bin ich der Auffassung, dass die genannte Frage als unzulässig zurückzuweisen ist, wie Herr Watson, die Law Society of England and Wales und die tschechische Regierung geltend gemacht haben.

#### *B – Zur Vereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung*

84. In diesem Abschnitt wird die Frage behandelt, ob die Mitgliedstaaten von der durch Art. 15 Abs. 1 der Richtlinie 2002/58 gebotenen Befugnis Gebrauch machen können, um eine generelle Verpflichtung zur Vorratsspeicherung einzuführen. Hingegen werden nicht die besonderen Voraussetzungen geprüft, die die Mitgliedstaaten bei der Wahrnehmung dieser Befugnis zu beachten haben; sie werden in einem späteren Abschnitt eingehend untersucht<sup>14</sup>.

11 — Gemäß Art. 6 Abs. 1 Unterabs. 3 EUV und Art. 52 Abs. 7 der Charta sind die Erläuterungen zur Charta bei deren Auslegung zu berücksichtigen (vgl. Urteile vom 26. Februar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 20, und vom 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 47). Gemäß diesen Erläuterungen entspricht Art. 7 der Charta Art. 8 der EMRK, während Art. 8 der Charta in der EMRK keine Entsprechung hat.

12 — Vgl. insbesondere Urteile vom 9. November 2010, Volker und Markus Schecke und Eifert (C-92/09 und C-93/09, EU:C:2010:662, Rn. 40 und die dort angeführte Rechtsprechung), sowie vom 24. April 2012, Kamberaj (C-571/10, EU:C:2012:233, Rn. 42 und die dort angeführte Rechtsprechung).

13 — Vgl. insbesondere Urteil vom 16. September 1982, Vlaeminck (132/81, EU:C:1982:294, Rn. 13), Beschluss vom 24. März 2011, Abt u. a. (C-194/10, EU:C:2011:182, Rn. 36 und 37 und die dort angeführte Rechtsprechung), und Urteil vom 24. Oktober 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, Rn. 46 und die dort angeführte Rechtsprechung).

14 — Siehe Nrn. 126 bis 262 dieser Schlussanträge.

85. Die Open Rights Group und Privacy International machen geltend, die genannte Verpflichtung sei unvereinbar mit der durch die Richtlinie 2002/58 geschaffenen harmonisierten Regelung, und zwar unabhängig davon, ob die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 ergebenden Voraussetzungen eingehalten würden, weil der Wesensgehalt der Rechte und der Regelung, die durch die Richtlinie geschaffen worden seien, durch die genannte Verpflichtung beseitigt würde.

86. Bevor ich auf dieses Vorbringen eingehe, werde ich prüfen, ob eine generelle Verpflichtung zur Vorratsspeicherung in den Anwendungsbereich der genannten Richtlinie fällt.

1. Zur Geltung einer generellen Verpflichtung zur Vorratsspeicherung im Anwendungsbereich der Richtlinie 2002/58

87. Keiner der Beteiligten, die dem Gerichtshof Erklärungen vorgelegt haben, stellt in Frage, dass eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren in Rede stehende unter die „Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft“ im Sinne von Art. 3 der Richtlinie 2002/58 fällt.

88. Die tschechische, die französische und die polnische Regierung sowie die Regierung des Vereinigten Königreichs machen jedoch geltend, eine generelle Verpflichtung zur Vorratsspeicherung falle unter die Ausnahmeregelung nach Art. 1 Abs. 3 der Richtlinie 2002/58. Zum einen betreffen die nationalen Bestimmungen über den Datenzugang und die Nutzung der Daten durch die Polizei- und Justizbehörden der Mitgliedstaaten die öffentliche Sicherheit, die Landesverteidigung oder die Sicherheit des Staates oder gehörten zumindest in den strafrechtlichen Bereich. Zum anderen bestehe der alleinige Zweck der Vorratsspeicherung darin, den Polizei- und Justizbehörden den Zugang zu diesen Daten sowie deren Nutzung zu ermöglichen. Eine Verpflichtung zur Vorratsspeicherung von Daten sei daher nach Maßgabe der oben angeführten Bestimmung vom Anwendungsbereich der genannten Richtlinie ausgenommen.

89. Diese Argumentation überzeugt mich aus folgenden Gründen nicht.

90. Erstens bestätigt der Wortlaut von Art. 15 Abs. 1 der Richtlinie 2002/58, dass die von den Mitgliedstaaten auferlegte Verpflichtung zur Vorratsspeicherung in den Anwendungsbereich dieser Richtlinie fällt. Nach dieser Bestimmung „können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden“. Es lässt sich meines Erachtens kaum die Auffassung vertreten, dass die Verpflichtung zur Vorratsspeicherung vom Anwendungsbereich der Richtlinie ausgeschlossen ist, obwohl Art. 15 Abs. 1 der Richtlinie die Möglichkeit regelt, solche Verpflichtungen aufzustellen.

91. Wie Herr Watson, Herr Brice und Herr Lewis, die belgische, die dänische, die deutsche und die finnische Regierung sowie die Kommission ausgeführt haben, stellt eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren in Rede stehende in Wirklichkeit eine Durchführung des Art. 15 Abs. 1 der Richtlinie 2002/58 dar.

92. Zweitens bedeutet der Umstand, dass die Bestimmungen über den Zugang unter die Ausschlussregelung des Art. 1 Abs. 3 der Richtlinie 2002/58<sup>15</sup> fallen können, nicht, dass die Verpflichtung zur Vorratsspeicherung ebenfalls unter diese Regelung fällt und damit nicht zum Anwendungsbereich der Richtlinie gehört.

15 — Siehe Nrn. 123 bis 125 dieser Schlussanträge.

93. Insoweit hat der Gerichtshof bereits festgestellt, dass die Tätigkeiten nach Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46/EG<sup>16</sup>, dessen Wortlaut in seiner Tragweite mit dem des Art. 1 Abs. 3 der Richtlinie 2002/58 zu vergleichen ist, spezifische Tätigkeiten der Staaten oder der staatlichen Stellen sind und mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben<sup>17</sup>.

94. Die in den Ausgangsverfahren in Rede stehende Verpflichtung zur Vorratsspeicherung wird jedoch privaten Wirtschaftsteilnehmern im Rahmen einer privaten Tätigkeit der Bereitstellung elektronischer Kommunikationsdienste auferlegt, wie die Kommission geltend macht. Ferner gilt die genannte Verpflichtung unabhängig davon, ob die Polizei- und Justizbehörden einen Antrag auf Zugang gestellt haben oder ob ganz allgemein staatliche Stellen im Rahmen der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder im strafrechtlichen Bereich tätig geworden sind.

95. Drittens bestätigt die Entscheidung des Gerichtshofs im Urteil Irland/Parlament und Rat, dass eine generelle Verpflichtung zur Vorratsspeicherung nicht in den Bereich des Strafrechts fällt<sup>18</sup>. Der Gerichtshof hat nämlich festgestellt, dass die Richtlinie 2006/24, die diese Verpflichtung einführt, nicht dem strafrechtlichen Bereich, sondern dem Funktionieren des Binnenmarkts zuzurechnen ist, so dass Art. 95 EG (jetzt Art. 114 AEUV) die geeignete Rechtsgrundlage für die Richtlinie war.

96. Der Gerichtshof hat dieses Ergebnis insbesondere auf die Feststellung gestützt, dass die Bestimmungen dieser Richtlinie im Wesentlichen auf die Tätigkeiten der Diensteanbieter beschränkt sind und nicht den Zugang zu den Daten oder deren Nutzung durch die Polizei- und Justizbehörden der Mitgliedstaaten regeln<sup>19</sup>. Ich schliesse hieraus, dass Bestimmungen des nationalen Rechts, die eine Verpflichtung zur Vorratsspeicherung ähnlich der in der Richtlinie 2006/24 vorgesehenen einführen, ebenfalls nicht in den strafrechtlichen Bereich fallen.

97. Nach alledem bin ich der Ansicht, dass eine generelle Verpflichtung zur Vorratsspeicherung nicht von der Ausnahmeregelung des Art. 1 Abs. 3 der Richtlinie 2002/58 erfasst wird und daher in den Anwendungsbereich der genannten Richtlinie fällt.

2. Zur Möglichkeit, durch die Einführung einer generellen Verpflichtung zur Vorratsspeicherung von der durch die Richtlinie 2002/58 geschaffenen Regelung abzuweichen

98. Es ist nunmehr zu prüfen, ob eine generelle Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung vereinbar ist.

99. Insoweit stellt sich die Frage, ob ein Mitgliedstaat von der durch Art. 15 Abs. 1 der Richtlinie 2002/58 gebotenen Befugnis Gebrauch machen kann, um eine solche Verpflichtung einzuführen.

100. Vier Argumente sind hiergegen vorgebracht worden, insbesondere von der Open Rights Group und Privacy International.

101. Das erste Argument besagt, dass das Harmonisierungsziel, das mit der Richtlinie 2002/58 erreicht werden sollte, in Frage gestellt wäre, wollte man den Mitgliedstaaten die Befugnis einräumen, eine generelle Verpflichtung zur Vorratsspeicherung einzuführen. Ausweislich ihres Art. 1 Abs. 1 sehe nämlich die Richtlinie die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich

16 — 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).

17 — Urteil vom 6. November 2003, Lindqvist (C-101/01, EU:C:2003:596, Rn. 43 und 44).

18 — Urteil vom 10. Februar 2009 (C-301/06, EU:C:2009:68).

19 — Urteil vom 10. Februar 2009, Irland/Parlament und Rat (C- 301/06, EU:C:2009:68, Rn. 80).

seien, 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 Union zu gewährleisten.

102. Somit könne Art. 15 Abs. 1 der Richtlinie 2002/58 nicht dahin ausgelegt werden, dass er den Mitgliedstaaten die Befugnis verleihe, eine so weitreichende Abweichung von der durch die Richtlinie geschaffenen Regelung vorzusehen, dass den Bemühungen um eine Harmonisierung die praktische Wirksamkeit genommen würde.

103. Nach dem zweiten Argument soll es auch der Wortlaut des Art. 15 Abs. 1 der Richtlinie 2002/58 verbieten, die Befugnis der Mitgliedstaaten, von der durch die genannte Richtlinie geschaffenen Regelung abzuweichen, derart weit auszulegen. Nach dieser Bestimmung können „[d]ie Mitgliedstaaten ... 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*“ (Hervorhebung nur hier).

104. Eine generelle Verpflichtung zur Vorratsspeicherung würde die in dieser Bestimmung genannten Rechte und Pflichten nicht lediglich „beschränken“, sondern aufheben. Dies gelte für

- die Verpflichtung, die Vertraulichkeit der Verkehrsdaten sicherzustellen, und die Verpflichtung, die Speicherung von Informationen an die Zustimmung des Nutzers zu knüpfen, die jeweils in Art. 5 Abs. 1 und 3 der Richtlinie 2002/58 geregelt seien,
- die Verpflichtung nach Art. 6 Abs. 1 der Richtlinie, die Verkehrsdaten zu löschen oder zu anonymisieren, und
- die Verpflichtung nach Art. 9 Abs. 1 der Richtlinie, für eine Verarbeitung die Standortdaten zu anonymisieren oder die Einwilligung des Nutzers einzuholen.

105. Diese ersten beiden Argumente sind meines Erachtens aus folgenden Gründen zurückzuweisen.

106. Zum einen spricht Art. 15 Abs. 1 der Richtlinie 2002/58 selbst von der Möglichkeit, dass Mitgliedstaaten „durch Rechtsvorschriften vorsehen, dass Daten ... während einer begrenzten Zeit aufbewahrt werden“. Diese ausdrückliche Bezugnahme auf die Verpflichtung zur Vorratsspeicherung bestätigt, dass die Verpflichtung als solche mit der durch die Richtlinie 2002/58 geschaffenen Regelung nicht unvereinbar ist. Die angeführte Formulierung sieht zwar nicht ausdrücklich vor, dass eine *generelle* Verpflichtung zur Vorratsspeicherung eingeführt werden kann, doch ist festzustellen, dass sie ihr auch nicht entgegensteht.

107. Zum anderen stellt der elfte Erwägungsgrund der Richtlinie 2002/58 klar, dass die Richtlinie keine Auswirkungen „auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten [hat], Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der [EMRK] erfolgt.“

108. Aus dem elften Erwägungsgrund ergibt sich meines Erachtens, dass der Gesetzgeber der Union das Recht der Mitgliedstaaten auf Erlass der in Art. 15 Abs. 1 der Richtlinie 2002/58 genannten Maßnahmen nicht antasten, sondern dieses Recht bestimmten Voraussetzungen unterwerfen wollte, die sich vor allem auf den verfolgten Zweck und die Verhältnismäßigkeit der Maßnahmen beziehen. Anders gesagt, eine generelle Verpflichtung zur Vorratsspeicherung ist mit der durch diese Richtlinie geschaffenen Regelung nicht unvereinbar, sofern sie bestimmte Voraussetzungen erfüllt.

109. Gemäß einem dritten Argument soll Art. 15 Abs. 1 der Richtlinie 2002/58 als Abweichung von der durch die Richtlinie geschaffenen Regelung eng auszulegen sein, und zwar aufgrund einer sich aus ständiger Rechtsprechung des Gerichtshofs ergebenden Auslegungsregel. Diese Regel der engen Auslegung verbiete es, die genannte Bestimmung dahin auszulegen, dass sie die Befugnis zur Einführung einer generellen Verpflichtung zur Vorratsspeicherung verleihe.

110. Meines Erachtens ist davon auszugehen, dass die in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehene Befugnis nicht als Abweichung eingestuft werden kann und folglich nicht eng auszulegen ist, wie die Kommission zu Recht geltend macht. Es scheint mir schwierig zu sein, diese Befugnis als Abweichung einzustufen, angesichts des vorstehend angeführten elften Erwägungsgrundes, dem zufolge die Richtlinie das Recht der Mitgliedstaaten auf Erlass der in dieser Bestimmung vorgesehenen Maßnahmen nicht berührt. Ich weise außerdem darauf hin, dass Art. 15 der Richtlinie mit „Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG“ überschrieben ist, während ihr Art. 10 ausdrücklich die Überschrift „Ausnahmen“ trägt. Diese Überschriften bestärken mich in meiner Überzeugung, dass die in Art. 15 geregelte Befugnis nicht als Abweichung eingestuft werden kann.

111. Nach einem vierten und letzten Argument soll die Unvereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung dadurch bestätigt werden, dass durch die – mit dem DRI-Urteil für ungültig erklärte – Richtlinie 2006/24 Art. 15 Abs. 1a in die Richtlinie 2002/58 eingefügt worden sei. Diesem Argument zufolge soll diese Unvereinbarkeit den Gesetzgeber der Union veranlasst haben, Art. 15 Abs. 1 der Richtlinie 2002/58 für unanwendbar auf die von der Richtlinie 2006/24 vorgesehene Regelung der generellen Vorratsspeicherung zu erklären.

112. Dieses Argument beruht meines Erachtens auf einem falschen Verständnis der Tragweite des Art. 15 Abs. 1a der Richtlinie 2002/58. Nach dieser Bestimmung „[gilt Art. 15 Abs. 1 der Richtlinie 2002/58] nicht für Daten, für die in der Richtlinie 2006/24 ... eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist“.

