



Jurisprudentie

CONCLUSIE VAN ADVOCaat-GENERAAL
H. SAUGMANDSGAARD ØE
van 19 juli 2016¹

Gevoegde zaken C-203/15 en C-698/15

Tele2 Sverige AB
tegen
Post- och telestyrelsen (C-203/15)
en
Secretary of State for the Home Department
tegen
Tom Watson,
Peter Brice,
Geoffrey Lewis (C-698/15)
in aanwezigheid van
Open Rights Group,
Privacy International,
Law Society of England and Wales

[verzoeken van Kamarrätten i Stockholm (hogerberoepsrechter in bestuurszaken, Stockholm, Zweden) en de Court of Appeal (England & Wales) (Civil Division) [hogerberoepsrechter (Engeland & Wales) in civiele zaken]

om een prejudiciële beslissing]

„Prejudiciële verwijzing — Richtlijn 2002/58/EG — Verwerking van persoonsgegevens en bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie — Nationale wetgeving die voorziet in een algemene verplichting om gegevens over elektronische communicaties te bewaren — Artikel 15, lid 1 — Handvest van de grondrechten van de Europese Unie — Artikel 7 — Recht op eerbiediging van het privéleven — Artikel 8 — Recht op bescherming van persoonsgegevens — Ernstige inmenging — Rechtvaardiging — Artikel 52, lid 1 — Voorwaarden — Legitieme doelstelling van bestrijding van ernstige criminaliteit — Vereiste van een wettelijke grondslag in het nationale recht — Vereiste van strikte noodzakelijkheid — Vereiste van evenredigheid in een democratische samenleving”

Inhoud

I — Inleiding	3
II — Toepasselijke bepalingen	5

¹ — Oorspronkelijke taal: Frans.

A – Richtlijn 2002/58	5
B – Zweeds recht	5
1. Omvang van de bewaringsverplichting	6
2. Toegang tot bewaarde gegevens	6
a) De LEK	6
b) De RB	6
c) Wet 2012:278	7
3. Bewaringstermijn	7
4. Bescherming en beveiliging van bewaarde gegevens	8
C – Recht van het Verenigd Koninkrijk	8
1. Omvang van de bewaringsverplichting	9
2. Toegang tot bewaarde gegevens	9
3. Bewaringstermijn	10
4. Bescherming en beveiliging van bewaarde gegevens	10
III – Hoofdgedingen en prejudiciële vragen	11
A – Zaak C-203/15	11
B – Zaak C-698/15	12
IV – Procedure bij het Hof	12
V – Analyse van de prejudiciële vragen	13
A – Ontvankelijkheid van de tweede vraag in zaak C-698/15	14
B – Verenigbaarheid van een algemene verplichting tot bewaring van gegevens met de regeling van richtlijn 2002/58	15
1. Valt een algemene verplichting tot bewaring van gegevens binnen de werkingssfeer van richtlijn 2002/58?	16
2. Mogelijkheid om af te wijken van de regeling van richtlijn 2002/58 door de invoering van een algemene verplichting tot bewaring van gegevens	17
C – Toepasbaarheid van het Handvest op een algemene verplichting tot bewaring van gegevens ...	20
D – Verenigbaarheid van een algemene verplichting tot bewaring van gegevens met de door artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest gestelde vereisten	21
1. Vereiste van een wettelijke grondslag in het nationale recht	22

2. Eerbiediging van de wezenlijke inhoud van de door de artikelen 7 en 8 van het Handvest erkende rechten	25
3. Bestaan van een door de Unie erkende doelstelling van algemeen belang die een algemene verplichting tot bewaring van gegevens kan rechtvaardigen	26
4. Redelijkheid, noodzakelijkheid en evenredigheid van een algemene verplichting tot bewaring van gegevens in het licht van de bestrijding van ernstige criminaliteit	28
5. Noodzakelijkheid van een algemene verplichting tot bewaring van gegevens voor de bestrijding van ernstige criminaliteit	29
a) Strikte noodzakelijkheid van een algemene verplichting tot bewaring van gegevens	31
b) Dwingend karakter van de door het Hof in de punten 60-68 van het arrest DRI genoemde waarborgen in het licht van het vereiste van strikte noodzakelijkheid	34
6. Evenredigheid, in een democratische samenleving, van een algemene verplichting tot bewaring van gegevens in het licht van de doelstelling van bestrijding van ernstige criminaliteit	38
VI – Conclusie	42

I – Inleiding

1. In 1788 schreef James Madison, een van de auteurs van de Grondwet van de Verenigde Staten: „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”².

2. De onderhavige zaken voeren ons tot de kern van de door Madison onderscheiden „grote moeilijkheid”. Zij betreffen de verenigbaarheid met het Unierecht van nationale regelingen die aanbieders van voor het publiek toegankelijke elektronische communicatiediensten (hierna: „aanbieders”) verplichten tot bewaring van gegevens over elektronische communicaties (hierna: „communicatiegegevens”), welke verplichting geldt voor alle communicatiemiddelen en alle gebruikers (hierna: „algemene verplichting tot bewaring van gegevens”).

2 — „Als mensen engelen waren zou er geen overheid nodig zijn. Als engelen zouden regeren over mensen zou er noch extern noch intern toezicht op de overheid nodig zijn. Bij de afbakening van de grenzen van een bestuur van mensen over mensen bestaat de grote moeilijkheid hierin: de overheid moet eerst in staat worden gesteld haar burgers te controleren en vervolgens worden verplicht zichzelf te controleren”: Madison, J., „Federalist No. 51”, in Hamilton, A., Madison, J. en Jay, J., red. Genovese, M. A., *The Federalist Papers*, Palsgrave Macmillan, New York, 2009, blz. 120, vrije vertaling. Madison was een van de belangrijkste auteurs en een van de 39 ondertekenaars van de Grondwet van de Verenigde Staten (1787). Hij werd vervolgens de vierde president van de Verenigde Staten (van 1809 tot 1817).

3. Enerzijds stelt de bewaring van communicatiegegevens de overheid in staat „haar burgers te controleren”, door de bevoegde autoriteiten een onderzoeksmiddel te bieden dat van zeker nut kan zijn bij de bestrijding van zware criminaliteit, en met name bij de bestrijding van terrorisme. In feite verschaft de bewaring van die gegevens de autoriteiten een beperkt vermogen om het „verleden te lezen”, doordat zij gegevens kunnen inzien over de communicaties die een persoon heeft gevoerd nog voordat hij ervan werd verdacht betrokken te zijn bij een ernstig strafbaar feit.³

4. Anderzijds is het echter absoluut noodzakelijk om de overheid „te verplichten zichzelf te controleren”, zowel wat de bewaring van gegevens als de toegang daartoe betreft, gelet op de ernstige risico's die het bestaan van databestanden waarin alle op het nationale grondgebied gevoerde communicaties worden bewaard met zich brengt. Deze enorme databestanden stellen eenieder die er toegang toe heeft immers in staat een hele relevante bevolkingsgroep onmiddellijk te categoriseren.⁴ Die risico's moeten nauwkeurig worden beoordeeld, met name door te onderzoeken of een algemene verplichting tot bewaring van gegevens, als in de hoofdgedingen aan de orde, strikt noodzakelijk en evenredig is.

5. In het kader van de onderhavige zaken wordt het Hof en de verwijzende rechters derhalve verzocht om een evenwicht vast te stellen tussen de verplichting van de lidstaten om de veiligheid te waarborgen van de personen die zich op hun grondgebied bevinden, en de door de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”) erkende grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens.

6. Ik zal de in de onderhavige zaken aan het Hof gestelde vragen onderzoeken in het licht van die „grote moeilijkheid”. Die vragen betreffen in concreto de verenigbaarheid van nationale regelingen waarin een algemene verplichting tot bewaring van gegevens is opgenomen, met richtlijn 2002/58/EG⁵ en met de artikelen 7 en 8 van het Handvest. Met het oog op de beantwoording van die vragen dient het Hof met name te verduidelijken welke uitlegging er in een nationale context moet worden gegeven aan het arrest *Digital Rights Ireland e.a.* (hierna: „arrest DRI”)⁶, waarin de Grote kamer van het Hof richtlijn 2006/24/EG⁷ ongeldig heeft verklaard.

7. Om de redenen die ik hierna zal uiteenzetten, ben ik van mening dat een door een lidstaat opgelegde algemene verplichting tot bewaring van gegevens verenigbaar kan zijn met de door het Unierecht erkende grondrechten, mits strikt omgeven door een serie waarborgen die ik in de loop van mijn betoog zal aangeven.

3 — Dat beperkte vermogen om „het verleden te lezen” kan met name zeer nuttig blijken bij de opsporing van mogelijke medeplichtigen: zie de punten 178-184 van deze conclusie.

4 — Zie de punten 252-261 van deze conclusie.

5 — Richtlijn van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB 2002, L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (PB 2009, L 337, blz. 11).

6 — Arrest van 8 april 2014 (C-293/12 en C-594/12, EU:C:2014:238).

7 — Richtlijn van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB 2006, L 105, blz. 54).

II – Toepasselijke bepalingen

A – Richtlijn 2002/58

8. Artikel 1 van richtlijn 2002/58, „Onderwerp en werkingssfeer”, bepaalt:

„1. Deze richtlijn voorziet in de harmonisering van de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden – met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid – bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecomunicatieapparatuur en -diensten in de [Europese Unie].

2. Voor de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op richtlijn [95/46]. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn.

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het [VWEU] vallen, zoals die bedoeld in de titels V en VI van het [VEU], en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied.”

9. Artikel 15, lid 1, van richtlijn 2002/58, „Toepassing van een aantal bepalingen van richtlijn [95/46]”, luidt als volgt:

„De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische communicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn 95/46/EG. Daartoe kunnen de lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, [VEU].”

B – Zweeds recht

10. Richtlijn 2006/24, die inmiddels ongeldig is verklaard, is in Zweeds recht omgezet door wijziging van de lagen (2003:389) om elektronisk kommunikation (wet 2003:389 betreffende elektronische communicatie; hierna: „LEK”) en van de förordningen (2003:396) om elektronisk kommunikation (verordening 2003:396 betreffende elektronische communicatie; hierna: „FEK”), beide in werking getreden op 1 mei 2012.

1. Omvang van de bewaringsverplichting

11. Volgens hoofdstuk 6, § 16 a, LEK zijn aanbieders verplicht de communicatiegegevens te bewaren die nodig zijn voor het identificeren van de bron en de bestemming van een communicatie, het bepalen van de datum, het tijdstip, de duur en de aard van een communicatie, de gebruikte communicatieapparatuur en de locatie van mobiele communicatieapparatuur bij de aanvang en de beëindiging van de communicatie. Welke soorten gegevens bewaard moeten worden is nader uitgewerkt in de §§ 38 tot en met 43 LEK.

12. Die bewaringsverplichting betreft gegevens die zijn verwerkt in het kader van telefoondiensten, telefoondiensten via mobiele aansluitingspunten, systemen voor elektronisch berichtenverkeer, en diensten die toegang tot het internet verschaffen of capaciteit voor internettoegang ter beschikking stellen.

13. De te bewaren gegevens omvatten niet slechts alle gegevens die in het kader van richtlijn 2006/24 moesten worden bewaard, maar ook gegevens over niet tot stand gekomen communicaties en gegevens over de locatie bij de beëindiging van een communicatie via mobiele telefonie. Overeenkomstig de regeling die in die richtlijn was voorzien mag de inhoud van de communicaties niet worden bewaard.

2. Toegang tot bewaarde gegevens

14. De toegang tot bewaarde gegevens is geregeld in drie wetten, te weten de LEK, de Rättegångsbalken (wetboek van burgerlijke rechtsvordering; hierna: „RB”) en de lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (wet 2012:278 betreffende de verzameling van gegevens over elektronische communicaties bij de opsporingsactiviteiten van handhavingsautoriteiten; hierna: „wet 2012:278”).

a) De LEK

15. Volgens hoofdstuk 6, § 22, eerste alinea, punt 2, LEK moet iedere aanbieder desgevraagd abonnementsgegevens verstrekken aan het openbaar ministerie, de politie, de Säkerhetspolisen (Zweedse inlichtingendienst; hierna: „Säpo”) of iedere andere strafrechtelijke autoriteit, indien die gegevens verband houden met de verdenking van een strafbaar feit. Volgens die bepaling hoeft er geen sprake te zijn van een ernstig strafbaar feit.

16. Met abonnementsgegevens worden met name bedoeld de naam, de aanspreektitel, het postadres, het telefoonnummer en het IP-adres van de abonnee.

17. De verstrekking van abonnementsgegevens op grond van de LEK is niet onderworpen aan een voorafgaande toetsing, maar kan achteraf administratief worden getoetst. Voorts is er geen beperking gesteld aan het aantal autoriteiten dat toegang kan krijgen tot de gegevens.

b) De RB

18. De RB regelt de controle van elektronische communicaties in het kader van opsporingsonderzoeken.

19. De controle van elektronische communicaties kan in wezen slechts worden bevolen wanneer er een redelijke verdenking bestaat dat een bepaalde persoon een strafbaar feit heeft gepleegd waarop ten minste zes maanden gevangenisstraf staat, of een van de andere specifiek opgesomde strafbare feiten, indien die maatregel bijzonder noodzakelijk is voor het onderzoek.

20. Daarnaast kan tot een dergelijke controle worden overgegaan om in het kader van het onderzoek van een strafbaar feit waarop ten minste twee jaar gevangenisstraf staat, vast te kunnen stellen wie de vermoedelijke dader ervan is, indien die maatregel bijzonder noodzakelijk is voor het onderzoek.

21. Ingevolge hoofdstuk 27, § 21, RB moet het openbaar ministerie in de regel vooraf toestemming krijgen van de bevoegde rechter voor het controleren van elektronische communicaties.

22. Indien echter het verkrijgen van rechterlijke toestemming voorafgaand aan de controle op elektronische communicaties – terwijl die maatregel voor het onderzoek dringend noodzakelijk is – onverenigbaar lijkt met de spoed die de uitvoering ervan vereist of een belemmering ervoor vormt, wordt de toestemming, in afwachting van de beslissing van de bevoegde rechter, verleend door het openbaar ministerie, dat de bevoegde rechter daarvan onverwijld schriftelijk in kennis stelt. De bevoegde rechter moet vervolgens ten spoedigste onderzoeken of de maatregel gerechtvaardigd is.

c) Wet 2012:278

23. In het kader van het opsporingsonderzoek en krachtens § 1 van wet 2012:278 kunnen de nationale politie, de Säpo en het Tullverket (Zweedse douane), onder de door die wet gestelde voorwaarden, bij de aanbieder communicatiegegevens verzamelen.

24. Volgens §§ 2 en 3 van wet 2012:278 kunnen gegevens worden verzameld indien de omstandigheden van dien aard zijn dat de maatregel bijzonder noodzakelijk is voor het voorkomen, verhinderen, of vaststellen van een criminele activiteit die ofwel een of meer strafbare feiten waarop ten minste twee jaar gevangenisstraf staat omvat, ofwel een van de in § 3 opgesomde handelingen (waaronder met name verschillende vormen van sabotage en spionage).

25. De beslissing om tot een dergelijke maatregel over te gaan wordt genomen door het hoofd van de betrokken autoriteit of een daartoe gemachtigde persoon.

26. De beslissing moet de criminele activiteit en de betrokken periode vermelden, alsook het telefoonnummer, de adressen, de communicatieapparatuur en de geografische zone waarop zij betrekking heeft. De periode waarvoor de toestemming geldt mag niet langer zijn dan noodzakelijk is en mag vanaf de datum van de toestemmingsbeslissing niet meer dan een maand bedragen.

27. Dit type maatregel is niet onderworpen aan een voorafgaande toetsing. Krachtens § 6 van wet 2012:278 moet de Säkerhets- och integritetsskyddsmyndigheten (veiligheids- en integriteitscommissie, Zweden) evenwel in kennis worden gesteld van elke beslissing waarbij toestemming wordt verleend voor het verzamelen van gegevens. Op grond van § 1 van de lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (wet 2007:980 betreffende het toezicht op bepaalde wetshandhavingsactiviteiten) moet die commissie erop toezien dat de handhavingsautoriteiten de wet toepassen.

3. Bewaringstermijn

28. Uit hoofdstuk 6, § 16 d, LEK blijkt dat gegevens als bedoeld in § 16 a van dat hoofdstuk moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd. Zij moeten vervolgens onverwijld worden gewist, tenzij in hoofdstuk 6, § 16 d, tweede alinea, LEK anders is bepaald. Op grond van laatstgenoemde bepaling moeten gegevens die vóór het verstrijken van de bewaringstermijn zijn opgevraagd maar nog niet zijn verstrekt, na die verstrekking onverwijld worden gewist.

4. Bescherming en beveiliging van bewaarde gegevens

29. Hoofdstuk 6, § 20, eerste alinea, LEK verbiedt het zonder toestemming verspreiden of gebruiken van communicatiegegevens.

30. Volgens hoofdstuk 6, § 3 a, LEK, dienen de aanbieders passende technische en organisatorische maatregelen te nemen om de bescherming van gegevens bij de verwerking ervan te garanderen. Uit de totstandkomingsgeschiedenis van deze bepaling blijkt dat het beschermingsniveau niet mag worden bepaald op basis van een afweging tussen technische overwegingen, kosten, en de risico's van piraterij en hacking.

31. Nadere voorschriften voor gegevensbescherming zijn opgenomen in § 37, FEK en in de instructies en richtsnoeren van de Post- och telestyrelsen (Zweedse toezichthoudende autoriteit voor post en telecommunicatie; hierna: „PTS”) betreffende beschermingsmaatregelen in het kader van de bewaring en de verwerking van gegevens met het oog op misdaadbestrijding (PTSFS nr. 2012:4). Uit die voorschriften blijkt met name dat de aanbieders maatregelen dienen te nemen om gegevens te beschermen tegen onopzettelijke of ongeoorloofde vernietiging, tegen ongeoorloofde bewaring, verwerking en toegang, en tegen ongeoorloofde openbaarmaking. De aanbieder dient de gegevens tevens voortdurend en stelselmatig te beveiligen, rekening houdend met de aan de bewaringsverplichting verbonden bijzondere risico's.

32. In het Zweedse recht ontbreken bepalingen over de plaats waar de gegevens dienen te worden bewaard.

33. De toezichthoudende autoriteit is op grond van hoofdstuk 7 van de LEK bevoegd om bevelen en verboden uit te vaardigen tegen aanbieders die hun verplichtingen niet nakomen, eventueel op straffe van een dwangsom, en om een gehele of gedeeltelijke bedrijfsbeëindiging te gelasten.

C – Recht van het Verenigd Koninkrijk

34. De bewaring van gegevens is geregeld in de Data Retention and Investigatory Powers Act 2014 (wet van 2014 betreffende de bewaring van gegevens en de onderzoeksbevoegdheden; hierna: „DRIPA”), in de Data Retention Regulations 2014 (SI 2014/2042) (besluit van 2014 betreffende de bewaring van gegevens; hierna: „Regulations 2014”) en in de Retention of Communications (Data) Code of Practice (gedragscode voor de bewaring van gegevens; hierna: „code of practice on data retention”).

