CONCLUSIE VAN ADVOCAAT-GENERAAL
M. CAMPOS SÁNCHEZ-BORDONA
van 15 januari 2020[1]

Gevoegde zaken C-511/18 en C-512/18

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

[verzoek van de Conseil d'État (hoogste bestuursrechter, Frankrijk) om een prejudiciële beslissing]

„Prejudiciële verwijzing – Verwerking van persoonsgegevens en bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie – Bescherming van de nationale veiligheid en bestrijding van terrorisme – Richtlijn 2002/58/EG – Werkingssfeer – Artikel 1, lid 3 – Artikel 15, lid 3 – Artikel 4, lid 2, VEU – Handvest van de grondrechten van de Europese Unie – Artikelen 6, 7, 8, 11 en 47 en artikel 52, lid 1 – Algemene en ongedifferentieerde bewaring van verbindingsgegevens en gegevens waardoor de makers van inhoud kunnen worden geïdentificeerd – Verzameling van verkeers- en locatiegegevens – Toegang tot de gegevens"

1. In de afgelopen jaren heeft het Hof een vaste lijn aangehouden in zijn rechtspraak met betrekking tot de bewaring van en de toegang tot persoonsgegevens, met als belangrijkste mijlpalen:

– zijn arrest van 8 april 2014, Digital Rights Ireland e.a.[2], waarbij richtlijn 2006/24/EG[3] ongeldig is verklaard omdat die een onevenredige inmenging in de in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest") neergelegde rechten mogelijk maakte;

– zijn arrest van 21 december 2016, Tele2 Sverige en Watson e.a.[4], waarin het artikel 15, lid 1, van richtlijn 2002/58/EG[5] heeft uitgelegd, en

1 Oorspronkelijke taal: Spaans.

2 Gevoegde zaken C-293/12 en C-594/12, EU:C:2014:238; hierna: „arrest Digital Rights".

3 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 elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB 2006, L 105, blz. 54).

4 Gevoegde zaken C-203/15 en C-698/15, EU:C:2016:970; hierna: „arrest Tele2 Sverige en Watson".

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).

– zijn arrest van 2 oktober 2018, Ministerio Fiscal [6], waarin het de uitlegging van dezelfde bepaling van richtlijn 2002/58 heeft bevestigd.

2. Deze arresten (in het bijzonder het tweede) baren de autoriteiten van bepaalde lidstaten zorgen, omdat die hun een instrument zouden ontnemen dat zij noodzakelijk achten om de nationale veiligheid te waarborgen en criminaliteit en terrorisme te bestrijden. Sommige van deze lidstaten pleiten er daarom voor dat het Hof terugkomt van deze rechtspraak of deze nuanceert.

3. Enkele rechterlijke instanties van de lidstaten hebben diezelfde bezorgdheid geuit in vier prejudiciële verwijzingen [7], waarin ik heden conclusie neem.

4. In die vier zaken rijst allereerst de vraag of richtlijn 2002/58 van toepassing is op activiteiten die verband houden met de nationale veiligheid en de bestrijding van terrorisme. Indien deze richtlijn in die context van toepassing is, moet vervolgens worden nagegaan in hoeverre de lidstaten de door de richtlijn beschermde privacyrechten kunnen beperken. Ten slotte moet worden onderzocht in hoeverre de verschillende nationale wettelijke regelingen ter zake (de Britse [8], de Belgische [9] en de Franse [10]) verenigbaar zijn met het Unierecht, zoals dat door het Hof is uitgelegd.

I. Toepasselijke bepalingen

A. Unierecht

1. Richtlijn 2002/58

5. Artikel 1 („Werkingssfeer en doelstelling”) luidt:

„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 elektronischecommunicatieapparatuur en -diensten in de Gemeenschap.

[…]

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het EG-Verdrag vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, 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.”

6 Zaak C-207/16, EU:C:2018:788; hierna: „arrest Ministerio Fiscal”.

7 Naast de onderhavige twee zaken (C-511/18 en C-512/18), betreft het de zaak Privacy International (C-623/17) en de zaak Ordre des barreaux francophones et germanophone e.a. (C-520/18).

8 Zaak Privacy International, C-623/17.

9 Zaak Ordre des barreaux francophones et germanophone e.a., C-520/18.

10 Gevoegde zaken La Quadrature du Net e.a., C-511/18 en C-512/18.

6. Artikel 3 („Betrokken diensten”) bepaalt:

„Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.”

7. Artikel 5 („Vertrouwelijk karakter van de communicatie”) bepaalt in lid 1:

„De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.”

8. Artikel 6 („Verkeersgegevens”) bepaalt:

„1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.

2. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.”

9. Artikel 15 („Toepassing van een aantal bepalingen van richtlijn 95/46/EG[11]”) bepaalt in lid 1:

„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, d.w.z. 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 o.a. 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, van het Verdrag betreffende de Europese Unie.”

11 Richtlijn 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).

2. Richtlijn 2000/31

10. Artikel 14 van richtlijn 2000/31/EG [12] luidt:

„1. De lidstaten zorgen ervoor dat, wanneer een dienst van de informatiemaatschappij bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, de dienstverlener niet aansprakelijk is voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat:

[…]

3. Dit artikel doet geen afbreuk aan de mogelijkheid voor een rechtbank of een administratieve autoriteit om in overeenstemming met het rechtsstelsel van de lidstaat te eisen dat de dienstverlener een inbreuk beëindigt of voorkomt. Het doet evenmin afbreuk aan de mogelijkheid voor lidstaten om procedures vast te stellen om informatie te verwijderen of de toegang daartoe onmogelijk te maken."

11. Artikel 15 bepaalt:

„1. Met betrekking tot de levering van de in de artikelen 12, 13 en 14 bedoelde diensten leggen de lidstaten de dienstverleners geen algemene verplichting op om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.

2. De lidstaten kunnen voorschrijven dat dienstverleners de bevoegde autoriteiten onverwijld in kennis dienen te stellen van vermeende onwettige activiteiten of informatie door afnemers van hun dienst, alsook dat zij de bevoegde autoriteiten op hun verzoek informatie dienen te verstrekken waarmee de afnemers van hun dienst met wie zij opslagovereenkomsten hebben gesloten, kunnen worden geïdentificeerd."

3. Verordening 2016/679

12. Artikel 2 („Materieel toepassingsgebied") van verordening (EU) 2016/679 [13] luidt:

„1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;

12 Richtlijn van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („richtlijn inzake elektronische handel") (PB 2000, L 178, blz. 1).

13 Verordening van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46 (algemene verordening gegevensbescherming) (PB 2016, L 119, blz. 1).

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[…]"

13. Artikel 23 („Beperkingen") bepaalt in lid 1:

„De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met [22], worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

a) de nationale veiligheid;

b) landsverdediging;

c) de openbare veiligheid;

d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de onder a), tot en met e), en g) bedoelde gevallen;

i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;

j) de inning van civielrechtelijke vorderingen."

14. Artikel 95 („Verhouding tot richtlijn 2002/58/EG") luidt:

„Deze verordening legt natuurlijke personen of rechtspersonen geen aanvullende verplichtingen op met betrekking tot verwerking in verband met het verstrekken van openbare elektronische-communicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van richtlijn 2002/58/EG onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling."

B. Nationaal recht

1. Code de la sécurité intérieure

15. Artikel L. 851-1 van de code de la sécurité intérieure (Frans wetboek binnenlandse veiligheid) bepaalt:

„Onder de in titel II, hoofdstuk 1, van dit boek vastgestelde voorwaarden kan machtiging worden verleend om bij de exploitanten van elektronischecommunicatiemiddelen, bij de in artikel L. 34-1 van de code des postes et des communications électroniques (Frans wetboek post en elektronischecommunicatiemiddelen) genoemde personen, en bij de personen genoemd in artikel 6, I, punten 1 en 2, van de loi nº 2004-575 […] pour la confiance dans l'économie numérique (Franse wet nr. 2004-575 ter bevordering van het vertrouwen in de digitale economie) informatie of documenten op te vragen die werden verwerkt of opgeslagen door hun netwerken of elektronischecommunicatiediensten, met inbegrip van de technische gegevens betreffende de identificatie van abonnements- of verbindingsnummers voor elektronischecommunicatiediensten, de identificatie van alle abonnements- of verbindingsnummers van een bepaalde persoon, de locatie van de gebruikte eindapparatuur en de communicatie van een abonnee bestaande uit de lijst van opgeroepen en oproepnummers, de duur en datum van de communicatie […]."

16. De artikelen L. 851-2 en L. 851-4 regelen, voor verschillende doeleinden en op verschillende manieren, de administratieve toegang in real time tot de aldus opgeslagen verbindingsgegevens.

17. Op grond van artikel L. 851-2 kunnen, uitsluitend ter voorkoming van terrorisme, bij dezelfde personen de in artikel L. 851-1 bedoelde informatie of documenten worden opgevraagd. Deze opvraging, die slechts betrekking heeft op één of meer personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging, wordt in real time uitgevoerd. Hetzelfde geldt voor artikel L. 851-4, op grond waarvan exploitanten uitsluitend technische gegevens over de locatie van de eindapparatuur in real time mogen doorgeven. [14]

18. Op grond van artikel L. 851-3 kan aan exploitanten van elektronischecommunicatiemiddelen en technische dienstverleners de verplichting worden opgelegd „om op hun netwerken geautomatiseerde bewerkingen toe te passen die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken". [15]

19. Volgens artikel L. 851-5 kan onder bepaalde voorwaarden „het gebruik van een technisch systeem worden toegestaan waarmee de locatie van een persoon, een voertuig of een voorwerp in real time kan worden bepaald".

20. Overeenkomstig artikel L. 851-6, I, is het onder bepaalde voorwaarden mogelijk om „rechtstreeks, door middel van apparatuur of een technisch systeem als bedoeld in artikel 226-3, lid 1, van de code pénal (Frans wetboek strafrecht), de technische verbindingsgegevens aan de hand waarvan de eindapparatuur of het abonnementsnummer van de gebruiker kan worden geïdentificeerd, alsmede de gegevens over de locatie van de gebruikte eindapparatuur te verzamelen".

14 Volgens de verwijzende rechter leggen deze technieken voor de dienstverleners geen extra bewaringsverplichting op naast wat noodzakelijk is voor de facturering van hun diensten, de commercialisering ervan en de levering van diensten met toegevoegde waarde.

15 Volgens de verwijzende rechter is deze techniek, die geen algemene en ongedifferentieerde bewaring behelst, uitsluitend bedoeld om, gedurende een welbepaalde periode, binnen alle door deze personen behandelde verbindingsgegevens die gegevens te verzamelen welke in verband kunnen worden gebracht met een dergelijk ernstig misdrijf.

2. Code des postes et des communications électroniques

21. Artikel L. 34-1 luidde, in de versie die gold ten tijde van de feiten:

„I. Het onderhavige artikel is van toepassing op de verwerking van persoonsgegevens in verband met de levering van elektronischecommunicatiediensten aan het publiek. Het is met name van toepassing op netwerken die systemen voor gegevensverzameling en identificatie ondersteunen.

II. De exploitanten van elektronischecommunicatiemiddelen, en met name de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, wissen of anonimiseren alle verkeersgegevens, met inachtneming van het bepaalde in III, IV, V en VI.

De personen die elektronischecommunicatiediensten aan het publiek aanbieden, stellen in overeenstemming met de bepalingen van de vorige alinea interne procedures vast om gevolg te geven aan verzoeken van bevoegde autoriteiten.

Personen van wie de hoofd- of nevenberoepsactiviteit erin bestaat het publiek een aansluiting voor online communicatie via toegang tot het netwerk aan te bieden, ook gratis, dienen de bepalingen na te leven die krachtens dit artikel van toepassing zijn op de exploitanten van elektronischecommunicatiediensten.