113. Ich verstehe diese Bestimmung wie folgt. In Bezug auf die Daten, deren Vorratsspeicherung in der Richtlinie 2006/24 zu den dort aufgeführten Zwecken vorgeschrieben war, verloren die Mitgliedstaaten die in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehene Befugnis, den Umfang der in dieser Bestimmung genannten Rechte und Pflichten zu beschränken, insbesondere über zusätzliche Pflichten zur Vorratsspeicherung. Anders gesagt, Art. 15 Abs. 1a sah eine abschließende Harmonisierung bezüglich der Daten vor, deren Vorratsspeicherung in der Richtlinie 2006/24 zu den dort aufgeführten Zwecken vorgeschrieben war.

114. Diese Auslegung wird durch den zwölften Erwägungsgrund der Richtlinie 2006/24 bestätigt, wonach „Artikel 15 Absatz 1 der Richtlinie 2002/58 ... *weiterhin* für Daten [gilt], einschließlich Daten im Zusammenhang mit erfolglosen Anrufversuchen, deren Vorratsspeicherung nach der vorliegenden Richtlinie nicht ausdrücklich vorgeschrieben ist und *die daher nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen*, und für die Vorratsspeicherung *zu anderen* – einschließlich justiziellen – *Zwecken als denjenigen, die durch die vorliegende Richtlinie abgedeckt werden*“ (Hervorhebung nur hier).

115. Durch Einfügen des Art. 15 Abs. 1a in die Richtlinie 2002/58 wird daher nicht die Unvereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit der durch diese Richtlinie eingeführten Regelung bestätigt, sondern der Wille des Gesetzgebers der Union, beim Erlass der Richtlinie 2006/24 eine abschließende Harmonisierung herzustellen.

116. Nach alledem bin ich der Auffassung, dass eine generelle Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung vereinbar ist und dass ein Mitgliedstaat von der durch Art. 15 Abs. 1 der Richtlinie eingeräumten Befugnis Gebrauch machen kann, um eine solche Verpflichtung aufzuerlegen<sup>20</sup>. Die Inanspruchnahme dieser Befugnis ist jedoch von der Einhaltung strenger Voraussetzungen abhängig, die sich nicht nur aus der genannten Bestimmung, sondern auch aus den einschlägigen Bestimmungen der Charta im Licht des DRI-Urteils ergeben, die ich in einem späteren Abschnitt untersuchen werde<sup>21</sup>.

### *C – Zur Anwendbarkeit der Charta auf eine generelle Verpflichtung zur Vorratsspeicherung*

117. Vor der inhaltlichen Prüfung der Anforderungen, die die Charta in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58 stellt, wenn ein Staat sich für die Einführung einer generellen Verpflichtung zur Vorratsspeicherung entschließt, ist zu prüfen, ob die Charta auf eine derartige Verpflichtung überhaupt anwendbar ist.

118. Die Anwendbarkeit der Charta auf eine generelle Verpflichtung zur Vorratsspeicherung hängt im Wesentlichen davon ab, ob die Richtlinie 2002/58 auf diese Verpflichtung anwendbar ist.

119. Nach ihrem Art. 51 Abs. 1 Satz 1 „[gilt die] Charta ... für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union“. Die Erläuterungen zu Art. 51 der Charta verweisen insoweit auf die Rechtsprechung des Gerichtshofs, wonach die Verpflichtung zur Einhaltung der im Rahmen der Union definierten Grundrechte für die Mitgliedstaaten nur dann gilt, wenn sie im Anwendungsbereich des Unionsrechts handeln<sup>22</sup>.

120. Die tschechische, die französische und die polnische Regierung sowie die Regierung des Vereinigten Königreichs, die die Anwendbarkeit der Richtlinie 2002/58 auf eine generelle Verpflichtung zur Vorratsspeicherung verneinen<sup>23</sup>, sind auch der Auffassung, dass die Charta nicht für diese Verpflichtung gelte.

121. Ich habe bereits dargelegt, weshalb mit der Einführung einer generellen Verpflichtung zur Vorratsspeicherung meines Erachtens von der Befugnis nach Art. 15 Abs. 1 der Richtlinie 2002/58 Gebrauch gemacht wird<sup>24</sup>.

20 — Da die Richtlinie 2002/58 als *lex specialis* gegenüber der Richtlinie 95/46 gelten kann (vgl. insoweit Art. 1 Abs. 2 der Richtlinie 2002/58), halte ich es nicht für erforderlich, die Vereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit der durch die Richtlinie 95/46 geschaffenen Regelung zu prüfen, die zudem nicht Gegenstand der Vorlagefragen ist. Der Vollständigkeit halber möchte ich jedoch darauf hinweisen, dass der Wortlaut des Art. 13 Abs. 1 der Richtlinie 95/46 den Mitgliedstaaten einen größeren Spielraum gewährt als Art. 15 Abs. 1 der Richtlinie 2002/58, der dessen Umfang im Rahmen der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste regelt. Da es die in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehene Befugnis einem Mitgliedstaat erlaubt, eine generelle Verpflichtung zur Vorratsspeicherung einzuführen, schließe ich hieraus, dass Art. 13 Abs. 1 der Richtlinie 95/46 dies ebenfalls erlaubt.

21 — Siehe Nrn. 126 bis 262 dieser Schlussanträge.

22 — Nach ständiger Rechtsprechung des Gerichtshofs finden nämlich die in der Unionsrechtsordnung garantierten Grundrechte Anwendung in allen unionsrechtlich geregelten Fallgestaltungen, aber nicht außerhalb derselben. Insoweit hat der Gerichtshof bereits festgestellt, dass er eine nationale Regelung nicht im Hinblick auf die Charta beurteilen kann, wenn sie nicht in den Geltungsbereich des Unionsrechts fällt. Sobald dagegen eine solche Regelung in den Geltungsbereich des Unionsrechts fällt, hat der im Rahmen eines Vorabentscheidungsersuchens angerufene Gerichtshof dem vorlegenden Gericht alle Auslegungshinweise zu geben, die es benötigt, um die Vereinbarkeit dieser Regelung mit den Grundrechten beurteilen zu können, deren Wahrung er sichert (vgl. Urteil vom 26. Februar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 19 und die dort angeführte Rechtsprechung).

23 — Siehe Nr. 88 dieser Schlussanträge.

24 — Siehe Nrn. 90 bis 97 dieser Schlussanträge.

122. Die Bestimmungen der Charta finden daher gemäß ihrem Art. 51 Abs. 1 auf die nationalen Maßnahmen Anwendung, mit denen diese Verpflichtung eingeführt wird, wie dies Herr Watson, Herr Brice und Herr Lewis, die Open Rights Group und Privacy International, die dänische, die deutsche und die finnische Regierung sowie die Kommission geltend machen<sup>25</sup>.

123. Dieses Ergebnis wird nicht dadurch in Frage gestellt, dass die nationalen Bestimmungen, die den Zugang zu den auf Vorrat gespeicherten Daten regeln, als solche nicht in den Anwendungsbereich der Charta fallen.

124. Soweit sie die „Tätigkeiten des Staates im strafrechtlichen Bereich“ betreffen, fallen zwar die nationalen Bestimmungen, die den Zugang der Polizei- oder Justizbehörden zu den auf Vorrat gespeicherten Daten zum Zweck der Bekämpfung schwerer Kriminalität regeln, unter den Ausschluss nach Art. 1 Abs. 3 der Richtlinie 2002/58<sup>26</sup>. Diese nationalen Bestimmungen führen daher nicht das Unionsrecht durch, so dass die Charta für sie nicht gilt.

125. Eine Verpflichtung zur Vorratsspeicherung besteht jedoch deshalb, weil den Strafverfolgungsbehörden der Zugang zu den auf Vorrat gespeicherten Daten ermöglicht werden soll, so dass die Problematik der Vorratsspeicherung und die des Zugangs nicht vollständig voneinander getrennt werden können. Wie die Kommission zu Recht ausführt, sind die Bestimmungen über den Zugang von entscheidender Bedeutung für die Beurteilung der Frage, ob die Bestimmungen zur Einführung einer generellen Verpflichtung zur Vorratsspeicherung, mit denen Art. 15 Abs. 1 der Richtlinie 2002/58 durchgeführt wird, mit der Charta vereinbar sind. Die Bestimmungen zur Regelung des Zugangs sind insbesondere bei der Beurteilung der Erforderlichkeit und Verhältnismäßigkeit einer solchen Verpflichtung zu berücksichtigen<sup>27</sup>.

*D – Zur Vereinbarkeit einer generellen Verpflichtung zur Vorratsspeicherung mit den Anforderungen des Art. 15 Abs. 1 der Richtlinie 2002/58 und der Art. 7, 8 und 52 Abs. 1 der Charta*

126. Nun bleibt noch die schwierige Frage zu erörtern, ob eine generelle Verpflichtung zur Vorratsspeicherung mit den Anforderungen des Art. 15 Abs. 1 der Richtlinie 2002/58 und der Art. 7, 8 und 52 Abs. 1 der Charta im Licht des DRI-Urteils vereinbar ist. Diese Frage betrifft allgemeiner die notwendige Anpassung der rechtlichen Rahmenbestimmungen für die staatlichen Überwachungsmöglichkeiten, die durch jüngere technische Entwicklungen stark erweitert wurden<sup>28</sup>.

127. Der erste Schritt einer Analyse in diesem Zusammenhang führt zur Feststellung, dass ein Eingriff in die in der Richtlinie 2002/58 verankerten Rechte und die in den Art. 7 und 8 der Charta verankerten Grundrechte vorliegt.

25 — Konkret bestimmt Art. 51 Abs. 1 Satz 2 der Charta, dass die Mitgliedstaaten die durch die Charta garantierten Rechte bei der Durchführung des Rechts der Union zu wahren haben.

26 — Zum Umfang dieses Ausschlusses siehe Nrn. 90 bis 97 dieser Schlussanträge.

27 — Siehe Nrn. 185 bis 262 dieser Schlussanträge.

28 — Vgl. insbesondere Menschenrechtsrat der Vereinten Nationen, Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung vom 17. April 2013, A/HRC/23/40, Nr. 33: „Bedingt durch den technologischen Fortschritt führt der Staat Überwachungstätigkeiten aus, die nach Umfang oder Dauer keinen Beschränkungen mehr unterliegen. ... Der Staat verfügt daher gegenwärtig mehr denn je über zusätzliche Möglichkeiten, Überwachungstätigkeiten gleichzeitig, unter Eingriff in die Privatsphäre, gezielt und in großem Maßstab vorzunehmen ...“ Vgl. auch Nr. 50: „Allgemein hat die Gesetzgebung mit dem Tempo des technologischen Wandels nicht Schritt gehalten. In den meisten Staaten sind Rechtsvorschriften entweder nicht vorhanden oder ungeeignet, um den modernen Bedingungen der Kommunikationsüberwachung zu begegnen.“

128. Die genannte Verpflichtung stellt einen schweren Eingriff in das durch Art. 7 der Charta garantierte Recht auf Achtung der Privatsphäre und in das durch Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar. Ich halte es nicht für sinnvoll, bei dieser Feststellung, die der Gerichtshof in den Rn. 32 bis 37 des DRI-Urteils eindeutig bestätigt hat, länger zu verweilen<sup>29</sup>. Eine generelle Verpflichtung zur Vorratsspeicherung stellt auch einen Eingriff in mehrere in der Richtlinie 2002/58 verankerte Rechte dar<sup>30</sup>.

129. In einem zweiten Schritt der Analyse ist zu prüfen, ob und unter welchen Voraussetzungen dieser schwere Eingriff in die in der Richtlinie 2002/58 verankerten Rechte und in die in den Art. 7 und 8 der Charta verankerten Grundrechte gerechtfertigt werden kann.

130. Die Voraussetzungen, die erfüllt sein müssen, damit dieser zweifache Eingriff gerechtfertigt ist, sind in zwei Vorschriften normiert: Art. 15 Abs. 1 der Richtlinie 2002/58, der die Befugnis der Mitgliedstaaten regelt, den Umfang bestimmter in der Richtlinie niedergelegter Rechte zu beschränken, und Art. 52 Abs. 1 der Charta im Licht des DRI-Urteils, der Einschränkungen bei der Ausübung der in der Charta verankerten Rechte regelt.

131. Zu beachten ist, dass diese Voraussetzungen als *kumulativ* zu verstehen sind. Die Einhaltung der in Art. 15 Abs. 1 der Richtlinie 2002/58 aufgestellten Anforderungen bedeutet für sich genommen nicht, dass die in Art. 52 Abs. 1 der Charta vorgesehenen Anforderungen erfüllt sind, und umgekehrt<sup>31</sup>. Eine generelle Verpflichtung zur Vorratsspeicherung kann daher nur dann als mit dem Unionsrecht vereinbar angesehen werden, wenn sie sowohl die Anforderungen nach Art. 15 Abs. 1 der Richtlinie 2002/58 als auch die nach Art. 52 Abs. 1 der Charta erfüllt, wie die Law Society of England and Wales dargelegt hat<sup>32</sup>.

132. Diese beiden Bestimmungen stellen zusammen sechs Voraussetzungen auf, die erfüllt sein müssen, damit der durch die generelle Verpflichtung zur Vorratsspeicherung herbeigeführte Eingriff gerechtfertigt ist:

- Die Vorratsspeicherungspflicht muss eine gesetzliche Grundlage haben;
- sie muss den Wesensgehalt der in der Charta verankerten Rechte wahren;
- sie muss einer dem Gemeinwohl dienenden Zielsetzung entsprechen;
- sie muss zur Verfolgung dieses Ziels geeignet sein;
- sie muss für die Verfolgung des genannten Ziels erforderlich sein, und
- sie muss in einer demokratischen Gesellschaft in angemessenem Verhältnis zur Verfolgung dieses Ziels stehen.

29 — Ich werde jedoch auf die spezifischen Gefahren, die in der Entwicklung von Datenbanken dieser Größe liegen, im Rahmen des Erfordernisses der Verhältnismäßigkeit einer generellen Vorratsspeicherungspflicht wie der in den Ausgangsverfahren fraglichen in einer demokratischen Gesellschaft zurückkommen, siehe Nrn. 252 bis 261 dieser Schlussanträge.

30 — Vgl. insoweit das Vorbringen der Open Rights Group und von Privacy International, das in Nr. 104 dieser Schlussanträge zusammengefasst ist.

31 — Diese kumulative Natur wird bestätigt durch den letzten Satz von Art. 15 Abs. 1 der Richtlinie 2002/58, wonach „[a]lle in diesem Absatz genannten Maßnahmen ... den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des [EUV] niedergelegten Grundsätzen entsprechen [müssen]“. Nach Art. 6 Abs. 1 EUV erkennt „[d]ie Union ... die Rechte, Freiheiten und Grundsätze an, die in der Charta ... niedergelegt sind; die Charta ... und die Verträge sind rechtlich gleichrangig“.

32 — Aus dieser kumulativen Natur ergibt sich folgerichtig, dass, wenn sich die von diesen beiden Bestimmungen aufgestellten Voraussetzungen überschneiden, die Voraussetzung zu gelten hat, die am strengsten ist oder, mit anderen Worten, die die in Rede stehenden Rechte am stärksten schützt.

