Jurisprudentie

ARREST VAN HET HOF (Grote kamer)

6 oktober 2020*

[Zoals gerectificeerd bij beschikking van 16 november 2020]

Inhoud

* Procestaal: Frans.

„Prejudiciële verwijzing – Verwerking van persoonsgegevens in de sector elektronische communicatie – Aanbieders van elektronischecommunicatiediensten – Aanbieders van opslagdiensten en aanbieders van toegang tot het internet – Algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens – Geautomatiseerde analyse van de gegevens – Toegang in real time tot de gegevens – Bescherming van de nationale veiligheid en bestrijding van terrorisme – Bestrijding van criminaliteit – Richtlijn 2002/58/EG – Werkingssfeer – Artikel 1, lid 3, en artikel 3 – Vertrouwelijk karakter van elektronische communicatie – Bescherming – Artikel 5 en artikel 15, lid 1 – Richtlijn 2000/31/EG – Werkingssfeer – Handvest van de grondrechten van de Europese Unie – Artikelen 4, 6 tot en met 8 en 11 en artikel 52, lid 1 – Artikel 4, lid 2, VEU”

In de gevoegde zaken C-511/18, C-512/18 en C-520/18,

betreffende verzoeken om een prejudiciële beslissing krachtens artikel 267 VWEU, ingediend door de Conseil d'État (hoogste bestuursrechter, Frankrijk) bij beslissingen van 26 juli 2018, ingekomen bij het Hof op 3 augustus 2018 (C-511/18 en C-512/18), en door het Grondwettelijk Hof (België) bij beslissing van 19 juli 2018, ingekomen bij het Hof op 2 augustus 2018 (C-520/18), in de procedures

La Quadrature du Net (C-511/18 en C-512/18),

French Data Network (C-511/18 en C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 en C-512/18),

Igwan.net (C-511/18)

tegen

Premier ministre (C-511/18 en C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 en C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18),

in tegenwoordigheid van:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

en

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten VZW,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

tegen

Ministerraad,

in tegenwoordigheid van:

Child Focus (C-520/18),

wijst

HET HOF (Grote kamer),

samengesteld als volgt: K. Lenaerts, president, R. Silva de Lapuerta, vicepresident, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb en L. S. Rossi, kamerpresidenten, J. Malenovský, L. Bay Larsen, T. von Danwitz (rapporteur), C. Toader, K. Jürimäe, C. Lycourgos en N. Piçarra, rechters,

advocaat-generaal: M. Campos Sánchez-Bordona,

griffier: C. Strömholm, administrateur,

gezien de stukken en na de terechtzitting op 9 en 10 september 2019,

gelet op de opmerkingen van:

– La Quadrature du Net, de Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net en het Center for Democracy and Technology, vertegenwoordigd door A. Fitzjean Ò Cobhthaigh, avocat,

– French Data Network, vertegenwoordigd door Y. Padova, avocat,

– Privacy International, vertegenwoordigd door H. Roy, avocat,

– de Ordre des barreaux francophones et germanophone, vertegenwoordigd door E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart en J.-F. Henrotte, avocats,

– de Académie Fiscale ASBL en UA, vertegenwoordigd door J.-P. Riquet,

– de Liga voor Mensenrechten VZW, vertegenwoordigd door J. Vander Velpen, advocaat,

– de Ligue des Droits de l'Homme ASBL, vertegenwoordigd door R. Jespers en J. Fermon, avocats,

– VZ, WY en XX, vertegenwoordigd door D. Pattyn, advocaat,

– Child Focus, vertegenwoordigd door N. Buisseret, K. de Meester en J. van Cauter, advocaten,

– de Franse regering, aanvankelijk vertegenwoordigd door D. Dubois, F. Alabrune, D. Colas, E. de Moustier en A.-L. Desjonquères, vervolgens door D. Dubois, F. Alabrune, E. de Moustier en A.-L. Desjonquères als gemachtigden,

– de Belgische regering, vertegenwoordigd door J.-C. Halleux, P. Cottin en C. Pochet als gemachtigden, bijgestaan door J. Vanpraet, Y. Peeters, S. Depré en E. de Lophem, avocats,

– de Tsjechische regering, vertegenwoordigd door M. Smolek, J. Vláčil en O. Serdula als gemachtigden,