III. Met het oog op het onderzoeken, vaststellen en vervolgen van strafbare feiten of van een inbreuk op de in artikel L. 336-3 van de code de la propriété intellectuelle (Frans wetboek intellectuele eigendom) omschreven verplichting, of met het oog op het voorkomen van aanvallen op geautomatiseerde gegevensverwerkingssystemen als bepaald en strafbaar gesteld in de artikelen 323-1 tot en met 323-3-1 van de code pénal en met als enige doel, indien nodig, de terbeschikkingstelling mogelijk te maken aan de rechterlijke autoriteit of aan de in artikel L. 331-12 van de code de la propriété intellectuelle bedoelde hoge autoriteit, of aan de in artikel L. 2321-1 van de code de la défense (Frans wetboek defensie) bedoelde nationale autoriteit voor de veiligheid van de informatiesystemen, kan het wissen of anonimiseren van bepaalde categorieën technische gegevens voor een periode van maximaal één jaar worden uitgesteld. Bij decreet vastgesteld na advies van de Conseil d'État (hoogste bestuursrechter, Frankrijk) en van de Commission nationale de l'informatique et des libertés (Franse nationale commissie voor informatica en vrijheden), worden binnen de in VI vastgestelde grenzen deze soorten gegevens en de duur van hun bewaring vastgesteld, naargelang van de activiteit van de exploitanten en de aard van de communicatie, alsook de wijze waarop, in voorkomend geval, de aanwijsbare en specifieke extra kosten verbonden aan de in dit verband door de exploitanten op verzoek van de staat verleende diensten worden gecompenseerd.

[…]

VI. De gegevens die worden bewaard en verwerkt onder de in III, IV en V vastgestelde voorwaarden, hebben uitsluitend betrekking op de identificatie van de gebruikers van de door de exploitanten verleende diensten, de technische kenmerken van de door deze exploitanten verleende communicatiediensten en de locatie van de eindapparatuur.

Zij mogen in geen geval verwijzen naar de inhoud van de correspondentie of naar de informatie die in het kader van deze communicatie in welke vorm dan ook is geraadpleegd.

De gegevens worden opgeslagen en verwerkt met inachtneming van de bepalingen van loi nº 78-17, du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés (Franse wet nr. 78-17 van 6 januari 1978 betreffende informatica, bestanden en vrijheden).

De exploitanten nemen alle maatregelen om te voorkomen dat deze gegevens voor andere dan de in dit artikel genoemde doeleinden worden gebruikt."

22. Op grond van artikel R. 10-13, I, zijn exploitanten verplicht de volgende gegevens te bewaren met het oog op het onderzoeken, vaststellen en vervolgen van strafbare feiten:

„a) gegevens aan de hand waarvan de gebruiker kan worden geïdentificeerd;

b) gegevens betreffende de gebruikte communicatie-eindapparatuur;

c) technische kenmerken, alsmede de datum, het tijdstip en de duur van elke communicatie;

d) gegevens betreffende de gevraagde of gebruikte aanvullende diensten en hun leveranciers;

e) gegevens aan de hand waarvan de ontvanger of ontvangers van de communicatie kunnen worden geïdentificeerd".

23. Overeenkomstig II van dit artikel moet de exploitant in geval van telefonieactiviteiten bovendien de gegevens bewaren die de bepaling van de oorsprong en de locatie van de communicatie vergemakkelijken.

24. Overeenkomstig III van dit artikel moeten de vermelde gegevens gedurende een jaar worden bewaard, te rekenen vanaf de datum van registratie ervan.

3. Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

25. Artikel 6, II, eerste alinea, van loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(wet nr. 2004-575 van 21 juni 2004 ter bevordering van het vertrouwen in de digitale economie)] bepaalt dat de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, en de natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, „de gegevens zodanig beheren en bewaren dat het mogelijk is eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of om het even welke inhoud van de diensten waarvan zij aanbieder zijn".

26. De derde alinea van II bepaalt dat de rechterlijke autoriteit die personen kan verzoeken om de in de eerste alinea bedoelde gegevens mee te delen.

27. De laatste alinea van II bepaalt dat een na advies van de Conseil d'État vastgesteld decreet „de in de eerste alinea bedoelde gegevens definieert en vaststelt hoelang en op welke wijze zij worden bewaard". [16]

16 De definitie is vastgesteld bij décret nº 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Frans decreet nr. 2011-219 van 25 februari 2011 betreffende de bewaring en mededeling van gegevens die het mogelijk maken om personen te identificeren die hebben bijgedragen aan de creatie van online geplaatste inhoud). In dit decreet zijn de volgende bepalingen het meest relevant: a) artikel 1, lid 1, op grond waarvan personen die toegang verlenen tot online communicatiediensten de volgende gegevens moeten bewaren: de identificator van de verbinding, de aan de abonnee toegekende identificator, de identificator van de voor de verbinding gebruikte eindapparatuur, de datum en het tijdstip van het begin en einde van de verbinding, de kenmerken van de lijn van de abonnee; b) artikel 1, lid 2, op grond waarvan personen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, verplicht zijn om voor elke verrichting de volgende gegevens te bewaren: de identificator van de verbinding aan de oorsprong van de communicatie, de identificator die is toegekend aan de inhoud die het voorwerp van de verrichting is, de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud, de aard van de verrichting, de datum en het tijdstip van de verrichting, de identificator die is gebruikt door de auteur van de verrichting; en ten slotte c) artikel 1, lid 3, op grond waarvan de in de twee voorgaande leden bedoelde personen de volgende informatie moeten bewaren die door een gebruiker is verstrekt bij de ondertekening van het contract of het aanmaken van een account: de identificator van de verbinding bij het aanmaken van het account, de naam, achternaam of bedrijfsnaam, de bijbehorende postadressen, de gebruikte pseudoniemen, de bijbehorende e-mail- of accountadressen, telefoonnummers, bijgewerkte wachtwoorden en gegevens voor de verificatie of wijziging ervan.

II. Feiten van het hoofdgeding en prejudiciële vragen

A. Zaak C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net en de Fédération des fournisseurs d'accès à Internet associatifs (hierna: „verzoekers") hebben bij de Conseil d'État een vordering ingesteld tot nietigverklaring van verschillende decreten tot uitvoering van een aantal bepalingen van de code de la sécurité intérieure. [17]

29. Verzoekers stellen in wezen dat zowel de bestreden decreten als de betrokken bepalingen van de code de la sécurité intérieure inbreuk maken op het recht op eerbiediging van de persoonlijke levenssfeer, het recht op bescherming van persoonsgegevens en dat op een doeltreffende voorziening in rechte, die door respectievelijk de artikelen 7, 8 en 47 van het Handvest worden gewaarborgd.

30. In die omstandigheden heeft de Conseil d'État het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

„1) Moet de verplichting tot algemene en ongedifferentieerde bewaring die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van [richtlijn 2002/58], in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest […], en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 [VEU] uitsluitend op de lidstaten rust?

2) Dient [richtlijn 2002/58], gelezen in het licht van het Handvest […], aldus te worden uitgelegd dat zij het mogelijk maakt om wetgevende maatregelen te nemen, zoals maatregelen voor het in real time opvragen van verkeers- en locatiegegevens van welbepaalde personen, die weliswaar van invloed zijn op de rechten en verplichtingen van de aanbieders van een elektronischecommunicatiedienst, maar hun geen specifieke verplichting opleggen tot bewaring van hun gegevens?

3) Moet [richtlijn 2002/58], gelezen in het licht van het Handvest […], aldus worden uitgelegd dat zij de regelmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk stelt van het vereiste om de betrokken personen te informeren wanneer dergelijke informatie het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, dan wel dat dergelijke procedures als regelmatig kunnen worden beschouwd gelet op alle andere bestaande procedurele waarborgen, wanneer deze waarborgen de doeltreffendheid van het recht op beroep garanderen?"

17 Tegen de volgende decreten wordt opgekomen: a) décret n° 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (decreet nr. 2015-1885 van 28 september 2015 houdende aanwijzing van gespecialiseerde inlichtingendiensten); b) décret n° 2015 -1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (decreet nr. 2015-1211 van 1 oktober 2015 betreffende geschillen inzake het gebruik van aan machtiging onderworpen inlichtingentechnieken en van voor de staatsveiligheid relevante bestanden); c) décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure (decreet nr. 2015-1639 van 11 december 2015 tot aanwijzing van diensten, andere dan de gespecialiseerde inlichtingendiensten, die gemachtigd zijn om gebruik te maken van de technieken opgenomen in boek VIII, titel V, van de code de la sécurité intérieure), en d) décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (decreet nr. 2016-67 van 29 januari 2016 betreffende de technieken voor het inwinnen van inlichtingen).

B. Zaak C-512/18

31. Verzoekers in het geding in zaak C-511/18, met uitzondering van Igwan.net, hebben de Conseil d'État eveneens verzocht om nietigverklaring van het (stilzwijgende) besluit tot afwijzing van hun verzoek tot intrekking van artikel R. 10-13 van de code des postes et des communications électroniques en van décret nº 2011-219 du 25 février 2011.

32. Volgens verzoekers leggen de bestreden regelingen een verplichting tot bewaring van verkeers-, locatie- en verbindingsgegevens op die door haar algemene aard een onevenredige inbreuk vormt op het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op vrijheid van meningsuiting, zoals gewaarborgd door de artikelen 7, 8 en 11 van het Handvest, en een schending oplevert van artikel 15, lid 1, van richtlijn 2002/58.

33. In het kader van dit verzoek heeft de Conseil d'État het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

„1) Moet de verplichting tot algemene en ongedifferentieerde bewaring die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van [richtlijn 2002/58], met name gelet op de waarborgen en controles die vervolgens gelden voor zowel het opvragen als het gebruiken van die verbindingsgegevens, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest […] en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 [VEU] uitsluitend op de lidstaten rust?

2) Moeten de bepalingen van [richtlijn 2000/31], gelezen tegen de achtergrond van de artikelen 6, 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest […], aldus worden uitgelegd dat zij toestaan dat een staat een nationale regeling invoert die de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, en de natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, verplicht om gegevens te bewaren die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, zodat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken om de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven?"

III. Procedure bij het Hof en standpunten van partijen

34. De verzoeken om een prejudiciële beslissing zijn op 3 augustus 2018 ingekomen ter griffie van het Hof.

35. Schriftelijke opmerkingen zijn ingediend door La Quadrature du Net, de Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, de Duitse en de Belgische regering, de regering van het Verenigd Koninkrijk, de Tsjechische, de Cypriotische, de Deense, de Spaanse, de Estse, de Franse, de Hongaarse, de Ierse, de Poolse en de Zweedse regering alsmede de Commissie.

36. De openbare terechtzitting voor deze zaak heeft plaatsgevonden op 9 september 2019, samen met die voor de zaak Privacy International (C-623/17), en de zaak Ordre des barreaux francophones et germanophone e.a. (C-520/18). Op die terechtzitting zijn de partijen bij de vier prejudiciële verwijzingen verschenen, alsook de voornoemde regeringen en de Nederlandse en de Noorse regering, de Commissie en de Europese Toezichthouder voor gegevensbescherming.

IV. Beoordeling

37. De vragen van de Conseil d'État kunnen in drie groepen worden ingedeeld:

– ten eerste, de vraag of het Unierecht zich verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting oplegt tot algemene en ongedifferentieerde bewaring van verbindingsgegevens (eerste vraag in de zaken C-511/18 en C-512/18), en in het bijzonder van gegevens die het mogelijk maken om de identiteit vast te stellen van de makers van de inhoud die door deze aanbieders wordt aangeboden (tweede vraag in zaak C-512/18);

– ten tweede, de vraag of de rechtmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk is van het vereiste om de betrokken personen te informeren wanneer zulks het onderzoek niet in gevaar kan brengen (derde vraag in zaak C-511/18);

– ten derde, de vraag of het in real time opvragen van verkeers- en locatiegegevens, zonder verplichting tot bewaring van deze gegevens, verenigbaar is – en onder welke voorwaarden – met richtlijn 2002/58 (tweede vraag in zaak C-511/18).