35. De bepalingen inzake de toegang tot gegevens bevinden zich in deel 1, hoofdstuk 2 van de Regulation of Investigatory Powers Act 2000 (wet van 2000 tot regeling van de onderzoeksbevoegdheden; hierna: „RIPA”), in de Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) (besluit van 2010 tot regeling van de onderzoeksbevoegdheden betreffende communicatiegegevens), zoals gewijzigd bij de Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015 (SI 2015/228) (besluit van 2015 tot wijziging van de regeling van de onderzoeksbevoegdheden betreffende communicatiegegevens), en in de Acquisition and Disclosure of Communications Data Code of Practice (gedragscode voor de vergaring en de verspreiding van communicaties; hierna: „code of practice on data acquisition”).

1. Omvang van de bewaringsverplichting

36. Volgens section 1 van de DRIPA kan de Secretary of State for the Home Department (minister van Binnenlandse Zaken, Verenigd Koninkrijk; hierna: „minister”) aanbieders verplichten tot bewaring van alle communicatiegegevens. Die verplichting kan in wezen betrekking hebben op alle gegevens over communicaties die zijn verzonden via een postdienst of een telecommunicatiesysteem, met uitzondering van de inhoud van die communicaties. Die gegevens omvatten onder meer de locatie van de gebruiker van de dienst en de gegevens waarmee kan worden vastgesteld welk IP-adres (internet protocol) of andere identicator, toebehoort aan de afzender of de ontvanger van een communicatie.

37. Tot de doeleinden die een dergelijke bewaringsmaatregel kunnen rechtvaardigen, behoren de belangen van de nationale veiligheid, de voorkoming en opsporing van strafbare feiten en de voorkoming van verstoringen van de openbare orde, de belangen van het economisch welzijn van het Verenigd Koninkrijk voor zover die belangen eveneens relevant zijn voor de belangen van de nationale veiligheid, de belangen van de openbare veiligheid, de bescherming van de volksgezondheid, de toetsing van de oplegging of inning van aan de overheid verschuldigde belastingen, bijdragen of andere bedragen, de voorkoming van lichamelijk of geestelijk letsel in noodsituaties, de ondersteuning van onderzoek naar gerechtelijke dwalingen, de identificatie van overledenen en van personen die zichzelf, anders dan als gevolg van een misdrijf, niet kunnen identificeren (bijvoorbeeld in het geval van een natuurramp of een ongeval), de uitoefening van functies met betrekking tot de regulering van financiële diensten en markten of met betrekking tot de financiële stabiliteit, en elk ander doel dat wordt vermeld in een door de minister krachtens section 22(2), DRIPA uitgevaardigd bevel.

38. De nationale wetgeving stelt het bewaringsbevel niet afhankelijk van de verlening van voorafgaande toestemming door een rechter of een onafhankelijke instantie. De minister moet nagaan of de bewaringsverplichting „noodzakelijk is voor en evenredig aan” een of meer doeleinden waarvoor relevante communicatiegegevens mogen worden bewaard.

2. Toegang tot bewaarde gegevens

39. Op grond van section 22(4) RIPA kunnen overheidsinstanties door middel van een bevel aanbieders verplichten hen communicatiegegevens te verstrekken. De vorm en de inhoud van die bevelen is geregeld in section 23(2) RIPA. Een dergelijk bevel wordt beperkt in de tijd door bepalingen over de intrekking en de hernieuwing ervan.

40. De verkrijging van communicatiegegevens moet noodzakelijk zijn voor en evenredig zijn aan één of meer van de in section 22 RIPA genoemde doeleinden, die overeenkomen met de in punt 37 van deze conclusie beschreven doeleinden die de bewaring van gegevens kunnen rechtvaardigen.

41. Uit de code of practice on data acquisition blijkt dat rechterlijke toestemming is vereist indien met een verzoek om toegang wordt beoogd de bron van een journalist te achterhalen of indien het verzoek afkomstig is van een lokale autoriteit.

42. Buiten die gevallen is de toegang van overheidsinstanties onderworpen aan de toestemming van een daartoe aangewezen persoon binnen de betrokken overheidsinstantie. Dit is een persoon die bij die overheidsinstantie een ambt, rang of positie bekleedt en is aangewezen met het oog op de verkrijging van communicatiegegevens, overeenkomstig het besluit van 2015 tot regeling van de onderzoeksbevoegdheden betreffende communicatiegegevens.

43. Toestemming van een rechter of een onafhankelijke instantie is niet specifiek vereist voor de toegang tot communicatiegegevens die zijn beschermd door een wettelijk beroepsgeheim of betrekking hebben op communicaties van artsen, parlementsleden of geestelijken. De code of practice on data acquisition bepaalt slechts dat bijzondere aandacht moet worden besteed aan de noodzaak en de evenredigheid van verzoeken om toegang tot dergelijke gegevens.

3. Bewaringstermijn

44. Section 1(5) DRIPA en section 4(2) van de Regulations 2014 bepalen dat gegevens gedurende een periode van ten hoogste twaalf maanden mogen worden bewaard. Volgens de code of practice on data retention mag die periode niet langer zijn dan noodzakelijk en evenredig is. Regulation 6 van de Regulations 2014 verlangt van de minister dat hij bewaringsbevelen doorlopend evalueert.

4. Bescherming en beveiliging van bewaarde gegevens

45. Ingevolge section 1 DRIPA mogen aanbieders bewaarde gegevens slechts verstrekken indien die verstrekking in overeenstemming is met deel 1, hoofdstuk 2, RIPA, met een rechterlijke beslissing of elke andere rechterlijke goedkeuring of machtiging, of met een door de minister krachtens section 1 DRIPA vastgestelde regeling.

46. Volgens Regulation 7 en Regulation 8 van de Regulations 2014 moeten de aanbieders de integriteit en veiligheid van de bewaarde gegevens garanderen, ervoor zorgen dat de gegevens niet per ongeluk of onrechtmatig worden vernietigd, per ongeluk verloren gaan of worden gewijzigd, of zonder toestemming of onrechtmatig worden bewaard, verwerkt, geraadpleegd of openbaar gemaakt. Zij moeten de gegevens zodanig vernietigen dat ze niet langer meer kunnen worden geraadpleegd indien de bewaring ervan niet langer is toegestaan, en beveiligingssystemen installeren. Regulation 9 van de Regulations 2014 belast de Information Commissioner met het toezicht op de naleving van deze verplichtingen door de aanbieders.

47. De autoriteiten waaraan de aanbieders communicatiegegevens verstrekken, dienen die gegevens, en ieder afschrift, uittreksel of samenvatting ervan, veilig te verwerken en te bewaren. Ingevolge de code of practice on data acquisition moeten de vereisten die zijn opgenomen in de Data Protection Act (hierna: „DPA”), waarbij richtlijn 95/46 is omgezet, worden nageleefd.

48. De RIPA voorziet in een Interception of Communications Commissioner (hierna: „commissioner”) die is belast met het onafhankelijk toezicht op de uitoefening en de vervulling van de in deel 1, hoofdstuk II, RIPA opgenomen bevoegdheden en verplichtingen. De commissioner houdt geen toezicht op het gebruik dat van section 1 DRIPA wordt gemaakt. Hij moet regelmatig voor het publiek en het parlement bestemde rapporten opstellen [sections 57(2) en 58 RIPA] en bijhouden wat de overheidsinstanties hebben bewaard en gerapporteerd (code of practice on data acquisition, sections 6.1–6.8). Indien er een reden is om te veronderstellen dat gegevens op onjuiste wijze zijn verworven, kan een klacht worden ingediend bij het Investigatory Powers Tribunal (section 65 RIPA).

49. Uit de code of practice on data acquisition blijkt dat de commissioner niet bevoegd is om een zaak naar dat gerecht te verwijzen. Hij mag iemand slechts informeren over een vermoedelijk onrechtmatig gebruik van bevoegdheden indien hij kan „aantonen dat een persoon is benadeeld door een door opzet of onvoorzichtigheid veroorzaakt verzuim”. Hij mag evenwel niet overgaan tot openbaarmaking indien daardoor de nationale veiligheid in gevaar wordt gebracht, zelfs niet indien hij van mening is dat er sprake is van een door opzet of onvoorzichtigheid veroorzaakt verzuim.

III – Hoofdingen en prejudiciële vragen

A – Zaak C-203/15

50. Op 9 april 2014, de dag na de uitspraak in de zaak DRI, informeerde Tele2 Sverige de PTS dat zij had besloten te stoppen met de bewaring van gegevens als bedoeld in hoofdstuk 6 van de LEK. Ook zou zij de gegevens verwijderen die zij tot dan toe had bewaard op grond van dat hoofdstuk. Tele2 Sverige was van mening dat de Zweedse wetgeving tot omzetting van richtlijn 2006/24 niet in overeenstemming was met het Handvest.

51. Op 15 april 2014 diende de Rikspolisstyrelsen (algemene directie van de nationale politie, Zweden; hierna: „RPS”) een klacht in bij de PTS omdat Tele2 Sverige was gestopt met het doorgeven aan haar van gegevens met betrekking tot bepaalde elektronische communicaties. Die weigering van Tele2 Sverige had volgens de RPS grote gevolgen voor de handhavingsactiviteiten van de politie.

52. Op 27 juni 2014 beval de PTS Tele2 Sverige om de bewaring van gegevens uiterlijk op 25 juli 2014 te hervatten op grond van hoofdstuk 6, § 16 a, LEK en de §§ 37 tot en met 43, FEK.

53. Tele2 Sverige stelde bij het Förvaltningsrätten i Stockholm (bestuursrechter, Stockholm, Zweden) beroep in tegen de beslissing van de PTS. Bij uitspraak van 13 oktober 2014 verwierp het Förvaltningsrätten i Stockholm dat beroep.

54. Tele2 Sverige stelde vervolgens hoger beroep in bij de verwijzende rechter, strekkende tot vernietiging van de beslissing van het Förvaltningsrätten i Stockholm.

55. De Kammarrätten i Stockholm (hogerberoepsrechter in bestuurszaken, Stockholm, Zweden) is van oordeel dat er argumenten zijn zowel voor als tegen de opvatting dat een vergaande verplichting als die van hoofdstuk 6, § 16 a, LEK verenigbaar is met de bepalingen van artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest. Het heeft derhalve besloten de behandeling van de zaak te schorsen en het Hof de volgende prejudiciële vragen te stellen:

- „1) Is een algemene verplichting tot bewaring van gegevens die van toepassing is op alle personen, alle elektronischecomunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel, de bestrijding van ernstige criminaliteit, [zoals beschreven in de punten 13-18 van de verwijzingsbeslissing], verenigbaar met artikel 15, lid 1, van richtlijn 2002/58, gelet op de artikelen 7, 8 en 52, lid 1, van het Handvest?
- 2) Indien de eerste vraag ontkennend wordt beantwoord, kan een dergelijke bewaringsverplichting dan niettemin zijn toegestaan:
- a) indien de toegang van de nationale autoriteiten tot de bewaarde gegevens is geregeld op de wijze als beschreven in de punten 19-36 [van de verwijzingsbeslissing], en
 - b) indien de vereisten van bescherming en beveiliging zijn geregeld op de wijze als beschreven in de punten 38-43 [van de verwijzingsbeslissing], en
 - c) alle betrokken gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd alvorens te worden gewist, zoals is uiteengezet in punt 37 [van de verwijzingsbeslissing]?”

B – *Zaak C-698/15*

56. Tom Watson, Peter Brice en Geoffrey Lewis hebben ieder bij de High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) [rechter van eerste aanleg (Engeland & Wales), afdeling van de bank van de Koningin (bestuurszaken)] beroep ingesteld tot toetsing van de rechtmatigheid („judicial review”) van de in section 1 DRIPA opgenomen regeling inzake gegevensbewaring, die de minister machtigt exploitanten van openbare telecommunicatiediensten te verplichten alle communicatiegegevens, met uitzondering van de inhoud van de betrokken communicaties, te bewaren gedurende een termijn van ten hoogste twaalf maanden.

57. Open Rights Group, Privacy International en de Law Society of England and Wales hebben toestemming gekregen in elk van die procedures te interveniëren.

58. Bij uitspraak van 17 juli 2015 verklaarde dat gerecht die regeling onverenigbaar met het Unierecht, omdat zij niet voldeed aan de door het arrest DRI gestelde vereisten die, volgens dat gerecht, van toepassing zijn op regelingen van de lidstaten inzake de bewaring van elektronischecommunicatiegegevens en de toegang daartoe. De minister heeft tegen deze uitspraak hoger beroep ingesteld bij de verwijzende rechter.

59. Bij arrest van 20 november 2015 stelde de Court of Appeal (England & Wales) (Civil Division) [hogerberoepsrechter (Engeland & Wales) in civiele zaken] zich op het voorlopige standpunt dat het arrest DRI geen dwingende vereisten van Unierecht heeft opgelegd aan de nationale wetgevingen, maar slechts heeft onderscheiden en beschreven welke bescherming in de geharmoniseerde Unieregeling ontbrak.

60. De Court of Appeal (England & Wales) (Civil Division) is evenwel van mening dat de antwoorden op die vragen van Unierecht niet duidelijk zijn, maar wel noodzakelijk zijn voor de uitspraak in deze procedures. Hij heeft dan ook besloten de behandeling van de zaak te schorsen en het Hof de volgende prejudiciële vragen voor te leggen:

- „1) Legt het arrest [DRI] (waaronder met name de punten 60 en 62 ervan) dwingende vereisten van Unierecht op die van toepassing zijn op de nationale regeling van een lidstaat inzake de toegang tot gegevens die overeenkomstig de nationale wetgeving worden bewaard, teneinde te voldoen aan de artikelen 7 en 8 van het [Handvest]?
- 2) Verruimt het arrest [DRI] de werkingssfeer van de artikelen 7 en/of 8 van het Handvest ten opzichte van die van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden („EVRM”), zoals vastgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens („EHRM”)?”

IV – Procedure bij het Hof

61. De prejudiciële verzoeken zijn bij de griffie van het Hof ingeschreven op 4 mei 2015 (zaak C-203/15) en op 28 december 2015 (zaak C-698/15).

62. Bij beschikking van 1 februari 2016 heeft het Hof beslist om zaak C-698/15 te behandelen volgens de versnelde procedure van artikel 105, lid 1, van het Reglement voor de procesvoering van het Hof.

63. In zaak C-203/15 zijn schriftelijke opmerkingen ingediend door Tele2 Sverige, de Belgische, de Tsjechische, de Deense, de Duitse, de Estse, de Ierse, de Spaanse, de Franse, de Hongaarse, de Nederlandse en de Zweedse regering, de regering van het Verenigd Koninkrijk en de Europese Commissie.

64. In zaak C-698/15 zijn schriftelijke opmerking ingediend door Watson, Brice en Lewis, Open Rights Group, Privacy International, de Law Society of England and Wales, de Tsjechische, de Deense, de Duitse, de Estse, de Ierse, de Franse, de Cypriotische, de Poolse en de Finse regering, de regering van het Verenigd Koninkrijk en de Commissie.

65. Bij beschikking van het Hof van 10 maart 2016 zijn deze twee zaken gevoegd voor de mondelinge behandeling en het arrest.

66. Tijdens de pleitzitting van 12 april 2016 zijn de vertegenwoordigers van Tele2 Sverige, Watson, Brice en Lewis, Open Rights Group, Privacy International, de Law Society of England and Wales, de Tsjechische, de Deense, de Duitse, de Estse, de Ierse, de Spaanse, de Franse, de Finse en de Zweedse regering, de regering van het Verenigd Koninkrijk en de Commissie in hun opmerkingen gehoord.

V – Analyse van de prejudiciële vragen

67. Met de eerste vraag in zaak C-203/15 wenst de verwijzende rechter van het Hof te vernemen of, in het licht van het arrest DRI, artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest aldus moeten worden uitgelegd dat zij zich ertegen verzetten dat een lidstaat aanbieders een algemene verplichting tot bewaring van gegevens oplegt als in de hoofdgedingen aan de orde, en wel los van de eventuele waarborgen waarmee die verplichting gepaard gaat.

68. Indien die vraag ontkennend wordt beantwoord beogen de tweede vraag in zaak C-203/15 en de eerste vraag in zaak C-698/15 vast te stellen of die bepalingen aldus moeten worden uitgelegd dat zij zich ertegen verzetten dat een lidstaat aanbieders een algemene verplichting tot bewaring van gegevens oplegt, indien die verplichting niet gepaard gaat met alle door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen inzake de toegang tot de gegevens, de bewaringstermijn, en de bescherming en beveiliging van de gegevens.

69. Aangezien deze drie vragen nauw met elkaar zijn verbonden zal ik ze in het vervolg van mijn uiteenzetting samen onderzoeken.

70. Daarentegen verlangt de tweede vraag in zaak C-698/15 afzonderlijke behandeling. Met die vraag wenst de verwijzende rechter van het Hof te vernemen of het arrest DRI de werkingssfeer van de artikelen 7 en/of 8 van het Handvest heeft verruimd ten opzichte van die van artikel 8 EVRM. Ik zal in de volgende paragraaf uiteenzetten waarom ik van mening ben dat deze vraag niet-ontvankelijk moet worden verklaard.

71. Alvorens met het onderzoek van deze vragen te beginnen acht ik het zinvol om in herinnering te brengen op welke soorten gegevens de in de hoofdgedingen betrokken bewaringsverplichtingen betrekking hebben. Volgens de verwijzende rechters is de omvang van die verplichtingen in wezen gelijk aan die van de verplichting die was opgenomen in artikel 5 van richtlijn 2006/24.⁸ Schematisch kunnen de communicatiegegevens die het voorwerp van die verplichtingen vormen worden verdeeld in vier categorieën⁹:

- gegevens waarmee zowel de bron als de bestemming van de communicatie kan worden onderscheiden;
- gegevens waarmee de locatie van zowel de bron als de bestemming van de communicatie kan worden vastgesteld;

8 — Die gelijkheid is begrijpelijk aangezien die nationale regelingen tot doel hadden die, thans ongeldige, richtlijn om te zetten.

9 — Zie voor de beschrijving van de in de hoofdgedingen betrokken nationale regelingen de punten 11-13 en 36 van deze conclusie.

- gegevens met betrekking tot de datum, het tijdstip en de duur van de communicatie, en
- gegevens waarmee het soort communicatie en het soort apparatuur dat daarbij is gebruikt kan worden vastgesteld.

72. De inhoud van de communicaties valt niet onder de in de hoofdingen betrokken algemene verplichtingen tot bewaring van gegevens, zoals ook was bepaald in artikel 5, lid 2, van richtlijn 2006/24.

A – Ontvankelijkheid van de tweede vraag in zaak C-698/15

73. De tweede vraag in zaak C-698/15 verzoekt het Hof vast te stellen of het arrest DRI de werkingssfeer van de artikelen 7 en/of 8 van het Handvest verruimt ten opzichte van die van artikel 8 EVRM, zoals uitgelegd door het EHRM.