– de Deense regering, aanvankelijk vertegenwoordigd door J. Nymann-Lindegren, M. Wolff en P. Ngo, vervolgens door J. Nymann-Lindegren en M. Wolff als gemachtigden,

– de Duitse regering, aanvankelijk vertegenwoordigd door J. Möller, M. Hellmann, E. Lankenau, R. Kanitz en T. Henze, vervolgens door J. Möller, M. Hellmann, E. Lankenau en R. Kanitz als gemachtigden,

– de Estse regering, vertegenwoordigd door N. Grünberg en A. Kalbus als gemachtigden,

– de Ierse regering, vertegenwoordigd door A. Joyce, M. Browne en G. Hodge als gemachtigden, bijgestaan door D. Fennelly, BL,

– de Spaanse regering, aanvankelijk vertegenwoordigd door L. Aguilera Ruiz en A. Rubio González, vervolgens door L. Aguilera Ruiz als gemachtigden,

– de Cypriotische regering, vertegenwoordigd door E. Neofytou als gemachtigde,

– de Letse regering, vertegenwoordigd door V. Soņeca als gemachtigde,

– de Hongaarse regering, aanvankelijk vertegenwoordigd door M. Z. Fehér en Z. Wagner, vervolgens door M. Z. Fehér als gemachtigden,

– de Nederlandse regering, vertegenwoordigd door M. K. Bulterman en M. A. M. de Ree als gemachtigden,

– de Poolse regering, vertegenwoordigd door B. Majczyna, J. Sawicka en M. Pawlicka als gemachtigden,

– de Zweedse regering, aanvankelijk vertegenwoordigd door H. Shev, H. Eklinder, C. Meyer-Seitz en A. Falk, vervolgens door H. Shev, H. Eklinder, C. Meyer-Seitz en J. Lundberg als gemachtigden,

– de regering van het Verenigd Koninkrijk, vertegenwoordigd door S. Brandon als gemachtigde, bijgestaan door G. Facenna, QC, en C. Knight, barrister,

[streepje ingetrokken bij beschikking van 16 november 2020]

– de Europese Commissie, aanvankelijk vertegenwoordigd door H. Kranenborg, M. Wasmeier en P. Costa de Oliveira, vervolgens door H. Kranenborg en M. Wasmeier als gemachtigden,

– de Europese Toezichthouder voor gegevensbescherming, vertegenwoordigd door T. Zerdick en A. Buchta als gemachtigden,

gehoord de conclusie van de advocaat-generaal ter terechtzitting van 15 januari 2020,

het navolgende

Arrest

1 De verzoeken om een prejudiciële beslissing betreffen de uitlegging van 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) (PB 2002, L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (PB 2009, L 337, blz. 11) (hierna: „richtlijn 2002/58”), en van de artikelen 12 tot en met 15 van richtlijn 2000/31/EG 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), gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 4, 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”).

2 Het verzoek in zaak C-511/18 is ingediend in het kader van gedingen tussen La Quadrature du Net, French Data Network, de Fédération des fournisseurs d'accès à Internet associatifs en Igwan.net, enerzijds, en de Premier ministre (eerste minister, Frankrijk), de Garde des Sceaux, ministre de la Justice (minister van Justitie, Frankrijk), de ministre de l'Intérieur (minister van Binnenlandse Zaken, Frankrijk) en de ministre des Armées (minister van de Strijdkrachten, Frankrijk), anderzijds, over de rechtmatigheid van décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (decreet nr. 2015-1185 van 28 september 2015 houdende aanwijzing van de gespecialiseerde inlichtingendiensten) (JORF van 29 september 2015, tekst 1 van 97; hierna: „decreet nr. 2015-1185"), décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (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) (JORF van 2 oktober 2015, tekst 7 van 108; hierna: „decreet nr. 2015-1211"), décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (decreet nr. 2015-1639 van 11 december 2015 tot aanwijzing van de andere diensten dan de gespecialiseerde inlichtingendiensten, die gemachtigd zijn om gebruik te maken van de in boek VIII, titel V, van de code de la sécurité intérieure genoemde technieken, vastgesteld op grond van artikel L. 811-4 van de code de la sécurité intérieure) (JORF van 12 december 2015, tekst 28 van 127; hierna: „decreet nr. 2015-1639"), en décret nº 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) (JORF van 31 januari 2016, tekst 2 van 113; hierna: „decreet nr. 2016-67").