133. Mehrere dieser Voraussetzungen hat der Gerichtshof im DRI-Urteil angesprochen. Aus Gründen der Klarheit und in Anbetracht der Besonderheiten der vorliegenden Rechtssachen im Vergleich zur DRI-Rechtssache möchte ich jedoch auf jede einzelne von ihnen eingehen und die Anforderungen, die sich auf die Rechtsgrundlage, die Erforderlichkeit und die Verhältnismäßigkeit einer Vorratsspeicherungspflicht in einer demokratischen Gesellschaft beziehen, ausführlicher prüfen.

#### 1. Zum Erfordernis einer gesetzlichen Grundlage im innerstaatlichen Recht

134. Sowohl Art. 52 Abs. 1 der Charta als auch Art. 15 Abs. 1 der Richtlinie 2002/58 stellen Voraussetzungen bezüglich der gesetzlichen Grundlage auf, auf die sich ein Mitgliedstaat zur Einführung einer generellen Verpflichtung zur Vorratsspeicherung stützen muss.

135. Erstens muss nach Art. 52 Abs. 1 der Charta jede Einschränkung der Ausübung der in ihr anerkannten Rechte „gesetzlich vorgesehen“ sein. Ich weise darauf hin, dass der Gerichtshof dieses Erfordernis im DRI-Urteil, das einen von einer Richtlinie vorgesehenen Eingriff betraf, nicht ausdrücklich geprüft hat.

136. Bis zu dem unlängst ergangenen Urteil *WebMindLicenses*<sup>33</sup> hat der Gerichtshof nie über die genaue Tragweite dieses Erfordernisses entschieden, auch nicht, wenn er ausdrücklich feststellte, dass dieses Erfordernis erfüllt<sup>34</sup> oder nicht erfüllt<sup>35</sup> war. In Rn. 81 dieses Urteils hat die Dritte Kammer des Gerichtshofs Folgendes ausgeführt:

„Hierzu ist darauf hinzuweisen, dass die Anforderung, dass jede Einschränkung der Ausübung dieses Rechts gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für die Verwendung der in der vorangegangenen Randnummer erwähnten Beweise durch die Steuerbehörde hinreichend klar und genau sein muss und dass sie dadurch, dass sie selbst den Umfang der Einschränkung der Ausübung des durch Art. 7 der Charta garantierten Rechts festlegt, einen gewissen Schutz gegen etwaige willkürliche Eingriffe der Steuerbehörde bietet (vgl. u. a. Urteile des Europäischen Gerichtshofs für Menschenrechte vom 2. August 1984, *Malone/Vereinigtes Königreich*, Serie A, Bd. 82, Nr. 67, sowie vom 12. Januar 2010, *Gillan und Quinton/Vereinigtes Königreich*, Beschwerde Nr. 4158/05, EGMR 2010, Nr. 77).“

137. Die Große Kammer des Gerichtshofs sollte in den vorliegenden Rechtssachen aus folgenden Gründen an dieser Auslegung festhalten.

138. Wie Generalanwalt Cruz Villalón in seinen Schlussanträgen in der Rechtssache *Scarlet Extended*<sup>36</sup> ausgeführt hat, hat der EGMR eine umfangreiche Rechtsprechung zu diesem Erfordernis im Kontext der EMRK begründet, die dadurch gekennzeichnet ist, dass der Begriff „Gesetz“ im materiellen und nicht im formellen Sinne zu verstehen ist<sup>37</sup>.

33 — Urteil vom 17. Dezember 2015 (C-419/14, EU:C:2015:832).

34 — Vgl. insbesondere Urteile vom 17. Oktober 2013, *Schwarz* (C-291/12, EU:C:2013:670, Rn. 35) (Eingriff durch eine europäische Verordnung), vom 27. Mai 2014, *Spasic* (C-129/14 PPU, EU:C:2014:586, Rn. 57) (Eingriff durch das am 19. Juni 1990 in Schengen unterzeichnete und am 26. März 1995 in Kraft getretene Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen), vom 6. Oktober 2015, *Delvigne* (C-650/13, EU:C:2015:648, Rn. 47) (Eingriff durch den Code électoral [französisches Wahlgesetzbuch] und den Code pénal [französisches Strafgesetzbuch]), und vom 17. Dezember 2015, *Neptune Distribution* (C-157/14, EU:C:2015:823, Rn. 69) (Eingriff durch eine europäische Verordnung und eine europäische Richtlinie).

35 — Urteil vom 1. Juli 2010, *Knauf Gips/Kommission* (C-407/08 P, EU:C:2010:389, Rn. 87 bis 92) (Eingriff ohne gesetzliche Grundlage).

36 — C-70/10, EU:C:2011:255, Rn. 94 bis 100.

37 — Vgl. insbesondere EGMR vom 14. September 2010, *Sanoma Uitgevers B.V./Niederlande* (CE:ECHR:2010:0914JUD003822403, § 83).

139. Nach dieser Rechtsprechung beinhaltet der Ausdruck „gesetzlich vorgesehen“, dass die gesetzliche Grundlage hinreichend zugänglich und vorhersehbar ist, d. h. so genau formuliert ist, dass der Einzelne sein Verhalten, gegebenenfalls nach Einholung sachkundigen Rates, danach richten kann. Diese gesetzliche Grundlage muss auch geeigneten Schutz gegen Willkür bieten und damit den Umfang und die Art und Weise der Ausübung der den zuständigen Behörden verliehenen Befugnis hinreichend klar definieren (Grundsatz der Rechtsstaatlichkeit)<sup>38</sup>.

140. Meiner Ansicht nach muss dem in Art. 52 Abs. 1 der Charta verwendeten Ausdruck „gesetzlich vorgesehen“ aus folgenden Gründen dieselbe Bedeutung beigemessen werden, wie sie dieser Ausdruck im Zusammenhang der EMRK hat.

141. Zum einen kann nach Art. 53 der Charta und den Erläuterungen zu diesem Artikel das durch die Charta gebotene Schutzniveau nie geringer sein als das von der EMRK garantierte Schutzniveau. Dieses Verbot, die „EMRK-Schwelle“ zu passieren, beinhaltet, dass die Auslegung des in Art. 52 Abs. 1 der Charta verwendeten Ausdrucks „gesetzlich vorgesehen“ durch den Gerichtshof mindestens ebenso streng sein muss wie die des EGMR im Kontext der EMRK<sup>39</sup>.

142. Zum anderen wäre es angesichts des horizontalen Charakters dieses Erfordernisses, das für zahlreiche Arten von Eingriffen sowohl im Kontext der Charta als auch in dem der EMRK Geltung haben kann<sup>40</sup>, unzweckmäßig, für die Mitgliedstaaten unterschiedliche Kriterien festzulegen, je nachdem, ob der Eingriff anhand des einen oder des anderen dieser Rechtsinstrumente geprüft wird<sup>41</sup>.

143. Wie die estnische Regierung und die Kommission bin ich daher der Auffassung, dass der in Art. 52 Abs. 1 der Charta enthaltene Ausdruck „gesetzlich vorgesehen“ im Licht der in Nr. 139 dieser Schlussanträge zusammengefassten Rechtsprechung des EGMR dahin auszulegen ist, dass eine Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren in Rede stehende in einer gesetzlichen Grundlage vorgesehen sein muss, die hinreichend zugänglich und vorhersehbar ist und einen geeigneten Schutz gegen Willkür bietet.

144. Zweitens ist zu bestimmen, welchen Inhalt die in Art. 15 Abs. 1 der Richtlinie 2002/58 aufgestellten Anforderungen bezüglich der gesetzlichen Grundlage haben, die ein Mitgliedstaat heranziehen muss, der von der durch diese Bestimmung eingeräumten Befugnis Gebrauch machen will.

145. Hierzu ist festzustellen, dass es Unterschiede zwischen den Sprachfassungen des ersten Satzes der genannten Bestimmung gibt.

146. In der englischen („legislative measures“), der französischen („mesures législatives“), der italienischen („disposizioni legislative“), der portugiesischen („medidas legislativas“), der rumänischen („măsuri legislative“) und der schwedischen („genom lagstiftning vidta åtgärder“) Fassung verlangt Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 Maßnahmen des Gesetzgebers.

38 — Vgl. insbesondere EGMR vom 26. März 1987, Leander/Schweden (CE:ECHR:1987:0326JUD000924881, §§ 50 und 51), EGMR vom 26. Oktober 2000, Hassan und Tchaouch/Bulgarien (CE:ECHR:2000:1026JUD003098596, § 84), EGMR vom 4. Dezember 2008, S. und Marper/Vereinigtes Königreich (CE:ECHR:2008:1204JUD003056204, § 95), EGMR vom 14. September 2010, Sanoma Uitgevers B.V./Niederlande (CE:ECHR:2010:0914JUD003822403, §§ 81 bis 83), EGMR vom 31. März 2016, Stoyanov u. a./Bulgarien (CE:ECHR:2016:0331JUD005538810, §§ 124 bis 126).

39 — Genauer gesagt kann der Gerichtshof meines Erachtens keine Auslegung vertreten, die weniger streng wäre als die des EGMR; dies hätte zur Folge, dass eine größere Zahl von Eingriffen möglich wäre als nach der Auslegung dieses Erfordernisses durch den EGMR.

40 — Der Ausdruck „gesetzlich vorgesehen“ wird in Art. 8 Abs. 2 (Recht auf Achtung des Privat- und Familienlebens), Art. 9 Abs. 2 (Gedanken-, Gewissens- und Religionsfreiheit), Art. 10 Abs. 2 (Freiheit der Meinungsäußerung) und Art. 11 Abs. 2 (Versammlungs- und Vereinigungsfreiheit) der EMRK verwendet. Im Kontext der Charta gilt Art. 52 Abs. 1 für jede Einschränkung der Ausübung der in dieser Charta verankerten Rechte, vorausgesetzt, die Einschränkung ist zulässig.

41 — Vgl. in diesem Sinne Peers, S., „Article 52 – Scope of guaranteed rights“, in Peers, S., u. a., *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, Nr. 52.39.

147. Dagegen können die dänische („retsfor skrifter“), die deutsche („Rechtsvorschriften“), die niederländische („wettelijke maatregelen“) und die spanische („medidas legales“) Fassung dieses Satzes dahin ausgelegt werden, dass sie entweder Maßnahmen des Gesetzgebers oder Vorschriften der vollziehenden Gewalt verlangt.

148. Nach ständiger Rechtsprechung schließt die Notwendigkeit der einheitlichen Anwendung und damit der einheitlichen Auslegung eines Rechtsakts der Union es aus, ihn in einer seiner Fassungen isoliert zu betrachten, sondern gebietet es vielmehr, ihn nach dem wirklichen Willen seines Urhebers und dem von diesem verfolgten Zweck im Licht seiner Fassung in allen anderen Amtssprachen auszulegen. Falls die Fassungen voneinander abweichen, muss die betreffende Vorschrift daher grundsätzlich anhand der allgemeinen Systematik und des Zwecks der Regelung ausgelegt werden, zu der sie gehört<sup>42</sup>.

149. Im vorliegenden Fall regelt Art. 15 Abs. 1 der Richtlinie 2002/58 die Befugnis der Mitgliedstaaten, von den in den Art. 7 und 8 der Charta verankerten Grundrechten abzuweichen, deren Schutz durch diese Richtlinie verwirklicht wird. Ich halte es daher für zweckmäßig, das von Art. 15 Abs. 1 der Richtlinie 2002/58 vorgeschriebene Erfordernis der gesetzlichen Grundlage im Licht der Charta, insbesondere des Art. 52 Abs. 1 der Charta, auszulegen.

150. Die von Art. 15 Abs. 1 der Richtlinie 2002/58 geforderten „Rechtsvorschriften“ müssen, wie in Nr. 143 dieser Schlussanträge ausgeführt, zugänglich und vorhersehbar sein und einen geeigneten Schutz gegen Willkür bieten. Aus diesen Merkmalen, vor allem aus dem Erfordernis eines geeigneten Schutzes gegen Willkür, ergibt sich insbesondere, dass diese Rechtsvorschriften für die nationalen Behörden, denen das Recht auf Zugang zu den auf Vorrat gespeicherten Daten gewährt wird, *verbindlich* sein müssen. Es würde insbesondere nicht genügen, dass die mit dem Zugang zu diesen Daten einhergehenden Garantien in Verwaltungsvorschriften oder internen Leitlinien vorgesehen sind, die diesen verbindlichen Charakter nicht haben, wie die Law Society of England and Wales zu Recht hervorgehoben hat.

151. Der allen Sprachfassungen des Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 gemeinsame Ausdruck „[d]ie Mitgliedstaaten können [Vorschriften] erlassen“ schließt meines Erachtens aus, dass eine innerstaatliche, und sei es ständige, Rechtsprechung eine hinreichende gesetzliche Grundlage für die Durchführung dieser Bestimmung sein kann. Ich weise darauf hin, dass die genannte Bestimmung insoweit über die sich aus der Rechtsprechung des EGMR ergebenden Anforderungen hinausgeht<sup>43</sup>.

152. Zudem erscheint es mir wünschenswert, dass in Anbetracht der Schwere des Eingriffs in die Grundrechte der Art. 7 und 8 der Charta, den eine generelle Verpflichtung zur Vorratsspeicherung bedeutet, der Wesensgehalt der in Frage stehenden Regelung, vor allem aber der Inhalt der mit dieser Verpflichtung einhergehenden Garantien, in einer Maßnahme der gesetzgebenden Gewalt festgelegt wird, deren Anwendung sodann von der Exekutive näher zu regeln ist.

153. Nach alledem bin ich der Ansicht, dass Art. 15 Abs. 1 der Richtlinie 2002/58 und Art. 52 Abs. 1 der Charta dahin auszulegen sind, dass die Regelung, die eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren fragliche vorsieht, durch Rechtsvorschriften aufgestellt werden muss, die zugänglich und vorhersehbar sind und einen geeigneten Schutz gegen Willkür bieten.

42 — Vgl. insbesondere Urteile vom 30. Mai 2013, *Asbeek Brusse und de Man Garabito* (C-488/11, EU:C:2013:341, Rn. 26), vom 24. Juni 2015, *Hotel Sava Rogaška* (C-207/14, EU:C:2015:414, Rn. 26), und vom 26. Februar 2015, *Christie's France* (C-41/14, EU:C:2015:119, Rn. 26).

43 — Vgl. insbesondere EGMR vom 14. September 2010, *Sanoma Uitgevers B.V./Niederlande* (CE:ECHR:2010:0914JUD003822403, § 83): „[Der Begriff ‚Gesetz‘ in den Art. 8 bis 11 EMRK umfasst] zugleich das ‚geschriebene Recht‘, das sowohl die Vorschriften unterhalb Gesetzesrang als auch die Rechtsakte einschließt, die eine berufsständische Vereinigung kraft Ermächtigung des Gesetzgebers im Rahmen ihrer autonomen Rechtsetzungsbefugnis erlässt, und das ‚ungeschriebene Recht‘. Das ‚Gesetz‘ ist so zu verstehen, dass darunter sowohl das geschriebene Recht als auch das ‚Richterrecht‘ fällt.“

154. Es ist Sache der vorlegenden Gerichte, die Einhaltung dieses Erfordernisses zu prüfen, da sie am besten in der Lage sind, ihre jeweiligen nationalen Regelungen zu beurteilen.