74. Deze vraag weerspiegelt met name het door de minister voor de verwijzende rechter aangevoerde argument dat het EHRM noch verlangt dat voor de toegang tot gegevens vooraf toestemming moet worden verleend door een onafhankelijk orgaan, noch dat de bewaring van en de toegang tot die gegevens wordt beperkt tot de bestrijding van ernstige criminaliteit.

75. Ik ben van mening dat deze vraag om de volgende redenen als niet-ontvankelijk moet worden afgewezen. Het is duidelijk dat de door het Hof in het arrest DRI geformuleerde overwegingen en de oplossing waarvoor het heeft gekozen van doorslaggevend belang zijn voor de beslechting van de hoofdingen. De omstandigheid dat dit arrest mogelijk de werkingssfeer van de artikelen 7 en/of 8 van het Handvest heeft verruimd ten opzichte van die van artikel 8 EVRM is echter op zichzelf hiervoor niet relevant.

76. Het is in dit verband van belang eraan te herinneren dat volgens artikel 6, lid 3, VEU de door het EVRM gewaarborgde grondrechten als algemene beginselen deel uitmaken van het Unierecht. Zolang de Unie geen partij is bij dat verdrag, vormt het EVRM echter geen formeel in de rechtsorde van de Unie opgenomen rechtsinstrument.¹⁰

77. De eerste zin van artikel 52, lid 3, van het Handvest schrijft weliswaar voor dat, voor zover het Handvest rechten bevat die corresponderen met door het EVRM gegarandeerde rechten, die rechten aldus moeten worden uitgelegd dat „de inhoud en reikwijdte ervan dezelfde [zijn] als die welke er door genoemd verdrag aan worden toegekend”.

78. Maar volgens de tweede zin van artikel 52, lid 3, van het Handvest „verhindert [deze bepaling] niet dat het recht van de Unie een ruimere bescherming biedt”. In mijn ogen volgt uit deze zin dat het Hof, indien het dat in de context van het Unierecht nodig acht, de werkingssfeer van bepalingen van het Handvest kan verruimen ten opzichte van die van de corresponderende bepalingen van het EVRM.

10 — Advies 2/13 van 18 december 2014 (EU:C:2014:2454, punt 179) en arrest van 15 februari 2016, N. (C-601/15 PPU, EU:C:2016:84, punt 45 en aldaar aangehaalde rechtspraak).

79. Ik voeg daar subsidiair aan toe dat artikel 8 van het Handvest, zoals het Hof het heeft uitgelegd in het arrest DRI, een recht verleent dat met geen enkel door het EVRM gegarandeerd recht correspondeert, namelijk het recht op bescherming van persoonsgegevens, hetgeen overigens wordt bevestigd door de toelichting bij artikel 52 van het Handvest.¹¹ Bijgevolg is de uitleggingsregel van artikel 52, lid 3, eerste zin, van het Handvest in elk geval niet van toepassing op de uitlegging van artikel 8 van het Handvest, zoals Brice en Lewis, Open Rights Group en Privacy International, de Law Society of England and Wales, en de Tsjechische, de Ierse en de Finse regering hebben opgemerkt.

80. Uit het voorgaande volgt dat het Unierecht zich niet ertegen verzet dat de artikelen 7 en 8 van het Handvest een verdergaande bescherming bieden dan het EVRM. Bijgevolg is de omstandigheid dat het arrest DRI de werkingssfeer van die bepalingen van het Handvest mogelijkerwijs heeft verruimd ten opzichte van die van artikel 8 EVRM, op zichzelf niet relevant voor de beslechting van de hoofdgedingen. De voor die gedingen te kiezen oplossing hangt voornamelijk af van de voorwaarden waaronder een algemene verplichting tot bewaring van gegevens verenigbaar kan worden geacht met artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest, uitgelegd in het licht van het arrest DRI, hetgeen precies het voorwerp vormt van de drie andere in de onderhavige zaken gestelde vragen.

81. Volgens vaste rechtspraak kan het Hof een verzoek van een nationale rechter slechts afwijzen, wanneer de verlangde uitlegging van het Unierecht duidelijk geen verband houdt met een reëel geschil of met het voorwerp van het hoofdgeding, wanneer het probleem hypothetisch is, of wanneer het Hof niet beschikt over de feitelijke en juridische gegevens die het nodig heeft om een nuttig antwoord op de gestelde vragen te kunnen geven.¹²

82. In casu, en om de hiervoor uiteengezette redenen, is de tweede vraag in zaak C-698/15 mijns inziens slechts van theoretisch belang, aangezien een eventueel antwoord op die vraag de verwijzende rechter geen gegevens kan verschaffen voor een uitlegging van het Unierecht die hem van nut kunnen zijn bij de beslechting van het bij hem aanhangige geding met toepassing van dit recht.¹³

83. In deze omstandigheden ben ik van mening dat die vraag als niet-ontvankelijk moet worden afgewezen, zoals Watson, de Law Society of England and Wales, en de Tsjechische regering terecht hebben aangevoerd.

B – Verenigbaarheid van een algemene verplichting tot bewaring van gegevens met de regeling van richtlijn 2002/58

84. In deze paragraaf onderzoek ik of de lidstaten voor het opleggen van een algemene verplichting tot bewaring van gegevens gebruik kunnen maken van de door artikel 15, lid 1, van richtlijn 2002/58 geboden mogelijkheid. Ik onderzoek hierin echter niet de bijzondere vereisten waaraan lidstaten moeten voldoen indien zij van die mogelijkheid gebruik wensen te maken. Die vereisten komen in een latere paragraaf uitgebreid aan bod.¹⁴

11 — Overeenkomstig artikel 6, lid 1, derde alinea, VEU en artikel 52, lid 7, van het Handvest moet de toelichting bij het Handvest voor de uitlegging ervan in aanmerking worden genomen (zie arresten van 26 februari 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punt 20, en 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punt 47). Volgens die toelichting correspondeert artikel 7 van het Handvest met artikel 8 van het EVRM, terwijl artikel 8 van het Handvest met geen enkel recht van het EVRM correspondeert.

12 — Zie met name arresten van 9 november 2010, Volker und Markus Schecke en Eifert (C-92/09 en C-93/09, EU:C:2010:662, punt 40 en aldaar aangehaalde rechtspraak), en 24 april 2012, Kamberaj (C-571/10, EU:C:2012:233, punt 42 en aldaar aangehaalde rechtspraak).

13 — Zie met name arrest van 16 september 1982, Vlaeminck (132/81, EU:C:1982:294, punt 13), beschikking van 24 maart 2011, Abt e.a. (C-194/10, EU:C:2011:182, punten 36 en 37 en aldaar aangehaalde rechtspraak) en arrest van 24 oktober 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, punt 46 en aldaar aangehaalde rechtspraak).

14 — Zie de punten 126-262 van deze conclusie.

85. Open Rights Group en Privacy International stellen namelijk dat een dergelijke verplichting, los van de naleving van de uit artikel 15, lid 1, van richtlijn 2002/58 voortvloeiende vereisten, onverenigbaar is met de geharmoniseerde regeling van richtlijn 2002/58, omdat zij het wezen van die regeling en van de door deze richtlijn gevestigde rechten zou tenietdoen.

86. Alvorens dit argument te onderzoeken moet worden nagegaan of een algemene verplichting tot bewaring van gegevens binnen de werkingssfeer van die richtlijn valt.

1. Valt een algemene verplichting tot bewaring van gegevens binnen de werkingssfeer van richtlijn 2002/58?

87. Geen van de partijen die schriftelijke opmerkingen hebben ingediend bij het Hof bestrijdt dat een algemene verplichting tot bewaring van gegevens zoals in de hoofdgedingen aan de orde is, valt onder het begrip „verwerking van persoonsgegevens in verband met de levering van openbare elektronische communicatiediensten over openbare communicatienetwerken in de [Unie]” in de zin van artikel 3 van richtlijn 2002/58.

88. De Tsjechische, de Franse en de Poolse regering en de regering van het Verenigd Koninkrijk stellen echter dat een algemene verplichting tot bewaring van gegevens valt onder de uitzondering van artikel 1, lid 3, van richtlijn 2002/58. Enerzijds zouden de nationale bepalingen die de toegang tot de gegevens en het gebruik ervan door de politie en de justitiële autoriteiten van de lidstaten regelen, verband houden met de openbare veiligheid, defensie of de staatsveiligheid, of op zijn minst onder het strafrecht vallen. Anderzijds zou de bewaring van gegevens slechts tot doel hebben om die politie en justitiële autoriteiten in staat te stellen om toegang tot die gegevens te krijgen en ze te gebruiken. Bijgevolg zou op grond van de hierboven genoemde bepaling een algemene verplichting tot bewaring van gegevens zijn uitgesloten van de werkingssfeer van die richtlijn.

89. Ik ben niet overtuigd van deze redenering om de volgende redenen.

90. In de eerste plaats bevestigen de bewoordingen van artikel 15, lid 1, van richtlijn 2002/58 dat door de lidstaten opgelegde bewaringsverplichtingen binnen de werkingssfeer van deze richtlijn vallen. Volgens deze bepaling „kunnen de lidstaten [namelijk] onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd”. Het lijkt mij op zijn minst moeilijk vol te houden dat bewaringsverplichtingen van de werkingssfeer van die richtlijn zijn uitgesloten terwijl artikel 15, lid 1, van die richtlijn het mogelijk maakt om dergelijke verplichtingen vast te stellen.

91. In feite, en zoals Watson, Brice en Lewis, de Belgische, de Deense, de Duitse en de Finse regering als ook de Commissie hebben aangevoerd, geeft een algemene verplichting tot bewaring van gegevens als in de hoofdgedingen aan de orde, uitvoering aan artikel 15, lid 1, van richtlijn 2002/58.

92. In de tweede plaats impliceert het feit dat de bepalingen die de toegang regelen kunnen vallen onder de uitzondering van artikel 1, lid 3, van richtlijn 2002/58¹⁵ niet dat de bewaringsverplichting daar eveneens onder valt en bijgevolg buiten de werkingssfeer van deze richtlijn blijft.

15 — Zie de punten 123-125 van deze conclusie.

93. Het Hof heeft in dit verband reeds gelegenheid gehad te preciseren dat de activiteiten die worden genoemd in artikel 3, lid 2, eerste streepje, van richtlijn 95/46/EG¹⁶, dat bewoordingen van gelijke strekking bevat als artikel 1, lid 3, van richtlijn 2002/58, specifieke activiteiten van de staten of de overheidsdiensten zijn en niets van doen hebben met activiteiten van particulieren.¹⁷

94. De in de hoofdgedingen betrokken bewaringsverplichtingen zijn evenwel, zoals de Commissie heeft opgemerkt, opgelegd aan particuliere aanbieders in het kader van private elektronischecommunicatiediensten. Bovendien gelden deze verplichtingen los van ieder toegangsverzoek van de politie of de justitiële autoriteiten, en meer in het algemeen los van elke handeling van overheidsinstanties op het gebied van de openbare veiligheid, defensie, de staatsveiligheid of het strafrecht.

95. In de derde plaats bevestigt de uitspraak van het Hof in het arrest Ierland/Parlement en Raad dat een algemene verplichting tot bewaring van gegevens niet onder het strafrecht valt.¹⁸ Het Hof oordeelde namelijk dat richtlijn 2006/24, die in een dergelijke verplichting voorzag, niet onder het strafrecht viel maar onder de werking van de interne markt, zodat artikel 95 EG (thans artikel 114 VWEU) de juiste rechtsgrondslag vormde voor de vaststelling van die richtlijn.

96. Het Hof heeft hieraan met name ten grondslag gelegd dat de bepalingen van die richtlijn voornamelijk waren beperkt tot de activiteiten van de aanbieders van diensten en niet de toegang tot gegevens noch het gebruik daarvan door de politie of de justitiële autoriteiten van de lidstaten regelden.¹⁹ Daaruit leid ik af dat nationale bepalingen die een met die van richtlijn 2006/24 vergelijkbare verplichting tot bewaring van gegevens invoeren ook niet onder het strafrecht vallen.

97. Gelet op het voorgaande ben ik van mening dat een algemene verplichting tot bewaring van gegevens niet onder de uitzondering van artikel 1, lid 3, van richtlijn 2002/58 en bijgevolg wel degelijk binnen de werkingssfeer van die richtlijn valt.

2. Mogelijkheid om af te wijken van de regeling van richtlijn 2002/58 door de invoering van een algemene verplichting tot bewaring van gegevens

98. Thans moet worden vastgesteld of een algemene verplichting tot bewaring van gegevens verenigbaar is met de regeling van richtlijn 2002/58.

99. In dit verband rijst de vraag of een lidstaat voor het opleggen van een dergelijke verplichting gebruik kan maken van de door artikel 15, lid 1, van richtlijn 2002/58 geboden mogelijkheid.

100. Daartegen zijn vier argumenten aangevoerd, met name door Open Rights Group en Privacy International.

101. Volgens het eerste argument zou het aan de lidstaten toekennen van de bevoegdheid om een algemene verplichting tot bewaring van gegevens vast te stellen afbreuk doen aan de harmonisatiedoelstelling die de bestaansgrond van richtlijn 2002/58 vormt. Deze richtlijn voorziet immers, volgens artikel 1, lid 1, ervan, in de harmonisatie van de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden – met name

16 — Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281, blz. 31).

17 — Arrest van 6 november 2003, Lindqvist (C-101/01, EU:C:2003:596, punten 43 en 44).

18 — Arrest van 10 februari 2009 (C-301/06, EU:C:2009:68).

19 — Arrest van 10 februari 2009, Ierland/Parlement en Raad (C-301/06, EU:C:2009:68, punt 80).

het recht op een persoonlijke levenssfeer en vertrouwelijkheid – bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecomunicatieapparatuur en -diensten in de Unie.

102. Derhalve zou artikel 15, lid 1, van richtlijn 2002/58 niet aldus kunnen worden uitgelegd dat het de lidstaten de bevoegdheid verleent om een zodanig vergaande uitzondering op de regeling van die richtlijn vast te stellen dat dit streven naar harmonisatie elk nuttig effect wordt ontnomen.

103. Volgens het tweede argument verzetten ook de bewoordingen van artikel 15, lid 1, van richtlijn 2002/58 zich tegen een dergelijke ruime uitlegging van de bevoegdheid van de lidstaten om af te wijken van de regeling van die richtlijn. Volgens deze bepaling kunnen de lidstaten immers „wettelijke maatregelen treffen *ter beperking van de reikwijdte* van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten” (cursivering van mij).

104. Een algemene verplichting tot bewaring van gegevens zou echter niet slechts „de reikwijdte beperken” van de in die bepaling vermelde rechten en plichten, maar die rechten en plichten volledig tenietdoen. Dit zou gelden voor:

- de verplichting om het vertrouwelijke karakter van verkeersgegevens te garanderen en de verplichting om de opslag van informatie afhankelijk te stellen van de toestemming van de gebruiker, als bedoeld in respectievelijk artikel 5, leden 1 en 3, van richtlijn 2002/58;
- de verplichting om verkeersgegevens te wissen of anoniem te maken, als bedoeld in artikel 6, lid 1, van die richtlijn, en
- de verplichting om locatiegegevens anoniem te maken en om toestemming te krijgen van de gebruiker voor verwerking van die gegevens, als bedoeld in artikel 9, lid 1, van die richtlijn.

105. Deze eerste twee argumenten moeten mijns inziens worden afgewezen om de volgende redenen.

106. Enerzijds vermelden de bewoordingen van artikel 15, lid 1, van richtlijn 2002/58 de mogelijkheid dat de lidstaten „wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren”. Deze uitdrukkelijke verwijzing naar verplichtingen tot bewaring van gegevens bevestigt dat dergelijke verplichtingen op zichzelf niet onverenigbaar zijn met de regeling van richtlijn 2002/58. Hoewel die formulering niet uitdrukkelijk voorziet in de mogelijkheid van een *algemene* verplichting tot bewaring van gegevens, moet worden vastgesteld dat zij zich hiertegen ook niet verzet.

107. Anderzijds preciseert overweging 11 van richtlijn 2002/58 dat die richtlijn niets verandert „aan het bestaande evenwicht tussen het recht van personen op persoonlijke levenssfeer en de mogelijkheid voor de lidstaten om de in artikel 15, lid 1, van deze richtlijn bedoelde maatregelen te nemen die nodig zijn voor de bescherming van de openbare veiligheid, defensie, de staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied”. Bijgevolg „doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane intercepties van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het [EVRM] in acht nemen”.

108. Uit deze overweging 11 volgt mijns inziens dat de Uniewetgever niet de bedoeling heeft gehad afbreuk te doen aan de bevoegdheid van de lidstaten om de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde maatregelen te treffen, maar die bevoegdheid afhankelijk heeft willen stellen van bepaalde vereisten verband houdend met de door die maatregelen nagestreefde doelen en de evenredigheid ervan. Met andere woorden, een algemene verplichting tot bewaring van gegevens is mijns inziens niet onverenigbaar met de regeling van deze richtlijn, mits zij aan bepaalde voorwaarden voldoet.

109. Volgens het derde argument zou artikel 15, lid 1, van richtlijn 2002/58, als uitzondering op de regeling van die richtlijn, strikt moeten worden uitgelegd conform een uit de vaste rechtspraak van het Hof voortvloeiende uitleggingsregel. Die regel zou verbieden deze bepaling aldus uit te leggen dat zij de oplegging van een algemene verplichting tot bewaring van gegevens toelaat.

110. Ik ben in dit verband van mening dat de door artikel 15, lid 1, van richtlijn 2002/58 geboden mogelijkheid niet als uitzondering kan worden gekwalificeerd en derhalve niet strikt mag worden uitgelegd, zoals de Commissie terecht heeft aangevoerd. Deze mogelijkheid kan mijns inziens immers moeilijk als uitzondering worden gekwalificeerd gelet op de hierboven weergegeven overweging 11, volgens welke die richtlijn geen afbreuk doet aan de mogelijkheid voor de lidstaten om de in die bepaling bedoelde maatregelen vast te stellen. Ik merk bovendien op dat artikel 15 van die richtlijn het opschrift draagt „Toepassing van een aantal bepalingen van Richtlijn 95/46”, terwijl artikel 10 van die richtlijn is voorzien van het uitdrukkelijke opschrift „Uitzonderingen”. Die opschriften sterken mij in de gedachte dat de mogelijkheid waarin artikel 15 voorziet niet kan worden gekwalificeerd als „uitzondering”.

111. Volgens het vierde en laatste argument zou de onverenigbaarheid van een algemene verplichting tot bewaring van gegevens met de regeling van richtlijn 2002/58 worden ondersteund door de toevoeging van artikel 15, lid 1 bis, aan die richtlijn bij de vaststelling van de door het arrest DRI ongeldig verklaarde richtlijn 2006/24. Die onverenigbaarheid zou de Uniewetgever ertoe zou hebben gebracht artikel 15, lid 1, van richtlijn 2002/58 niet van toepassing te verklaren op de algemene bewaringsregeling van richtlijn 2006/24.

112. Dit argument lijkt mij voort te komen uit een onjuiste opvatting van de strekking van artikel 15, lid 1 bis, van richtlijn 2002/58. Volgens deze bepaling „[is artikel 15, lid 1, van richtlijn 2002/58] niet van toepassing op de uit hoofde van richtlijn [2006/24] te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden”.