3 Het verzoek in zaak C-512/18 is ingediend in het kader van gedingen tussen French Data Network, La Quadrature du Net en de Fédération des fournisseurs d'accès à Internet associatifs, enerzijds, en de Premier ministre (eerste minister, Frankrijk) en de Garde des Sceaux, ministre de la justice (minister van Justitie, Frankrijk), anderzijds, over de rechtmatigheid van artikel R. 10-13 van de code des postes et des communications électroniques (wetboek post en elektronische communicatie; hierna: „CPCE") en van 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 (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) (JORF van 1 maart 2011, tekst 32 van 170; hierna: „decreet nr. 2011-219").

4 Het verzoek in zaak C-520/18 is ingediend in het kader van gedingen tussen de Ordre des barreaux francophones et germanophone, de Académie Fiscale ASBL, UA, de Liga voor Mensenrechten VZW, de Ligue des Droits de l'Homme ASBL, VZ, WY en XX, enerzijds, en de Ministerraad (België), anderzijds, over de rechtmatigheid van de Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (*Belgisch Staatsblad*, 18 juli 2016, blz. 44717; hierna: „wet van 29 mei 2016").

Toepasselijke bepalingen

Unierecht

Richtlijn 95/46

5 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281, blz. 31) is met ingang van 25 mei 2018 ingetrokken bij verordening (EU) 2016/679 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). Artikel 3, lid 2, van richtlijn 95/46 luidde als volgt:

„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 zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie 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;

– die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht."

6 Artikel 22 van richtlijn 95/46, dat was opgenomen in hoofdstuk III („Beroep op de rechter, aansprakelijkheid en sancties") van deze richtlijn, bepaalde:

„Onverminderd de administratieve voorziening die met name bij de in artikel 28 bedoelde toezichthoudende autoriteit kan worden getroffen voordat de zaak aanhangig wordt gemaakt voor de rechter, bepalen de lidstaten dat eenieder zich tot de rechter kan wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden."

Richtlijn 97/66

7 Artikel 5 van richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (PB 1997, L 24, blz. 1), met het opschrift „Vertrouwelijk karakter van de oproepen", luidde als volgt:

„1. De lidstaten garanderen in hun nationale reglementering het vertrouwelijk karakter van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers, indien de betrokken gebruikers daarmee niet hebben ingestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 14, lid 1.

2. Lid 1 is niet van toepassing op de wettelijk toegestane registratie van oproepen in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van enigerlei andere zakelijke oproep."

Richtlijn 2000/31

8 In de overwegingen 14 en 15 van richtlijn 2000/31 staat te lezen:

„(14) De bescherming van individuen met betrekking tot de verwerking van persoonsgegevens is alleen geregeld bij [richtlijn 95/46] en bij [richtlijn 97/66], die volledig van toepassing zijn op diensten van de informatiemaatschappij. Die richtlijnen vormen reeds een communautair wettelijk kader op het gebied van persoonsgegevens, en het is daarom niet nodig die kwestie in deze richtlijn op te nemen om een soepele werking van de interne markt te garanderen, met name wat betreft het vrije verkeer van persoonsgegevens tussen lidstaten. Deze richtlijn moet worden uitgevoerd en toegepast met volledige inachtneming van de beginselen inzake de

bescherming van persoonsgegevens, met name wat ongevraagde commerciële communicatie en de aansprakelijkheid van tussenpersonen betreft. Deze richtlijn kan het anonieme gebruik van open netwerken zoals Internet niet voorkomen.

(15) De vertrouwelijkheid van berichten wordt gewaarborgd door artikel 5 van [richtlijn 97/66]. Op basis van die richtlijn moeten de lidstaten iedere vorm van onderschepping of bewaking van deze berichten door andere personen dan de verzender en de adressaat verbieden, tenzij dit wettelijk toegestaan is."

9 Artikel 1 van richtlijn 2000/31 bepaalt:

„1. Deze richtlijn heeft tot doel bij te dragen aan de goede werking van de interne markt door het vrije verkeer van de diensten van de informatiemaatschappij tussen lidstaten te waarborgen.