## 2. Zur Wahrung des Wesensgehalts der durch die Art. 7 und 8 der Charta anerkannten Rechte

155. Nach Art. 52 Abs. 1 muss jede Einschränkung der in der Charta anerkannten Rechte „den Wesensgehalt dieser Rechte achten“<sup>44</sup>. Dieser Aspekt, den der Gerichtshof in den Rn. 39 und 40 des DRI-Urteils im Zusammenhang mit der Richtlinie 2006/24 geprüft hat, wirft meines Erachtens in den vorliegenden Rechtssachen kein spezifisches Problem auf, wie die spanische und die irische Regierung sowie die Kommission dargelegt haben.

156. In Rn. 39 des DRI-Urteils hat der Gerichtshof festgestellt, dass die genannte Richtlinie den Wesensgehalt des Rechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte nicht antastet, da sie es nicht gestattet, vom Inhalt elektronischer Kommunikation als solchem Kenntnis zu erlangen.

157. Diese Beurteilung kann meines Erachtens auf die in den Ausgangsverfahren in Rede stehenden nationalen Regelungen übertragen werden, da diese es ebenfalls nicht gestatten, vom Inhalt elektronischer Kommunikation als solchem Kenntnis zu erlangen<sup>45</sup>.

158. In Rn. 40 des DRI-Urteils hat der Gerichtshof entschieden, dass die Richtlinie 2006/24 den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten nicht antastet, da die Grundsätze des Datenschutzes und der Datensicherheit von den Betreibern nach Art. 7 der genannten Richtlinie eingehalten werden müssen und die Mitgliedstaaten nach diesen Grundsätzen sicherzustellen haben, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen.

159. Meines Erachtens ist auch diese Beurteilung auf die in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen übertragbar, da sie vergleichbare Garantien für den Schutz und die Sicherheit der von den Betreibern auf Vorrat gespeicherten Daten vorsehen und diese Garantien einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen sollen<sup>46</sup>.

160. Das vorliegende Gericht hat jedoch zu prüfen, ob die in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen den Wesensgehalt der durch die Art. 7 und 8 der Charta anerkannten Rechte unter Berücksichtigung der vorstehenden Erwägungen tatsächlich wahren.

## 3. Zum Bestehen einer dem Gemeinwohl dienenden Zielsetzung, die von der Union anerkannt wird und die eine generelle Verpflichtung zur Vorratsspeicherung rechtfertigen kann

161. Sowohl Art. 15 Abs. 1 der Richtlinie 2002/58 als auch Art. 52 Abs. 1 der Charta verlangen, dass jeder Eingriff in die darin verankerten Rechte einer dem Gemeinwohl dienenden Zielsetzung entspricht.

44 — Dieses Erfordernis ergibt sich aus den in den Nrn. 99 bis 116 dieser Schlussanträge genannten Gründen weder aus dem Wortlaut des Art. 15 Abs. 1 der Richtlinie 2002/58 noch aus der Systematik dieser Richtlinie.

45 — Vgl. die Darstellung der in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen, insbesondere in den Nrn. 13 und 36 dieser Schlussanträge.

46 — DRI-Urteil, Rn. 54. Vgl. die Darstellung der in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen in den Nrn. 29 bis 33 sowie 45 und 46 dieser Schlussanträge.

162. In den Rn. 41 bis 44 des DRI-Urteils hat der Gerichtshof zum einen festgestellt, dass die von der Richtlinie 2006/24 vorgeschriebene generelle Verpflichtung zur Vorratsspeicherung „zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit“ beiträgt, und zum anderen, dass diese Bekämpfung eine dem Gemeinwohl dienende Zielsetzung der Union darstellt.

163. Nach der Rechtsprechung des Gerichtshofs stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union dar. Dasselbe gilt für die Bekämpfung schwerer Kriminalität, um die öffentliche Sicherheit zu gewährleisten. Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat<sup>47</sup>.

164. Diese Beurteilung ist übertragbar auf die in den Ausgangsverfahren in Rede stehenden generellen Verpflichtungen zur Vorratsspeicherung, die durch das Ziel der Bekämpfung schwerer Kriminalität gerechtfertigt sein können.

165. Bestimmte vor dem Gerichtshof vorgetragene Argumente geben allerdings Anlass zur Prüfung der Frage, ob diese Verpflichtung durch eine andere dem Gemeinwohl dienende Zielsetzung als die der Bekämpfung schwerer Kriminalität gerechtfertigt werden kann.

166. Art. 52 Abs. 1 der Charta führt insoweit allgemein die „von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen“ und die „Erfordernisse des Schutzes der Rechte und Freiheiten anderer“ an.

167. In Art. 15 Abs. 1 der Richtlinie 2002/58 sind die Zielsetzungen, die einen Eingriff in die durch diese Richtlinie begründeten Rechte rechtfertigen können, genauer beschrieben. Nach dieser Bestimmung müssen die betreffenden Maßnahmen dazu beitragen, „gemäß Artikel 13 Absatz 1 der Richtlinie 95/46 ... 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“ zu gewährleisten.

168. Zudem hat der Gerichtshof im Urteil *Promusicae*<sup>48</sup> festgestellt, dass diese Bestimmung im Licht des Art. 13 Abs. 1 der Richtlinie 95/46 auszulegen ist, der Abweichungen von den in dieser Richtlinie vorgesehenen Rechten zulässt, wenn sie durch „den Schutz ... der Rechte und Freiheiten anderer Personen“ gerechtfertigt sind. Demgemäß hat er entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58 den Mitgliedstaaten die Möglichkeit gibt, eine Pflicht des Betreibers zur Weitergabe personenbezogener Daten vorzusehen, damit im Rahmen eines zivilrechtlichen Verfahrens festgestellt werden kann, ob eine Verletzung von Urheberrechten an Musikaufnahmen und audiovisuellen Aufnahmen vorliegt.

169. Die Regierung des Vereinigten Königreichs stützt sich auf das genannte Urteil, um geltend zu machen, dass jede Zielsetzung, die in Art. 15 Abs. 1 der Richtlinie 2002/58 oder in Art. 13 Abs. 1 der Richtlinie 95/46 genannt sei, eine Verpflichtung zur Vorratsspeicherung rechtfertigen könne. Diese Verpflichtung könne durch den Nutzen gerechtfertigt sein, den die auf Vorrat gespeicherten Daten bei der Bekämpfung „einfacher“ (im Gegensatz zu „schwerer“) Kriminalität oder auch im Kontext nicht strafrechtlicher Verfahren für die von diesen Bestimmungen angeführten Zielsetzungen hätten.

170. Dieses Argument überzeugt mich aus folgenden Gründen nicht.

47 — DRI-Urteil, Rn. 42 und die dort angeführte Rechtsprechung.

48 — Urteil vom 29. Januar 2008 (C-275/06, EU:C:2008:54, Rn. 50 bis 54).

171. Erstens ist, wie Herr Watson sowie die Open Rights Group und Privacy International vorgetragen haben, der vom Gerichtshof im Urteil *Promusicae*<sup>49</sup> verfolgte Ansatz nicht auf die vorliegenden Rechtssachen übertragbar, da dieses Urteil den Antrag einer Vereinigung von Urheberrechtsinhabern auf Zugang zu Daten betrifft, die spontan von einem Betreiber, Telefónica de España, auf Vorrat gespeichert wurden. Mit anderen Worten, dieses Urteil befasste sich nicht mit Zielsetzungen, die eine Rechtfertigung für schwerwiegende Grundrechtseingriffe sein können, zu denen eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren in Rede stehende führt.

172. Zweitens schließt es meines Erachtens das Erfordernis der Verhältnismäßigkeit in einer demokratischen Gesellschaft aus, dass die Bekämpfung einfacher Kriminalität oder der ordnungsgemäße Ablauf von nicht strafrechtlichen Verfahren eine Rechtfertigung für eine generelle Verpflichtung zur Vorratsspeicherung sein kann. Die erheblichen Gefahren, die von einer solchen Verpflichtung ausgehen, stehen nämlich außer Verhältnis zu den Vorteilen, die sie bei der Bekämpfung leichter Kriminalität oder im Kontext nicht strafrechtlicher Verfahren verschaffen würde<sup>50</sup>.

173. Nach alledem bin ich der Ansicht, dass Art. 15 Abs. 1 der Richtlinie 2002/58 und Art. 52 Abs. 1 der Charta dahin auszulegen sind, dass im Unterschied zur Bekämpfung einfacher Kriminalität oder zum ordnungsgemäßen Ablauf von nicht strafrechtlichen Verfahren die Bekämpfung schwerer Kriminalität eine dem Gemeinwohl dienende Zielsetzung darstellt, die eine generelle Verpflichtung zur Vorratsspeicherung rechtfertigen kann.

174. Folglich sind Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit dieser Verpflichtung im Licht des Ziels der Bekämpfung schwerer Kriminalität zu prüfen.

4. Zur Geeignetheit einer generellen Verpflichtung zur Vorratsspeicherung im Hinblick auf die Bekämpfung schwerer Kriminalität

175. Die Erfordernisse der Geeignetheit, der Erforderlichkeit<sup>51</sup> und der Verhältnismäßigkeit<sup>52</sup> ergeben sich sowohl aus Art. 15 Abs. 1 der Richtlinie 2002/58 als auch aus Art. 52 Abs. 1 der Charta.

176. Aufgrund des ersten Erfordernisses muss eine generelle Verpflichtung zur Vorratsspeicherung wie die in den Ausgangsverfahren fragliche geeignet sein, zu der oben bezeichneten dem Gemeinwohl dienenden Zielsetzung beizutragen, d. h. zur Bekämpfung schwerer Kriminalität.

177. Dieses Erfordernis bereitet im Zusammenhang der vorliegenden Rechtssachen keine besonderen Schwierigkeiten. Wie der Gerichtshof im Wesentlichen in Rn. 49 des DRI-Urteils ausgeführt hat, bieten die auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden eine zusätzliche Ermittlungsmöglichkeit zur Verhütung oder Aufklärung schwerer Straftaten. Die genannte Verpflichtung trägt daher zur Bekämpfung schwerer Kriminalität bei.

178. Dennoch möchte ich näher auf den Nutzen eingehen, den eine generelle Verpflichtung zur Vorratsspeicherung bei der Bekämpfung schwerer Kriminalität haben kann. Wie die französische Regierung zu Recht geltend gemacht hat, ermöglicht es diese Verpflichtung in gewissem Umfang den Strafverfolgungsbehörden – anders als bei gezielten Überwachungsmaßnahmen –, durch Abfragen der auf Vorrat gespeicherten Daten die „Vergangenheit zu entschlüsseln“.

49 — Urteil vom 29. Januar 2008 (C-275/06, EU:C:2008:54).

50 — Siehe Nrn. 252 bis 261 dieser Schlussanträge.

51 — Zur Erforderlichkeit siehe Nrn. 185 bis 245 dieser Schlussanträge.

52 — Zur Verhältnismäßigkeit im engeren Sinne siehe Nrn. 246 bis 262 dieser Schlussanträge.

179. Eine gezielte Überwachungsmaßnahme ist auf Personen gerichtet, bei denen zuvor festgestellt wurde, dass sie in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnten. Solche gezielten Maßnahmen erlauben es den Strafverfolgungsbehörden, auf Kommunikationsdaten dieser Personen oder sogar auf den Inhalt der betreffenden Kommunikationsvorgänge zuzugreifen. Allerdings kann dieser Zugang nur die Kommunikationsvorgänge erfassen, die von den betreffenden Personen *nach* ihrer Identifizierung abgewickelt wurden.

180. Dagegen erfasst eine generelle Verpflichtung zur Vorratsspeicherung alle Kommunikationsvorgänge sämtlicher Nutzer, ohne dass irgendein Bezug zu einer schweren Straftat erforderlich ist. Diese Verpflichtung ermöglicht es den zuständigen Behörden, auf alle zurückliegenden Kommunikationsvorgänge einer Person zuzugreifen, bevor bei ihr ein solcher Bezug festgestellt wurde. Insofern verleiht diese Verpflichtung den Strafverfolgungsbehörden die begrenzte Fähigkeit zur Entschlüsselung der Vergangenheit, indem sie ihnen Zugang zu den Kommunikationsvorgängen gewährt, die diese Personen *vor* ihrer Identifizierung abwickeln<sup>53</sup>.

181. Mit anderen Worten, der Nutzen, den eine generelle Verpflichtung zur Vorratsspeicherung bei der Bekämpfung schwerer Kriminalität haben kann, liegt in der begrenzten Fähigkeit, die Vergangenheit mit Hilfe von Daten zu entschlüsseln, die die Kommunikationsvorgänge einer Person aus einer Zeit nachzeichnen, in der diese noch nicht im Verdacht stand, zu einer schweren Straftat in Beziehung zu stehen<sup>54</sup>.

182. Bei der Vorlage des Richtlinienvorschlags, der zum Erlass der Richtlinie 2006/24 geführt hat, machte die Kommission diesen Nutzen an mehreren konkreten Beispielen deutlich, in denen insbesondere wegen Terrorismus, Mord, Entführung und Kinderpornografie ermittelt worden war<sup>55</sup>.

183. Mehrere ähnliche Beispiele sind dem Gerichtshof im Rahmen der vorliegenden Verfahren vorgetragen worden, insbesondere von der französischen Regierung, die auf die positive Verpflichtung der Mitgliedstaaten hingewiesen hat, die Sicherheit der sich in ihrem jeweiligen Hoheitsgebiet aufhaltenden Personen zu gewährleisten. Die französische Regierung ist der Auffassung, dass bei den Ermittlungen im Zusammenhang mit der Zerschlagung von Banden, die die Ausreise von in Frankreich ansässigen Personen in irakische und syrische Konfliktregionen organisierten, der Zugang zu den auf Vorrat gespeicherten Daten bei der Identifizierung von Personen, die diese Ausreise unterstützt hätten, eine entscheidende Rolle spiele. Der Zugang zu den Kommunikationsdaten der an den jüngsten Terroranschlägen von Januar und November 2015 in Frankreich beteiligten Personen sei

53 — Auch die Kommission hat darauf hingewiesen, dass der Mehrwert einer generellen Verpflichtung zur Vorratsspeicherung gegenüber einer gezielten Datenspeicherung in der begrenzten Fähigkeit liegt, die Vergangenheit zu entschlüsseln, vgl. Commission Staff Working Document als Anlage zum Richtlinienvorschlag, der zum Erlass der Richtlinie 2006/24 geführt hat, SEK(2005) 1131, 21. September 2005, Nr. 3.6, „Data Preservation versus Data Retention“: „[W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects.“

54 — Die französische Regierung bezieht sich insoweit auf den Rapport du Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, S. 209 und 210. Der Conseil d'État hebt hervor, dass ein Mechanismus gezielter Überwachungsmaßnahmen unter dem Gesichtspunkt der nationalen Sicherheit und der Fahndung nach dem Straftäter „deutlich weniger effizient wäre als die systematische Vorratsspeicherung. Der Mechanismus erlaubt keinen nachträglichen Zugriff auf Daten, die ausgetauscht wurden, bevor die Behörde eine Bedrohung oder Straftat feststellte. Seine Funktionsfähigkeit würde somit davon abhängen, dass die Behörden in der Lage sind, die Identität der Personen vorauszusehen, deren Verbindungsdaten von Nutzen sein können, was im Rahmen der kriminalpolizeilichen Arbeit nicht möglich ist. Bei einer Straftat z. B. könnte die Justizbehörde nicht auf Kommunikationsvorgänge zugreifen, die vor dieser Straftat stattfanden, obwohl diese Daten aufschlussreich und für die Identifizierung des Straftäters und seiner Komplizen gelegentlich sogar unentbehrlich sind, wie sich in einigen Fällen terroristischer Anschläge in jüngerer Zeit gezeigt hat. Im Bereich der Verhütung von Verstößen gegen die nationale Sicherheit beruhen die neuen technischen Programme auf dem Vermögen, schwache Signale zu erkennen, was unvereinbar mit der Idee des Pretargeting der Gefährder ist.“

55 — Commission Staff Working Document als Anlage zum Richtlinienvorschlag, der zum Erlass der Richtlinie geführt hat, 2006/24 SEK(2005) 1131, 21. September 2005, Nr. 1.2, „The importance of traffic data for law enforcement“.

für die Ermittler bei der Aufdeckung der Komplizen dieser Anschläge äußerst hilfreich gewesen. Auch könnten bei der Suche nach einer vermissten Person die Daten über den Aufenthaltsort dieser Person zur Zeit der letzten Nachrichtenverbindung vor ihrem Verschwinden eine entscheidende Rolle für die Ermittlungen spielen.