113. Mijn lezing van die bepaling is de volgende. Ten aanzien van de gegevens waarvan de bewaring werd voorgeschreven door richtlijn 2006/24 en voor de erin neergelegde doeleneinden, verloren de lidstaten de in artikel 15, lid 1, van richtlijn 2002/58 genoemde bevoegdheid om de reikwijdte van de in die bepaling bedoelde rechten en plichten verder te beperken, met name door middel van aanvullende verplichtingen tot bewaring van gegevens. Met andere woorden, artikel 15, lid 1 bis, voorziet, wat de gegevens betreft waarvan de bewaring werd voorgeschreven door richtlijn 2006/24 en voor de erin neergelegde doeleinden, in een volledige harmonisatie.

114. Ik vind bevestiging voor deze uitlegging in overweging 12 van richtlijn 2006/24, volgens welke „[a]rtikel 15, lid 1, van richtlijn [2002/58] *van toepassing [blijft]* op gegevens, met inbegrip van gegevens met betrekking tot oproepingen zonder resultaat, die ingevolge de huidige richtlijn niet specifiek moeten worden bewaard en *derhalve niet onder het toepassingsgebied daarvan [vallen]*, alsook [op de] bewaring van gegevens *voor doelstellingen*, inclusief van justitiële aard, *andere dan die welke onder deze richtlijn vallen*” (cursivering van mij).

115. De invoeging van artikel 15, lid 1 bis, van richtlijn 2002/58 bevestigt derhalve niet de onverenigbaarheid van een algemene verplichting tot bewaring van gegevens met de regeling van die richtlijn, maar de wens van de Uniewetgever om bij de vaststelling van richtlijn 2006/24 een volledige harmonisatie tot stand te brengen.

116. Gelet op het voorgaande ben ik van mening dat een algemene verplichting tot bewaring van gegevens verenigbaar is met de regeling van richtlijn 2002/58 en dat een lidstaat bijgevolg gebruik kan maken van de mogelijkheid die artikel 15, lid 1, van die richtlijn biedt om een dergelijke verplichting op te leggen.²⁰ Het beroep op die mogelijkheid is evenwel onderworpen aan de naleving van strikte vereisten, die niet slechts voortvloeien uit die bepaling maar eveneens uit de relevante bepalingen van het Handvest gelezen in het licht van het arrest DRI, die in een volgende paragraaf zullen worden onderzocht.²¹

C – Toepasbaarheid van het Handvest op een algemene verplichting tot bewaring van gegevens

117. Alvorens de inhoud te onderzoeken van de eisen die het Handvest samen met artikel 15, lid 1, van richtlijn 2002/58 stelt wanneer een lidstaat ervoor kiest een algemene verplichting tot bewaring van gegevens op te leggen, moet worden nagegaan of het Handvest van toepassing is op een dergelijke verplichting.

118. De toepasselijkheid van het Handvest op een algemene verplichting tot bewaring van gegevens hangt voornamelijk af van de toepasselijkheid van richtlijn 2002/58 op een dergelijke verplichting.

119. Artikel 51, lid 1, eerste zin, van het Handvest bepaalt immers dat „[d]e bepalingen van dit Handvest [...] uitsluitend wanneer zij het recht van de Unie ten uitvoer brengen tot de lidstaten [zijn gericht]”. De toelichting bij artikel 51 van het Handvest verwijst in dit verband naar de rechtspraak van het Hof, volgens welke de verplichting om de in het kader van de Unie vastgestelde grondrechten te eerbiedigen alleen geldt voor de lidstaten wanneer deze optreden binnen het toepassingsgebied van het recht van de Unie.²²

120. De Tsjechische, de Franse en de Poolse regering alsook de regering van het Verenigd Koninkrijk, die de toepasselijkheid van richtlijn 2002/58 op een algemene verplichting tot bewaring van gegevens betwisten²³, stellen eveneens dat het Handvest niet van toepassing is op een dergelijke verplichting.

121. Ik heb reeds uiteengezet waarom ik van mening ben dat een algemene verplichting tot bewaring van gegevens uitvoering geeft aan de mogelijkheid die is gegeven in artikel 15, lid 1, van richtlijn 2002/58.²⁴

122. Ik meen derhalve dat de bepalingen van het Handvest, op grond van artikel 51, lid 1, ervan, van toepassing zijn op nationale maatregelen die een dergelijke verplichting opleggen, zoals Watson, Brice en Lewis, Open Rights Group en Privacy International, de Deense, de Duitse en de Finse regering alsook de Commissie hebben aangevoerd.²⁵

20 — Aangezien richtlijn 2002/58 kan worden gekwalificeerd als „lex specialis” ten opzichte van richtlijn 95/46 (zie in dit verband artikel 1, lid 2, van richtlijn 2002/58) is het mijns inziens niet nodig de verenigbaarheid na te gaan van een algemene verplichting tot bewaring van gegevens met de regeling van richtlijn 95/46, die bovendien niet wordt genoemd in de aan het Hof gestelde vragen. Volledigheidshalve wil ik niettemin preciseren dat de bewoordingen van artikel 13, lid 1, van richtlijn 95/46 de lidstaten meer handelingsvrijheid bieden dan die van artikel 15, lid 1, van richtlijn 2002/58, dat de draagwijdte ervan nader bepaalt in het kader van de levering van voor het publiek toegankelijke elektronischecomunicatiediensten. Uit het feit dat artikel 15, lid 1, van richtlijn 2002/58 de lidstaten de mogelijkheid biedt een algemene verplichting tot bewaring van gegevens vast te stellen, leid ik af dat artikel 13, lid 1, van richtlijn 95/46 die mogelijkheid ook biedt.

21 — Zie de punten 126-262 van deze conclusie.

22 — Uit vaste rechtspraak van het Hof volgt namelijk dat de in de rechtsorde van de Unie gewaarborgde grondrechten toepassing kunnen vinden in alle situaties die door het Unierecht worden beheerst, maar niet daarbuiten. In zoverre heeft het Hof reeds eraan herinnerd dat het een nationale regeling die niet binnen het kader van het Unierecht valt, niet aan het Handvest kan toetsen. Wanneer daarentegen een nationale regeling binnen het toepassingsgebied van het Unierecht valt, moet het Hof, ingeval het om een prejudiciële beslissing wordt verzocht, alle uitleggingsgegevens verschaffen die de nationale rechter nodig heeft om te kunnen beoordelen of deze regeling verenigbaar is met de grondrechten waarvan het de eerbiediging verzekert (zie arrest van 26 februari 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punt 19 en aldaar aangehaalde rechtspraak).

23 — Zie punt 88 van deze conclusie.

24 — Zie de punten 90-97 van deze conclusie.

25 — Meer in het bijzonder bepaalt artikel 51, lid 1, tweede zin, van het Handvest dat de lidstaten de door het Handvest gewaarborgde rechten moeten eerbiedigen wanneer zij het recht van de Unie ten uitvoer brengen.

123. Deze gevolgtrekking wordt niet tegengesproken door het feit dat de nationale bepalingen die de toegang tot bewaarde gegevens regelen, als zodanig niet binnen de werkingssfeer van het Handvest vallen.

124. Voor zover zij betrekking hebben op „activiteiten van de staat op strafrechtelijk gebied” vallen nationale bepalingen die de toegang van de politie en de justitiële autoriteiten tot bewaarde gegevens regelen met het oog op de bestrijding van ernstige criminaliteit, mijns inziens onder de uitzondering van artikel 1, lid 3, van richtlijn 2002/58.²⁶ Dergelijke nationale bepalingen brengen bijgevolg niet het recht van de Unie ten uitvoer, zodat het Handvest er niet op van toepassing is.

125. Het bestaansrecht van een algemene verplichting tot bewaring van gegevens is nochtans erin gelegen dat de handhavingsautoriteiten toegang kunnen krijgen tot de bewaarde gegevens. De problematieken van bewaring en toegang staan derhalve niet geheel los van elkaar. Zoals de Commissie terecht heeft opgemerkt, zijn de toegangsregels van doorslaggevend belang voor de beoordeling van de verenigbaarheid met het Handvest van bepalingen die een algemene verplichting tot bewaring van gegevens opleggen, welke bepalingen uitvoering geven aan artikel 15, lid 1, van richtlijn 2002/58. Meer in het bijzonder moeten de bepalingen die de toegang regelen in acht worden genomen bij de beoordeling van de noodzakelijkheid en de evenredigheid van een dergelijke verplichting.²⁷

D – Verenigbaarheid van een algemene verplichting tot bewaring van gegevens met de door artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest gestelde vereisten

126. Rest mij thans de moeilijke vraag of een algemene verplichting tot bewaring van gegevens verenigbaar is met de vereisten van artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8 en 52, lid 1, van het Handvest, gelezen in het licht van het arrest DRI. Deze vraag betreft meer in het algemeen de noodzakelijke aanpassing van het wettelijke kader dat de controlemogelijkheden van de lidstaten regelt; die mogelijkheden zijn als gevolg van recente technologische ontwikkelingen belangrijk toegenomen.²⁸

127. De eerste stap van elke analyse in deze context bestaat in de vaststelling dat er inmenging plaatsvindt in de door richtlijn 2002/58 erkende rechten en in de door de artikelen 7 en 8 van het Handvest erkende grondrechten.

128. Een dergelijke verplichting vormt namelijk een ernstige inmenging in het door artikel 7 van het Handvest erkende recht op eerbiediging van het privéleven en het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens. Aangezien het Hof die inmenging duidelijk heeft vastgesteld in de punten 32 tot en met 37 van het arrest DRI acht ik het niet nodig hierover verder uit te weiden.²⁹ Een algemene verplichting tot bewaring van gegevens vormt tevens een inmenging in een aantal van de door richtlijn 2002/58 erkende rechten.³⁰

26 — Zie voor de omvang van die uitzondering de punten 90-97 van deze conclusie.

27 — Zie de punten 185-262 van deze conclusie.

28 — Zie met name United Nations Commission on Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 april 2013, A/HRC/23/40, nr. 33: „Door technologische ontwikkelingen kunnen staten controleactiviteiten verrichten die niet langer zijn beperkt wat schaal of duur betreft. [...] Bijgevolg beschikken staten thans over meer middelen dan ooit om gelijktijdig, gericht en op grote schaal controleactiviteiten uit te oefenen die inbreuk maken op het privéleven [...]”. Zie ook nr. 50: „In algemene zin heeft de wetgeving het tempo van de technologische veranderingen niet bijgehouden. In de meeste staten zijn de juridische normen ofwel niet-bestaand, ofwel ontoereikend om het hoofd te bieden aan de hedendaagse omstandigheden waarin de controle op communicaties plaatsvindt [...]”.

29 — Ik kom niettemin nog terug op de specifieke risico's van het aanleggen van omvangrijke databestanden, in het kader van de bespreking van het vereiste van evenredigheid, in een democratische samenleving, van algemene verplichtingen tot bewaring van gegevens als in de hoofdingingen aan de orde: zie de punten 252-261 van deze conclusie.

30 — Zie in dit verband het door Open Rights Group en Privacy International aangevoerde argument dat is samengevat in punt 104 van deze conclusie.

129. De tweede stap van de analyse bestaat erin te bepalen of, en onder welke voorwaarden, die ernstige inmenging in de door richtlijn 2002/58 erkende rechten en de door de artikelen 7 en 8 van het Handvest erkende grondrechten kan worden gerechtvaardigd.

130. Twee bepalingen schrijven voor aan welke vereisten moet zijn voldaan wil die dubbele inmenging gerechtvaardigd zijn: artikel 15, lid 1, van richtlijn 2002/58, dat de mogelijkheid definieert waarover de lidstaten beschikken om de omvang van bepaalde in die richtlijn neergelegde rechten te beperken, en artikel 52, lid 1, van het Handvest, gelezen in het licht van het arrest DRI, dat het kader vormt voor elke beperking van de uitoefening van door het Handvest erkende rechten.

131. Ik wil benadrukken dat het *cumulatieve* vereisten betreft. De naleving van de vereisten van artikel 15, lid 1, van richtlijn 2002/58 impliceert immers op zichzelf niet dat aan de vereisten van artikel 52, lid 1, van het Handvest is voldaan, en vice versa.³¹ Bijgevolg kan een algemene verplichting tot bewaring van gegevens slechts verenigbaar met het Unierecht worden geacht wanneer zij zowel de in artikel 15, lid 1, van richtlijn 2002/58 neergelegde rechten als die van artikel 52, lid 1, van het Handvest eerbiedigt, zoals is opgemerkt door de Law Society of England and Wales.³²

132. Samen bevatten deze twee bepalingen zes vereisten waaraan moet zijn voldaan wil een door een algemene verplichting tot bewaring van gegevens veroorzaakte inmenging gerechtvaardigd zijn:

- de bewaringsverplichting moet een wettelijke grondslag hebben;
- zij moet de wezenlijke inhoud van de door het Handvest erkende rechten eerbiedigen;
- zij moet een doelstelling van algemeen belang nastreven;
- zij moet geschikt zijn voor het nastreven van die doelstelling;
- zij moet noodzakelijk zijn voor het nastreven van die doelstelling, en
- zij moet evenredig zijn, in een democratische samenleving, aan het nagestreefde doel.

133. Een aantal van die vereisten is reeds door het Hof besproken in het arrest DRI. Voor de duidelijkheid en gelet op de bijzonderheden van de onderhavige zaken ten opzichte van de zaak DRI zou ik niettemin op elk ervan willen ingaan en de vereisten van wettelijke grondslag, noodzakelijkheid, en evenredigheid in een democratische samenleving van een algemene verplichting tot bewaring van gegevens aan een nader onderzoek onderwerpen.

1. Vereiste van een wettelijke grondslag in het nationale recht

134. Zowel artikel 52, lid 1, van het Handvest als artikel 15, lid 1, van richtlijn 2002/58 stelt eisen aan de wettelijke grondslag die een lidstaat moet gebruiken voor het opleggen van een algemene verplichting tot bewaring van gegevens.

31 — Ik vind bevestiging voor die cumulatieve aard in de laatste zin van artikel 15, lid 1, van richtlijn 2002/58, volgens welke „[a]lle in dit lid bedoelde maatregelen [...] in overeenstemming [dienen] te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, [VEU]”. Volgens artikel 6, lid 1, VEU „erkent [de Unie] de rechten, vrijheden en beginselen die zijn vastgesteld in het [Handvest], dat dezelfde juridische waarde als de Verdragen heeft”.

32 — Uit deze cumulatieve aard volgt logischerwijs dat, voor zover de vereisten van deze twee bepalingen elkaar overlappen, het meest strikte van de twee toepassing moet vinden of, met andere woorden, het vereiste dat de betrokken rechten het best beschermt.

135. In de eerste plaats moet volgens artikel 52, lid 1, van het Handvest elke beperking van de uitoefening van de daarin erkende rechten „bij wet worden gesteld”. Ik wijs erop dat dit vereiste niet formeel is onderzocht door het Hof in het arrest DRI, dat betrekking had op een inmenging waarin was voorzien in een richtlijn.

136. Tot aan het recente arrest *WebMindLicenses*³³ had het Hof zich nog nooit uitgesproken over de precieze draagwijdte van dit vereiste, zelfs niet wanneer het uitdrukkelijk vaststelde dat er wel³⁴ of niet³⁵ aan was voldaan. In punt 81 van dat arrest oordeelde het Hof als volgt:

„In dat verband zij benadrukt dat het vereiste dat een beperking op de uitoefening van dat recht bij wet is vastgesteld, impliceert dat de wettelijke grondslag voor het gebruik van de in het vorige punt vermelde bewijzen door de belastingdienst voldoende duidelijk en nauwkeurig moet zijn, en een zekere bescherming biedt tegen eventueel willekeurig optreden van deze dienst doordat in die wettelijke grondslag zelf de reikwijdte van de beperking op de uitoefening van het door artikel 7 van het Handvest beschermde recht wordt omschreven (zie met name EHRM, *Malone/Verenigd Koninkrijk*, 2 augustus 1984, serie A nr. 82, § 67, alsook *Gillan en Quinton/Verenigd Koninkrijk*, 12 januari 2010, nr. 4158/05, § 77, EHRM 2010).”

137. Ik geef de Grote kamer van het Hof in overweging deze uitlegging in de onderhavige zaken te bevestigen om de volgende redenen.

138. Zoals advocaat-generaal Cruz Villalón terecht heeft opgemerkt in zijn conclusie in de zaak *Scarlet Extended*³⁶, bestaat er een omvangrijke rechtspraak van het EHRM over dit vereiste in de context van het EVRM, die wordt gekenmerkt door een „materiële” en niet door een „formele” opvatting van de term „wet”.³⁷

139. Volgens die rechtspraak impliceert de uitdrukking „bij wet gesteld” dat de wettelijke grondslag voldoende toegankelijk en voorzienbaar moet zijn, dat wil zeggen nauwkeurig genoeg geformuleerd om een persoon in staat te stellen – zo nodig na het inwinnen van deskundig advies – zijn gedrag erop af te stemmen. Die wettelijke grondslag moet eveneens naar behoren tegen willekeur beschermen en bijgevolg voldoende duidelijk de omvang en de wijze van uitoefening van de aan de autoriteiten toegekende bevoegdheid definiëren (beginsel van de rechtsstaat).³⁸

140. Ik ben van mening dat aan de in artikel 52, lid 1, van het Handvest gebruikte uitdrukking „bij wet gesteld” dezelfde betekenis moet worden toegekend als deze uitdrukking heeft in de context van het EVRM, om de volgende redenen.

33 — Arrest van 17 december 2015 (C-419/14, EU:C:2015:832).

34 — Zie met name arresten van 17 oktober 2013, *Schwarz* (C-291/12, EU:C:2013:670, punt 35) (inmenging voorzien in een Europese verordening); 27 mei 2014, *Spasic* (C-129/14 PPU, EU:C:2014:586, punt 57) (inmenging voorzien in de overeenkomst ter uitvoering van het tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek op 14 juni 1985 te Schengen gesloten akkoord betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen, ondertekend te Schengen op 19 juni 1990 en in werking getreden op 26 maart 1995); 6 oktober 2015, *Delvigne* (C-650/13, EU:C:2015:648, punt 47) (inmenging voorzien in de Franse kieswet en in het Franse wetboek van strafrecht), en 17 december 2015, *Neptune Distribution* (C-157/14, EU:C:2015:823, punt 69) (inmenging voorzien in een Europese verordening en in een Europese richtlijn).

35 — Arrest van 1 juli 2010, *Knauf Gips/Commissie* (C-407/08 P, EU:C:2010:389, punten 87-92) (inmenging zonder wettelijke grondslag).

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

37 — Zie met name EHRM, 14 september 2010, *Sanoma Uitgevers B.V./Nederland*, CE:ECHR:2010:0914JUD003822403, § 83.