38. Uiteindelijk gaat het erom te bepalen of het Unierecht zich verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten twee soorten verplichtingen oplegt: a) enerzijds, het *verzamelen* van bepaalde gegevens, maar niet het bewaren ervan; b) anderzijds, het *bewaren* van verbindingsgegevens en van gegevens die het mogelijk maken om de identiteit vast te stellen van de makers van de inhoud die door deze aanbieders wordt aangeboden.

39. Vooraf moet worden uitgemaakt of richtlijn 2002/58 van toepassing is, precies wegens de context [18] waarin de nationale regeling is vastgesteld (dat wil zeggen, in omstandigheden waarin de nationale veiligheid in gevaar kan komen).

A. Toepasselijkheid van richtlijn 2002/58

40. De verwijzende rechter gaat ervan uit dat de in casu aan de orde zijnde regeling binnen de werkingssfeer van richtlijn 2002/58 valt. Dit blijkt volgens hem uit de rechtspraak in het arrest Tele2 Sverige en Watson, die is bevestigd in het arrest Ministerio Fiscal.

41. Enkele van de interveniërende regeringen voeren daarentegen aan dat de bestreden regeling niet binnen die werkingssfeer valt. Ter verdediging van hun standpunt beroepen zij zich, naast andere argumenten, op het arrest van 30 mei 2006, Parlement/Raad en Commissie. [19]

42. Ik ben het eens met de Conseil d'État dat dit deel van het debat reeds werd opgehelderd in het arrest Tele2 Sverige en Watson, waarin is bevestigd dat richtlijn 2002/58 in beginsel van toepassing is wanneer aanbieders van elektronische diensten wettelijk worden verplicht om de gegevens van hun abonnees te bewaren en de overheid daar toegang toe te verlenen. Aan dit standpunt wordt niet afgedaan door het feit dat de verplichtingen aan aanbieders worden opgelegd om redenen van nationale veiligheid.

18 „Een context [van] ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name […] terreurgevaar", zoals aangegeven in de eerste vraag in zaak C-511/18.

19 Gevoegde zaken C-317/04 en C-318/04, EU:C:2006:346; hierna: „arrest Parlement/Raad en Commissie".

43. Reeds in dit stadium moet ik erop wijzen dat, in geval van discrepantie tussen het arrest Tele2 Sverige en Watson en vroegere arresten, eerstgenoemd arrest als doorslaggevend moet worden beschouwd, aangezien het van latere datum is en is bevestigd door het arrest Ministerio Fiscal. Zoals ik zal trachten uit te leggen, is er mijns inziens echter geen sprake van een dergelijke discrepantie.

1. Arrest Parlement/Raad en Commissie

44. De zaken die bij het arrest Parlement/Raad en Commissie zijn afgedaan, hadden betrekking op:

– de overeenkomst tussen de Europese Gemeenschap en de Verenigde Staten van Amerika inzake de verwerking en overdracht van PNR-gegevens [PNR: Passenger Name Records (passagiersgegevens)] door luchtvaartmaatschappijen aan de autoriteiten van de Verenigde Staten van Amerika [20];

– de passende bescherming van persoonsgegevens in de Passenger Name Records die aan die autoriteiten worden doorgegeven. [21]

45. Het Hof concludeerde toen dat de doorgifte van dergelijke gegevens een verwerking was die betrekking had op de openbare veiligheid en de activiteiten van de staat op strafrechtelijk gebied. Overeenkomstig artikel 3, lid 2, eerste streepje, van richtlijn 95/46 vielen het bestreden besluit en de bestreden beschikking niet binnen de werkingssfeer van richtlijn 95/46.

46. De gegevens werden aanvankelijk door luchtvaartmaatschappijen verzameld in het kader van een onder het Unierecht vallende activiteit, namelijk de verkoop van tickets. De verwerking van deze gegevens, zoals bedoeld in de beschikking, was echter „niet […] noodzakelijk […] voor een dienstverrichting, maar [werd] noodzakelijk […] geacht voor het waarborgen van de openbare veiligheid en voor de wetshandhaving”. [22]

20 Besluit 2004/496/EG van de Raad van 17 mei 2004 betreffende de sluiting van een overeenkomst tussen de Europese Gemeenschap en de Verenigde Staten van Amerika inzake de verwerking en overdracht van PNR-gegevens door luchtvaartmaatschappijen aan het Bureau of Customs and Border Protection van het ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PB 2004, L 183, blz. 83, met rectificatie in PB 2005, L 255, blz. 168) (zaak C-317/04).

21 Beschikking 2004/535/EG van de Commissie van 14 mei 2004 betreffende de passende bescherming van persoonsgegevens in het Passenger Name Record van vliegtuigpassagiers die aan het Bureau of Customs and Border Protection van de Verenigde Staten worden doorgegeven (PB 2004, L 235, blz. 11) (zaak C-318/04).

22 Arrest Parlement/Raad en Commissie, punt 57. In punt 58 wordt benadrukt dat „het feit dat de [gegevens] door particuliere marktdeelnemers voor commerciële doeleinden zijn verzameld en het deze laatste zijn die ze doorgeven naar een derde land” niet betekent dat een dergelijke doorgifte niet een van de in artikel 3, lid 2, eerste streepje, van richtlijn 95/46 genoemde gevallen van niet-toepassing van die richtlijn vormt, aangezien „[d]eze doorgifte geschiedt […] binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid”.

47. Het Hof heeft aldus gekozen voor een teleologische benadering, waarbij rekening wordt gehouden met het beoogde doel van de gegevensverwerking: indien daarmee de bescherming van de openbare veiligheid wordt nagestreefd, moet die verwerking worden geacht buiten de werkingssfeer van richtlijn 95/46 te vallen. Dit doel was echter niet het enige bepalende criterium [23] en in het arrest is dan ook benadrukt dat „[d]eze doorgifte geschiedt […] binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid”. [24]

48. Het arrest Parlement/Raad en Commissie maakt het dus mogelijk tot een juist begrip te komen van het onderscheid tussen de uitsluitingsbepaling en de bepalingen van richtlijn 95/46 die beperkingen bevatten (vergelijkbaar met die van richtlijn 2002/58). Het is evenwel juist dat beide soorten bepalingen naar doelstellingen van algemeen belang verwijzen, hetgeen enige verwarring omtrent de draagwijdte ervan onderhoudt, zoals advocaat-generaal Bot heeft opgemerkt. [25]

49. Deze verwarring ligt waarschijnlijk ten grondslag aan het standpunt van de lidstaten die voor de niet-toepasselijkheid van richtlijn 2002/58 in deze context pleiten. Volgens hen wordt het belang van de nationale veiligheid alleen gewaarborgd door de in artikel 1, lid 3, van richtlijn 2002/58 vervatte uitsluiting. Vast staat echter dat hetzelfde belang wordt gediend door de beperkingen die bij artikel 15, lid 1, van die richtlijn zijn toegestaan, waaronder de beperking met betrekking tot de nationale veiligheid. Laatstbedoelde bepaling zou overbodig zijn indien richtlijn 2002/58 sowieso niet van toepassing is wanneer belangen van nationale veiligheid worden ingeroepen.

2. Arrest Tele2 Sverige en Watson

50. In het arrest Tele2 Sverige en Watson is onderzocht of bepaalde nationale regelingen die aanbieders van openbaar beschikbare elektronischecommunicatiediensten een algemene verplichting opleggen om de gegevens betreffende die communicatie te bewaren, verenigbaar zijn met het Unierecht. De omstandigheden waren dus in wezen identiek aan die welke in de onderhavige prejudiciële verwijzingen aan de orde zijn.

51. Opnieuw geconfronteerd met vragen over de toepasselijkheid van het Unierecht – ditmaal in de vorm van richtlijn 2002/58 – heeft het Hof er om te beginnen op gewezen dat „bij de beoordeling van de omvang van de werkingssfeer van richtlijn 2002/58 met name rekening moet worden gehouden met de algemene opzet van deze richtlijn”. [26]

23 Dit zou later door de betreurde advocaat-generaal Bot worden onderstreept in zijn conclusie in de zaak Ierland/Parlement en Raad (C-301/06, EU:C:2008:558), waarin hij het volgende verklaarde: „[Het] arrest [Parlement/Raad en Commissie] kan […] niet betekenen dat alleen het onderzoek van het doel van de verwerking van persoonsgegevens relevant is om een dergelijke verwerking al dan niet binnen de werkingssfeer van het bij richtlijn 95/46 opgezette stelsel van gegevensbescherming te brengen. Het is ook van belang, na te gaan in het kader van welke soort activiteiten een gegevensverwerking gebeurt. Alleen wanneer een dergelijke verwerking gebeurt voor de uitoefening van specifieke activiteiten van de staten of van de overheidsorganen die niets te maken hebben met de activiteiten van particulieren, valt zij overeenkomstig artikel 3, lid 2, eerste streepje, van richtlijn 95/46 buiten het bij deze richtlijn opgezette communautaire stelsel van bescherming van persoonsgegevens” (punt 122).

24 Arrest Parlement/Raad en Commissie, punt 58. Het hoofddoel van de overeenkomst was de luchtvaartmaatschappijen die passagiersvervoersdiensten tussen de Unie en de Verenigde Staten exploiteren, te verplichten aan de autoriteiten van de Verenigde Staten elektronische toegang tot PNR-gegevens in hun geautomatiseerde boekings- en vertrekcontrolesystemen te verschaffen. Met de overeenkomst werd dus een vorm van internationale samenwerking tussen de Unie en de Verenigde Staten voor de bestrijding van terrorisme en andere ernstige criminaliteit ingesteld, waarbij werd getracht dit doel te verzoenen met het doel om de persoonsgegevens van passagiers te beschermen. In die context was er geen groot onderscheid tussen de aan de ondernemingen opgelegde verplichting en een rechtstreekse uitwisseling van gegevens tussen overheidsinstanties.

25 Conclusie van advocaat-generaal Bot in de zaak Ierland/Parlement en Raad (C-301/06, EU:C:2008:558, punt 127).

26 Arrest Tele2 Sverige en Watson, punt 67.

52. In dit verband heeft het Hof opgemerkt: „De in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen betreffen specifieke activiteiten van de staten of van de overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien […]. Bovendien blijken de doelstellingen die dergelijke maatregelen volgens die bepaling moeten nastreven, in het onderhavige geval het waarborgen van de nationale veiligheid […] grotendeels overeen te stemmen met de doelstellingen van de in artikel 1, lid 3, van die richtlijn bedoelde activiteiten.” [27]

53. De doelstelling van de maatregelen die de lidstaten krachtens artikel 15, lid 1, van richtlijn 2002/58 kunnen nemen om het recht op bescherming van de persoonlijke levenssfeer te beperken, stemt dus (op dit punt) overeen met de doelstelling die rechtvaardigt dat bepaalde activiteiten van de staat overeenkomstig artikel 1, lid 3, ervan aan de werkingssfeer van de richtlijn worden onttrokken.

54. Het Hof heeft echter geoordeeld dat „[g]elet op de algemene opzet van richtlijn 2002/58” uit die omstandigheid „niet [kon] worden afgeleid dat de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen van de werkingssfeer van deze richtlijn zijn uitgesloten, omdat daardoor aan deze bepaling elk nuttig effect zou worden ontnomen. Deze bepaling vooronderstelt immers noodzakelijkerwijs dat de aldaar bedoelde nationale maatregelen […] binnen de werkingssfeer van die richtlijn vallen, omdat in deze laatste uitdrukkelijk wordt bepaald dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de aldaar geformuleerde voorwaarden”. [28]

55. Daarbij komt dat de door artikel 15, lid 1, van richtlijn 2002/58 toegestane beperkingen „de activiteit van de aanbieders van elektronischecommunicatiediensten voor de in die bepaling vermelde doeleinden [regelen]”. Derhalve moet deze bepaling, gelezen in samenhang met artikel 3 van die richtlijn, „in die zin worden uitgelegd dat dergelijke wettelijke maatregelen binnen de werkingssfeer van die richtlijn vallen”. [29]

56. Het Hof heeft dan ook geoordeeld dat een wettelijke maatregel die aanbieders „de verplichting oplegt om de verkeersgegevens en de locatiegegevens te bewaren” binnen de werkingssfeer van richtlijn 2002/58 valt, „omdat een dergelijke activiteit noodzakelijkerwijs inhoudt dat de aanbieders persoonsgegevens verwerken” [30] en dat binnen die werkingssfeer ook een wettelijke maatregel valt die betrekking heeft op de toegang van de autoriteiten tot de door die aanbieders bewaarde gegevens. [31]

57. De uitlegging die het Hof aan richtlijn 2002/58 heeft gegeven in het arrest Tele2 Sverige en Watson, wordt herhaald in het arrest Ministerio Fiscal.