184. Nach alledem bin ich der Ansicht, dass eine generelle Verpflichtung zur Vorratsspeicherung geeignet ist, zur Bekämpfung schwerer Kriminalität beizutragen. Es bleibt jedoch noch festzustellen, ob die Verpflichtung für die Erreichung dieses Ziels erforderlich ist und ob sie zu ihm in einem angemessenen Verhältnis steht.

5. Zur Erforderlichkeit einer generellen Verpflichtung zur Vorratsspeicherung für die Bekämpfung schwerer Kriminalität

185. Nach ständiger Rechtsprechung kann eine Maßnahme nur dann als erforderlich angesehen werden, wenn es keine andere Maßnahme gibt, die genauso geeignet, jedoch weniger belastend ist<sup>56</sup>.

186. Die Voraussetzung der Geeignetheit läuft letztlich auf eine Bewertung der „absoluten“ Wirksamkeit – unabhängig von jeder anderen denkbaren Maßnahme – einer generellen Verpflichtung zur Vorratsspeicherung in Bezug auf die Bekämpfung schwerer Kriminalität hinaus. Die Voraussetzung der Erforderlichkeit führt demgegenüber zur Beurteilung der Effizienz – oder „relativen“ Wirksamkeit, also ihrer Wirksamkeit im Vergleich zu jeder anderen denkbaren Maßnahme – einer solchen Verpflichtung<sup>57</sup>.

187. Im Kontext der vorliegenden Rechtssachen ist bei der Erforderlichkeitsprüfung zu untersuchen, ob zum einen andere Maßnahmen bei der Bekämpfung schwerer Kriminalität genauso wirksam sein könnten wie die generelle Verpflichtung zur Vorratsspeicherung und ob zum anderen diese etwaigen Maßnahmen die in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta verankerten Rechte weniger beeinträchtigen<sup>58</sup>.

188. Ich erinnere ferner an die in Rn. 52 des DRI-Urteils angeführte ständige Rechtsprechung, wonach der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das „absolut Notwendige“ beschränken müssen<sup>59</sup>.

56 — Vgl. insbesondere Urteile vom 22. Januar 2013, *Sky Österreich* (C-283/11, EU:C:2013:28, Rn. 54 bis 57), vom 13. November 2014, *Reindl* (C-443/13, EU:C:2014:2370, Rn. 39), und vom 16. Juli 2015, *CHEZ Razpredelenie Bulgaria* (C-83/14, EU:C:2015:480, Rn. 120 bis 122). In der Literatur vgl. insbesondere Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, S. 29: „Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value.“

57 — Vgl. Rivers, J., „Proportionality and variable intensity of review“, 65(1) *Cambridge Law Journal* (2006) 174, S. 198: „The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest.“

58 — Zu diesen beiden Gesichtspunkten bei der Erforderlichkeitsprüfung vgl. Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, S. 323 bis 331.

59 — Vgl. insbesondere Urteile vom 9. November 2010, *Volker und Markus Schecke und Eifert* (C-92/09 und C-93/09, EU:C:2010:662, Rn. 77 und 86), und vom 7. November 2013, *IPI* (C-473/12, EU:C:2013:715, Rn. 39).

189. Zwei Fragen, die sich auf das Erfordernis des absolut Notwendigen im Kontext der vorliegenden Rechtssachen beziehen, sind von den Beteiligten, die vor dem Gerichtshof Erklärungen abgegeben haben, eingehend erörtert worden; sie entsprechen im Wesentlichen den beiden Fragen des vorliegenden Gerichts in der Rechtssache C-203/15:

- Ist davon auszugehen, dass unter Berücksichtigung der Rn. 56 bis 59 des DRI-Urteils eine generelle Verpflichtung zur Vorratsspeicherung als solche über das für die Bekämpfung schwerer Kriminalität absolut Notwendige hinausgeht, und zwar unabhängig davon, ob etwaige Garantien mit dieser Verpflichtung einhergehen?
- Wenn davon auszugehen wäre, dass diese generelle Verpflichtung als solche nicht über das absolut Notwendige hinausgeht, müssen mit ihr alle vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien einhergehen, um die Verletzung der in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta verankerten Rechte auf das absolut Notwendige zu beschränken?

190. Vor einer Prüfung dieser Fragen halte ich es für angebracht, ein von der Regierung des Vereinigten Königreichs vorgebrachtes Argument zurückzuweisen, wonach die im DRI-Urteil aufgestellten Kriterien im Kontext der vorliegenden Rechtssachen unerheblich seien, weil das genannte Urteil keine innerstaatliche Regelung, sondern eine vom Unionsgesetzgeber erlassene Regelung betreffe.

191. Insoweit weise ich darauf hin, dass im DRI-Urteil die Art. 7, 8 und 52 Abs. 1 der Charta ausgelegt worden sind und dass diese Bestimmungen auch Gegenstand der in den Ausgangsverfahren gestellten Fragen sind. Meines Erachtens ist es nicht möglich, die Bestimmungen der Charta anders auszulegen, je nachdem, ob die betreffende Regelung auf Unionsebene oder auf innerstaatlicher Ebene aufgestellt wurde, wie Herr Brice und Herr Lewis sowie die Law Society of England and Wales zu Recht ausgeführt haben. Wenn festgestellt worden ist, dass die Charta Anwendung findet, wie dies in den vorliegenden Rechtssachen der Fall ist<sup>60</sup>, muss die Charta auf gleiche Weise unabhängig von der betreffenden Regelung angewandt werden. Die vom Gerichtshof im DRI-Urteil herangezogenen Kriterien sind daher für die Beurteilung der in den vorliegenden Rechtssachen in Rede stehenden innerstaatlichen Regelungen relevant, wie insbesondere die dänische und die irische Regierung sowie die Kommission geltend gemacht haben.

a) Zur Voraussetzung der absoluten Notwendigkeit einer generellen Verpflichtung zur Vorratsspeicherung

192. Nach einer Auffassung, die von Tele2 Sverige, der Open Rights Group und Privacy International vertreten wird, ist davon auszugehen, dass eine generelle Verpflichtung zur Vorratsspeicherung als solche nach dem DRI-Urteil über das für die Bekämpfung schwerer Kriminalität absolut Notwendige hinausgeht, und zwar unabhängig davon, ob etwaige Garantien mit dieser Verpflichtung einhergehen.

193. Nach einer anderen Auffassung, die von der Mehrheit der übrigen Beteiligten vertreten wird, die vor dem Gerichtshof Erklärungen abgegeben haben, geht eine solche Verpflichtung nicht über das absolut Notwendige hinaus, sofern mit ihr bestimmte Garantien einhergehen, die den Zugang zu den Daten, die Dauer der Vorratsspeicherung und den Schutz und die Sicherheit der Daten betreffen.

194. Aus folgenden Gründen schließe ich mich der zweiten Auffassung an.

<sup>60</sup> — Siehe Nrn. 117 bis 125 dieser Schlussanträge.

195. Erstens hat nach meinem Verständnis des DRI-Urteils der Gerichtshof dort festgestellt, dass eine generelle Verpflichtung zur Vorratsspeicherung über das absolut Notwendige hinausgeht, wenn sie *nicht einhergeht* mit strengen Garantien bezüglich des Datenzugangs, der Dauer der Vorratsspeicherung sowie des Schutzes und der Sicherheit der Daten. Dagegen hat der Gerichtshof nicht darüber befunden, ob eine generelle Verpflichtung zur Vorratsspeicherung, die mit diesen Garantien *einhergeht*, mit dem Unionsrecht vereinbar ist, da eine solche Regelung nicht Gegenstand der dem Gerichtshof in jener Rechtssache vorgelegten Fragen war.

196. In dieser Hinsicht betone ich, dass in den Rn. 56 bis 59 des DRI-Urteils eine Feststellung des Gerichtshofs dahin, dass eine Verpflichtung zur Vorratsspeicherung als solche über das absolut Notwendige hinausginge, nicht enthalten ist.

197. In den Rn. 56 und 57 dieses Urteils stellt der Gerichtshof fest, dass die in der Richtlinie 2006/24 vorgesehene Vorratsspeicherungspflicht alle elektronischen Kommunikationsmittel, alle Nutzer sowie alle Verkehrsdaten erfasst, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

198. In den Rn. 58 und 59 des genannten Urteils stellt der Gerichtshof die praktischen Folgen dieser mangelnden Differenzierung ausführlicher dar. Zum einen erfasst die Vorratsspeicherungspflicht auch Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zum anderen verlangt die Richtlinie keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung nicht auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte.

199. Damit stellt der Gerichtshof fest, dass eine generelle Verpflichtung zur Vorratsspeicherung dadurch gekennzeichnet ist, dass es an einer Differenzierung anhand des Ziels der Bekämpfung schwerer Straftaten fehlt. Er hat jedoch nicht entschieden, dass die mangelnde Differenzierung bedeutet, dass die Verpflichtung als solche über das absolut Notwendige hinausgeht.

200. Der Gerichtshof hat vielmehr erst am Ende der Prüfung der in der Richtlinie 2006/24 vorgesehenen Regelung und nach der Feststellung, dass bestimmte – von mir im Folgenden<sup>61</sup> zu prüfende – Garantien fehlen, in Rn. 69 des DRI-Urteils entschieden:

„Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste.“ (Hervorhebung nur hier)

201. Wenn, wie die deutsche und die niederländische Regierung geltend gemacht haben, allein die generelle Vorratsspeicherung genügt hätte, um zur Ungültigkeit der Richtlinie 2006/24 zu führen, hätte der Gerichtshof das Fehlen der in den Rn. 60 bis 68 des Urteils angeführten Garantien nicht – und nicht so ausführlich – untersuchen müssen.

61 — Siehe Nrn. 216 bis 245 dieser Schlussanträge.

202. Die in der Richtlinie 2006/24 vorgesehene generelle Verpflichtung zur Vorratsspeicherung ging somit als solche nicht über das absolut Notwendige hinaus. Die Richtlinie ging über das absolut Notwendige hinaus wegen des Zusammenwirkens der generellen Vorratsspeicherung und des Fehlens von Garantien, die die Verletzung der in den Art. 7 und 8 der Charta verankerten Rechte auf das absolut Notwendige beschränken. Wegen dieses Zusammenwirkens war die Richtlinie insgesamt für ungültig zu erklären<sup>62</sup>.

203. Zweitens wird diese Auslegung in Rn. 93 des Urteils Schrems<sup>63</sup> bestätigt, wo es heißt:

„Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, *ohne* irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen *und ohne* ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen (vgl. in diesem Sinne, in Bezug auf die Richtlinie 2006/24 ..., [DRI-Urteil], Rn. 57 bis 61).“ (Hervorhebung nur hier)

204. Auch hier hat der Gerichtshof nicht festgestellt, dass die in jener Rechtssache in Rede stehende Regelung allein deswegen über das absolut Notwendige hinausging, weil sie eine generelle Vorratsspeicherung personenbezogener Daten gestattet. In dem Fall waren die Grenzen des absolut Notwendigen überschritten wegen des Zusammenwirkens der Möglichkeit einer solchen generellen Vorratsspeicherung und des Fehlens einer Garantie hinsichtlich des Zugangs, um den Eingriff auf das absolut Notwendige zu beschränken.

205. Aus dem Vorstehenden ziehe ich den Schluss, dass bei einer generellen Verpflichtung zur Vorratsspeicherung nicht immer davon ausgegangen werden muss, dass sie als solche über das für die Bekämpfung schwerer Kriminalität absolut Notwendige hinausgeht. Eine solche Verpflichtung geht jedoch über das absolut Notwendige stets dann hinaus, wenn mit ihr keine Garantien hinsichtlich des Datenzugangs, der Dauer der Vorratsspeicherung sowie des Schutzes und der Sicherheit der Daten einhergehen.

206. Drittens wird meine Auffassung dadurch bestätigt, dass konkret geprüft werden muss, ob das Erfordernis des absolut Notwendigen im Kontext der in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen erfüllt ist.

207. Wie in Nr. 187 dieser Schlussanträge dargelegt, verlangt das Erfordernis des absolut Notwendigen die Prüfung, ob andere Maßnahmen bei der Bekämpfung schwerer Kriminalität genauso wirksam sein könnten wie die generelle Verpflichtung zur Vorratsspeicherung, dabei jedoch die in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta verankerten Rechte weniger beeinträchtigen würden.

208. Dies ist im spezifischen Kontext der jeweiligen innerstaatlichen Regelung zu beurteilen, die eine generelle Verpflichtung zur Vorratsspeicherung vorsieht. Zum einen verlangt diese Beurteilung, dass die Wirksamkeit der genannten Verpflichtung mit der Wirksamkeit jeder anderen denkbaren Maßnahme im innerstaatlichen Zusammenhang verglichen und dabei berücksichtigt wird, dass die genannte Verpflichtung den zuständigen Behörden die begrenzte Fähigkeit verleiht, anhand der auf Vorrat gespeicherten Daten die Vergangenheit zu entschlüsseln<sup>64</sup>.

62 — Vgl. DRI-Urteil, Rn. 65: „Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, *ohne dass* sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.“ (Hervorhebung nur hier)

63 — Urteil vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650).

64 — Siehe Nrn. 178 bis 183 dieser Schlussanträge.

209. In Anbetracht des Erfordernisses des absolut Notwendigen ist es unerlässlich, dass die Gerichte sich nicht mit der Prüfung des bloßen Nutzens einer generellen Verpflichtung zur Vorratsspeicherung begnügen, sondern genau untersuchen, ob eine andere Maßnahme oder eine Kombination von Maßnahmen, insbesondere aber eine gezielte Vorratsspeicherungspflicht, mit der andere Ermittlungsinstrumente einhergehen, bei der Bekämpfung schwerer Kriminalität nicht dieselbe Wirksamkeit aufweisen. Ich weise insoweit darauf hin, dass eine Reihe von Studien, die dem Gerichtshof vorgelegt worden sind, die Erforderlichkeit dieser Art von Verpflichtung zur Bekämpfung schwerer Kriminalität in Frage stellen<sup>65</sup>.