38 — Zie met name EHRM, 26 maart 1987, *Leander/Zweden*, CE:ECHR:1987:0326JUD000924881, §§ 50 en 51; EHRM, 26 oktober 2000, *Hassan en Tchaouch/Bulgarije*, CE:ECHR:2000:1026JUD003098596, § 84; EHRM, 4 december 2008, *S. en Marper/Verenigd Koninkrijk*, CE:ECHR:2008:1204JUD003056204, § 95; EHRM, 14 september 2010, *Sanoma Uitgevers B.V./Nederland*, CE:ECHR:2010:0914JUD003822403, §§ 81-83, en EHRM, 31 maart 2016, *Stoyanov e.a./Bulgarije*, CE:ECHR:2016:0331JUD005538810, §§ 124-126.

141. Enerzijds kan ingevolge artikel 53 van het Handvest en de toelichting op dat artikel het door het Handvest geboden beschermingsniveau nooit lager zijn dan het door het EVRM gewaarborgde niveau. Dit gebod om de „EVRM-drempel” te bereiken impliceert dat de uitlegging door het Hof van de in artikel 52, lid 1, van het Handvest gebruikte uitdrukking „bij wet gesteld” ten minste zo strikt moet zijn als die van het EHRM in de context van het EVRM.³⁹

142. Anderzijds zou het, gelet op de horizontale aard van dit vereiste, dat van toepassing kan zijn op vele soorten inmengingen, zowel in de context van het Handvest als in die van het EVRM⁴⁰, niet juist zijn de lidstaten te onderwerpen aan verschillende criteria naargelang de inmenging wordt getoetst aan het ene of het andere van die instrumenten.⁴¹

143. Ik ben derhalve van mening dat, zoals de Estse regering en de Commissie hebben aangevoerd, de uitdrukking „bij wet gesteld” in artikel 52, lid 1, van het Handvest, in het licht van de rechtspraak van het EHRM die ik in punt 139 van deze conclusie heb samengevat, aldus moet worden uitgelegd dat een algemene verplichting tot bewaring van gegevens als in de hoofdingen aan de orde, enerzijds moet berusten op een voldoende toegankelijke en voorzienbare wettelijke grondslag en anderzijds naar behoren tegen willekeur moet beschermen.

144. In de tweede plaats moet de inhoud worden bepaald van de eisen die artikel 15, lid 1, van richtlijn 2002/58 stelt aan de wettelijke grondslag die moet worden gekozen door een lidstaat die gebruik wenst te maken van de door die bepaling geboden mogelijkheid.

145. In dit verband zij opgemerkt dat de taalversies van de eerste zin van deze bepaling onderling afwijken.

146. In de Engelse („*legislative measures*”), de Franse („*mesures législatives*”), de Italiaanse („*disposizioni legislative*”), de Portugese („*medidas legislativas*”), de Roemeense („*măsuri legislative*”) en de Zweedse („*genom lagstiftning vidta åtgärder*”) taalversie schrijft artikel 15, lid 1, eerste zin, van richtlijn 2002/58 mijns inziens maatregelen voor die zijn vastgesteld door de wetgevende macht.

147. Daarentegen kunnen de Deense („*retsfor skrifter*”), de Duitse („*Rechtsvorschriften*”), de Zweedse („*lagstiftning vidta åtgärder*”), de Nederlandse („*wettelijke maatregelen*”) en de Spaanse („*medidas legales*”) taalversie van deze zin aldus worden uitgelegd dat zij maatregelen voorschrijven die ofwel door de wetgevende macht, ofwel door de uitvoerende macht zijn vastgesteld.

148. Volgens vaste rechtspraak brengt het vereiste van uniforme toepassing en dus uitlegging van een Uniehandeling mee dat deze handeling niet op zichzelf in een van haar versies mag worden beschouwd, maar moet worden uitgelegd zowel naar de werkelijke bedoeling van degene van wie de handeling afkomstig is, als naar het doel dat hij nastreeft, gelet op onder meer de versies in alle andere officiële talen. Indien die versies onderling afwijken, dan moet die bepaling in principe worden uitgelegd met inachtneming van de algemene opzet en de doelstelling van de regeling waarvan zij een onderdeel vormt.⁴²

39 — Met name kan het Hof mijns inziens geen uitlegging aan dit vereiste geven die ruimer is dan die van het EHRM, aangezien dat tot gevolg zou hebben dat meer gevallen van inmenging zouden worden toegestaan dan mogelijk is op basis van de uitlegging van dit vereiste door het EHRM.

40 — Deze uitdrukking „bij wet gesteld” wordt gebruikt in artikel 8, lid 2 (recht op eerbiediging van het privéleven en van het familie- en gezinsleven), in artikel 9, lid 2 (vrijheid van gedachte, geweten en godsdienst), in artikel 10, lid 2 (vrijheid van meningsuiting), en in artikel 11, lid 2 (vrijheid van vereniging en vergadering) van het EVRM. In de context van het Handvest is artikel 52, lid 1, van toepassing op elke beperking van de erin erkende rechten, gesteld dat een dergelijke beperking is toegestaan.

41 — Zie in die zin Peers, S., „Article 52 – Scope of guaranteed rights”, in Peers, S., e.a., *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, nr. 52.39.

42 — Zie met name arresten van 30 mei 2013, Asbeek Brusse en de Man Garabito (C-488/11, EU:C:2013:341, punt 26); 24 juni 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414, punt 26), en 26 februari 2015, Christie's France (C-41/14, EU:C:2015:119, punt 26).

149. In casu regelt artikel 15, lid 1, van richtlijn 2002/58 de mogelijkheid voor de lidstaten om af te wijken van de door de artikelen 7 en 8 van het Handvest erkende grondrechten, in de bescherming waarvan deze richtlijn voorziet. Het lijkt mij dan ook juist om het door artikel 15, lid 1, van richtlijn 2002/58 gestelde vereiste van wettelijke grondslag uit te leggen in het licht van het Handvest en in het bijzonder van artikel 52, lid 1, ervan.

150. De door artikel 15, lid 1, van richtlijn 2002/58 voorgeschreven „maatregelen” moeten derhalve dwingend beschikken over de in punt 143 van deze conclusie vermelde kenmerken, dus toegankelijk en voorzienbaar zijn en naar behoren beschermen tegen willekeur. Uit deze kenmerken, en met name uit het vereiste dat die maatregelen naar behoren moeten beschermen tegen willekeur, volgt dat deze maatregelen *bindend* moeten zijn voor de nationale autoriteiten die toegang krijgen tot de bewaarde gegevens. Het zou met name niet volstaan indien de waarborgen die de toegang tot die gegevens omgeven zouden zijn opgenomen in niet-bindende interne gedragscodes of richtsnoeren, zoals terecht is opgemerkt door de Law Society of England and Wales.

151. Bovendien sluit de uitdrukking „de lidstaten kunnen [...] maatregelen treffen”, die in alle taalversies van artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gelijk is, mijns inziens uit dat nationale rechtspraak, zelfs wanneer die vast is, een voldoende wettelijke grondslag kan vormen voor de toepassing van die bepaling. Ik wijs erop dat die bepaling in dit opzicht verder gaat dan de eisen die de rechtspraak van het EHRM stelt.⁴³

152. Ik voeg daaraan toe dat het mij, gelet op de ernst van de door een algemene verplichting tot bewaring van gegevens veroorzaakte inmenging in de door de artikelen 7 en 8 van het Handvest erkende grondrechten, wenselijk lijkt dat de wezenlijke inhoud van de betrokken regeling, en met name de waarborgen die deze verplichting omgeven, wordt vastgelegd in een door de wetgevende macht vastgestelde maatregel, waarvan de uitvoerende macht de uitvoeringsbepalingen preciseert.

153. Gelet op het voorgaande ben ik van mening dat artikel 15, lid 1, van richtlijn 2002/58 en artikel 52, lid 1, van het Handvest aldus moeten worden uitgelegd dat regelingen die een algemene verplichting tot bewaring van gegevens opleggen, als in de hoofdingen aan de orde, moeten worden vastgesteld bij wettelijke of bestuursrechtelijke maatregelen die voldoende toegankelijk en voorzienbaar zijn en naar behoren beschermen tegen willekeur.

154. Het staat aan de verwijzende rechters om de naleving van dit vereiste na te gaan, gelet op hun bevoorrechte positie waar het de beoordeling van hun respectieve nationale regelingen betreft.

2. Eerbiediging van de wezenlijke inhoud van de door de artikelen 7 en 8 van het Handvest erkende rechten

155. Volgens artikel 52, lid 1, moeten beperkingen van de uitoefening van de door het Handvest erkende rechten en vrijheden „de wezenlijke inhoud van die rechten en vrijheden eerbiedigen”.⁴⁴ Dit aspect, dat het Hof heeft onderzocht in de punten 39 en 40 van het arrest DRI in de context van richtlijn 2006/24, lijkt geen bijzondere problemen op te leveren in het kader van de onderhavige zaken, zoals is opgemerkt door de Spaanse en de Ierse regering en de Commissie.

43 — Zie met name EHRM, 14 september 2010, Sanoma Uitgevers B.V./Nederland, CE:ECHR:2010:0914JUD003822403, § 83: „[de in de artikelen 8-11 EVRM opgenomen term ‚wet’ omvat] zowel het ‚geschreven recht’, waaronder regelgeving van lagere rang en regelgevingshandelingen die door beroepsorganisaties zijn vastgesteld in het kader van hun door de wetgever gedelegeerde normatieve bevoegdheid, als het ‚ongeschreven recht’. De term ‚wet’ kan derhalve zowel het geschreven recht als het ‚rechtersrecht’ omvatten.”

44 — Een dergelijk vereiste blijkt niet uit de bewoordingen van artikel 15, lid 1, van richtlijn 2002/58, noch uit de systematiek van die richtlijn, zoals ik in de punten 99-116 van deze richtlijn heb uiteengezet.

156. In punt 39 van het arrest DRI besliste het Hof dat die richtlijn geen afbreuk deed aan de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven en de andere door artikel 7 van het Handvest erkende rechten, omdat zij niet toestond bood om kennis te nemen van de inhoud zelf van de elektronische communicaties.

157. Deze uitspraak is mijns inziens toepasbaar op de in de hoofdgedingen betrokken nationale regelingen, aangezien die ook niet toestaan kennis te nemen van de inhoud zelf van de elektronische communicaties.⁴⁵

158. In punt 40 van het arrest DRI oordeelde het Hof dat richtlijn 2006/24 geen afbreuk deed aan de wezenlijke inhoud van het door artikel 8 van het Handvest erkende grondrecht op bescherming van persoonsgegevens, gelet op de beginselen van gegevensbescherming en -beveiliging die de aanbieders ingevolge artikel 7 van die richtlijn moesten eerbiedigen, mits de lidstaten ervoor zorgden dat passende technische en organisatorische maatregelen werden genomen om te vermijden dat de gegevens per ongeluk of onrechtmatig werden vernietigd dan wel per ongeluk verloren raakten of werden gewijzigd.

159. Ook die uitspraak is mijns inziens toepasbaar op de in de hoofdgedingen betrokken nationale regelingen, aangezien deze vergelijkbare waarborgen bevatten voor de bescherming en de beveiliging van de door de aanbieders opgeslagen gegevens en deze waarborgen een doeltreffende bescherming van persoonsgegevens tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens mogelijk moet maken.⁴⁶

160. Het staat niettemin aan de verwijzende rechters om na te gaan of de in de hoofdgedingen betrokken nationale regelingen de wezenlijke inhoud van de door de artikelen 7 en 8 van het Handvest erkende rechten daadwerkelijk eerbiedigen in het licht van het voorgaande.

3. Bestaan van een door de Unie erkende doelstelling van algemeen belang die een algemene verplichting tot bewaring van gegevens kan rechtvaardigen

161. Zowel artikel 15, lid 1, van richtlijn 2002/58 als artikel 52, lid 1, van het Handvest vereist dat inmengingen in de door die instrumenten erkende rechten een doelstelling van algemeen belang nastreven.

162. In de punten 41 tot en met 44 van het arrest DRI oordeelde het Hof enerzijds dat de door richtlijn 2006/24 opgelegde algemene verplichting tot bewaring van gegevens bijdroeg tot „de bestrijding van ernstige criminaliteit en aldus uiteindelijk tot de openbare veiligheid”, en anderzijds dat die bestrijding van ernstige criminaliteit een doelstelling van algemeen belang van de Unie vormde.

163. Uit de rechtspraak van het Hof blijkt namelijk dat de bestrijding van terrorisme ter handhaving van de internationale vrede en veiligheid een doel van algemeen belang van de Unie vormt. Hetzelfde geldt voor de bestrijding van ernstige criminaliteit ter waarborging van de openbare veiligheid. In dit verband zij voorts opgemerkt dat artikel 6 van het Handvest bepaalt dat eenieder niet alleen recht heeft op vrijheid, maar ook op veiligheid.⁴⁷

45 — Zie de beschrijving van de in de hoofdgedingen betrokken nationale regelingen in, met name, de punten 13 en 36 van deze conclusie.

46 — Arrest DRI, punt 54. Zie de beschrijving van de in de hoofdgedingen betrokken nationale regelingen in de punten 29-33, 45 en 46 van deze conclusie.

47 — Arrest DRI, punt 42 en aldaar aangehaalde rechtspraak.

164. Dit oordeel is toepasbaar op de in de hoofdgedingen betrokken algemene verplichtingen tot bewaring van gegevens, die kunnen worden gerechtvaardigd door de doelstelling van bestrijding van ernstige criminaliteit.

165. Gelet op bepaalde voor het Hof aangevoerde argumenten moet niettemin worden vastgesteld of een dergelijke verplichting kan worden gerechtvaardigd door een andere doelstelling van algemeen belang dan de bestrijding van ernstige criminaliteit.

166. In dit verband verwijzen de bewoordingen van artikel 52, lid 1, van het Handvest in algemene zin naar „door de Unie erkende doelstellingen van algemeen belang” en „de eisen van de bescherming van de rechten en vrijheden van anderen”.

167. Artikel 15, lid 1, van richtlijn 2002/58 omschrijft de doelstellingen die een inmenging in de door deze richtlijn erkende rechten kunnen rechtvaardigen preciezer. Volgens deze bepaling moeten de desbetreffende maatregelen namelijk bijdragen aan de „waarborging van de nationale, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van ongevoegd gebruik van het elektronischcommunicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn 95/46”.

168. Het Hof oordeelde voorts in het arrest *Promusicae*⁴⁸ dat deze bepaling moet worden uitgelegd in het licht van artikel 13, lid 1, van richtlijn 95/46, dat afwijkingen van de in die richtlijn neergelegde rechten toestaat wanneer deze worden gerechtvaardigd door „de bescherming van de rechten en vrijheden van anderen”. Het Hof oordeelde bijgevolg dat artikel 15, lid 1, van richtlijn 2002/58 de lidstaten de mogelijkheid bood om een aanbieder te verplichten persoonsgegevens te verstrekken, zodat in een civiele procedure kon worden vastgesteld of er sprake was van een inbreuk op auteursrechten op muzikale en audiovisuele opnamen.

169. De regering van het Verenigd Koninkrijk heeft op grond van dit arrest aangevoerd dat een algemene verplichting tot bewaring van gegevens kan worden gerechtvaardigd door ieder in artikel 15, lid 1, van richtlijn 2002/58 en artikel 13, lid 1, van richtlijn 95/46 vermeld doel. Volgens die regering kan een dergelijke verplichting worden gerechtvaardigd door het nut dat de bewaarde gegevens hebben voor de bestrijding van „lichte” criminaliteit (tegenover „ernstige”) en zelfs in de context van niet-strafrechtelijke procedures die verband houden met de in die bepalingen vermelde doelen.

170. Dit argument overtuigt mij niet om de volgende redenen.

171. In de eerste plaats, en zoals Watson, Open Rights Group, en Privacy International terecht stellen, is de benadering die het Hof in het arrest *Promusicae*⁴⁹ heeft gekozen niet toepasbaar op de onderhavige zaken, aangezien dat arrest een door een vereniging van houders van auteursrechten ingediend verzoek om toegang tot gegevens betrof die uit eigen beweging door een aanbieder, Telefónica de España, waren bewaard. Met andere woorden, dit arrest betrof niet de doelstellingen die de ernstige inmengingen in de grondrechten die inherent zijn aan algemene verplichtingen tot bewaring van gegevens als in de hoofdgedingen aan de orde, kunnen rechtvaardigen.

172. In de tweede plaats ben ik van mening dat het vereiste van evenredigheid in een democratische samenleving uitsluit dat de bestrijding van lichte criminaliteit of het goede verloop van niet-strafrechtelijke procedures een algemene verplichting tot bewaring van gegevens zou kunnen rechtvaardigen. De aanzienlijke risico's die een dergelijke verplichting met zich brengt staan immers niet in verhouding tot de voordelen die zij zou hebben voor de bestrijding van lichte criminaliteit of in de context van niet-strafrechtelijke procedures.⁵⁰

48 — Arrest van 29 januari 2008 (C-275/06, EU:C:2008:54, punten 50-54).

49 — Arrest van 29 januari 2008 (C-275/06, EU:C:2008:54).

50 — Zie de punten 252-261 van deze conclusie.

173. Gelet op het voorgaande ben ik van mening dat artikel 15, lid 1, van richtlijn 2002/58 en artikel 52, lid 1, van het Handvest aldus moeten worden uitgelegd dat de bestrijding van ernstige criminaliteit een doelstelling van algemeen belang vormt die een algemene verplichting tot bewaring van gegevens kan rechtvaardigen, in tegenstelling tot de bestrijding van lichte criminaliteit of het goede verloop van niet-strafrechtelijke procedures.

174. Bijgevolg moeten de redelijkheid, noodzakelijkheid en evenredigheid van een dergelijke verplichting worden onderzocht in het licht van de bestrijding van ernstige criminaliteit.

4. Redelijkheid, noodzakelijkheid en evenredigheid van een algemene verplichting tot bewaring van gegevens in het licht van de bestrijding van ernstige criminaliteit

175. De vereisten van redelijkheid, noodzakelijkheid⁵¹ en evenredigheid⁵² vloeien zowel voort uit artikel 15, lid 1, van richtlijn 2002/58 als uit artikel 52, lid 1, van het Handvest.

176. Ingevolge het eerste van deze vereisten moeten algemene verplichtingen tot bewaring van gegevens, als hier aan de orde, geschikt zijn om bij te dragen tot de hiervoor onderscheiden doelstelling van algemeen belang, te weten de bestrijding van ernstige criminaliteit.

177. Dit vereiste levert geen bijzondere moeilijkheid op in de context van de onderhavige zaken. Zoals het Hof heeft opgemerkt in punt 49 van het arrest DRI, bieden de bewaarde gegevens de nationale strafvervolgingsautoriteiten een extra onderzoeksmiddel om ernstige gevallen van criminaliteit te voorkomen of op te helderen. Een dergelijke verplichting draagt derhalve bij aan de bestrijding van ernstige criminaliteit.

178. Ik wil niettemin verduidelijken welk nut een algemene verplichting tot bewaring van gegevens kan hebben voor de bestrijding van ernstige criminaliteit. Zoals de Franse regering terecht heeft aangevoerd, stelt een dergelijke maatregel, anders dan gerichte controlemaatregelen, de strafrechtelijke autoriteiten tot op zekere hoogte in staat om door de raadpleging van de bewaarde gegevens het „verleden te lezen”.