58. Kan het arrest Tele2 Sverige en Watson als een – min of meer impliciete – ommekeer ten opzichte van de rechtspraak in het arrest Parlement/Raad en Commissie worden beschouwd? De regering van Ierland, bijvoorbeeld, is die mening toegedaan. Volgens haar is alleen de laatstbedoelde rechtspraak verenigbaar met de rechtsgrondslag van richtlijn 2002/58 en in overeenstemming met artikel 4, lid 2, VEU. [32]

27 Ibidem, punt 72.

28 Ibidem, punt 73.

29 Ibidem, punt 74.

30 Ibidem, punt 75.

31 Ibidem, punt 76.

32 Punten 15 en 16 van de schriftelijke opmerkingen van de Ierse regering.

59. De Franse regering is van haar kant van mening dat deze tegenspraak kan worden opgelost indien er rekening mee wordt gehouden dat de rechtspraak in het arrest Tele2 Sverige en Watson betrekking heeft op de activiteiten van de lidstaten op strafrechtelijk gebied, terwijl de rechtspraak in het arrest Parlement/Raad en Commissie ziet op de veiligheid van de staat en de landsverdediging. Op het in casu onderzochte geval zou dus niet de rechtspraak in het arrest Tele2 Sverige en Watson van toepassing zijn, maar de oplossing waarvoor is gekozen in het arrest Parlement/Raad en Commissie. [33]

60. Zoals ik reeds heb uiteengezet, denk ik dat beide arresten met elkaar kunnen worden verzoend op een andere manier dan die welke door de Franse regering naar voren is gebracht. De benadering van deze laatste deel ik niet, omdat de overwegingen in het arrest Tele2 Sverige en Watson die expliciet verwijzen naar de bestrijding van terrorisme [34] volgens mij kunnen worden uitgebreid tot elke andere bedreiging voor de nationale veiligheid (waarvan terrorisme er slechts één is).

3. Mogelijkheid van een uitlegging die het arrest Parlement/Raad en Commissie en het arrest Tele2 Sverige en Watson verzoent

61. Mijns inziens heeft het Hof in het arrest Tele2 Sverige en Watson en het arrest Ministerio Fiscal rekening gehouden met de bestaansreden van de uitsluitings- en de beperkende bepalingen, alsook met het systematische verband tussen de twee soorten bepalingen.

62. Als het Hof in de zaak Parlement/Raad en Commissie heeft geoordeeld dat de verwerking van gegevens buiten de werkingssfeer van richtlijn 95/46 viel, dan is dat, zoals ik reeds in herinnering heb gebracht, te wijten aan het feit dat, in de context van de samenwerking tussen de Europese Unie en de Verenigde Staten in een typisch internationaal kader, de staatsdimensie van de activiteit moest prevaleren boven het feit dat die verwerking ook een commerciële of particuliere dimensie had. Een van de destijds besproken kwesties was precies de juiste rechtsgrondslag voor het bestreden besluit.

63. Wat betreft de nationale maatregelen die in het arrest Tele2 Sverige en Watson en het arrest Ministerio Fiscal zijn onderzocht, heeft het Hof daarentegen de interne reikwijdte van de gegevensverwerking op de voorgrond geplaatst: die gegevensverwerking vond uitsluitend plaats binnen het nationale rechtskader, dus zonder de externe dimensie die kenmerkend was voor het voorwerp van het arrest Parlement/Raad en Commissie.

64. Het verschillende gewicht van de internationale en de interne (commerciële en particuliere) dimensie van de gegevensverwerking heeft ertoe geleid dat de verwerking in het eerste geval werd uitgesloten van het Unierecht, omdat dit passender werd geacht om het algemene belang van de nationale veiligheid te beschermen. In het tweede geval kon datzelfde belang daarentegen doeltreffend worden gediend met de in artikel 15, lid 1, van richtlijn 2002/58 vervatte beperking.

65. Daarnaast moet nog worden ingegaan op een ander onderscheid, dat verband houdt met de verschillende wetgevende context: beide arresten waren toegespitst op de uitlegging van twee bepalingen die, afgezien van hun vorm, niet gelijk zijn.

66. Zo heeft het Hof zich in het arrest Parlement/Raad en Commissie uitgesproken over de uitlegging van artikel 3, lid 2, van richtlijn 95/46, terwijl het zich in het arrest Tele2 Sverige en Watson heeft uitgesproken over artikel 1, lid 3, van richtlijn 2002/58. Uit een zorgvuldige lezing van deze artikelen blijkt dat er voldoende verschillen zijn om de betekenis van de beslissingen van het Hof in beide gevallen te ondersteunen.

33 Punten 34-50 van de schriftelijke opmerkingen van de Franse regering.

34 Arrest Tele2 Sverige en Watson, punten 103 en 119.

67. Artikel 3, lid 2, van richtlijn 95/46 luidt: „De bepalingen van deze richtlijn *zijn niet van toepassing op de verwerking van persoonsgegevens* […] die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt […] en in ieder geval *verwerkingen* die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat (waaronder de economie van de staat, wanneer deze *verwerkingen* in verband staan met vraagstukken van staatsveiligheid), en de activiteiten van de staat op strafrechtelijk gebied." [35]

68. Artikel 1, lid 3, van richtlijn 2002/58 bepaalt van zijn kant: „Deze richtlijn *is niet van toepassing op activiteiten* die niet onder het EG-Verdrag vallen […], 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." [36]

69. Terwijl artikel 3, lid 2, van richtlijn 95/46 de *verwerking van gegevens* uitsluit die – voor zover hier van belang – betrekking heeft op de veiligheid van de staat, sluit artikel 1, lid 3, van richtlijn 2002/58 *activiteiten* uit die – eveneens voor zover hier van belang – gericht zijn op de bescherming van de staatsveiligheid.

70. Dit verschil is niet onbeduidend. Richtlijn 95/46 was niet van toepassing op een activiteit (de „verwerking van persoonsgegevens") die door iedereen kan worden uitgevoerd. Van deze activiteit werden specifiek de verwerkingen uitgesloten die onder andere tot doel hadden de staatsveiligheid te waarborgen. De hoedanigheid van de *persoon* die de gegevensverwerking uitvoerde, was echter irrelevant. De benadering die was gekozen om de uitgesloten handelingen te bepalen, was dus teleologisch of doelconform en maakte geen onderscheid naar de persoon die de handeling uitvoerde.

71. In de zaak Parlement/Raad en Commissie heeft het Hof dus in de eerste plaats gelet op het doel dat met de gegevensverwerking werd nagestreefd. Het was niet van belang dat „de [gegevens] door particuliere marktdeelnemers voor commerciële doeleinden zijn verzameld en het deze laatste zijn die ze doorgeven naar een derde land", aangezien het fundamentele punt was dat „[d]eze doorgifte geschiedt […] binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid." [37]

72. Daarentegen kunnen de „activiteiten die verband houden met staatsveiligheid", die buiten de in het arrest Tele2 Sverige en Watson onderzochte werkingssfeer van richtlijn 2002/58 vallen, niet worden toegeschreven aan om het even welke persoon, maar alleen aan de staat zelf. Bovendien omvatten zij niet de wetgevende of regelgevende functies van de staat, maar alleen de materiële handelingen van de overheid.

73. De in artikel 1, lid 3, van richtlijn 2002/58 genoemde *activiteiten* „zijn [immers] in alle gevallen specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien". [38] Dergelijke „activiteiten" kunnen evenwel niet regelgevend van aard zijn. Indien dat het geval was, zouden alle door de lidstaten vastgestelde bepalingen betreffende de verwerking van persoonsgegevens buiten de werkingssfeer van richtlijn 2002/58 vallen, zolang zij maar gerechtvaardigd lijken te zijn om de veiligheid van de staat te waarborgen.

35 Cursivering van mij.

36 Cursivering van mij.

37 Arrest Parlement/Raad en Commissie, punt 58.

38 Arrest Ministerio Fiscal, punt 32. Zie in dezelfde zin arrest Tele2 Sverige en Watson, punt 72.

74. Enerzijds zou de richtlijn hierdoor duidelijk aan doeltreffendheid inboeten, aangezien de lidstaten zich slechts op een dermate vaag juridisch begrip als de nationale veiligheid zouden hoeven te beroepen om de door de Uniewetgever ontwikkelde waarborgen ter bescherming van de persoonsgegevens van de burgers naast zich neer te kunnen leggen. Deze bescherming is onuitvoerbaar zonder medewerking van de lidstaten, en moet – voor de burger – ook tegenover de nationale overheden worden gewaarborgd.

75. Anderzijds zou een uitlegging van het begrip „activiteiten van de staat" die ook de activiteiten omvat die leiden tot de vaststelling van regels en wettelijke voorschriften, zorgen voor de uitholling van artikel 15 van richtlijn 2002/58, dat de lidstaten juist de bevoegdheid verleent om – ter bescherming van, onder andere, de nationale veiligheid – „wettelijke maatregelen" te treffen om de reikwijdte van bepaalde in die richtlijn neergelegde rechten en plichten te beperken.[39]

76. Zoals het Hof in het arrest Tele2 Sverige en Watson heeft opgemerkt, „[moet] bij de beoordeling van de omvang van de werkingssfeer van richtlijn 2002/58 met name rekening […] worden gehouden met de algemene opzet van deze richtlijn".[40] Vanuit dit oogpunt kunnen artikel 1, lid 3, en artikel 15, lid 1, van richtlijn 2002/58 op zinvolle wijze en zonder verlies aan doeltreffendheid worden uitgelegd door in de eerstgenoemde bepaling een materiële uitsluiting te zien van de *activiteiten* die door de lidstaten worden verricht op het gebied van de nationale veiligheid (en daarmee gelijk te stellen activiteiten), en in de laatstgenoemde bepaling de machtiging om *wettelijke maatregelen* (dit wil zeggen regels met algemene toepassing) vast te stellen die, met het oog op de nationale veiligheid, gevolgen teweegbrengen voor de activiteiten van personen die onder het gezag van de lidstaten vallen, en die de door richtlijn 2002/58 gewaarborgde rechten beperken.

4. Uitsluiting van de nationale veiligheid in richtlijn 2002/58

77. De nationale veiligheid (of het synoniem daarvan, „staatsveiligheid", zoals vermeld in artikel 15, lid 1) wordt in richtlijn 2002/58 op twee manieren benaderd. Enerzijds vormt zij een grond tot *uitsluiting* (van de toepassing van die richtlijn) voor alle activiteiten van de lidstaten die specifiek daarmee „verband houden". Anderzijds is zij een – bij wet in te voeren – grond tot *beperking* van de rechten en verplichtingen waarin richtlijn 2002/58 voorziet, dat wil zeggen voor activiteiten van particuliere of commerciële aard die buiten de sfeer vallen van de activiteiten die aan de staat zijn voorbehouden.[41]

78. Op welke activiteiten heeft artikel 1, lid 3, van richtlijn 2002/58 betrekking? Naar mijn mening geeft de Conseil d'État zelf een goed voorbeeld door de artikelen L. 851-5 en L. 851-6 van de code de la sécurité intérieure te noemen, waarin wordt verwezen naar „technieken voor het inwinnen van inlichtingen die rechtstreeks door de staat worden toegepast zonder dat de activiteiten van aanbieders van elektronischecommunicatiediensten worden geregeld door oplegging van specifieke verplichtingen".[42]

39 Het valt immers moeilijk vol te houden dat artikel 15, lid 1, van richtlijn 2002/58 voorziet in de beperking van de vastgestelde rechten en plichten die het afkondigt op een gebied dat, zoals de nationale veiligheid, in beginsel buiten de werkingssfeer van de richtlijn valt op grond van artikel 1, lid 3, van de richtlijn zelf. Zoals het Hof in punt 73 van het arrest Tele2 Sverige en Watson heeft geoordeeld, veronderstelt artikel 15, lid 1, van richtlijn 2002/58 „noodzakelijkerwijs dat de aldaar bedoelde nationale maatregelen […] binnen de werkingssfeer van die richtlijn vallen, omdat in deze laatste uitdrukkelijk wordt bepaald dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de aldaar geformuleerde voorwaarden".