210. Sollten andere Maßnahmen bei der Bekämpfung schwerer Kriminalität genauso wirksam sein können, so haben zum anderen die vorlegenden Gerichte gemäß der in Nr. 185 dieser Schlussanträge angeführten ständigen Rechtsprechung überdies zu prüfen, ob diese Maßnahmen die in Rede stehenden Grundrechte weniger verletzen als eine generelle Verpflichtung zur Vorratsspeicherung.

211. Unter Berücksichtigung von Rn. 59 des DRI-Urteils werden die vorlegenden Gerichte insbesondere zu prüfen haben, ob der materielle Umfang der Verpflichtung zur Vorratsspeicherung beschränkt werden kann, unter gleichzeitiger Wahrung der Wirksamkeit dieser Maßnahme bei der Bekämpfung schwerer Kriminalität<sup>66</sup>. Diese Verpflichtung kann nämlich je nach den von ihr erfassten Nutzern, geografischen Gebieten und Kommunikationsmitteln einen mehr oder weniger weiten materiellen Umfang haben<sup>67</sup>.

212. Meines Erachtens sollten, sofern die Technologie es zulässt, von der Vorratsspeicherungspflicht vor allem die Daten ausgenommen werden, die im Hinblick auf die in den vorliegenden Rechtssachen in Rede stehenden Grundrechte besonders sensibel sind, wozu die unter das Berufsgeheimnis fallenden Daten oder auch die Daten gehören, anhand deren die Informationsquellen von Journalisten identifiziert werden können.

213. Es muss jedoch bedacht werden, dass eine erhebliche Beschränkung des Umfangs der generellen Verpflichtung zur Vorratsspeicherung den Nutzen, den eine solche Regelung im Kampf gegen schwere Kriminalität hat, beträchtlich schmälern könnte. Zum einen haben mehrere Regierungen betont, dass es schwierig, wenn nicht gar unmöglich sei, im Voraus die Daten festzulegen, die mit einer schweren Straftat in Beziehung stehen könnten. Eine solche Beschränkung kann daher die Vorratsspeicherung von Daten ausschließen, die sich für die Bekämpfung schwerer Kriminalität als relevant erweisen könnten.

214. Zum anderen ist die schwere Kriminalität, wie die estnische Regierung ausgeführt hat, ein dynamisches Phänomen, das sich den Ermittlungsinstrumenten der Strafverfolgungsbehörden anpassen kann. Die Beschränkung auf ein bestimmtes geografisches Gebiet oder ein bestimmtes Kommunikationsmittel liefere daher Gefahr, eine Verlagerung der mit schwerer Kriminalität im Zusammenhang stehenden Aktivitäten in ein geografisches Gebiet und/oder auf ein Kommunikationsmittel herbeizuführen, die von dieser Regelung nicht erfasst werden.

65 — Vgl. Menschenrechtskommissar des Europarats, „Issue paper on the rule of law on the Internet and in the wider digital world“, Dezember 2014, CommDH/IssuePaper(2014)1, S. 115, Menschenrechtsrat der Vereinten Nationen, Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, 30. Juni 2014, A/HRC/27/37, Nr. 26, Generalversammlung der Vereinten Nationen, Bericht des Sonderberichterstatters über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus, 23. September 2014, A/69/397, Nrn. 18 und 19.

66 — Dieser Hinweis bezieht sich ausschließlich auf die generellen Verpflichtungen zur Vorratsspeicherung (die jeden treffen können, unabhängig von einem Bezug zu einer schweren Straftat), nicht aber auf die gezielten Überwachungsmaßnahmen (die Personen treffen, von denen zuvor festgestellt wurde, dass sie einen Bezug zu einer schweren Straftat haben); zu dieser Unterscheidung siehe Nrn. 178 bis 183 dieser Schlussanträge.

67 — Die deutsche Regierung hat in der mündlichen Verhandlung u. a. ausgeführt, dass das deutsche Parlament den E-Mail-Verkehr von der sich aus den deutschen Rechtsvorschriften ergebenden Vorratsspeicherungspflicht ausgenommen habe, dass aber die Regelung alle Nutzer und das gesamte Staatsgebiet erfasse.

215. Da diese Beurteilung eine komplexe Bewertung der in den Ausgangsverfahren in Rede stehenden innerstaatlichen Regelungen verlangt, ist sie meines Erachtens von den nationalen Gerichten vorzunehmen, wie die tschechische, die estnische, die irische, die französische und die niederländische Regierung sowie die Kommission ausgeführt haben.

b) Zum zwingenden Charakter der vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien im Hinblick auf das Erfordernis des absolut Notwendigen

216. Unterstellt, eine generelle Verpflichtung zur Vorratsspeicherung kann als absolut notwendig im Kontext der betreffenden innerstaatlichen Regelung angesehen werden, was zu beurteilen Sache des nationalen Gerichts ist, bleibt noch zu prüfen, ob mit dieser Verpflichtung alle vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils genannten Garantien einhergehen müssen, um die Verletzung der in der Richtlinie 2002/58 und den Art. 7 und 8 der Charta verankerten Rechte auf das absolut Notwendige zu beschränken.

217. Die genannten Garantien betreffen die Bestimmungen, die den Zugang und die Nutzung der auf Vorrat gespeicherten Daten durch die zuständigen Behörden (Rn. 60 bis 62 des DRI-Urteils), die Dauer der Vorratsspeicherung (Rn. 63 und 64 dieses Urteils) sowie die Sicherheit und den Schutz der von den Betreibern auf Vorrat gespeicherten Daten (Rn. 66 bis 68 dieses Urteils) regeln.

218. In den beim Gerichtshof eingereichten Erklärungen stehen sich bezüglich der Natur dieser Garantien zwei Auffassungen gegenüber.

219. Nach einer ersten Auffassung, die von Herrn Watson sowie von der Open Rights Group und Privacy International vertreten wird, sind die vom Gerichtshof in den Rn. 60 bis 68 angeführten Garantien zwingend. Der Gerichtshof habe Mindestgarantien aufgestellt, die *sämtlich* durch die betreffende innerstaatliche Regelung erfüllt werden müssten, um die Verletzung der Grundrechte auf das absolut Notwendige zu beschränken.

220. Nach einer zweiten Auffassung, die von der deutschen, der estnischen, der irischen und der französischen Regierung sowie von der Kommission vertreten wird, sind die vom Gerichtshof in den Rn. 60 bis 68 genannten Garantien nicht zwingend. Der Gerichtshof habe eine „Gesamtbeurteilung“ der in der Richtlinie 2006/24 fehlenden Garantien vorgenommen, ohne dass eine dieser Garantien, isoliert betrachtet, als zwingend im Hinblick auf das Erfordernis des absolut Notwendigen angesehen werden könne. Zur Verdeutlichung dieser These führt die deutsche Regierung das Bild der „kommunizierenden Röhren“ an, nach dem ein flexiblerer Ansatz in Bezug auf einen der drei vom Gerichtshof bezeichneten Aspekte (z. B. Zugang zu den auf Vorrat gespeicherten Daten) durch einen strikteren Ansatz bezüglich der beiden anderen Aspekte (Dauer der Vorratsspeicherung sowie Sicherheit und Schutz der Daten) ausgeglichen werden könne.

221. Ich bin aus folgenden Gründen der Auffassung, dass diese These der „kommunizierenden Röhren“ zurückzuweisen ist und *alle* vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien als zwingend anzusehen sind.

222. Erstens eignet sich die Sprache, die der Gerichtshof bei der Prüfung der absoluten Erforderlichkeit der von der Richtlinie 2006/24 aufgestellten Regelung benutzt, nicht für eine derartige Auslegung. In den Rn. 60 bis 68 des DRI-Urteils deutet der Gerichtshof an keiner Stelle an, dass ein flexiblerer Ansatz in Bezug auf einen der drei von ihm bezeichneten Aspekte durch einen strikteren Standpunkt bezüglich der beiden anderen Aspekte „ausgeglichen“ werden könnte.

223. Die These von den „kommunizierenden Röhren“ scheint mir das Ergebnis einer Verwechslung der Voraussetzung der Erforderlichkeit mit der Voraussetzung der Verhältnismäßigkeit im engeren Sinne zu sein, die der Gerichtshof im DRI-Urteil nicht geprüft hat. Wie ich in Nr. 186 dieser Schlussanträge ausgeführt habe, beinhaltet die Voraussetzung der Erforderlichkeit, dass jede ineffiziente Maßnahme zurückzuweisen ist. Es kann in diesem Kontext nicht um eine „Gesamtwürdigung“, einen „Ausgleich“ oder eine „Abwägung“ gehen, also um ein Vorgehen, das seinen Platz erst auf der Stufe der Verhältnismäßigkeitsprüfung im engeren Sinne hat<sup>68</sup>.

224. Zweitens nähme diese These der „kommunizierenden Röhren“ den vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien die praktische Wirksamkeit, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, nicht mehr über ausreichende Garantien verfügen würden, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen, wie dies in Rn. 54 des genannten Urteils gefordert wird.

225. Die destruktive Wirkung dieser Auffassung kann anhand folgender Beispiele leicht verdeutlicht werden. Eine innerstaatliche Regelung, die den Zugang strikt auf Zwecke der Terrorismusbekämpfung beschränkt und die Dauer der Vorratsspeicherung auf drei Monate begrenzt (striktter Ansatz in Bezug auf den Zugang und die Dauer der Vorratsspeicherung), aber die Betreiber nicht verpflichtet, die Daten auf Vorrat in ihrem Hoheitsgebiet verschlüsselt zu speichern (flexibler Ansatz in Bezug auf die Sicherheit), würde die gesamte Bevölkerung einer verstärkten Gefahr des unrechtmäßigen Zugangs zu den auf Vorrat gespeicherten Daten aussetzen. Ebenso würde eine innerstaatliche Regelung, die eine dreimonatige Dauer der Vorratsspeicherung sowie eine verschlüsselte Vorratsspeicherung der Daten in ihrem Hoheitsgebiet vorsieht (striktter Ansatz in Bezug auf die Dauer und die Sicherheit), aber allen Bediensteten aller staatlichen Stellen den Zugang zu den auf Vorrat gespeicherten Daten gestattet (flexibler Ansatz in Bezug auf den Zugang), die gesamte Bevölkerung der verstärkten Gefahr eines Missbrauchs seitens der staatlichen Stellen aussetzen.

226. An diesen Beispielen zeigt sich meines Erachtens, dass zur Wahrung der praktischen Wirksamkeit der vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien *jede einzelne* dieser Garantien als zwingend anzusehen ist. Der EGMR hat in seinem kürzlich erlassenen Urteil Szabó und Vissy/Ungarn unter ausdrücklicher Bezugnahme auf das DRI-Urteil ebenfalls die grundlegende Bedeutung dieser Garantien betont<sup>69</sup>.

227. Drittens bereitet die Umsetzung dieser Garantien durch die Mitgliedstaaten, die eine generelle Verpflichtung zur Vorratsspeicherung einführen wollen, keine größeren praktischen Schwierigkeiten. Tatsächlich erscheinen mir diese Garantien, wie Herr Watson ausgeführt hat, in vielerlei Hinsicht als „Mindest“-Garantien.

228. Mehrere dieser Garantien sind vor dem Gerichtshof erörtert worden, weil sie in den innerstaatlichen Regelungen, die in den Ausgangsverfahren in Rede stehen, möglicherweise nicht vorgesehen sind.

68 — Vgl. Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, S. 344: „The first three components of proportionality deal mainly with the relation between the limiting law’s purpose and the means to fulfil that purpose. ... Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing.* The test of proportionality *stricto sensu* is different. ... It focuses on the relation between the benefit in fulfilling the law’s purpose and the harm caused by limiting the constitutional right. *It is based on balancing.*“ (Hervorhebung nur hier)

69 — EGMR, 12. Januar 2016, Szabó und Vissy/Ungarn (CE:ECHR:2016:0112JUD003713814, § 68): „Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens’ trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens’ private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities’ enhanced technical possibilities to intercept private information.“

229. Als Erstes ergibt sich aus den Rn. 61 und 62 des DRI-Urteils, dass der Zugang zu den auf Vorrat gespeicherten Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind.

230. Tele2 Sverige und die Kommission sind der Auffassung, dass dieses Erfordernis von der in der Rechtssache C-203/15 in Rede stehenden schwedischen Regelung nicht erfüllt werde, die den Zugang zu den auf Vorrat gespeicherten Daten für die Bekämpfung einfacher Kriminalität zulasse. Die gleiche Kritik wird von Herrn Brice und Herrn Lewis sowie von Herrn Watson gegenüber der Regelung geäußert, die in der Rechtssache C-698/15 in Frage steht und die den Zugang für die Bekämpfung einfacher Kriminalität und sogar ohne Vorliegen einer Straftat erlaube.

231. Es ist zwar nicht Sache des Gerichtshofs, sich zum Inhalt dieser innerstaatlichen Regelungen zu äußern, doch hat er die dem Gemeinwohl dienenden Zielsetzungen zu bezeichnen, die einen schweren Eingriff in die von der Richtlinie und den Art. 7 und 8 der Charta vorgesehenen Rechte rechtfertigen können. Im vorliegenden Fall habe ich bereits die Gründe dargelegt, aus denen meines Erachtens *nur* die Bekämpfung schwerer Kriminalität einen solchen Eingriff rechtfertigen kann<sup>70</sup>.

232. Als Zweites muss der Zugang zu den auf Vorrat gespeicherten Daten nach Rn. 62 des DRI-Urteils einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegen, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll. Diese vorherige Kontrolle muss ferner im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten stattfinden.

233. Nach den Erklärungen von Tele2 Sverige und der Kommission fehlt diese Garantie einer unabhängigen Kontrolle als Voraussetzung für den Zugang teilweise in der schwedischen Regelung, die in der Rechtssache C-203/15 in Frage steht. Dieselbe Feststellung, deren Richtigkeit von der Regierung des Vereinigten Königreichs nicht in Frage gestellt wird, wird von Herrn Brice und Herrn Lewis, Herrn Watson sowie von der Open Rights Group und Privacy International in Bezug auf die in der Rechtssache C-698/15 in Rede stehende Regelung des Vereinigten Königreichs getroffen.

234. Ich sehe keinen Grund, dieses unbestreitbar aus dem Wortlaut von Rn. 62 des DRI-Urteils folgende Erfordernis einer vorherigen Kontrolle durch eine unabhängige Stelle abzuschwächen<sup>71</sup>. Dieses Erfordernis ist zunächst durch die Schwere des Eingriffs und der Gefahren bedingt, die durch die Einrichtung von Datenbanken verursacht werden, die praktisch die Gesamtheit der betroffenen Bevölkerung erfassen<sup>72</sup>. Ich weise darauf hin, dass eine Reihe von Experten auf dem Gebiet des Menschenrechtsschutzes bei der Bekämpfung des Terrorismus kritisiert haben, dass gegenwärtig die Tendenz bestehe, die herkömmlichen Verfahren für eine unabhängige Genehmigung und effektive Überwachung durch ein System zu ersetzen, in dem sich die Nachrichten- und Polizeidienste den Zugang selbst genehmigten<sup>73</sup>.

70 — Siehe Nrn. 170 bis 173 dieser Schlussanträge.