179. Een gerichte controlemaatregel heeft betrekking op personen van wie vooraf is vastgesteld dat zij betrokken kunnen zijn, al is het maar indirect of in de verte, bij een ernstig strafbaar feit. Dergelijke gerichte maatregelen geven de bevoegde autoriteiten toegang tot gegevens over door die personen gevoerde communicaties of zelfs tot de inhoud van die communicaties. Die toegang kan echter slechts communicaties betreffen die dergelijke personen hebben gevoerd *nadat* hun identiteit is vastgesteld.

180. Daarentegen betreft een algemene verplichting tot bewaring van gegevens alle communicaties van alle gebruikers, zonder dat enige betrokkenheid bij een ernstig strafbaar feit is vereist. Een dergelijke verplichting stelt de bevoegde autoriteiten in staat de communicatiegeschiedenis van een persoon te raadplegen vóórdat een dergelijke betrokkenheid van die persoon is vastgesteld. Het is in die zin dat een dergelijke verplichting de handhavingsautoriteiten een beperkt vermogen verleent om het verleden te lezen door hen toegang te bieden tot de communicaties die dergelijke personen hebben gevoerd *voordat* hun identiteit werd vastgesteld.⁵³

51 — Zie voor de noodzakelijkheid de punten 185-245 van deze conclusie.

52 — Zie voor de evenredigheid *stricto sensu* de punten 246-262 van deze conclusie.

53 — De Commissie heeft eveneens opgemerkt dat de toegevoegde waarde van een algemene verplichting tot bewaring van gegevens ten opzichte van een gerichte bewaring van gegevens ligt in dat beperkte vermogen om het verleden te lezen: zie Commission Staff Working Document, bijlage bij het richtlijnvoorstel dat heeft geleid tot de vaststelling van richtlijn 2006/24, SEC(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”.

181. Met andere woorden, het nut van een algemene verplichting tot bewaring van gegevens voor de bestrijding van ernstige criminaliteit ligt in dat beperkte vermogen om het verleden te lezen aan de hand van gegevens die de geschiedenis weergeven van de communicaties die een persoon heeft gevoerd vóórdat hij ervan werd verdacht betrokken te zijn bij een ernstig strafbaar feit.⁵⁴

182. Bij de indiening van het richtlijnvoorstel dat heeft geleid tot de vaststelling van richtlijn 2006/24 heeft de Commissie dit nut verduidelijkt aan de hand van een aantal concrete voorbeelden van onderzoeken inzake, met name, daden van terrorisme, moord, ontvoering en kinderpornografie.⁵⁵

183. Een aantal gelijksoortige voorbeelden is voor het Hof uiteengezet in het kader van de onderhavige zaken, met name door de Franse regering, die heeft gewezen op de positieve verplichting die op de lidstaten rust om de veiligheid te garanderen van personen die zich op hun grondgebied bevinden. Volgens die regering speelt in het kader van de onderzoeken naar de ontmanteling van netwerken die het vertrek van Franse onderdanen naar conflictgebieden in Irak of Syrië organiseerden, de toegang tot bewaarde gegevens een doorslaggevende rol bij de identificatie van personen die dat vertrek hebben bevorderd. Zij voegt daaraan toe dat de toegang tot de communicatiegegevens van personen die betrokken waren bij de recente terroristische aanslagen van januari en november 2015 in Frankrijk voor de opsporingsambtenaren buitengewoon nuttig is geweest voor de opsporing van medeplichtigen van de daders van die aanslagen. In het kader van de opsporing van een vermiste persoon kunnen gegevens met betrekking tot de locatie van die persoon tijdens de communicaties die hij vóór zijn verdwijning heeft gevoerd een doorslaggevende rol spelen voor het onderzoek.

184. Gelet op het voorgaande ben ik van mening dat een algemene verplichting tot bewaring van gegevens geschikt is om bij te dragen tot de bestrijding van ernstige criminaliteit. Niettemin moet nog worden nagegaan of een dergelijke verplichting voor dit doel zowel noodzakelijk als evenredig is.

5. Noodzakelijkheid van een algemene verplichting tot bewaring van gegevens voor de bestrijding van ernstige criminaliteit

185. Volgens vaste rechtspraak kan een maatregel slechts worden geacht noodzakelijk te zijn indien er geen andere maatregel is die even passend maar minder ingrijpend is.⁵⁶

54 — De Franse regering verwijst in dit verband naar het rapport van de Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, blz. 209 en 210. De Conseil d'État (Frankrijk) betoogt hierin dat een systeem van gerichte controlemaatregelen „vanuit het oogpunt van de nationale veiligheid en de opsporing van daders van strafbare feiten veel minder doeltreffend zou zijn dan een systematische bewaring. Het zou immers achteraf geen enkele toegang bieden tot uitwisselingen die hebben plaatsgevonden vóórdat de autoriteit een bedreiging of strafbaar feit vaststelde: de werking ervan zou derhalve afhangen van het vermogen van de autoriteiten om te anticiperen op de identiteit van personen wier verbindingsgegevens van nut zouden kunnen zijn, hetgeen niet mogelijk is in het kader van het opsporingsonderzoek. In het geval van een ernstig misdrijf, bijvoorbeeld, zouden de opsporingsdiensten geen toegang kunnen krijgen tot eerdere communicaties, die echter voor de vaststelling van de identiteit van de dader en zijn medeplichtigen waardevol en soms zelfs onontbeerlijk zijn, zoals een aantal recente terroristische aanslagen heeft aangetoond. Op het gebied van de voorkoming van inbreuken op de nationale veiligheid kunnen met de nieuwe technische programma's slechts zwakke signalen worden opgespoord, hetgeen onverenigbaar is met het idee van pre-targeting van gevaarlijke personen”.

55 — Commission Staff Working Document, bijlage bij het richtlijnvoorstel dat heeft geleid tot de vaststelling van richtlijn 2006/24, SEC(2005) 1131, 21 september 2005, nr. 1.2, „The importance of traffic data for law enforcement”.

56 — Zie met name arresten van 22 januari 2013, Sky Österreich (C-283/11, EU:C:2013:28, punten 54-57); 13 november 2014, Reindl (C-443/13, EU:C:2014:2370, punt 39), en 16 juli 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punten 120-122). Zie binnen de doctrine met name Pirkker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, blz. 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”.

186. Het redelijkheidsvereiste komt neer op een toetsing van de „absolute” doeltreffendheid – los van iedere andere denkbare maatregel – van een algemene verplichting tot bewaring van gegevens voor de bestrijding van ernstige criminaliteit. Het noodzakelijkheidsvereiste vergt daarentegen een beoordeling van de doelmatigheid – of „relatieve” doeltreffendheid, dat wil zeggen in vergelijking met andere denkbare maatregelen – van een dergelijke verplichting.⁵⁷

187. In de context van de onderhavige zaken verplicht de noodzakelijkheidstoets ertoe enerzijds na te gaan of andere maatregelen even doeltreffend kunnen zijn als een algemene verplichting tot bewaring van gegevens voor de bestrijding van ernstige criminaliteit, en anderzijds of die eventuele maatregelen minder inbreuk maken op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten.⁵⁸

188. Ik herinner voorts aan de in punt 52 van het arrest DRI weergegeven vaste rechtspraak van het Hof, volgens welke de bescherming van het grondrecht op eerbiediging van het privéleven vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het „strikt noodzakelijke” blijven.⁵⁹

189. Over twee vraagstukken die betrekking hebben op het vereiste van strikte noodzakelijkheid in de context van de onderhavige zaken is uitgebreid gediscussieerd door de partijen die opmerkingen hebben ingediend bij het Hof. Die vraagstukken komen in wezen overeen met de twee door de verwijzende rechter in zaak C-203/15 gestelde vragen:

- enerzijds, moet een algemene verplichting tot bewaring van gegevens in het licht van de punten 56 tot en met 59 van het arrest DRI worden geacht op zichzelf de grenzen te overschrijden van het strikt noodzakelijke voor de bestrijding van ernstige criminaliteit, los van de eventuele waarborgen waarmee die verplichting gepaard gaat?
- anderzijds, gesteld dat een dergelijke verplichting niet kan worden geacht op zichzelf de grenzen te overschrijden van het strikt noodzakelijke, moet zij dan gepaard gaan met alle waarborgen die het Hof heeft genoemd in de punten 60 tot en met 68 van het arrest DRI, teneinde de inbreuk op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten tot het strikt noodzakelijke te beperken?

190. Alvorens op deze vragen in te gaan wil ik het door de regering van het Verenigd Koninkrijk naar voren gebrachte argument afwijzen dat de in het arrest DRI geformuleerde criteria in de context van de onderhavige zaken niet relevant zijn omdat dat arrest geen betrekking had op een nationale regeling maar op een door de Uniewetgever vastgestelde regeling.

191. In dit verband wijs ik erop dat het arrest DRI uitlegging heeft gegeven aan de artikelen 7, 8 en 52, lid 1, van het Handvest en dat die bepalingen tevens het voorwerp vormen van de in de hoofdedingen gestelde vragen. Het is mijns inziens niet mogelijk om de bepalingen van het Handvest verschillend uit te leggen naargelang de betrokken regeling is vastgesteld op Unieniveau of op nationaal niveau, zoals Brice, Lewis en de Law Society of England and Wales terecht hebben opgemerkt. Wanneer is vastgesteld dat het Handvest van toepassing is, zoals in de onderhavige zaken het geval is⁶⁰, moet het

57 — Zie Rivers, J., „Proportionality and variable intensity of review”, 65(1) *Cambridge Law Journal* (2006) 174, blz. 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 realization of some other constitutional interest.”

58 — Zie over deze twee componenten van de noodzakelijkheidstoets Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, blz. 323–331.

59 — Zie met name arresten van 9 november 2010, Volker und Markus Schecke en Eifert (C-92/09 en C-93/09, EU:C:2010:662, punten 77 en 86), en 7 november 2013, IPI (C-473/12, EU:C:2013:715, punt 39).

60 — Zie de punten 117-125 van deze conclusie.

op dezelfde wijze worden toegepast, ongeacht de betrokken regeling. De door het Hof in het arrest DRI geformuleerde criteria zijn derhalve relevant voor de beoordeling van de in de hoofdgedingen betrokken nationale regelingen, zoals met name is aangevoerd door de Deense en de Ierse regering en door de Commissie.

a) Strikte noodzakelijkheid van een algemene verplichting tot bewaring van gegevens

192. Volgens een eerste benadering, verdedigd door Tele2 Sverige en door Open Rights Group en Privacy International, moet een algemene verplichting tot bewaring van gegevens na het arrest DRI worden geacht op zichzelf de grenzen te overschrijden van het strikt noodzakelijke voor de bestrijding van ernstige criminaliteit, los van de eventuele waarborgen waarmee die verplichting gepaard gaat.

193. Volgens een tweede benadering, ondersteund door de meerderheid van de andere partijen die opmerkingen hebben ingediend bij het Hof, overschrijdt een dergelijke verplichting niet de grenzen van het strikt noodzakelijke, mits zij gepaard gaat met bepaalde waarborgen inzake de toegang tot de gegevens, de bewaringstermijn, en de bescherming en beveiliging van de gegevens.

194. Ik kies voor de tweede benadering om de volgende redenen.

195. In de eerste plaats heeft het Hof in mijn lezing van het arrest DRI uitgemaakt dat een algemene verplichting tot bewaring van gegevens de grenzen van het strikt noodzakelijke overschrijdt wanneer zij *niet gepaard gaat* met strikte waarborgen inzake de toegang tot de gegevens, de bewaringstermijn, en de bescherming en beveiliging van de gegevens. Daarentegen heeft het Hof zich niet uitgesproken over de verenigbaarheid met het Unierecht van een algemene verplichting tot bewaring van gegevens die *wel gepaard gaat* met dergelijke waarborgen, aangezien de in die zaak aan het Hof gestelde vragen niet een dergelijke regeling betroffen.

196. Ik merk in dit verband op dat de punten 56 tot en met 59 van het arrest DRI geen enkele verklaring van het Hof bevatten in de zin dat een algemene verplichting tot bewaring van gegevens op zichzelf de grenzen zou overschrijden van het strikt noodzakelijke.

197. In de punten 56 en 57 van dat arrest stelt het Hof vast dat de in richtlijn 2006/24 opgenomen bewaringsverplichting van toepassing is op alle elektronische communicatiemiddelen, alle gebruikers en alle verkeersgegevens, zonder hier enige differentiatie, beperking of uitzondering op basis van het nagestreefde doel, de bestrijding van ernstige criminaliteit, aan toe te voegen.

198. In de punten 58 en 59 van dat arrest zet het Hof gedetailleerder uiteen wat de praktische gevolgen zijn van dit ontbreken van differentiatie. Enerzijds betrof die bewaringsverplichting zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of in de verte – verband kan houden met ernstige criminaliteit. Anderzijds vereiste die richtlijn geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkte met name de bewaring niet tot gegevens betrekking hebbend op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit.

199. Daarmee stelde het Hof vast dat een algemene verplichting tot bewaring van gegevens wordt gekenmerkt door het ontbreken van differentiatie op basis van het nagestreefde doel, de bestrijding van ernstige criminaliteit. Het oordeelde evenwel niet dat dit ontbreken van differentiatie betekent dat een dergelijke verplichting op zichzelf de grenzen van het strikt noodzakelijke overschrijdt.

200. In feite oordeelde het Hof pas na het onderzoek van de regeling van richtlijn 2006/24 en na te hebben vastgesteld dat bepaalde waarborgen, die ik hierna zal onderzoeken⁶¹, ontbraken, in punt 69 van het arrest DRI:

„Gelet op een en ander moet worden geoordeeld dat de wetgever van de Unie met de vaststelling van richtlijn 2006/24 de door het evenredigheidsbeginsel gestelde *grenzen heeft overschreden* die hij in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest in acht dient te nemen” (cursivering van mij).

201. Zoals de Duitse en de Nederlandse regering hebben aangevoerd, indien de algemene gegevensbewaring als zodanig reeds voldoende was geweest voor de ongeldigheid van richtlijn 2006/24, zou het Hof het ontbreken van de in de punten 60 tot en met 68 van dat arrest genoemde waarborgen niet gedetailleerd hebben hoeven onderzoeken.

202. De algemene verplichting tot bewaring van gegevens van richtlijn 2006/24 overschreed derhalve op zichzelf niet de grenzen van het strikt noodzakelijke. Die richtlijn overschreed de grenzen van het strikt noodzakelijke vanwege het *gecombineerde gevolg* van de algemene gegevensbewaring en de afwezigheid van waarborgen om de inbreuk op de in de artikelen 7 en 8 van het Handvest erkende rechten te beperken tot het strikt noodzakelijke. Door dit gecombineerde gevolg moest de richtlijn in haar geheel ongeldig worden verklaard.⁶²

203. In de tweede plaats vind ik steun voor deze uitlegging in punt 93 van het arrest Schrems⁶³, dat ik hier weergeef:

„Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, *zonder dat* enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en *zonder dat* wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens [zie in die zin aangaande richtlijn 2006/24, arrest DRI, punten 57-61]” (cursivering van mij).

204. Het Hof oordeelde opnieuw niet dat de in die zaak betrokken regeling de grenzen van het strikt noodzakelijke overschreed enkel omdat zij een algemene bewaring van persoonsgegevens toestond. In die zaak werden de grenzen van het strikt noodzakelijke overschreden vanwege het gecombineerde gevolg van de mogelijkheid van een dergelijke algemene gegevensbewaring en het ontbreken van waarborgen omtrent de toegang, bedoeld om de inmenging te beperken tot het strikt noodzakelijke.

205. Uit het voorgaande leid ik af dat een algemene verplichting tot bewaring van gegevens niet altijd moet worden geacht op zichzelf de grenzen van het strikt noodzakelijke voor de bestrijding van ernstige criminaliteit te overschrijden. Daarentegen overschrijdt een dergelijke verplichting altijd de grenzen van het strikt noodzakelijke wanneer zij niet gepaard gaat met waarborgen inzake de toegang tot de gegevens, de bewaringstermijn, en de bescherming en beveiliging van de gegevens.

206. In de derde plaats zie ik mijn visie in dit verband gestaafd door de noodzaak om concreet te onderzoeken of het vereiste van strikte noodzakelijkheid in acht is genomen in de context van de in de hoofdgedingen betrokken nationale regelingen.

61 — Zie de punten 216-245 van deze conclusie.

62 — Zie arrest DRI, punt 65: „Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, *zonder dat* deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke” (cursivering van mij).

63 — Arrest van 6 oktober 2015, Schrems (C-362/14, EU:C:2015:650).

207. Zoals ik heb uiteengezet in punt 187 van deze conclusie, verlangt het vereiste van strikte noodzakelijkheid dat wordt onderzocht of andere maatregelen even doeltreffend kunnen zijn voor de bestrijding van ernstige criminaliteit als een algemene verplichting tot bewaring van gegevens, maar minder inbreuk maken op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten.

208. Deze beoordeling moet plaatsvinden binnen de specifieke context van elke nationale regeling die in een algemene verplichting tot bewaring van gegevens voorziet. Enerzijds verlangt die beoordeling dat de doeltreffendheid van die verplichting wordt vergeleken met elke andere in de nationale context denkbare maatregel, rekening houdend met het feit dat die verplichting de bevoegde autoriteiten een beperkt vermogen verleent om via de bewaarde gegevens het verleden te lezen.⁶⁴

209. Gelet op het vereiste van strikte noodzakelijkheid is het van het grootste belang dat de rechters niet slechts het nut onderzoeken van een algemene verplichting tot bewaring van gegevens, maar nauwkeurig nagaan of geen enkele andere maatregel of combinatie van maatregelen, en met name een met andere onderzoeksinstrumenten gepaard gaande gerichte verplichting tot bewaring van gegevens, even doeltreffend kan zijn voor de bestrijding van ernstige criminaliteit. Ik merk in dit verband op dat een aantal onder de aandacht van het Hof gebrachte studies de noodzakelijkheid van dit type verplichting voor de bestrijding van ernstige criminaliteit ter discussie stellen.⁶⁵

210. Anderzijds, gesteld dat andere maatregelen even doeltreffend kunnen zijn voor de bestrijding van ernstige misdrijven, dan moeten de verwijzende rechters nog vaststellen of die maatregelen minder inbreuk maken op de betrokken grondrechten dan een algemene verplichting tot bewaring van gegevens, gelet op de in punt 185 van deze conclusie weergegeven vaste rechtspraak.

211. In het licht van punt 59 van het arrest DRI staat het aan de nationale rechters om met name na te gaan of het mogelijk is de materiële omvang van de bewaringsverplichting te beperken met behoud van de doeltreffendheid van deze maatregel voor de bestrijding van ernstige criminaliteit.⁶⁶ De materiële omvang van dergelijke verplichtingen kan immers variëren naargelang van de gebruikers, de geografische zones en de communicatiemiddelen die zij betreffen.⁶⁷

212. In mijn ogen zou het met name wenselijk zijn, indien de technologie dit toelaat, om van de bewaringsverplichting gegevens uit te sluiten die in het licht van de in de onderhavige zaken betrokken grondrechten bijzonder gevoelig zijn, zoals gegevens die onder het beroepsgeheim vallen of gegevens waarmee journalistieke bronnen van journalisten kunnen worden achterhaald.