40 Arrest Tele2 Sverige en Watson, punt 67.

41 Zoals advocaat-generaal Saugmandsgaard Øe in zijn conclusie in de zaak Ministerio Fiscal (C-207/16, EU:C:2018:300, punt 47) terloops heeft opgemerkt, „[moet] onderscheid […] worden gemaakt tussen enerzijds de persoonsgegevens die *rechtstreeks* in het kader van de – klassieke – activiteiten van de staat op strafrechtelijk gebied worden verwerkt en anderzijds die gegevens die in het kader van de – commerciële – activiteiten van een aanbieder van elektronische-communicatiediensten worden verwerkt en *vervolgens* door de bevoegde overheidsdiensten worden gebruikt".

42 Punten 18 en 21 van de verwijzingsbeslissing in zaak C-511/18.

79. Mijns inziens is dat het sleutelelement om de omvang van de in artikel 1, lid 3, van richtlijn 2002/58 vervatte uitsluiting te bepalen. De *activiteiten* die de overheid, met het oog op de bescherming van de nationale veiligheid, zelf uitvoert, zonder de medewerking van particulieren te vereisen en dus zonder hun verplichtingen op te leggen met betrekking tot hun bedrijfsvoering, vallen niet onder de regeling van die bepaling.

80. De lijst van overheidsactiviteiten die zijn vrijgesteld van de algemene regeling voor de verwerking van persoonsgegevens moet echter restrictief worden uitgelegd. Met name kan het begrip *nationale veiligheid*, waarvoor de uitsluitende verantwoordelijkheid krachtens artikel 4, lid 2, VEU bij elke lidstaat ligt, niet worden uitgebreid tot andere, min of meer aangrenzende, sectoren van het openbare leven.

81. Aangezien er in de onderhavige prejudiciële verwijzingen ook particulieren (namelijk personen die elektronischecommunicatiediensten aanbieden aan gebruikers), en dus niet alleen overheidsorganen, aan te pas komen, is het niet nodig om uitvoerig in te gaan op de precieze contouren van het begrip nationale veiligheid in strikte zin.

82. Naar mijn mening kan echter een richtsnoer worden gevonden in het criterium van kaderbesluit 2006/960/JBZ[43], waarvan artikel 2, onder a), een onderscheid maakt tussen rechtshandhavingsautoriteiten in ruime zin – waaronder „een nationale politie-, douane- of andere autoriteit die krachtens het nationale recht is gemachtigd om strafbare feiten of criminele activiteiten op te sporen, te voorkomen en te onderzoeken, en in het kader hiervan gezag uit te oefenen en dwangmaatregelen toe te passen" – en „bureaus of eenheden die zich specifiek bezighouden met aangelegenheden van nationale veiligheid".[44]

83. In overweging 11 van richtlijn 2002/58 staat dat deze richtlijn „evenmin als richtlijn 95/46/EG van toepassing [is] op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het [Unierecht] vallende activiteiten". Richtlijn 2002/58 „verandert bijgevolg niets 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 […] staatsveiligheid".

84. Wat de bevoegdheden van de lidstaten inzake nationale veiligheid betreft, bestaat er immers een continuïteit tussen richtlijn 95/46 en richtlijn 2002/58. Geen van beide is gericht op de bescherming van de grondrechten op dit specifieke gebied, waarbinnen de activiteiten van de lidstaten niet „onder het [Unierecht vallen]".

85. Het in die overweging bedoelde „evenwicht" vloeit voort uit de noodzaak om de bevoegdheden van de lidstaten op het gebied van de nationale veiligheid te eerbiedigen wanneer zij deze *rechtstreeks en met hun eigen middelen* uitoefenen. Wanneer echter, ook om diezelfde redenen van nationale veiligheid, de medewerking wordt vereist van particulieren, aan wie bepaalde verplichtingen worden opgelegd, valt de activiteit binnen een gebied (de bescherming van de persoonlijke levenssfeer die door deze particuliere actoren moet worden gewaarborgd) dat door het Unierecht wordt beheerst.

86. Zowel richtlijn 95/46 als richtlijn 2002/58 tracht dit evenwicht te bereiken door toe te staan dat de rechten van particulieren worden beperkt door wettelijke maatregelen die door de lidstaten worden getroffen op grond van artikel 13, lid 1, respectievelijk artikel 15, lid 1. Dienaangaande is er tussen beide richtlijnen geen enkel verschil.

43 Kaderbesluit van de Raad van 18 december 2016 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie (PB 2006, L 386, blz. 89).

44 In dezelfde geest is in artikel 1, lid 4, van kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (PB 2008, L 350, blz. 60) bepaald dat dit besluit „de wezenlijke nationale veiligheidsbelangen en het specifieke inlichtingenwerk op het gebied van de nationale veiligheid onverlet [laat]".

87. Wat betreft verordening 2016/679, die een (nieuw) algemeen kader voor de bescherming van persoonsgegevens instelt, sluit artikel 2, lid 2, uit dat de verordening van toepassing is op de „verwerking van persoonsgegevens" wanneer de lidstaten „activiteiten [uitvoeren] die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen".

88. Terwijl in richtlijn 95/46 de verwerking van persoonsgegevens alleen werd gekwalificeerd met het oog op het doel ervan, ongeacht wie de verwerking uitvoert, worden de uitgesloten verwerkingen in verordening nr. 2016/679 bepaald aan de hand van zowel het doel als de uitvoerders ervan: uitgezonderd worden de verwerkingen die door de lidstaten worden verricht in het kader van *activiteiten* die buiten de werkingssfeer van het Unierecht vallen [artikel 2, lid 2, onder a) en b)] en die welke door de autoriteiten worden verricht *met het oog op de bestrijding van strafbare feiten en de bescherming* tegen gevaren voor de openbare veiligheid.[45]

89. Deze activiteiten van de overheid moeten noodzakelijkerwijs restrictief worden bepaald, anders wordt het Unierecht inzake de bescherming van de persoonlijke levenssfeer zijn nuttige werking ontnomen. Artikel 23 van verordening 2016/679 voorziet – net als artikel 15, lid 1, van richtlijn 2002/58 – in de beperking, *door middel van wettelijke maatregelen*, van de daarin vastgestelde rechten en verplichtingen, wanneer dit nodig is om onder meer de staatsveiligheid, de landsverdediging of de openbare veiligheid te waarborgen. Nogmaals, indien de bescherming van deze doelstellingen voldoende zou zijn om ze van de werkingssfeer van verordening 2016/679 uit te sluiten, zou het overbodig zijn om de staatsveiligheid in te roepen als rechtvaardiging voor de invoering van wettelijke maatregelen om de door die verordening gewaarborgde rechten te beperken.

90. Net als bij richtlijn 2002/58 zou het inconsequent zijn dat de in artikel 23 van verordening 2016/679 bedoelde wettelijke maatregelen (die, zoals reeds vermeld, beperkingen van staatswege op het recht op persoonlijke levenssfeer van de burgers toestaat om redenen van staatsveiligheid) binnen de werkingssfeer van die verordening vallen, en dat tegelijkertijd de verordening zelf zonder meer buiten toepassing wordt gesteld door de bescherming van de staatsveiligheid, wat zou betekenen dat geen enkel subjectief recht wordt erkend.

B. Bevestiging en mogelijke ontwikkeling van de rechtspraak in het arrest Tele2 Sverige en Watson

91. In mijn conclusie in zaak C-520/18 maak ik een grondige analyse[46] van de rechtspraak van het Hof ter zake, en op basis daarvan stel ik voor om die rechtspraak te bevestigen en bied ik tegelijkertijd een interpretatieve manier om de inhoud ervan te verfijnen.

92. Ik verwijs naar die analyse, die hier, kortheidshalve, volgens mij niet opnieuw hoeft te worden weergegeven. De hiernavolgende overwegingen over de door de Conseil d'État voorgelegde prejudiciële vragen moeten derhalve worden gelezen in samenhang met de desbetreffende punten van mijn conclusie in zaak C-520/18.

45 Verordening 2016/679 sluit namelijk de verwerking van gegevens uit die door de lidstaten wordt uitgevoerd in het kader van *activiteiten* die buiten de werkingssfeer van het Unierecht vallen, alsmede de verwerkingen die door autoriteiten worden verricht *met het oog op de bescherming* van de openbare veiligheid.

46 Punten 27-68.

C. Beantwoording van de prejudiciële vragen

1. Verplichting tot bewaring van gegevens (eerste prejudiciële vraag in de zaken C-511/18 en C-512/18 en tweede prejudiciële vraag in zaak C-512/18)

93. Wat de aan de aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot bewaring van gegevens betreft, wenst de verwijzende rechter in het bijzonder te vernemen:

– of deze verplichting, die op grond van artikel 15, lid 1, van richtlijn 2002/58 is opgelegd, een inmenging vormt die wordt gerechtvaardigd door het „recht op veiligheid" als gewaarborgd door artikel 6 van het Handvest en door de vereisten van nationale veiligheid (eerste vraag in de zaken C-511/18 en C-512/18 en derde vraag in zaak C-511/18);

– of richtlijn 2000/31 de bewaring toestaat van gegevens die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud die online toegankelijk is voor het publiek (tweede vraag in zaak C-512/18).

a) Opmerking vooraf

94. De Conseil d'État verwijst naar de grondrechten die worden erkend in de artikelen 7 (eerbiediging van het privéleven en van het familie- en gezinsleven), 8 (bescherming van persoonsgegevens) en 11 (vrijheid van meningsuiting en informatie) van het Handvest. Naar het oordeel van het Hof zijn dit de rechten die kunnen worden aangetast door de verplichting tot bewaring van verkeersgegevens die door de nationale autoriteiten wordt opgelegd aan aanbieders van elektronischecommunicatiediensten. [47]

95. De verwijzende rechter vermeldt ook het door artikel 6 van het Handvest beschermde recht op veiligheid. Hij beroept er zich niet zozeer op als een recht dat eventueel is aangetast, maar eerder als een factor die het opleggen van die verplichting zou kunnen rechtvaardigen.

96. Ik ben het met de Commissie eens dat het beroep op artikel 6 in die zin dubbelzinnig kan zijn. Net als de Commissie ben ik van mening dat deze bepaling niet aldus mag worden uitgelegd dat zij het mogelijk maakt om „de Unie een positieve verplichting op te leggen om maatregelen te nemen die erop gericht zijn personen te beschermen tegen criminele handelingen". [48]

97. De veiligheid die door dat artikel van het Handvest wordt gewaarborgd, valt niet samen met de openbare veiligheid of, zo men wil, de door het Handvest gewaarborgde veiligheid heeft evenveel met de openbare veiligheid te maken als elk ander grondrecht, aangezien de openbare veiligheid een noodzakelijke voorwaarde is voor de uitoefening van de grondrechten en de fundamentele vrijheden.

98. Zoals de Commissie in herinnering roept, stemt artikel 6 van het Handvest overeen met artikel 5 van het Verdrag tot bescherming van de rechten van de mens (hierna: „EVRM"), hetgeen blijkt uit de toelichtingen bij het Handvest. Uit de lezing van artikel 5 EVRM volgt dat de „veiligheid" die het EVRM beschermt een strikt persoonlijke veiligheid is, die wordt opgevat als een garantie van het recht op fysieke vrijheid tegen willekeurige arrestatie of vasthouding. In wezen komt deze veiligheid erop neer dat niemand van zijn vrijheid mag worden beroofd, behalve in de gevallen, onder de voorwaarden en overeenkomstig de procedures die bij wet zijn voorgeschreven.