71 — Ich weise jedoch darauf hin, dass sich das Erfordernis einer vorherigen und unabhängigen Kontrolle nicht aus Art. 8 Abs. 3 der Charta herleiten lässt, da die Charta als solche nicht auf die innerstaatlichen Bestimmungen über den Zugang zu den auf Vorrat gespeicherten Daten anwendbar ist, siehe Nrn. 123 bis 125 dieser Schlussanträge.

72 — Siehe Nrn. 252 bis 261 dieser Schlussanträge.

73 — Menschenrechtsrat der Vereinten Nationen, Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus vom 28. Dezember 2009, A/HRC/13/37, Nr. 62: „Es darf weder ein geheimes Überwachungssystem geben, das nicht der Aufsicht durch eine wirksame Kontrollinstanz unterliegt, noch einen Eingriff, der nicht von einer unabhängigen Stelle genehmigt ist“ (vgl. auch Nr. 51). Vgl. auch Generalversammlung der Vereinten Nationen, Bericht des Sonderberichterstatters über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus, 23. September 2014, A/69/397, Nr. 61.

235. Sodann ist eine unabhängige Kontrolle als Voraussetzung für den Zugang zu den Daten erforderlich, um eine Verarbeitung der besonders sensiblen Daten im Einzelfall unter Berücksichtigung der in den vorliegenden Rechtssachen in Frage stehenden Grundrechte zu ermöglichen, wie der unter das Berufsgeheimnis fallenden Daten oder auch der Daten, anhand deren die Informationsquellen von Journalisten identifiziert werden können, wie die Law Society of England and Wales sowie die französische und die deutsche Regierung ausgeführt haben. Diese Kontrolle als Voraussetzung für den Zugang ist umso notwendiger, wenn es technisch schwierig ist, alle diese Daten bereits bei der Speicherung auszuschließen<sup>74</sup>.

236. Schließlich ist hinzuzufügen, dass keiner der drei von einem Antrag auf Zugang betroffenen Beteiligten praktisch in der Lage ist, eine wirksame Kontrolle über den Zugang zu den auf Vorrat gespeicherten Daten auszuüben. Die zuständigen Strafverfolgungsbehörden sind daran interessiert, einen möglichst weitgehenden Zugang zu diesen Daten zu beantragen. Die Betreiber, die die Ermittlungsakte nicht kennen, können nicht prüfen, ob der Antrag auf Zugang auf das absolut Notwendige beschränkt ist. Die Personen, deren Daten abgefragt werden, können nicht wissen, dass sie Gegenstand einer solchen Untersuchungsmaßnahme sind, und zwar auch im Fall einer missbräuchlichen oder unrechtmäßigen Nutzung, wie Herr Watson sowie Herr Brice und Herr Lewis vorgetragen haben. Diese Konstellation widerstreitender Interessen verlangt meines Erachtens das Tätigwerden einer unabhängigen Stelle, bevor die auf Vorrat gespeicherten Daten abgefragt werden, um die Personen, deren Daten auf Vorrat gespeichert sind, vor jedem Missbrauch durch die zuständigen Behörden zu schützen.

237. Vor diesem Hintergrund halte ich es für angemessen, dass einzelne Situationen von höchster Dringlichkeit, auf die sich das Vereinigte Königreich bezieht, einen sofortigen Zugang der Strafverfolgungsbehörden zu den auf Vorrat gespeicherten Daten ohne vorherige Kontrolle rechtfertigen können, um die Begehung schwerer Straftaten zu verhindern oder die Urheber dieser Straftaten zu verfolgen<sup>75</sup>. So weit wie möglich muss am Erfordernis der vorherigen Genehmigung festgehalten und für die Behandlung dieser Art von Zugangsanträgen ein Dringlichkeitsverfahren vor der unabhängigen Stelle eingerichtet werden. Ist jedoch die Befassung dieser Stelle mit dem Antrag auf Zugang offensichtlich unvereinbar mit der äußersten Dringlichkeit der Sache, müssen der Zugang und die Nutzung der Daten einer nachträglichen Kontrolle durch diese Stelle unterzogen werden, und zwar innerhalb kürzester Zeit.

238. Als Drittes verpflichtet Rn. 68 des DRI-Urteils die Betreiber, die Daten im Unionsgebiet auf Vorrat zu speichern, um zu gewährleisten, dass die Einhaltung der in den Rn. 66 und 67 des Urteils angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta gefordert, durch eine unabhängige Stelle überwacht wird.

239. Tele2 Sverige und die Kommission machen geltend, die Vorratsspeicherung der Daten im nationalen Staatsgebiet sei im Rahmen der in der Rechtssache C-203/15 fraglichen schwedischen Regelung nicht gewährleistet. Dieselbe Beanstandung erheben Herr Brice und Herr Lewis sowie Herr Watson in Bezug auf die in der Rechtssache C-698/15 fragliche Regelung des Vereinigten Königreichs.

74 — Siehe Nr. 212 dieser Schlussanträge. In Bezug auf die Informationsquellen von Journalisten hat der EGMR betont, dass die vorherige Genehmigung einer unabhängigen Stelle erforderlich ist, da eine nachträgliche Kontrolle die Vertraulichkeit der Quellen nicht wiederherstellen kann, vgl. EGMR vom 22. November 2012, *Telegraaf Media Nederland Landelijke Media B.V. u. a./Niederlande* (CE:ECHR:2012:1122JUD003931506, § 101), und EGMR vom 12. Januar 2016, *Szabó und Vissy/Ungarn* (CE:ECHR:2016:0112JUD003713814, § 77). Im Urteil *Kopp/Schweiz*, das die Überwachung der Telefongespräche eines Anwalts betraf, hat der EGMR beanstandet, dass ein öffentlicher Bediensteter der Verwaltung damit betraut war, unter das Berufsgeheimnis fallende Informationen zu filtern, ohne dass es eine Kontrolle durch einen unabhängigen Beamten gab, vgl. EGMR vom 25. März 1998, *Kopp/Schweiz* (CE:ECHR:1998:0325JUD002322494, § 74).

75 — Vgl. insoweit das in Nr. 22 dieser Schlussanträge beschriebene Verfahren. Ich weise darauf hin, dass der Gerichtshof diese Frage im DRI-Urteil nicht erörtert hat.

240. Insoweit sehe ich zum einen keinen Grund, dieses in Rn. 68 des DRI-Urteils aufgestellte Erfordernis abzuschwächen, da eine Vorratsspeicherung der Daten außerhalb des Unionsgebiets den Personen, deren Daten auf Vorrat gespeichert werden, das von der Richtlinie 2002/58 und den Art. 7, 8 und 52 Abs. 1 der Charta gewährte Schutzniveau nicht gewährleisten könnte<sup>76</sup>.

241. Es scheint mir zum anderen vernünftig zu sein, dieses Erfordernis, das der Gerichtshof im Kontext der Richtlinie 2006/24 aufgestellt hat, dem Kontext der innerstaatlichen Regelungen anzupassen und die Vorratsspeicherung der Daten im nationalen Staatsgebiet vorzusehen, wie die deutsche und die französische Regierung sowie die Kommission ausgeführt haben. Nach Art. 8 Abs. 3 der Charta hat nämlich jeder Mitgliedstaat zu gewährleisten, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit durch die in der innerstaatlichen Regelung bezeichneten Betreiber von einer unabhängigen Stelle überwacht wird. Ohne eine Koordinierung auf Unionsebene könnte aber diese nationale Stelle ihre Überwachungsaufgaben im Gebiet eines anderen Mitgliedstaats nicht erfolgreich wahrnehmen.

242. Als Viertes haben die vorlegenden Gerichte hinsichtlich der Dauer der Vorratsspeicherung die vom Gerichtshof in den Rn. 63 und 64 des DRI-Urteils aufgestellten Kriterien anzuwenden. Zum einen müssen diese Gerichte prüfen, ob die auf Vorrat gespeicherten Daten nach Maßgabe ihres Nutzens unterschieden werden können und, gegebenenfalls, ob die Dauer der Vorratsspeicherung nach Maßgabe dieses Kriteriums angepasst wurde. Zum anderen haben sie zu prüfen, ob die Dauer der Vorratsspeicherung auf objektiven Kriterien beruht, die gewährleisten können, dass sie auf das absolut Notwendige beschränkt wird.

243. Der EGMR hat in seinem kürzlich erlassenen Urteil *Roman Zakharov/Russland* festgestellt, dass für die Vorratsspeicherung eine Höchstdauer von sechs Monaten angemessen ist, zugleich aber beanstandet, dass keine Verpflichtung besteht, die Daten, die in keiner Beziehung zu dem Zweck ihrer Sammlung stehen, sofort zu vernichten<sup>77</sup>. Ich füge insoweit hinzu, dass die in den Ausgangsverfahren fraglichen innerstaatlichen Regelungen die Verpflichtung vorsehen müssen, alle Daten unwiederbringlich zu vernichten, sobald sie zur Bekämpfung schwerer Straftaten nicht mehr absolut notwendig sind. Diese Verpflichtung ist nicht nur von den Betreibern, die die Daten auf Vorrat speichern, sondern auch von den Behörden zu erfüllen, die Zugang zu den auf Vorrat gespeicherten Daten erhalten haben.

244. Nach alledem bin ich der Ansicht, dass alle vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten Garantien zwingend sind und daher mit einer generellen Verpflichtung zur Vorratsspeicherung einhergehen müssen, um die Verletzung der von der Richtlinie 2002/58 und den Art. 7 und 8 der Charta gewährten Rechte auf das absolut Notwendige zu beschränken.

245. Es ist Sache der vorlegenden Gerichte, zu prüfen, ob die in den Ausgangsverfahren fraglichen Regelungen alle diese Garantien enthalten.

76 — Vgl. hierzu Urteil vom 6. Oktober 2015, *Schrems* (C-362/14, EU:C:2015:650).

77 — Vgl. EGMR, 4. Dezember 2015, *Roman Zakharov/Russland* (CE:ECHR:2015:1204JUD004714306, §§ 254 und 255). Nach russischem Recht sind die abgefangenen Daten nach Ablauf einer Speicherungsfrist von sechs Monaten zu vernichten, sofern gegen die betreffende Person keine Anklage wegen einer Straftat erhoben wurde. Der EGMR hat die im russischen Recht für diese Daten festgesetzte maximale Speicherdauer, nämlich sechs Monate, für angemessen erachtet. Er hat jedoch beanstandet, dass keine Verpflichtung besteht, die Daten, die in keiner Beziehung zu dem Zweck ihrer Sammlung stehen, sofort zu vernichten, und darauf hingewiesen, dass die automatische, sechs Monate dauernde Vorratsspeicherung von Daten, an denen offensichtlich kein Interesse besteht, im Hinblick auf Art. 8 EMRK nicht als gerechtfertigt gelten kann.

6. Zur Verhältnismäßigkeit einer generellen Verpflichtung zur Vorratsspeicherung in einer demokratischen Gesellschaft unter Berücksichtigung des Ziels der Bekämpfung schwerer Kriminalität

246. Nach der Prüfung der Erforderlichkeit der in den Ausgangsverfahren fraglichen Regelungen haben die vorlegenden Gerichte noch zu prüfen, ob diese in einer demokratischen Gesellschaft unter Berücksichtigung des Ziels der Bekämpfung schwerer Kriminalität verhältnismäßig sind. Dieser Aspekt ist vom Gerichtshof im DRI-Urteil nicht untersucht worden, da die Regelung der Richtlinie 2006/24 über das für die Bekämpfung schwerer Kriminalität absolut Notwendige hinausging.

247. Das Erfordernis der Verhältnismäßigkeit in einer demokratischen Gesellschaft – oder Verhältnismäßigkeit „im engeren Sinne“ – ergibt sich sowohl aus Art. 15 Abs. 1 der Richtlinie 2002/58 als auch aus Art. 52 Abs. 1 der Charta und aus der ständigen Rechtsprechung. Nach dieser ständigen Rechtsprechung kann eine grundrechtsverletzende Maßnahme nur dann als verhältnismäßig angesehen werden, wenn die verursachten Nachteile nicht außer Verhältnis zu den verfolgten Zielen stehen<sup>78</sup>.

248. Im Unterschied zu den Erfordernissen der Geeignetheit und der Erforderlichkeit der betreffenden Maßnahme, die eine Bewertung der Wirksamkeit dieser Maßnahme unter Berücksichtigung des verfolgten Ziels beinhalten, umfasst das Erfordernis der Verhältnismäßigkeit im engeren Sinne eine Abwägung der Vorteile, die aus dieser Maßnahme unter Berücksichtigung des verfolgten legitimen Ziels resultieren, gegen die Nachteile, die sich aus ihr unter Berücksichtigung der in einer demokratischen Gesellschaft gewährten Grundrechte ergeben<sup>79</sup>. Dieses Erfordernis ist somit der Ausgangspunkt für eine Debatte über die Werte, die in einer demokratischen Gesellschaft gelten sollen, und letztlich über die Art von Gesellschaft, in der wir leben wollen<sup>80</sup>.

249. Somit ist, wie in Nr. 223 dieser Schlussanträge ausgeführt, die fragliche Regelung bei der Prüfung der Verhältnismäßigkeit im engeren Sinne einer Gesamtbeurteilung zu unterziehen, nicht aber bei der Prüfung der Erforderlichkeit, wie die Anhänger der These der „kommunizierenden Röhren“ meinen<sup>81</sup>.

250. Gemäß der oben in Nr. 247 angeführten Rechtsprechung sind die Vor- und Nachteile einer generellen Verpflichtung zur Vorratsspeicherung gegeneinander abzuwägen. Diese Vorteile und diese Nachteile stehen in engem Zusammenhang mit dem wesentlichen Merkmal einer solchen Verpflichtung – gewissermaßen als deren helle und dunkle Seite –, das darin besteht, dass sie alle Kommunikationsvorgänge sämtlicher Nutzer erfasst, ohne dass irgendein Bezug zu einer schweren Straftat erforderlich ist.

78 — Vgl. insbesondere Urteile vom 15. Februar 2016, N. (C-601/15 PPU, EU:C:2016:84, Rn. 54; die Erforderlichkeit wird in den Rn. 56 bis 67, die Verhältnismäßigkeit in den Rn. 68 und 69 geprüft), vom 16. Juli 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, Rn. 123; die Erforderlichkeit wird in den Rn. 120 bis 122, die Verhältnismäßigkeit in den Rn. 123 bis 127 geprüft), und vom 22. Januar 2013, Sky Österreich (C-283/11, EU:C:2013:28, Rn. 50; die Erforderlichkeit wird in den Rn. 54 bis 57, die Verhältnismäßigkeit in den Rn. 58 bis 67 geprüft).