213. Men moet evenwel in gedachten houden dat een vergaande beperking van de omvang van een algemene verplichting tot bewaring van gegevens het nut van een dergelijke regeling voor de bestrijding van ernstige criminaliteit aanzienlijk kan verminderen. Enerzijds heeft een aantal regeringen aangegeven dat het moeilijk, zo niet onmogelijk, is vooraf te bepalen welke gegevens verband zouden kunnen houden met een ernstig strafbaar feit. Bijgevolg kan een dergelijke beperking de bewaring uitsluiten van gegevens die relevant zouden kunnen blijken voor de bestrijding van ernstige criminaliteit.

64 — Zie de punten 178-183 van deze conclusie.

65 — Zie Commissaris voor de Rechten van de Mens van de Raad van Europa, „Issue paper on the rule of law on the Internet and in the wider digital world”, december 2014, CommDH/IssuePaper(2014)1, blz. 115; United Nations Human Rights Counsel, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 30 juni 2014, A/HRC/27/37, nr. 26; United Nations General Assembly, Report of the Special Rapporteur on promotion and protection of human rights while countering terrorism, 23 september 2014, A/69/397, nrs. 18 en 19.

66 — Deze opmerking betreft uitsluitend algemene verplichtingen tot bewaring van gegevens (die eenieder kunnen aangaan los van elke betrokkenheid bij een ernstig strafbaar feit) en niet-gerichte controlemaatregelen (die personen betreffen van wie vooraf is vastgesteld dat zij betrokken zijn bij een ernstig strafbaar feit): zie voor dit onderscheid de punten 178-183 van deze conclusie.

67 — De Duitse regering heeft op de pleitzitting met name aangegeven dat het Duitse parlement e-mailberichten heeft uitgesloten van de door de Duitse wetgeving opgelegde bewaringsverplichting, maar dat die regeling geldt voor alle gebruikers op het gehele nationale grondgebied.

214. Anderzijds is, zoals de Estse regering heeft aangevoerd, ernstige criminaliteit een dynamisch fenomeen dat zich kan aanpassen aan de onderzoeksinstrumenten waarover de handhavingsautoriteiten beschikken. Een beperking tot een geografische zone of een bepaald communicatiemiddel kan derhalve een verplaatsing uitlokken van met ernstige criminaliteit verband houdende activiteiten naar een geografische zone en/of communicatiemiddelen die niet worden bestreken door die regeling.

215. Aangezien zij een ingewikkeld onderzoek van de in de hoofdgedingen betrokken nationale regelingen vergt, ben ik van mening dat die beoordeling moet worden overgelaten aan de nationale rechters, zoals de Tsjechische, de Estse, de Ierse, de Franse en de Nederlandse regering alsook de Commissie hebben opgemerkt.

b) Dwingend karakter van de door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen in het licht van het vereiste van strikte noodzakelijkheid

216. Gesteld dat een algemene verplichting tot bewaring van gegevens kan worden geacht strikt noodzakelijk te zijn in de context van de betrokken nationale regeling, hetgeen door de nationale rechter moet worden beoordeeld, dan moet nog worden vastgesteld of een dergelijke verplichting gepaard moet gaan met alle door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen, teneinde de inbreuk op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten tot het strikt noodzakelijke te beperken.

217. Die waarborgen betreffen de regels voor de toegang tot en het gebruik van bewaarde gegevens door de bevoegde autoriteiten (punten 60-62 van arrest DRI), de bewaringstermijn (punten 63 en 64 van dat arrest) en de beveiliging en bescherming van door aanbieders opgeslagen gegevens (punten 66-68 van dat arrest).

218. In de bij het Hof ingediende opmerkingen staan twee theorieën over de aard van die waarborgen tegenover elkaar.

219. Volgens de eerste theorie, verdedigd door Watson, Brice en Lewis en door Open Rights Group en Privacy International, zijn de door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen dwingend. Volgens deze theorie heeft het Hof minimumwaarborgen geformuleerd die *alle* moeten worden vervuld door de betrokken nationale regeling teneinde de inbreuk op de grondrechten te beperken tot het strikt noodzakelijke.

220. Volgens de tweede theorie, die wordt gesteund door de Duitse, de Estse, de Ierse en de Franse regering en de regering van het Verenigd Koninkrijk, zijn de door het Hof in de punten 60 tot en met 68 van het arrest DRI vermelde waarborgen slechts indicatief. Het Hof zou de in de regeling van richtlijn 2006/24 ontbrekende waarborgen „globaal hebben beoordeeld”, zonder dat één van die waarborgen afzonderlijk kan worden geacht dwingend te zijn met het oog op het vereiste van strikte noodzakelijkheid. De Duitse regering heeft deze theorie geïllustreerd aan de hand van het beeld van „communicerende vaten” waarbij een soepelere benadering van een van de drie door het Hof onderscheiden aspecten (bijvoorbeeld de toegang tot bewaarde gegevens) kan worden gecompenseerd door een striktere benadering van de twee andere aspecten (de bewaringstermijn en de beveiliging en bescherming van de gegevens).

221. Ik ben om de volgende redenen van mening dat deze „communicerende vaten”-theorie moet worden afgewezen en dat *alle* door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen dwingend zijn.

222. In de eerste plaats leent het woordgebruik van het Hof bij zijn onderzoek van de strikte noodzakelijkheid van de regeling van richtlijn 2006/24 zich niet voor een dergelijke uitlegging. In het bijzonder zinspeelt het Hof nergens in de punten 60 tot en met 68 van dat arrest op de een of andere mogelijkheid om een soepelere benadering van een van de drie door het Hof onderscheiden aspecten te „compenseren” door een striktere benadering van de twee andere aspecten.

223. De „communicerende vaten”-theorie lijkt mij in feite verwarring te scheppen tussen het noodzakelijkheidsvereiste en het evenredigheidsvereiste *stricto sensu*, dat niet door het Hof is onderzocht in het arrest DRI. Zoals ik heb aangegeven in punt 186 van deze conclusie bestaat het noodzakelijkheidsvereiste immers in de verwerping van iedere niet-doelmatige maatregel. Er kan in die context geen sprake zijn van „globale beoordeling”, „compensatie” of „in evenwicht brengen”, methoden die pas aan de orde komen in het stadium van de evenredigheid *stricto sensu*.⁶⁸

224. In de tweede plaats ondermijnt deze „communicerende vaten”-theorie het nuttig effect van de door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen, zodat personen wier gegevens zijn bewaard niet meer over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens, zoals punt 54 van dit arrest eist.

225. De verderfelijke gevolgen van deze theorie kunnen eenvoudig worden geïllustreerd aan de hand van de volgende voorbeelden. Een nationale regeling die de toegang strikt beperkt tot de doelstelling van terrorismebestrijding en de bewaringstermijn tot drie maanden (strikte benadering van toegang en bewaringstermijn), maar de aanbieders niet verplicht de gegevens op het nationale grondgebied en in versleutelde vorm te bewaren (soepele benadering van de beveiliging), stelt de gehele bevolking bloot aan een hoog risico van onrechtmatige toegang tot de bewaarde gegevens. Evenzo stelt een nationale regeling die voorziet in een bewaringstermijn van drie maanden en een versleutelde bewaring van gegevens op het nationale grondgebied (strikte benadering van termijn en beveiliging), maar die alle ambtenaren toegang biedt tot de bewaarde gegevens (soepele benadering van de toegang) de gehele bevolking bloot aan een hoog risico van misbruik door nationale autoriteiten.

226. In mijn ogen volgt uit deze voorbeelden dat het behoud van het nuttig effect van de door het Hof in de punten 60 tot en met 68 van het arrest DRI vermelde waarborgen vereist dat *elk* van die waarborgen dwingend wordt geacht. Het EHRM heeft het fundamentele belang van deze waarborgen eveneens benadrukt in het recente arrest Szabó en Vissy/Hongarije, met uitdrukkelijke verwijzing naar het arrest DRI.⁶⁹

227. In de derde plaats levert de toepassing van deze waarborgen door lidstaten die een algemene verplichting tot bewaring van gegevens wensen op te leggen, mijns inziens geen grote praktische problemen op. In feite lijken deze waarborgen mij in veel opzichten „minimaal”, zoals Watson heeft betoogd.

228. Over een aantal van die waarborgen is voor het Hof gediscussieerd, omdat zij zouden ontbreken in de in de hoofdgedingen betrokken nationale regelingen.

68 — Zie Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, blz. 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*” (cursivering van mij).

69 — EHRM, 12 januari 2016, Szabó en Vissy/Hongarije, 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, emphasizing the importance of adequate legislation of sufficient safeguards in the face of the authorities’ enhanced technical possibilities to intercept private information.”

229. In de eerste plaats volgt uit de punten 61 en 62 van het arrest DRI dat de toegang tot en het latere gebruik van de bewaarde gegevens strikt gebonden moeten zijn aan het doel, nauwkeurig afgebakende ernstige criminaliteit voorkomen, opsporen of strafrechtelijk vervolgen.

230. Volgens Tele2 Sverige en de Commissie is dat vereiste niet in acht genomen in de in zaak C-203/15 betrokken Zweedse regeling, die toegang tot bewaarde gegevens zou toestaan in het kader van de bestrijding van lichte criminaliteit. Een vergelijkbare kritiek is geuit door Brice en Lewis en door Watson op de in zaak C-698/15 betrokken regeling van het Verenigd Koninkrijk, die toegang zou toestaan ten behoeve van de bestrijding van lichte criminaliteit en zelfs bij het ontbreken van elk strafbaar feit.

231. Ofschoon het niet aan het Hof staat om zich uit te spreken over de inhoud van die nationale regelingen, moet het wel de doelstellingen van algemeen belang aan te geven die een ernstige inmenging in de door de richtlijn en de artikelen 7 en 8 van het Handvest erkende rechten kunnen rechtvaardigen. Ik heb in het voorgaande reeds de redenen uiteengezet waarom ik van mening ben dat *alleen* de bestrijding van ernstige criminaliteit een dergelijke inmenging kan rechtvaardigen.⁷⁰

232. In de tweede plaats moet, volgens punt 62 van het arrest DRI, de toegang tot bewaarde gegevens vooraf worden getoetst door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt de toegang tot de gegevens en het gebruik ervan te beperken tot het strikt noodzakelijke voor de verwezenlijking van het nagestreefde doel. Die voorafgaande toetsing moet bovendien plaatsvinden naar aanleiding van een gemotiveerd verzoek van de autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten.

233. Volgens de opmerkingen van Tele2 Sverige en van de Commissie ontbreekt deze waarborg van onafhankelijke en voorafgaande toetsing gedeeltelijk in de in zaak C-203/15 betrokken Zweedse regeling. Hetzelfde geldt, volgens Brice en Lewis, Watson, en Open Rights Group en Privacy International, voor de in zaak C-698/15 betrokken regeling van het Verenigd Koninkrijk, hetgeen de regering van het Verenigd Koninkrijk niet heeft betwist.

234. Ik zie geen enkele reden tot versoepeling van dit vereiste van voorafgaande toetsing door een onafhankelijke instantie, dat ontegenzegglijk voortvloeit uit het woordgebruik van het Hof in punt 62 van het arrest DRI.⁷¹ Allereerst wordt dit vereiste ingegeven door de ernst van de inbreuk en de risico's die worden veroorzaakt door het aanleggen van databestanden die nagenoeg de gehele bevolking bestrijken.⁷² Ik merk op dat een aantal deskundigen op het gebied van de bescherming van mensenrechten bij de bestrijding van terrorisme kritiek hebben geuit op de huidige trend om traditionele procedures van onafhankelijke toestemming en daadwerkelijk toezicht te vervangen door procedures waarbij inlichtingen- en politiediensten „zichzelf machtigen” om gegevens te raadplegen.⁷³

70 — Zie de punten 170-173 van deze conclusie.

71 — Ik preciseer niettemin dat dit vereiste van voorafgaande en onafhankelijke toetsing mijns inziens niet kan worden gebaseerd op artikel 8, lid 3, van het Handvest, aangezien het Handvest als zodanig niet van toepassing is op nationale bepalingen die de toegang tot bewaarde gegevens regelen: zie de punten 123-125 van deze conclusie.

72 — Zie de punten 252-261 van deze conclusie.

73 — United Nations Council, Report of the Special Rapporteur on promotion and protection of human rights while countering terrorism, 28 december 2009, A/HRC/13/37, nr. 62: „Er mag geen enkel geheim controlesysteem bestaan dat niet onder supervisie staat van een instantie die doeltreffend toezicht uitoefent, noch enige inmenging waarvoor geen toestemming is verleend door een onafhankelijk orgaan” (zie ook nr. 51). Zie eveneens United Nations General Assembly, Report of the Special Rapporteur on promotion and protection of human rights while countering terrorism, 23 september 2014, A/69/397, nr. 61.

235. Vervolgens is een onafhankelijke en voorafgaande toetsing van de toegang tot gegevens noodzakelijk met het oog op een behandeling van geval tot geval van de in het licht van de grondrechten uiterst gevoelige gegevens waarvan in de onderhavige zaken sprake is, zoals gegevens die onder het beroepsgeheim vallen en gegevens waarmee bronnen van journalisten kunnen worden achterhaald, zoals de Law Society of England and Wales en de Franse en de Duitse regering hebben opgemerkt. Die aan de toegang voorafgaande toetsing is des te noodzakelijker in situaties waarin het technisch moeilijk is om al deze gegevens uit te sluiten in het stadium van de bewaring.⁷⁴

236. Tot slot voeg ik hieraan toe dat, praktisch gezien, geen van de drie bij een toegangsverzoek betrokken partijen in staat is de toegang tot de bewaarde gegevens daadwerkelijk te toetsen. De bevoegde handhavingsautoriteiten hebben alle belang bij een verzoek om een zo ruim mogelijk toegang. De aanbieders, die geen inzage hebben in het onderzoeksdossier, kunnen niet nagaan of het toegangsverzoek is beperkt tot het strikt noodzakelijke. De personen wier gegevens worden geraadpleegd, kunnen op geen enkele wijze weten of zij het voorwerp vormen van een dergelijke onderzoeksmaatregel, zelfs niet wanneer er sprake is van misbruik of onrechtmatig gebruik, zoals Watson en Brice en Lewis hebben opgemerkt. Deze configuratie van meespelende belangen vereist in mijn ogen de tussenkomst van een onafhankelijke instantie voorafgaand aan de raadpleging van de bewaarde gegevens, teneinde de personen wier gegevens worden bewaard te beschermen tegen ongerechtvaardigde toegang door de bevoegde autoriteiten.

237. Dat gezegd hebbende lijkt het mij redelijk om aan te nemen dat concrete situaties van extreme spoed, ter sprake gebracht door de regering van het Verenigd Koninkrijk, een onmiddellijke toegang tot bewaarde gegevens door handhavingsautoriteiten kunnen rechtvaardigen, zonder voorafgaande toetsing, teneinde ernstige strafbare feiten te voorkomen of de daders van dergelijke strafbare feiten te vervolgen.⁷⁵ Zo enigszins mogelijk moet worden vastgehouden aan het vereiste van voorafgaande toestemming en moet bij de onafhankelijke autoriteit worden voorzien in een spoedprocedure voor de behandeling van dit type toegangsverzoeken. Indien echter de indiening van een toegangsverzoek bij die instantie onverenigbaar lijkt met de extreme urgentie van de situatie, moeten de toegang tot en het gebruik van de gegevens a posteriori worden getoetst door die instantie, en wel zo spoedig mogelijk.

238. In de derde plaats verplicht punt 68 van het arrest DRI de aanbieders de gegevens te bewaren op het grondgebied van de Unie, teneinde te waarborgen dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de punten 66 en 67 van dat arrest genoemde vereisten inzake bescherming en beveiliging, zoals wordt voorgeschreven door artikel 8, lid 3, van het Handvest

239. Tele2 Sverige en de Commissie hebben aangevoerd dat de bewaring van gegevens op het nationale grondgebied niet is gewaarborgd in de in zaak C-203/15 betrokken Zweedse regeling. Dezelfde kritiek is naar voren gebracht door Brice en Lewis en door Watson met betrekking tot de in zaak C-698/15 betrokken regeling van het Verenigd Koninkrijk.

240. Ik zie in dit verband, enerzijds, geen enkele reden om dit in punt 68 van het arrest DRI neergelegde vereiste af te zwakken, aangezien bewaring van gegevens buiten het grondgebied van de Unie de personen wier gegevens zijn bewaard niet het in richtlijn 2002/58 en in de artikelen 7, 8 en 52, lid 1, van het Handvest geboden beschermingsniveau kan garanderen.⁷⁶

74 — Zie punt 212 van deze conclusie. Met betrekking tot bronnen van journalisten heeft het EHRM gewezen op de noodzaak van voorafgaande toestemming door een onafhankelijke instantie, aangezien een toetsing a posteriori de vertrouwelijkheid van dergelijke bronnen niet kan herstellen: zie EHRM, 22 november 2012, Telegraaf Media Nederland Landelijke Media B.V. e.a./Nederland, CE:ECHR:2012:1122JUD003931506, § 101 en EHRM, 12 januari 2016, Szabó en Vissy/Hongarije, CE:ECHR:2016:0112JUD003713814, § 77. In het arrest Kopp/Zwitserland, dat betrekking had op het af luisteren van telefoonlijnen van een advocaat, bekritiseerde het EHRM het feit dat een overheidsambtenaar was belast met het filteren van informatie die onder het beroepsgeheim viel, zonder dat er sprake was van toetsing door een onafhankelijke rechter: zie EHRM, 25 maart 1998, Kopp/Zwitserland, CE:ECHR:1998:0325JUD002322494, § 74.

75 — Zie in dit verband de in punt 22 van deze conclusie beschreven procedure. Ik wijs erop dat het Hof deze problematiek niet heeft behandeld in het arrest DRI.

76 — Zie in dit verband arrest van 6 oktober 2015, Schrems (C-362/14, EU:C:2015:650).

241. Het lijkt mij, anderzijds, redelijk om dit door het Hof in de context van richtlijn 2006/24 uitgedrukte vereiste af te stemmen op de context van de nationale regelingen en voor te schrijven dat de bewaring van gegevens dient plaats te vinden op het nationale grondgebied, zoals de Duitse en de Franse regering en de Commissie hebben aangevoerd. Ingevolge artikel 8, lid 3, van het Handvest dienen de lidstaten immers te garanderen dat een onafhankelijke autoriteit erop toeziet dat de aanbieders de in de nationale regeling opgenomen vereisten van bescherming en beveiliging naleven. Bij gebreke van coördinatie op Unieniveau kan het voor een dergelijke nationale autoriteit onmogelijk zijn haar toezichthoudende taken uit te oefenen op het grondgebied van een andere lidstaat.

242. In de vierde plaats moeten de verwijzende rechters ten aanzien van de bewaringstermijn de door het Hof in de punten 63 en 64 van het arrest DRI geformuleerde criteria toepassen. Zij moeten bepalen of de bewaarde gegevens kunnen worden onderscheiden naargelang van hun nut en, in voorkomend geval, of de bewaringstermijn is aangepast op basis van dat criterium. Verder moeten zij nagaan of de bewaringstermijn is gegrond op objectieve criteria die kunnen waarborgen dat die termijn is beperkt tot het strikt noodzakelijke.