47 Aldus het arrest Tele2 Sverige en Watson, punt 92, waarin naar analogie wordt verwezen naar het arrest Digital Rights, punten 25 en 70.
48 Punt 37 van de schriftelijke opmerkingen van de Commissie.

99. Het gaat dus om de *persoonlijke veiligheid*, die betrekking heeft op de voorwaarden waaronder de fysieke vrijheid van personen kan worden beperkt [49], en niet om de *openbare veiligheid* die inherent is aan het bestaan van de staat, die in een ontwikkelde samenleving noodzakelijk is om de uitoefening van het overheidsgezag te verzoenen met de uitoefening van individuele rechten.

100. Sommige regeringen verlangen niettemin dat het recht op veiligheid in de tweede betekenis wordt opgevat. In werkelijkheid is het Hof niet voorbijgegaan aan die betekenis. Het heeft die zelfs uitdrukkelijk vermeld in zijn arresten [50] en adviezen [51]. Het Hof heeft nooit het belang ontkend van de doelstellingen van algemeen belang, zoals de bescherming van de nationale veiligheid en de openbare orde [52], de bestrijding van internationaal terrorisme ter handhaving van de internationale vrede en veiligheid en de bestrijding van ernstige criminaliteit ter waarborging van de openbare veiligheid [53], die het terecht „van primordiaal belang" [54] heeft genoemd. Zoals het Hof destijds opmerkte, „draagt de bescherming van de openbare veiligheid ook bij tot de bescherming van de rechten en vrijheden van anderen". [55]

101. De onderhavige prejudiciële verwijzingen bieden een uitgelezen kans die zou kunnen worden benut om duidelijker voor te stellen hoe een evenwicht kan worden gevonden tussen het recht op veiligheid, enerzijds, en het recht op eerbiediging van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens, anderzijds. Op die manier zou de kritiek worden vermeden dat de laatstgenoemde rechten ten koste gaan van het eerstgenoemde.

102. Naar mijn mening wordt naar dit evenwicht verwezen in overweging 11 en in artikel 15, lid 1, van richtlijn 2002/58, wanneer daarin wordt vermeld dat maatregelen noodzakelijk en evenredig dienen te zijn *in een democratische samenleving*. Nogmaals, het recht op veiligheid is van wezenlijk belang voor het bestaan en het voortbestaan van een democratie, waardoor het gerechtvaardigd is dat er onverkort rekening mee wordt gehouden in de context van de beoordeling van die evenredigheid. Met andere woorden, de bescherming van het beginsel van vertrouwelijkheid van de gegevens in een democratische samenleving is van primordiaal belang, maar ook het belang van de veiligheid van die samenleving mag niet worden onderschat.

103. De context van ernstige en aanhoudende bedreigingen voor de nationale veiligheid, met name terreurgevaar, moet derhalve in aanmerking worden genomen, overeenkomstig hetgeen in de laatste zin van punt 119 van het arrest Tele2 Sverige en Watson is uiteengezet. Een nationaal systeem kan reageren op een wijze die in verhouding staat tot de aard en de intensiteit van de bedreigingen waarmee de staat wordt geconfronteerd, zonder dat deze reactie noodzakelijkerwijs identiek hoeft te zijn aan die van andere lidstaten.

104. Tot slot moet ik hieraan toevoegen dat bovenstaande overwegingen niet uitsluiten dat in strikt *uitzonderlijke* situaties, die worden gekenmerkt door een onmiddellijke dreiging die of een buitengewoon risico dat de officiële afkondiging van een noodsituatie in een lidstaat rechtvaardigt, de nationale wetgeving voorziet in de mogelijkheid om gedurende een beperkte periode een verplichting tot bewaring van gegevens op te leggen die zo ruim en algemeen is als noodzakelijk wordt geacht. [56]

49 Zo luidt de uitlegging van het Europees Hof voor de Rechten van de Mens. Zie zijn arrest van 5 juli 2016, Buzadji tegen Republiek Moldavië (CE:ECHR:2016:0705JUD002375507), waarin het in punt 87 oordeelt dat het fundamentele doel van het door artikel 5 EVRM erkende recht erin bestaat de willekeurige of ongerechtvaardigde vrijheidsbeneming van het individu te voorkomen.

50 Arrest Digital Rights, punt 42.

51 Advies 1/15 (PNR-overeenkomst EU-Canada) van 26 juli 2017 (EU:C:2017:592, punt 149 en aldaar aangehaalde rechtspraak; hierna: „advies 1/15").

52 Arrest van 15 februari 2016, N. (C-601/15 PPU, EU:C:2016:84, punt 53).

53 Arrest Digital Rights, punt 42 en aldaar aangehaalde rechtspraak.

54 Ibidem, punt 51.

55 Advies 1/15, punt 149.

56 Zie de punten 105-107 van mijn conclusie in zaak C-520/18.

105. Bijgevolg moet de eerste vraag in beide prejudiciële verwijzingen zo worden geherformuleerd dat zij betrekking heeft op de mogelijkheid om de inmenging te rechtvaardigen op grond van de nationale veiligheid. Dan is het de vraag of de aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting verenigbaar is met artikel 15, lid 1, van richtlijn 2002/58.

b) Beoordeling

1) Kwalificatie van de nationale regels, zoals die zijn uiteengezet in de twee prejudiciële verwijzingen, in het licht van de rechtspraak van het Hof

106. Uit de verwijzingsbeslissingen blijkt dat de in de hoofdgedingen aan de orde zijnde regeling een verplichting tot bewaring van gegevens oplegt aan:

– exploitanten van elektronischecommunicatiediensten en, met name, personen die online toegang tot communicatiediensten aan het publiek aanbieden, en

– natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de online terbeschikkingstelling aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard.[57]

107. De exploitanten zijn gehouden gedurende één jaar na de datum van registratie ervan gegevens te bewaren aan de hand waarvan de gebruiker kan worden geïdentificeerd, alsmede gegevens betreffende de gebruikte communicatie-eindapparatuur, technische kenmerken, de datum, het tijdstip en de duur van elke oproep, gegevens betreffende de gevraagde of gebruikte aanvullende diensten en hun leveranciers, en gegevens aan de hand waarvan de ontvanger van de communicatie kan worden geïdentificeerd alsook, in het geval van telefonieactiviteiten, de oorsprong en de locatie van de communicatie.[58]

108. Wat met name de internettoegangsdiensten en opslagdiensten betreft, lijkt de nationale wetgeving de bewaring te vereisen van IP-adressen[59], wachtwoorden en, wanneer voor de ondertekening van een contract of het openen van een account moet worden betaald, het soort betaling dat is verricht, alsmede de referentie, het bedrag, de datum en het tijdstip van de transactie[60].

109. Deze verplichting tot bewaring is vereist met het oog op het onderzoeken, vaststellen en vervolgen van strafbare feiten.[61] Met andere woorden, in tegenstelling – zoals zal blijken – tot wat er gebeurt met de verplichting om verkeers- en locatiegegevens te *verzamelen*, is de verplichting om deze gegevens te *bewaren* niet alleen gericht op het voorkomen van terrorisme.[62]

57 Dit volgt uit artikel L. 851-1 van de code de la sécurité intérieure, waarin wordt verwezen naar artikel L. 34-1 van de code des postes et des communications électroniques, en naar artikel 6 van loi n° 2004-575 pour la confiance dans l'économie numérique.

58 Zie artikel R. 10-13 van de code des postes et des communications électroniques.

59 Het staat aan de verwijzende rechter om dit punt, waarover de meningen ter terechtzitting uiteenliepen, na te gaan.

60 Artikel 1 van décret n° 2011-219.

61 Artikel R. 10-13 van de code des postes et des communications électroniques.

62 Zowel La Quadrature du Net als de Fédération des fournisseurs d'accès à Internet associatifs wijst op de omvang van de doelstellingen van de bewaring, de beoordelingsvrijheid die aan de autoriteiten is toegekend, het ontbreken van objectieve criteria in de omschrijving ervan en het belang dat is toegekend aan vormen van criminaliteit die niet als ernstig kunnen worden aangemerkt.

110. Wat de voorwaarden voor *toegang* tot de bewaarde gegevens betreft, blijkt uit de informatie in het procesdossier dat ofwel de voorwaarden van de gewone regeling (optreden van de rechterlijke autoriteit) gelden, ofwel de toegang beperkt is tot individueel aangewezen en gemachtigde personen, nadat de minister-president zijn toestemming heeft gegeven op basis van een niet-bindend advies van een onafhankelijke administratieve autoriteit.[63]

111. Het kan moeilijk worden ontkend dat, zoals de Commissie heeft opgemerkt[64], de gegevens waarvan de bewaring door de nationale regels wordt vereist, in wezen overeenkomen met die welke door het Hof zijn onderzocht in het arrest Digital Rights en het arrest Tele2 Sverige en Watson.[65] Net als toen geldt voor deze gegevens een „verplichting tot algemene en ongedifferentieerde bewaring", zoals de Conseil d'État aan het begin van zijn prejudiciële vragen onomwonden opmerkt.

112. Indien dat het geval is – en dit staat uiteindelijk ter beoordeling van de verwijzende rechter – kan enkel worden geconcludeerd dat de betrokken regeling neerkomt op een „ingreep […] in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten [die] groot [is] en […] als bijzonder ernstig [moet] worden beschouwd".[66]

113. Geen van de partijen heeft betwist dat een dergelijke regeling inmenging in die rechten inhoudt. Het is niet nodig om daar nu bij stil te staan, en zelfs niet om eraan te herinneren dat de inbreuk op die rechten onvermijdelijk leidt tot ondergraving van de fundamenten van een samenleving die ernaar streeft om, naast andere waarden, de door het Handvest gewaarborgde persoonlijke levenssfeer te eerbiedigen.

114. De toepassing van de rechtspraak die is gevestigd met het arrest Tele2 Sverige en Watson en is bevestigd in het arrest Ministerio Fiscal zou er natuurlijk op neerkomen dat een regeling als in het hoofdgeding aan de orde „verder [gaat] dan strikt noodzakelijk is, en […] niet [kan] worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist".[67]

115. Net als de in het arrest Tele2 Sverige en Watson beoordeelde regeling, voorziet de in casu aan de orde zijnde regeling „die algemeen geldt voor alle abonnees en geregistreerde gebruikers en ziet op alle elektronischecommunicatiemiddelen en op alle verkeersgegevens, in geen enkele differentiatie, beperking of uitzondering naargelang van het nagestreefde doel".[68] Bijgevolg „is [zij] dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – verband houdt met ernstige strafbare feiten", en dit zonder enige uitzondering, „zodat zij zelfs van toepassing is op personen van wie de communicaties naar nationaal recht onder het beroepsgeheim vallen".[69]

63 De Commission nationale de contrôle des techniques de renseignement (nationale controlecommissie voor inlichtingentechnieken). Zie in dit verband de punten 145-148 van de schriftelijke opmerkingen van de Franse regering.

64 Punt 60 van de schriftelijke opmerkingen van de Commissie.

65 In werkelijkheid gaan ze nog een stap verder, omdat ze in het geval van internettoegangsdiensten ook de bewaring van IP-adressen of de wachtwoorden lijken te behelzen.

66 Arrest Tele2 Sverige en Watson, punt 100.

67 Ibidem, punt 107.

68 Ibidem, punt 105.

69 Ibidem.

116. Voorts geldt dat de bestreden regeling „geen enkel verband [eist] tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt de bewaring met name niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij de bestrijding van criminaliteit”. [70]

117. Uit het voorgaande volgt dat deze regeling „verder [gaat] dan strikt noodzakelijk is, en […] niet [kan] worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist”. [71]

118. Naar het oordeel van het Hof volstond dit om te concluderen dat betrokken nationale regels niet verenigbaar waren met artikel 15, lid 1, van richtlijn 2002/58, aangezien zij „ter bestrijding van criminaliteit, [voorzagen] in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen.” [72]

119. De vraag die nu rijst is of de rechtspraak van het Hof inzake de bewaring van persoonsgegevens kan worden aangepast, en zo niet, dan toch in elk geval kan worden genuanceerd wanneer terrorismebestrijding het doel is dat met deze „algemene en ongedifferentieerde” bewaring wordt gediend. De eerste vraag in zaak C-511/18 wordt – terecht – gesteld „in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar”.