79 — Vgl. Rivers, J., „Proportionality and variable intensity of review“, 65(1) *Cambridge Law Journal* (2006) 174, S. 198: „It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable.“

80 — Vgl. Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, S. 30: „In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail.“

81 — Die Besonderheit des Erfordernisses der Verhältnismäßigkeit im engeren Sinne im Vergleich zu den Erfordernissen der Geeignetheit und der Erforderlichkeit kann anhand des folgenden Beispiels verdeutlicht werden. Angenommen, ein Mitgliedstaat schreibt vor, dass jedem, der seinen Wohnsitz im Hoheitsgebiet dieses Mitgliedstaats hat, ein elektronischer Mikrochip zur Standortbestimmung eingesetzt wird, der den Behörden die Nachverfolgung ermöglicht, wann und wo sich der Träger des Chips im vergangenen Jahr aufgehalten hat. Diese Maßnahme könnte als „erforderlich“ angesehen werden, wenn keine andere Maßnahme im Kampf gegen schwere Kriminalität denselben Grad von Wirksamkeit erreichen kann. Die Maßnahme wäre jedoch in einer demokratischen Gesellschaft unverhältnismäßig, da die Nachteile, die sich aus der Verletzung des Rechts auf körperliche Unversehrtheit, auf Achtung des Privatlebens und auf Schutz personenbezogener Daten ergeben, außer Verhältnis zu den Vorteilen stünden, die die Maßnahme bei der Bekämpfung schwerer Kriminalität zur Folge hätte.

251. Die Vorteile, die die Vorratsspeicherung aller im nationalen Staatsgebiet entstandenen Kommunikationsdaten bei der Bekämpfung schwerer Straftaten bieten, einerseits habe ich bereits oben in den Nrn. 178 bis 183 dargelegt.

252. Die Nachteile einer generellen Verpflichtung zur Vorratsspeicherung andererseits rühren daher, dass die überwältigende Mehrheit der auf Vorrat gespeicherten Daten Personen betreffen, die niemals in einem Bezug zu einer schweren Straftat stehen werden. Insoweit ist es wichtig, die Art der Nachteile zu verdeutlichen, die diese Personen treffen werden. Diese Nachteile sind unterschiedlicher Art, je nach Ausmaß des Eingriffs in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten.

253. Im Rahmen eines „individuellen“ Eingriffs, der sich auf ein bestimmtes Individuum auswirkt, wurden die Nachteile einer generellen Verpflichtung zur Vorratsspeicherung sehr nachdrücklich von Generalanwalt Cruz Villalón in den Nrn. 72 bis 74 seiner Schlussanträge in der DRI-Rechtssache beschrieben<sup>82</sup>. Wie er ausführt, kann die Auswertung dieser Daten es ermöglichen, „eine ebenso zuverlässige wie erschöpfende Kartografie eines erheblichen Teils der Verhaltensweisen einer Person, die allein ihr Privatleben betreffen, oder gar ein komplettes und genaues Abbild der privaten Identität dieser Person zu erstellen“.

254. Mit anderen Worten, in einem individuellen Kontext ermöglicht die generelle Verpflichtung zur Vorratsspeicherung genauso schwere Eingriffe wie eine gezielte Überwachungsmaßnahme, einschließlich einer Maßnahme, die den Inhalt der Nachrichtenübermittlungen abfängt.

255. Auch wenn die Schwere dieser individuellen Eingriffe nicht unterschätzt werden darf, zeigen sich die spezifischen Gefahren, die von einer generellen Verpflichtung zur Vorratsspeicherung ausgehen, doch bei den „massenhaften“ Eingriffen.

256. Im Unterschied nämlich zu gezielten Überwachungsmaßnahmen kann diese Verpflichtung massenhafte Eingriffe erheblich erleichtern, d. h. solche Eingriffe, die sich auf einen wesentlichen Teil oder gar die Gesamtheit der relevanten Bevölkerung auswirken, was anhand der folgenden Beispiele verdeutlicht werden kann.

257. Nehmen wir erstens an, eine Person, die Zugang zu den auf Vorrat gespeicherten Daten hat, will in der Bevölkerung des Mitgliedstaats alle Personen mit psychischen Störungen ermitteln. Die Auswertung des Inhalts aller im nationalen Staatsgebiet übermittelten Nachrichten würde insoweit erhebliche Mittel in Anspruch nehmen. Dagegen würde die Auswertung der Datenbanken für Kommunikationsvorgänge eine sofortige Identifizierung aller Personen ermöglichen, die sich im Verlauf der Datenspeicherfrist mit einem Psychologen in Verbindung gesetzt haben<sup>83</sup>. Diese Technik könnte auf alle in einem Mitgliedstaat registrierten medizinischen Fachgebiete ausgedehnt werden<sup>84</sup>.

82 — C-293/12 und C-594/12, EU:C:2013:845. Vgl. auch DRI-Urteil, Rn. 27 und 37.

83 — Die auf Vorrat gespeicherten Daten beinhalten die Identität der Quelle und des Adressaten der Nachricht. Es würde ausreichen, diese Daten mit den Telefonnummern der im nationalen Staatsgebiet tätigen Psychologen abzugleichen.

84 — Vgl. insoweit Menschenrechtsrat der Vereinten Nationen, Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus, 28. Dezember 2009, A/HRC/13/37, Nr. 42: „[I]n Deutschland [haben] Untersuchungen auf eine beunruhigende Folge der Richtlinie zur Vorratsdatenspeicherung hingewiesen ...: 52 % der befragten Personen gaben an, wegen des Gesetzes über die Vorratsspeicherung sei es wenig wahrscheinlich, dass sie Fernsprengeräte benutzen würden, um sich mit einem Toxikologen, einem Psychotherapeuten oder einem Eheberater in Verbindung zu setzen.“

258. Nehmen wir zweitens an, dass dieselbe Person diejenigen ermitteln möchte, die gegen die Politik der amtierenden Regierung sind. Die Auswertung des Inhalts der übermittelten Nachrichten würde insoweit wiederum erhebliche Mittel in Anspruch nehmen. Dagegen würde die Auswertung der Kommunikationsdaten die Identifizierung aller Personen ermöglichen, die auf Verteilerlisten für E-Mails mit regierungskritischem Inhalt eingetragen sind. Diese Daten würden zudem auch die Identifizierung der Personen ermöglichen, die an einer öffentlichen Demonstration gegen die Regierung teilnehmen<sup>85</sup>.

259. Ich lege Wert auf den Hinweis, dass die Gefahren, die mit dem Zugang zu den Kommunikationsdaten („Metadaten“) verbunden sind, gleich groß oder auch größer sein können als die Gefahren, die sich aus dem Zugang zum Inhalt dieser Kommunikationsvorgänge ergeben, wie die Open Rights Group und Privacy International, die Law Society of England and Wales sowie ein kürzlich erstellter Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte dargelegt haben<sup>86</sup>. Wie die vorstehend angeführten Beispiele zeigen, ermöglichen die „Metadaten“ praktisch eine sofortige Katalogisierung der gesamten Bevölkerung, was der Inhalt der Kommunikationsvorgänge nicht ermöglicht.

260. Die Gefahren eines missbräuchlichen oder unrechtmäßigen Zugangs zu den auf Vorrat gespeicherten Daten sind keineswegs theoretisch. Zum einen ist die Gefahr eines missbräuchlichen Zugangs durch die zuständigen Behörden im Zusammenhang mit der extrem hohen Zahl von Anträgen auf Zugang zu sehen, über die in den beim Gerichtshof eingereichten Erklärungen berichtet wird. Im Rahmen der schwedischen Regelung weist Tele2 Sverige darauf hin, dass sie monatlich ungefähr 10 000 Anträge auf Zugang erhalte, wobei diese Zahl nicht die an andere im schwedischen Staatsgebiet tätige Betreiber gerichteten Anträge enthalte. Bezüglich der Regelung des Vereinigten Königreichs hat Herr Watson Zahlen aus einem amtlichen Bericht vorgelegt, der sich auf 517 236 Genehmigungen und 55 346 mündliche Dringlichkeitsgenehmigungen allein im Jahr 2014 bezieht. Zum anderen ist die Gefahr des unrechtmäßigen Zugangs durch eine beliebige Person schon durch das Vorhandensein einer Datenbank gegeben<sup>87</sup>.

261. Meines Erachtens ist es Sache der vorlegenden Gerichte, zu beurteilen, ob die Nachteile, die die in den Ausgangsverfahren fragliche generelle Verpflichtung zur Vorratsspeicherung verursacht, in Anwendung der oben in Nr. 247 angeführten Rechtsprechung in einer demokratischen Gesellschaft nicht außer Verhältnis zu den verfolgten Zielen stehen. Im Rahmen dieser Beurteilung werden die vorlegenden Gerichte die Vorteile und Nachteile gegeneinander abzuwägen haben, die mit der genannten Verpflichtung verbunden sind, nämlich

85 — Da die auf Vorrat gespeicherten Daten den Standort der Quelle und des Adressaten einer Nachricht umfassen, kann jede Person, die bei einer Demonstration eine Nachricht einleitet oder empfängt, mit Hilfe der auf Vorrat gespeicherten Daten ohne Weiteres identifiziert werden. Hierzu berichtet Marc Goodman, ein Experte beim FBI und bei Interpol auf dem Gebiet der mit den neuen Technologien verbundenen Gefahren, dass in jüngster Vergangenheit die ukrainische Regierung bei einer Demonstration der Opposition alle Mobiltelefone identifizierte, die in der Nähe von Auseinandersetzungen zwischen Ordnungskräften und Regierungskritikern lokalisiert wurden. Alle diese Telefone empfingen eine Nachricht, von der der Verfasser meint, sie sei eine „orwellsche“ Nachricht, die nicht ihresgleichen habe: „Lieber Teilnehmer, Sie sind als Beteiligter an einer schweren Störung der öffentlichen Ordnung erfasst“ (M. Goodman, *Future Crimes*, Anchor Books, New York, 2016, S. 153, frei übersetzt). Vgl. auch Menschenrechtsrat der Vereinten Nationen, Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, 17. April 2013, A/HRC/23/40, Nr. 75, und Menschenrechtsrat der Vereinten Nationen, Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, 30. Juni 2014, A/HRC/27/37, Nr. 3.

86 — Vgl. insoweit Menschenrechtsrat der Vereinten Nationen, Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, 30. Juni 2014, A/HRC/27/37, Nr. 19: „In diesem Zusammenhang wird behauptet, dass das Abfangen – oder die Erhebung – von Daten über einen Kommunikationsvorgang – und nicht mehr über den Inhalt der Kommunikation – für sich genommen keinen Eingriff in das Privatleben darstelle. Unter dem Gesichtspunkt des Rechts auf Privatsphäre ist diese Unterscheidung nicht überzeugend. Die Informationsaggregationen, die gemeinhin als ‚Metadaten‘ bezeichnet werden, können Hinweise geben zu dem Verhalten einer Person, ihren sozialen Beziehungen, ihren privaten Vorlieben und ihrer Identität, die weit über das hinausgehen, was durch Zugang zum Inhalt eines privaten Kommunikationsvorgangs erreicht werden kann“ (Hervorhebung nur hier). Vgl. auch Generalversammlung der Vereinten Nationen, Bericht des Sonderberichterstatters über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus, 23. September 2014, A/69/397, Nr. 53.

87 — Vgl. insbesondere Menschenrechtsrat der Vereinten Nationen, Bericht des Sonderberichterstatters der Vereinten Nationen über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung vom 17. April 2013, A/HRC/23/40, Nr. 67: „Die Datenbanken für Kommunikationsdaten werden anfällig für Diebstahl, Betrug und versehentliche Offenlegung.“

- einerseits die Vorteile, die mit der Verleihung einer begrenzten Fähigkeit zur Entschlüsselung der Vergangenheit an die für die Bekämpfung schwerer Kriminalität zuständigen Behörden verbunden sind<sup>88</sup>, und
- andererseits die schwerwiegenden Gefahren, die sich in einer demokratischen Gesellschaft aus der Fähigkeit, eine Kartografie des Privatlebens einer Person zu erstellen, und aus der Fähigkeit, eine ganze Bevölkerung zu katalogisieren, ergeben.

262. Diese Beurteilung hat unter Berücksichtigung aller relevanten Merkmale der in den Ausgangsverfahren fraglichen innerstaatlichen Regelungen zu erfolgen. Ich weise insoweit darauf hin, dass die vom Gerichtshof in den Rn. 60 bis 68 des DRI-Urteils angeführten zwingenden Garantien nur Mindestgarantien darstellen, um die Verletzung der von der Richtlinie 2002/58 und den Art. 7 und 8 der Charta gewährten Rechte auf das absolut Notwendige zu beschränken. Es ist somit nicht ausgeschlossen, dass eine innerstaatliche Regelung, die alle diese Garantien enthält, dennoch in einer demokratischen Gesellschaft als unverhältnismäßig angesehen werden muss wegen des Missverhältnisses zwischen den schwerwiegenden Gefahren, die durch diese Verpflichtung in einer demokratischen Gesellschaft entstehen, und den Vorteilen, die sich aus ihr bei der Bekämpfung schwerer Kriminalität ergeben.

## VI – Ergebnis

263. Nach alledem schlage ich dem Gerichtshof vor, auf die Vorlagefragen des Kammarrätt i Stockholm (Verwaltungsgerichtshof Stockholm, Schweden) und des Court of Appeal (England & Wales) (Civil Division) (Berufungsgericht [England und Wales] [Abteilung für Zivilsachen], Vereinigtes Königreich), 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 der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung sowie die Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union sind dahin auszulegen, dass sie einen Mitgliedstaat nicht daran hindern, den Betreibern eines elektronischen Kommunikationsdienstes eine generelle Verpflichtung zur Vorratsspeicherung aller die Nutzer ihrer Dienste betreffenden Kommunikationsdaten aufzuerlegen, wenn alle im Folgenden genannten Voraussetzungen erfüllt sind, was die vorlegenden Gerichte im Licht aller relevanten Merkmale der in den Ausgangsverfahren fraglichen innerstaatlichen Regelungen zu prüfen haben:

- Die genannte Verpflichtung und die mit ihr einhergehenden Garantien müssen durch Rechtsvorschriften geregelt sein, die zugänglich und vorhersehbar sind und einen geeigneten Schutz gegen Willkür bieten;
- die Verpflichtung und die mit ihr einhergehenden Garantien müssen den Wesensgehalt der von den Art. 7 und 8 der Charta der Grundrechte anerkannten Rechte wahren;
- die Verpflichtung muss zur Bekämpfung schwerer Straftaten absolut notwendig sein, was bedeutet, dass keine andere Maßnahme oder Kombination von Maßnahmen bei der Bekämpfung schwerer Kriminalität genauso wirksam sein könnte und zugleich die in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta der Grundrechte verankerten Rechte weniger beeinträchtigen würde;

<sup>88</sup> — Siehe Nrn. 178 bis 183 dieser Schlussanträge.

- mit der genannten Verpflichtung müssen alle vom Gerichtshof in den Rn. 60 bis 68 des Urteils vom 8. April 2014, *Digital Rights Ireland u. a.* (C-293/12 und C-594/12, EU:C:2014:238), benannten Garantien, die den Zugang zu den Daten, die Dauer der Vorratsspeicherung sowie den Schutz und die Sicherheit der Daten betreffen, einhergehen, um die Verletzung der in der Richtlinie 2002/58 und in den Art. 7 und 8 der Charta der Grundrechte verankerten Rechte auf das absolut Notwendige zu beschränken, und
- die Verpflichtung muss in einem in einer demokratischen Gesellschaft angemessenen Verhältnis zur Bekämpfung schwerer Kriminalität stehen, was bedeutet, dass die schwerwiegenden Gefahren, die von dieser Verpflichtung in einer demokratischen Gesellschaft ausgehen, nicht außer Verhältnis zu den Vorteilen stehen dürfen, die sich aus ihr bei der Bekämpfung schwerer Kriminalität ergeben.