243. Ik merk op dat het EHRM in het recente arrest Roman Zakharov/Rusland een bewaringstermijn van ten hoogste zes maanden redelijk heeft geoordeeld, maar wel betreurde dat een verplichting om gegevens die geen verband vertonen met het doel waarvoor zij zijn verzameld onverwijld te vernietigen ontbrak.⁷⁷ Ik voeg daar in dit verband aan toe dat de in de hoofdgedingen betrokken nationale regelingen moeten voorzien in een verplichting om alle bewaarde gegevens onherstelbaar te vernietigen zodra zij niet meer strikt noodzakelijk zijn voor de bestrijding van ernstige criminaliteit. Deze verplichting moet niet alleen in acht worden genomen door de aanbieders die de gegevens bewaren, maar ook door de autoriteiten die toegang hebben gehad tot bewaarde gegevens.

244. Gelet op het voorgaande ben ik van mening dat alle door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde waarborgen een dwingend karakter hebben en bijgevolg samen moeten gaan met een algemene verplichting tot bewaring van gegevens, teneinde de inbreuk op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten te beperken tot het strikt noodzakelijke.

245. Het staat aan de verwijzende rechters om na te gaan of al die waarborgen zijn opgenomen in elk van de in de hoofdgedingen betrokken nationale regelingen.

6. Evenredigheid, in een democratische samenleving, van een algemene verplichting tot bewaring van gegevens in het licht van de doelstelling van bestrijding van ernstige criminaliteit

246. Na beoordeling van de noodzakelijkheid van de in de hoofdgedingen betrokken nationale regelingen dienen de verwijzende rechters nog te toetsen of deze in een democratische samenleving evenredig zijn in het licht van de doelstelling van bestrijding van ernstige criminaliteit. Dit aspect is niet door het Hof onderzocht in het arrest DRI, aangezien de regeling van richtlijn 2006/24 de grenzen van het strikt noodzakelijke voor de bestrijding van ernstige criminaliteit overschreed.

⁷⁷ — Zie in dit verband EHRM, 4 december 2015, Roman Zakharov/Rusland, CE:ECHR:2015:1204JUD004714306, §§ 254 en 255. Volgens het Russische recht moesten onderschepte gegevens worden vernietigd na een bewaringstermijn van zes maanden indien de betrokken persoon niet was beschuldigd van een strafbaar feit. Het EHRM oordeelde dat de maximale bewaringstermijn van zes maanden die in het Russische recht voor dergelijke gegevens gold redelijk was. Het betreurde echter het ontbreken van een verplichting om gegevens die geen enkel verband vertonen met het doel waarvoor zij zijn verzameld onverwijld te vernietigen en preciseerde dat de automatische bewaring, gedurende zes maanden, van gegevens die kennelijk zonder enig belang waren, niet gerechtvaardigd kon worden geacht in het licht van artikel 8 EVRM.

247. Dit vereiste van evenredigheid in een democratische samenleving – of evenredigheid „*stricto sensu*” – vloeit voort uit artikel 15, lid 1, van richtlijn 2002/58, uit artikel 52, lid 1, van het Handvest en uit vaste rechtspraak. Volgens die vaste rechtspraak kan een maatregel die inbreuk maakt op grondrechten slechts worden geacht evenredig te zijn indien de veroorzaakte nadelen niet onevenredig zijn aan het nagestreefde doel.⁷⁸

248. Anders dan de vereisten van redelijkheid en noodzakelijkheid van de betrokken maatregel, die een waardering van de doeltreffendheid ten opzichte van het nagestreefde doel omvatten, bestaat het evenredigheidsvereiste *stricto sensu* in het in evenwicht brengen van enerzijds de uit die maatregel voortvloeiende voordelen voor het nagestreefde legitieme doel, en anderzijds de eruit voortvloeiende nadelen voor de in een democratische samenleving erkende grondrechten.⁷⁹ Dit vereiste zet aldus een discussie in gang over de waarden die in een democratische samenleving moeten gelden, en uiteindelijk over het type samenleving waarin wij wensen te leven.⁸⁰

249. Bijgevolg, en zoals ik heb aangegeven in punt 223 van deze conclusie, dient de globale beoordeling van de betrokken regeling plaats te vinden in het stadium van het onderzoek van de evenredigheid in strikte zin, en niet in het stadium van het onderzoek van de noodzakelijkheid, zoals de voorstanders van de „communicerende vaten”-theorie hebben aangevoerd.⁸¹

250. Volgens de in punt 247 van deze conclusie weergegeven rechtspraak moet een evenwicht worden gevonden tussen de voor- en de nadelen, in een democratische samenleving, van een algemene verplichting tot bewaring van gegevens. Deze voor- en nadelen zijn nauw verbonden met het wezenlijke kenmerk van een dergelijke verplichting, waarvan zij als het ware de zon- en de schaduwzijde vertegenwoordigen, namelijk het feit dat die verplichting alle communicaties van alle gebruikers betreft zonder dat enige betrokkenheid bij een ernstig strafbaar feit is vereist.

251. Ik heb in de punten 178 tot en met 183 van deze conclusie reeds de voordelen uiteengezet die de bewaring van gegevens van alle op het nationale grondgebied gevoerde communicaties meebrengt voor de bestrijding van ernstige criminaliteit.

252. Anderzijds vloeien de nadelen van een algemene verplichting tot bewaring van gegevens voort uit het feit dat de overgrote meerderheid van de bewaarde gegevens personen betreft die nooit op enigerlei wijze betrokken zullen zijn bij een ernstig strafbaar feit. Het is in dit verband van belang te preciseren wat de aard is van de nadelen die deze personen ervan ondervinden. Die aard verschilt echter naargelang van de mate van inmenging in hun grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens.

78 — Zie met name arresten van 15 februari 2016, N. (C-601/15 PPU, EU:C:2016:84, punt 54; de noodzakelijkheid is onderzocht in de punten 56-67, de evenredigheid in de punten 68 en 69); 16 juli 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, punt 123; de noodzakelijkheid is onderzocht in de punten 120-122, de evenredigheid in de punten 123-127), en 22 januari 2013, Sky Österreich (C-283/11, EU:C:2013:28, punt 50; de noodzakelijkheid is onderzocht in de punten 54-57, de evenredigheid in de punten 58-67).

79 — Zie Rivers J., „Proportionality and variable intensity of review”, 65(1) *Cambridge Law Journal* (2006) 174, blz. 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 — Zie Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, blz. 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 — Het specifieke karakter van het evenredigheidsvereiste *stricto sensu* ten opzichte van de vereisten van redelijkheid en noodzakelijkheid kan worden geïllustreerd aan de hand van het volgende voorbeeld. Gesteld een lidstaat eist dat bij een ieder die op zijn grondgebied verblijft een geolocatietag wordt geïnjecteerd, die de autoriteiten in staat stelt om het komen en gaan van zijn drager gedurende het afgelopen jaar te achterhalen. Een dergelijke maatregel kan „noodzakelijk” worden geacht indien geen enkele andere maatregel met dezelfde mate van doeltreffendheid ernstige criminaliteit kan bestrijden. In mijn ogen is een dergelijke maatregel echter onevenredig in een democratische samenleving, omdat de eruit voortvloeiende inbreuk op de rechten op lichamelijke integriteit, eerbiediging van het privéleven en bescherming van persoonsgegevens onevenredig is aan de voordelen die eruit voortvloeien voor de bestrijding van ernstige criminaliteit.

253. In het kader van een „individuele” inmenging die één bepaalde persoon betreft, zijn de nadelen die voortvloeien uit een algemene verplichting tot bewaring van gegevens, zeer helder beschreven door advocaat–generaal Cruz Villalón in de punten 72 tot en met 74 van zijn conclusie in de zaak DRI.⁸² In zijn woorden kan de exploitatie van deze gegevens „een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart [...] brengen of zelfs een volledig en precies beeld [...] schetsen van zijn privé-identiteit”.

254. Met andere woorden, een algemene verplichting tot bewaring van gegevens kan, in een individuele context, net zulke ernstige inmengingen veroorzaken als gerichte controlemaatregelen, daaronder begrepen die welke de inhoud van de gevoerde communicaties onderscheppen.

255. Ofschoon de ernst van dergelijke individuele inmengingen niet kan worden onderschat, ben ik niettemin van mening dat de specifieke risico's die door een algemene verplichting tot bewaring van gegevens worden veroorzaakt aan het licht komen bij inmengingen „op grote schaal”.

256. Immers, anders dan gerichte controlemaatregelen kan een dergelijke verplichting inmengingen op grote schaal, dat wil zeggen inmengingen die een substantieel deel van of zelfs een gehele relevante bevolkingsgroep treffen, aanzienlijk bevorderen, zoals de volgende voorbeelden illustreren.

257. Stel, in de eerste plaats, dat een persoon die toegang heeft tot bewaarde gegevens van plan is binnen de bevolking van de lidstaat alle personen met een psychische stoornis te identificeren. De evaluatie van de inhoud van alle op het nationale grondgebied gevoerde communicaties zou een enorme inzet van middelen vergen. Daarentegen kunnen door de exploitatie van databestanden met communicatiegegevens onmiddellijk alle individuen worden geïdentificeerd die gedurende de bewaringstermijn contact hebben gehad met een psycholoog.⁸³ Ik voeg hieraan toe dat deze techniek kan worden uitgebreid tot elke in een lidstaat geregistreerde medisch specialisme.⁸⁴

258. Stel, in de tweede plaats, dat diezelfde persoon degenen wil identificeren die het niet eens zijn met het beleid van de zittende regering. De evaluatie die dat doel zou moeten worden verricht van de inhoud van communicaties zou wederom een enorme inzet van middelen vergen. Daarentegen kunnen door de exploitatie van communicatiegegevens alle personen worden geïdentificeerd die staan ingeschreven op verzendlijsten voor e-mailberichten waarin het regeringsbeleid wordt bekritiseerd. Die gegevens zouden het bovendien mogelijk maken personen te identificeren die deelnemen aan openbare antiregeringsmanifestaties.⁸⁵

82 — C-293/12 en C-594/12, EU:C:2013:845. Zie eveneens arrest DRI, punten 27 en 37.

83 — De bewaarde gegevens bevatten immers de bron en de ontvanger van een communicatie, gegevens die slechts hoeven te worden vergeleken met de lijst van telefoonnummers van op het nationale grondgebied werkzame psychologen.

84 — Zie in dit verband United Nations Council, Report of the Special Rapporteur on promotion and protection of human rights while countering terrorism, 28 december 2009, A/HRC/13/37, nr. 42: „[I]n Duitsland hebben studies een zorgwekkende consequentie van het gegevensbewaringsbeleid te zien gegeven: 52 % van de respondenten gaf aan dat het, als gevolg van de wetten inzake gegevensbewaring, onwaarschijnlijk was dat zij gebruik zouden maken van telecommunicatie om contact op te nemen met een toxicoloog, psychotherapeut of huwelijkstherapeut”.

85 — Aangezien de bewaarde gegevens ook de locaties van de bron en de ontvanger van een communicatie omvatten, kan eenieder die tijdens een manifestatie een communicatie initieert of ontvangt gemakkelijk worden geïdentificeerd dankzij de bewaarde gegevens. In dit verband beschrijft Marc Goodman, FBI- en Interpoldeskundige op het gebied van risico's die verband houden met nieuwe technologieën, dat in een recent verleden de Oekraïense regering tijdens een manifestatie van regeringstegenstanders alle mobiele telefoons heeft geïdentificeerd die zich bevonden in de buurt van straatrellen tussen politie en regeringstegenstanders. Al die telefoons ontvingen een bericht dat de auteur omschrijft als het meest „Orwelliaanse” dat ooit door een regering is verstuurd: „Geachte abonnee, u bent geregistreerd als deelnemer aan een ernstige verstoring van de openbare orde” (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, blz. 153, vrije vertaling). Zie eveneens United Nations Commission on Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 april 2013, A/HRC/23/40, nr. 75, en United Nations Human Rights Counsel, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 30 juni 2014, A/HRC/27/37, nr. 3.

259. Ik wijs erop dat de risico's die verband houden met de toegang tot communicatiegegevens (of „metagegevens”) gelijk aan of groter kunnen zijn dan die welke voortvloeien uit de toegang tot de inhoud van die communicaties, zoals is opgemerkt door Open Rights Group en Privacy International, de Law Society of England and Wales, alsook door de United Nations High Commissioner for Human Rights in een recent rapport.⁸⁶ In het bijzonder, en zoals de hiervoor weergegeven voorbeelden aantonen, kunnen op basis van „metagegevens” vrijwel onmiddellijk hele bevolkingsgroepen worden gecategoriseerd, hetgeen niet mogelijk is op basis van de inhoud van communicaties.

260. Ik voeg hieraan toe dat de risico's van ongerechtvaardigde of onrechtmatige toegang tot bewaarde gegevens zeker niet theoretisch zijn. Enerzijds moet het risico van ongerechtvaardigde toegang door bevoegde autoriteiten in verband worden gebracht met het extreem hoge aantal toegangsverzoeken dat is genoemd in de bij het Hof ingediende opmerkingen. In de context van de Zweedse regeling heeft Tele2 Sverige aangegeven ongeveer 10 000 toegangsverzoeken per maand te ontvangen, in welk cijfer niet zijn begrepen de verzoeken die worden ontvangen door andere aanbieders die op het Zweedse grondgebied actief zijn. Wat de regeling van het Verenigd Koninkrijk betreft, heeft Watson cijfers genoemd uit een officieel rapport dat melding maakt van 517 236 schriftelijke toestemmingen en 55 346 mondelinge toestemmingen, wegens spoed, enkel in het jaar 2014. Anderzijds is het risico van onrechtmatige toegang, door wie dan ook, onlosmakelijk verbonden met het bestaan van op informatiedragers bewaarde gegevens.⁸⁷

261. Het staat mijns inziens aan de verwijzende rechters om te beoordelen of de nadelen die de in de hoofdingen betrokken algemene verplichtingen tot bewaring van gegevens veroorzaken in een democratische samenleving niet onevenredig zijn aan de nagestreefde doelen, gelet op de in punt 247 van deze conclusie weergegeven rechtspraak. In het kader van deze beoordeling moeten die rechters de aan een dergelijke verplichting verbonden risico's en voordelen tegen elkaar af wegen, namelijk:

- enerzijds, de voordelen van het verlenen van een beperkt vermogen om het verleden te lezen aan de met de bestrijding van ernstige criminaliteit belaste autoriteiten⁸⁸ en,
- anderzijds, de ernstige risico's die in een democratische samenleving voortvloeien uit het vermogen om het privéleven van een persoon in kaart te brengen en om een hele bevolkingsgroep te categoriseren.

262. Die beoordeling moet plaatsvinden met inachtneming van alle relevante kenmerken van de in de hoofdingen betrokken nationale regelingen. Ik benadruk in dit verband dat de door het Hof in de punten 60 tot en met 68 van het arrest DRI genoemde dwingende waarborgen slechts minimumwaarborgen vormen om de inbreuk op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten te beperken tot het strikt noodzakelijke. Het is bijgevolg niet uitgesloten dat een nationale regeling die al die waarborgen bevat niettemin onevenredig moet worden geacht in een democratische samenleving vanwege de wanverhouding tussen de ernstige risico's die in een democratische samenleving door die verplichting worden veroorzaakt en de voordelen die eruit voortvloeien voor de bestrijding van ernstige criminaliteit.

86 — Zie in dit verband United Nations Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 30 juni 2014, A/HRC/27/37, nr. 19: „In dezelfde geest beweren sommigen dat het onderscheppen – of verzamelen – van gegevens over een communicatie, en niet van de inhoud ervan, op zichzelf geen inmenging in het privéleven vormt. Uit het oogpunt van het recht op privéleven is dit onderscheid echter niet overtuigend. De samenvoegingen van informatie die doorgaans worden aangeduid met „metagegevens” kunnen aanwijzingen geven over het gedrag van een individu, zijn sociale betrekkingen, zijn privévoorkeuren en zijn identiteit *die veel verder gaan dan hetgeen door raadpleging van de inhoud van een privécommunicatie wordt bereikt*” (cursivering van mij). Zie eveneens United Nations General Assembly, Report of the Special Rapporteur on promotion and protection of human rights while countering terrorism, 23 september 2014, A/69/397, nr. 53.

87 — Zie met name United Nations Commission on Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 april 2013, A/HRC/23/40, nr. 67: „Databestanden worden kwetsbaar voor diefstal, fraude en onopzettelijke openbaarmaking”.

88 — Zie de punten 178-183 van deze conclusie.

VI – Conclusie

263. Gelet op het voorgaande geef ik het Hof in overweging de prejudiciële vragen van de Kamarrätten i Stockholm (hogerberoepsrechter in bestuurszaken, Stockholm, Zweden) en de Court of Appeal (England & Wales) (Civil Division) [hogerberoepsrechter (Engeland & Wales) in civiele zaken, Verenigd Koninkrijk] als volgt te beantwoorden:

„Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn „privacy en elektronische communicatie”), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, en de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie moeten aldus worden uitgelegd dat zij zich niet er tegen verzetten dat een lidstaat aanbieders van elektronische communicatiediensten verplicht om alle gegevens betreffende de door de gebruikers van hun diensten gevoerde communicaties te bewaren indien is voldaan aan alle hiernavolgende vereisten, hetgeen door de verwijzende rechters moet worden getoetst in het licht van alle relevante kenmerken van de in de hoofdgedingen betrokken nationale regelingen:

- die verplichting en de waarborgen waarmee zij gepaard gaat moeten zijn voorzien in wettelijke of bestuursrechtelijke maatregelen die voldoende toegankelijk en voorzienbaar zijn en naar behoren bescherming bieden tegen willekeur;
- die verplichting en de waarborgen waarmee zij gepaard gaat moeten de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest van de grondrechten erkende rechten eerbiedigen;
- die verplichting moet strikt noodzakelijk zijn voor de bestrijding van ernstige criminaliteit, hetgeen impliceert dat geen enkele andere maatregel of combinatie van maatregelen net zo doeltreffend kan zijn voor de bestrijding van ernstige criminaliteit, maar minder inbreuk maakt op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest erkende rechten;
- die verplichting moet gepaard gaan met alle door het Hof in de punten 60 tot en met 68 van het arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU:C:2014:238) genoemde waarborgen inzake de toegang tot de gegevens, de bewaringstermijn en de bescherming en beveiliging van de gegevens, teneinde de inbreuk op de door richtlijn 2002/58 en de artikelen 7 en 8 van het Handvest van de grondrechten erkende rechten te beperken tot het strikt noodzakelijke, en
- die verplichting moet in een democratische samenleving evenredig zijn aan de doelstelling van bestrijding van ernstige criminaliteit, hetgeen betekent dat de ernstige risico's die in een democratische samenleving door die verplichting worden veroorzaakt niet onevenredig mogen zijn aan de voordelen die eruit voortvloeien voor de bestrijding van ernstige criminaliteit.”