120. Dit is weliswaar de *feitelijke context* waarin de verplichting tot bewaring van gegevens wordt opgelegd, maar feit is dat in haar *regelgevende context* niet alleen terrorisme in aanmerking wordt genomen. De regeling voor de bewaring van en toegang tot de gegevens die aan de orde is in de procedure voor de Conseil d’État, stelt deze verplichting afhankelijk van de doeleinden van het onderzoek, de vaststelling en de vervolging van strafbare feiten in het algemeen.

121. In elk geval wil ik erop wijzen dat de bestrijding van terrorisme niet buiten beschouwing is gelaten in de argumenten die werden aangevoerd in het arrest Tele2 Sverige en Watson, maar dat het Hof destijds niet van oordeel was dat deze vorm van criminaliteit een wijziging van zijn rechtspraak noodzakelijk maakte. [73]

122. Bijgevolg, en in beginsel, moet de vraag van de verwijzende rechter, die is toegespitst op het specifieke karakter van terreurgevaar, naar mijn mening in dezelfde zin worden beantwoord als de vraag waarover het Hof zich heeft uitgesproken in het arrest Tele2 Sverige en Watson.

123. Zoals ik in mijn conclusie in de zaak Stichting Brein heb opgemerkt, eist „[d]e rechtszekerheid […] van de rechterlijke instanties om, zo niet in absolute zin het stare decisis toe te passen, maar zich in elk geval wel met prudentie te houden aan wat zij zelf, na rijp beraad, over een bepaald juridisch probleem hebben beslist”. [74]

70 Arrest Tele2 Sverige en Watson, punt 106.

71 Ibidem, punt 107.

72 Ibidem, punt 112.

73 Ibidem, punt 103.

74 Zaak C-527/15, EU:C:2016:938, punt 41.

2) Beperkte bewaring van gegevens, in het licht van bedreigingen voor de nationale veiligheid, met inbegrip van terreurgevaar

124. Zou het niettemin mogelijk zijn deze rechtspraak te nuanceren of aan te vullen, gezien de implicaties ervan voor de bestrijding van terrorisme of voor de bescherming van de staat tegen andere soortgelijke bedreigingen voor de nationale veiligheid?

125. Zoals ik reeds heb benadrukt, vormt de loutere bewaring van persoonsgegevens een inmenging in de door de artikelen 7, 8 en 11 van het Handvest gewaarborgde grondrechten.[75] Afgezien van het feit dat met die bewaring uiteindelijk wordt beoogd om met terugwerkende kracht of simultaan de *toegang* tot de gegevens op een bepaald moment mogelijk te maken[76], leidt de loutere bewaring van gegevens die verder gaat dan strikt noodzakelijk is voor de doorgifte van een communicatie of voor de facturering van de door de aanbieder verrichte diensten, ertoe dat de in de artikelen 5 en 6 van richtlijn 2002/58 vastgestelde beperkingen niet worden nageleefd.

126. De gebruikers van deze diensten (in feite bijna alle burgers in de meest ontwikkelde samenlevingen) hebben een gewettigde verwachting of moeten een gewettigde verwachting kunnen hebben dat zonder hun toestemming niet méér hen betreffende gegevens worden bewaard dan die welke overeenkomstig deze voorschriften zijn opgeslagen. De uitzonderingen waarin artikel 15, lid 1, van richtlijn 2002/58 voorziet, moeten vanuit deze premisse worden gelezen.

127. Zoals ik reeds heb uitgelegd, heeft het Hof in het arrest Tele2 Sverige en Watson de algemene en ongedifferentieerde bewaring van persoonsgegevens ook met het oog op de bestrijding van terrorisme afgewezen.[77]

128. In het licht van de kritiek die daarop is geleverd, denk ik niet dat de in dat arrest ontwikkelde rechtspraak de terroristische dreiging onderschat als een vorm van bijzonder ernstige criminaliteit die expliciet tot doel heeft het gezag van de staat te ondermijnen en zijn instellingen te destabiliseren of te vernietigen. De bestrijding van terrorisme is letterlijk van vitaal belang voor de staat, en het welslagen ervan is een doelstelling van algemeen belang waarvan een rechtsstaat geen afstand kan doen.

129. Vrijwel alle in de procedure vertegenwoordigde regeringen en de Commissie zijn het erover eens dat een gedeeltelijke en gedifferentieerde opslag van persoonsgegevens, nog afgezien van de daarmee gepaard gaande technische moeilijkheden, de nationale inlichtingendiensten de mogelijkheid zou ontnemen om toegang te krijgen tot informatie die van essentieel belang is voor de herkenning van bedreigingen voor de openbare veiligheid en de verdediging van de staat, alsmede voor de vervolging van de daders van terroristische aanslagen.[78]

75 Zoals het Hof heeft uiteengezet in Advies 1/15, punt 124, „vormt de mededeling van persoonsgegevens aan een derde, zoals een openbare instantie, een inmenging in het in artikel 7 van het Handvest verankerde grondrecht, ongeacht het latere gebruik van de aldus meegedeelde gegevens. Dit geldt ook voor het bewaren van persoonsgegevens en voor de toegang tot die gegevens met het oog op het gebruik ervan door openbare instanties. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden".

76 Zoals advocaat-generaal Cruz Villalón in zijn conclusie in de zaak Digital Rights, C-293/12 en C-594/12 (EU:C:2013:845, punt 72), heeft opgemerkt, „[vormt] het verzamelen en vooral het bewaren, in gigantische databases, van de talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers van de Unie, een duidelijke inmenging in hun privéleven […], ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun persoonlijke alsook beroepsmatige activiteiten te kunnen controleren. Het verzamelen van deze gegevens creëert de voorwaarden voor een toezicht dat, ook al wordt dit slechts met terugwerkende kracht uitgevoerd bij de exploitatie van de gegevens, niettemin, zolang de gegevens worden bewaard, het recht van de burgers van de Unie op vertrouwelijkheid van hun persoonlijke levenssfeer permanent bedreigt. Het opgewekte vage gevoel van gecontroleerd worden leidt bijzonder acuut tot de vraag wat de bewaringstermijn van de gegevens is".

77 Arrest Tele2 Sverige en Watson, punt 103: „[men kan] niet […] rechtvaardigen dat een nationale regeling die voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens, noodzakelijk wordt geacht voor het voeren van deze strijd".

78 Dat is de uitleg van, bijvoorbeeld, de Franse regering, die deze opvatting illustreert aan de hand van concrete voorbeelden van het nut van algemene gegevensbewaring, waardoor de staat kon reageren op de ernstige terroristische aanslagen van de afgelopen jaren in haar land (punten 107 en 122-126 van de schriftelijke opmerkingen van de Franse regering).

130. In het licht van deze beoordeling lijkt het me gepast om erop te wijzen dat de strijd tegen terrorisme niet alleen mag worden benaderd uit het oogpunt van de doeltreffendheid ervan. Daarin ligt niet alleen de moeilijkheid, maar ook de grootsheid van die strijd, wanneer de gebruikte middelen en methoden voldoen aan de eisen van de rechtsstaat, die er bovenal door wordt gekenmerkt dat macht en kracht worden aangewend binnen de grenzen van het recht en, in het bijzonder, binnen een rechtsorde die aan de verdediging van de grondrechten zowel haar bestaansrecht als haar doel ontleent.

131. Terwijl voor het terrorisme geldt dat de ingezette middelen door geen ander criterium worden gerechtvaardigd dan de zuivere (en maximale) doeltreffendheid van zijn aanvallen op de gevestigde orde, geldt voor de rechtsstaat dat zijn doeltreffendheid wordt gemeten in termen die niet toestaan dat hij bij zijn verdediging procedures en garanties laat varen die van hem een legitieme orde maken. Door zich zonder meer over te geven aan doeltreffendheid alleen, zou de rechtsstaat de deugdelijkheid verliezen die hem onderscheidt en zou hij, in extreme gevallen, zelf een bedreiging voor de burger kunnen worden. Indien de overheid wordt toegerust met buitensporige instrumenten voor de vervolging van criminaliteit, waarmee zij de grondrechten kan negeren of uithollen, zou niets kunnen waarborgen dat haar onbeteugelde en volledig onbelemmerde optreden zich uiteindelijk ontplooit op een wijze die de vrijheid van iedereen aantast.

132. Nogmaals, de doeltreffendheid van het overheidsoptreden wordt gestuit door een onoverkomelijke barrière, namelijk de grondrechten van de burgers, waarvan de uitoefening – zoals bepaald in artikel 52, lid 1, van het Handvest – alleen kan worden onderworpen aan beperkingen die bij wet worden gesteld, die de wezenlijke inhoud van die rechten eerbiedigen, en die „noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen”.[79]

133. Wat de voorwaarden betreft waaronder het volgens het arrest Tele2 Sverige en Watson is toegestaan om gegevens *selectief* te bewaren, verwijs ik naar mijn conclusie in zaak C-520/18.[80]

134. Omstandigheden waarin rechtshandhavingsautoriteiten beschikken over informatie waarmee de ernstige verdenking kan worden hardgemaakt dat een terroristische aanslag wordt voorbereid, kunnen een legitieme basis vormen om een verplichting tot het bewaren van bepaalde gegevens op te leggen. Dit is des te meer het geval wanneer daadwerkelijk een aanslag wordt gepleegd. Terwijl – in dit laatste geval – het plegen van het strafbaar feit op zich een factor kan zijn die de vaststelling van deze maatregel rechtvaardigt, zouden bij een loutere verdenking van een eventuele aanslag de omstandigheden waarop die verdenking is gebaseerd, een minimum aan plausibiliteit moeten bieden, hetgeen van essentieel belang is voor een objectieve beoordeling van de aanwijzingen die deze maatregel kunnen rechtvaardigen.

135. Het is moeilijk maar niet onmogelijk om nauwkeurig en op basis van objectieve criteria te bepalen voor welke categorieën gegevens de bewaring essentieel wordt geacht en op welke groep personen de bewaring moet worden gericht. Uiteraard zou de meest *praktische en doeltreffende* oplossing bestaan in een algemene en ongedifferentieerde bewaring van alle gegevens die door aanbieders van elektronischecommunicatiediensten kunnen worden verzameld maar, zoals ik reeds heb opgemerkt, moet deze kwestie niet worden opgelost in termen van *praktische doeltreffendheid*, maar in termen van *juridische doeltreffendheid* en in de context van de rechtsstaat.

79 Arrest van 15 februari 2016, N. (C-601/15 PPU, EU:C:2016:84, punt 50). Het gaat hier dus om het moeilijke evenwicht tussen de openbare orde en de vrijheid, dat ik reeds heb vermeld en dat in beginsel in alle wetgeving van de Unie wordt nagestreefd, bijvoorbeeld in richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van besluit 2005/671/JBZ van de Raad (PB 2017, L 88, blz. 6). Artikel 20, lid 1, bepaalt dat de lidstaten ervoor moeten zorgen dat degenen die belast zijn met het onderzoek of de vervolging van terroristische misdrijven „beschikken over doeltreffende onderzoeksmiddelen”, maar in overweging 21 wordt verklaard dat bij het gebruik van die doeltreffende middelen „gericht gewerkt [dient] te worden en rekening [dient] te worden gehouden met het evenredigheidsbeginsel en met de aard en de ernst van de misdrijven waarnaar het onderzoek wordt gevoerd, en […] eveneens het recht op bescherming van persoonsgegevens [dient] te worden nageleefd”.

80 Punten 87-95.

136. De taak om het bovenstaande te bepalen, is een typische wetgevingsaangelegenheid, en moet binnen de in de rechtspraak van het Hof gestelde grenzen plaatsvinden. Ook nu verwijs ik naar mijn uiteenzetting hierover in mijn conclusie in zaak C-520/18. [81]

3) Toegang tot bewaarde gegevens

137. Ervan uitgaande dat de exploitanten gegevens hebben verzameld op een wijze die voldoet aan de voorschriften van richtlijn 2002/58 en dat deze gegevens zijn bewaard in overeenstemming met artikel 15, lid 1, ervan [82], moet de toegang van de bevoegde autoriteiten tot deze informatie vervolgens plaatsvinden onder de voorwaarden die het Hof heeft gesteld en die ik analyseer in mijn conclusie in zaak C-520/18, waarnaar ik verwijs. [83]

138. Een nationale regeling moet dus ook in dat geval de materiële en procedurele voorwaarden voor de toegang van de bevoegde autoriteiten tot de bewaarde gegevens bepalen. [84] In het kader van deze prejudiciële verwijzingen zouden deze voorwaarden toegang verlenen tot de gegevens van personen die ervan worden verdacht een terroristische daad te plannen, te gaan plegen of te hebben gepleegd, of bij een dergelijke daad betrokken te zijn. [85]

139. Van wezenlijk belang is al met al dat de toegang tot de gegevens in kwestie, behalve in naar behoren gerechtvaardigde gevallen van spoedeisendheid, wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit die haar beslissing geeft op een met redenen omkleed verzoek van de bevoegde autoriteiten. [86] Zo wordt gegarandeerd dat waar een kwestie niet abstract kan worden beoordeeld door de wet, zij concreet zal worden beoordeeld door deze onafhankelijke autoriteit, die zich in gelijke mate inzet voor het waarborgen van de veiligheid van de staat en de verdediging van de grondrechten van de burgers.

4) Verplichting tot bewaring van gegevens aan de hand waarvan de makers van inhoud kunnen worden geïdentificeerd, in het licht van richtlijn 2000/31 (tweede prejudiciële vraag in zaak C-512/18)

140. De verwijzende rechter verwijst naar richtlijn 2000/31 als referentiepunt om te achterhalen of het mogelijk is bepaalde personen [87] en exploitanten die het publiek communicatiediensten aanbieden, te verplichten tot het bewaren van gegevens „die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, zodat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken om de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven”.

81 Punten 100-107.

82 Met dien verstande dat aan de in punt 122 van het arrest Tele2 Sverige en Watson genoemde voorwaarden is voldaan: het Hof heeft erop gewezen dat artikel 15, lid 1, van richtlijn 2002/58 niet toestaat om af te wijken van artikel 4, leden 1 en 1 bis, van die richtlijn, op grond waarvan deze aanbieders maatregelen moeten treffen om de bewaarde gegevens doeltreffend te beschermen tegen het risico van misbruik en tegen onrechtmatige toegang tot deze gegevens. Het Hof heeft in die zin verklaard: „Gelet op de hoeveelheid bewaarde gegevens, op het gevoelige karakter van deze gegevens en op het risico van onrechtmatige toegang tot deze gegevens, moeten de aanbieders van elektronischecommunicatiediensten, om de volle integriteit en vertrouwelijkheid van die gegevens te verzekeren, door middel van passende technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging waarborgen. In het bijzonder moet de nationale regeling bepalen dat de gegevens op het grondgebied van de Unie worden bewaard en na afloop van de bewaarperiode onherstelbaar worden vernietigd.”

83 Punten 52-60.

84 Arrest Tele2 Sverige en Watson, punt 118.

85 Ibidem, punt 119.

86 Ibidem, punt 120.

87 Personen die „met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard”.

141. Ik ben het met de Commissie eens dat het ongepast zou zijn om de verenigbaarheid van deze verplichting met richtlijn 2000/31 te onderzoeken [88], aangezien artikel 1, lid 5, onder b), van deze richtlijn „kwesties in verband met diensten van de informatiemaatschappij die onder richtlijn 95/46/EG en richtlijn 97/66/EG vallen" van de werkingssfeer ervan uitsluit – die handelingen stemmen thans overeen met verordening nr. 2016/679 en richtlijn 2002/58 [89], waarvan artikel 23, lid 1, respectievelijk artikel 15, lid 1, naar mijn mening dienen te worden uitgelegd op de wijze die hierboven is uiteengezet.

2. Verplichting om in real time verkeers- en locatiegegevens te verzamelen (tweede prejudiciële vraag in zaak C-511/18)

142. Volgens de verwijzende rechter staat artikel L. 851-2 van de code de la sécurité intérieure toe dat, uitsluitend ter voorkoming van terrorisme, in real time informatie wordt opgevraagd met betrekking tot personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging. Evenzo mogen exploitanten op grond van artikel L. 851-4 van de code de la sécurité intérieure, in real time technische gegevens doorgeven over de locatie van de eindapparatuur.

143. Naar het oordeel van de verwijzende rechter leggen deze technieken de leveranciers geen extra bewaringsverplichting op naast wat noodzakelijk is voor de facturering en commercialisering van hun diensten.

144. Bovendien bepaalt artikel L. 851-3 van de code de la sécurité intérieure dat exploitanten van elektronischecommunicatiemiddelen en aanbieders van technische diensten kunnen worden verplicht „om op hun netwerken geautomatiseerde bewerkingen toe te passen die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken". Deze techniek houdt geen algemene en ongedifferentieerde bewaring van gegevens in en is bedoeld om gedurende een welbepaalde periode verbindingsgegevens te verzamelen die in verband kunnen worden gebracht met een misdrijf van terroristische aard.

145. Mijns inziens moeten de voorwaarden voor toegang tot bewaarde persoonsgegevens ook van toepassing zijn op de toegang in real time tot gegevens die in het kader van elektronische communicatie worden gegenereerd. Ik verwijs daarom naar wat er over dit onderwerp is gezegd. De vraag of de gegevens worden bewaard dan wel onmiddellijk worden verkregen, is irrelevant, aangezien in beide gevallen kennis wordt genomen van persoonsgegevens, ongeacht of deze oud of actueel zijn.

146. Met name wanneer de toegang in real time het resultaat is van verbindingen die zijn gedetecteerd door middel van een geautomatiseerde verwerking, zoals bedoeld in artikel L. 851-3 van de code de la sécurité intérieure, moeten de vooraf vastgestelde modellen en criteria voor een dergelijke verwerking specifiek, betrouwbaar en niet-discriminerend zijn teneinde de identificatie te vergemakkelijken van personen ten aanzien van wie er een redelijk vermoeden bestaat dat zij betrokken zijn bij terroristische activiteiten. [90]

88 Deze richtlijn wordt in algemene bewoordingen en zonder vermelding van een specifieke bepaling door de verwijzende rechter genoemd in de tweede vraag in zaak C-512/18.

89 Punten 112 en 113 van de schriftelijke opmerkingen van de Commissie.

90 Arrest Digital Rights, punt 59.

3. Verplichting om de betrokkenen te informeren (derde prejudiciële vraag in zaak C-511/18)

147. Het Hof heeft geoordeeld dat de autoriteiten die toegang krijgen tot de gegevens, de betrokkenen daarvan op de hoogte moeten brengen wanneer zulks de lopende onderzoeken niet in gevaar kan brengen. Deze plicht is ingegeven door het feit dat deze informatie noodzakelijk is om de betrokken personen in staat te stellen om, in geval van schending van hun rechten, gebruik te maken van het recht van beroep, waarin artikel 15, lid 2, van richtlijn 2002/58 uitdrukkelijk voorziet. [91]

148. De Conseil d'État wenst met zijn derde vraag in zaak C-511/18 te vernemen of dit informatievereiste in elk geval absoluut noodzakelijk is dan wel of ervan kan worden afgezien wanneer is voorzien in andere waarborgen, zoals die welke zijn beschreven in zijn verwijzingsbeslissing.

149. Uit de uiteenzetting van de verwijzende rechter [92] blijkt dat de vermelde garanties erop neerkomen dat personen die willen nagaan of een inlichtingentechniek onrechtmatig is toegepast, de mogelijkheid hebben zich tot de Conseil d'État zelf te wenden. Deze instantie kan in voorkomend geval de machtiging voor de maatregel nietig verklaren en de vernietiging van de ingewonnen gegevens bevelen in het kader van een procedure die niet voorziet in het beginsel van hoor en wederhoor dat gewoonlijk geldt in gerechtelijke procedures.

150. Volgens de verwijzende rechter schendt deze regeling het recht op effectieve rechterlijke bescherming niet. Ik ben echter van mening dat dit – in theorie – inderdaad juist zou kunnen zijn voor personen die besluiten om na te gaan of zij het voorwerp zijn van een inlichtingenoperatie. Dit recht wordt daarentegen niet in acht genomen wanneer de personen die het voorwerp zijn of waren van een dergelijke operatie niet daarvan in kennis worden gesteld, en zij zich dus niet eens kunnen afvragen of hun rechten al dan niet zijn geschonden.

151. De door de verwijzende rechter genoemde rechterlijke waarborgen lijken pas te gelden wanneer het initiatief wordt genomen door de persoon die vermoedt dat er informatie over hem wordt ingewonnen. Iedereen moet echter daadwerkelijke toegang tot de rechter hebben ten behoeve van de bescherming van zijn rechten, hetgeen betekent dat een persoon van wie de persoonsgegevens zijn verwerkt, de mogelijkheid moet hebben om de rechtmatigheid van die verwerking in rechte te betwisten en, bijgevolg, op de hoogte moet worden gebracht van het bestaan van die verwerking.

152. Uit de verstrekte informatie blijkt dat er weliswaar ambtshalve of door middel van een administratieve klacht een juridische procedure kan worden ingesteld, maar de betrokkene moet in elk geval de mogelijkheid krijgen om zelf die juridische procedure in te stellen, en daarvoor moet hij ervan in kennis zijn gesteld dat zijn persoonsgegevens in zekere mate zijn verwerkt. Voor de bescherming van zijn rechten kan een persoon zich niet verlaten op het feit dat hij via derden of met eigen middelen kennis krijgt van een dergelijke verwerking.

153. Voor zover het verloop van het onderzoek in het kader waarvan toegang tot bewaarde gegevens is verleend niet in het gedrang komt, moet de betrokkene dus in kennis worden gesteld van deze toegang.

154. De zaken liggen anders wanneer de betrokkene een rechtsvordering instelt, nadat hij in kennis is gesteld van de toegang tot zijn gegevens. Dan moet de daaropvolgende gerechtelijke procedure voldoen aan de vereisten van vertrouwelijkheid en geheimhouding die inherent zijn aan de controle op het optreden van de overheid op gevoelige gebieden zoals de staatsveiligheid en landsverdediging. Deze kwestie heeft echter niets van doen met de onderhavige prejudiciële verwijzingen, zodat het Hof hier mijns inziens geen uitspraak over hoeft te doen.

91 Arrest Tele2 Sverige en Watson, punt 121.

92 Punten 8-11 van de verwijzingsbeslissing.

V. Conclusie

155. Gelet op het bovenstaande geef ik het Hof in overweging om de vragen van de Conseil d'État te beantwoorden als volgt:

„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 betreffende privacy en elektronische communicatie), gelezen in samenhang met de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat:

1) het zich verzet tegen een nationale regeling die, in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar, aan exploitanten en aanbieders van elektronischecommunicatiediensten de verplichting oplegt tot algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens van alle abonnees, en van de gegevens die het mogelijk maken om de identiteit vast te stellen van de makers van de inhoud die door de aanbieders van deze diensten wordt aangeboden;

2) het zich verzet tegen een nationale regeling die niet voorziet in de verplichting om de betrokkenen te informeren over de verwerking van hun persoonsgegevens door de bevoegde autoriteiten voor zover deze mededeling het optreden van deze autoriteiten niet in gevaar brengt;

3) het zich niet verzet tegen een nationale regeling op grond waarvan in real time verkeers- en locatiegegevens over individuele personen kunnen worden verzameld voor zover deze handelingen worden verricht volgens de procedures voor toegang tot rechtmatig bewaarde persoonsgegevens en met dezelfde waarborgen worden omringd."