2. Voor zover voor de verwezenlijking van de in lid 1 genoemde doelstelling nodig, worden met deze richtlijn bepaalde nationale bepalingen nader tot elkaar gebracht die van toepassing zijn op de diensten van de informatiemaatschappij en betrekking hebben op de interne markt, de vestiging van de dienstverleners, de commerciële communicatie, langs elektronische weg gesloten contracten, de aansprakelijkheid van tussenpersonen, gedragscodes, de buitengerechtelijke geschillenregeling, rechtsgedingen en de samenwerking tussen lidstaten.

3. Deze richtlijn vormt een aanvulling op het communautaire recht dat van toepassing is op de diensten van de informatiemaatschappij en doet niet af aan het in de communautaire besluiten en nationale wetgeving ter uitvoering daarvan vastgelegde niveau van bescherming, inzonderheid van de volksgezondheid en de consumentenbelangen, voor zover de vrijheid om diensten van de informatiemaatschappij te verlenen daardoor niet beperkt wordt.

[...]

5. Deze richtlijn is niet van toepassing op:

[...]

b) kwesties in verband met diensten van de informatiemaatschappij die onder [richtlijn 95/46] en [richtlijn 97/66] vallen;

[...]"

10 Artikel 2 van richtlijn 2000/31 luidt als volgt:

„Voor de doeleinden van deze richtlijn wordt verstaan onder:

a) ‚diensten van de informatiemaatschappij': diensten zoals omschreven in artikel 1, lid 2, van richtlijn 98/34/EG [van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (PB 1998, L 204, blz. 37)], zoals gewijzigd bij richtlijn 98/48/EG [van het Europees Parlement en de Raad van 20 juli 1998 (PB 1998, L 217, blz. 18)];

[...]"

11 Artikel 15 van richtlijn 2000/31 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."

Richtlijn 2002/21

12 In overweging 10 van richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten (kaderrichtlijn) (PB 2002, L 108, blz. 33) wordt verklaard:

„De definitie van ‚dienst van de informatiemaatschappij' in artikel 1 van [richtlijn 98/34, zoals gewijzigd bij richtlijn 98/48,] bestrijkt een breed scala van economische activiteiten die online plaatsvinden; de meeste van deze activiteiten vallen niet binnen de werkingssfeer van de onderhavige richtlijn omdat zij niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronischecommunicatienetwerken; spraaktelefonie en de diensten voor het overbrengen van elektronische post vallen onder deze richtlijn; dezelfde onderneming, bijvoorbeeld een verstrekker van internetdiensten, kan een elektronischecommunicatiedienst aanbieden, zoals de toegang tot internet, en diensten die niet onder deze richtlijn vallen, zoals de levering van internet-inhoud."

13 Artikel 2 van richtlijn 2002/21 bepaalt:

„Voor de toepassing van deze richtlijn wordt verstaan onder:

[...]

c) ‚elektronischecommunicatiedienst': een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van [richtlijn 98/34], die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronischecommunicatienetwerken;

[...]"

Richtlijn 2002/58

14 In de overwegingen 2, 6, 7, 11, 22, 26 en 30 van richtlijn 2002/58 staat te lezen:

„(2) Deze richtlijn strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het [Handvest]. In het bijzonder strekt deze richtlijn tot volledige eerbiediging van de in de artikelen 7 en 8 [van het Handvest] bedoelde rechten.

[...]

(6) Het internet vervangt traditionele marktstructuren door te voorzien in een gemeenschappelijke, wereldwijde infrastructuur voor de levering van een breed scala van elektronischecommunicatiediensten. Algemeen beschikbare elektronischecommunicatiediensten via het internet bieden de gebruikers nieuwe mogelijkheden, maar houden ook nieuwe gevaren in voor de bescherming van hun persoonsgegevens en persoonlijke levenssfeer.

(7) Voor openbare communicatienetwerken moeten specifieke wettelijke, bestuursrechtelijke en technische bepalingen worden vastgesteld teneinde de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen te beschermen tegen met name de steeds grotere mogelijkheden in verband met de geautomatiseerde opslag en verwerking van gegevens met betrekking tot de abonnees en de gebruikers.

[...]

(11) Deze richtlijn is evenmin als [richtlijn 95/46] van toepassing op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het [Unierecht] vallende activiteiten. Zij 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 openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied. Bijgevolg doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het [op 4 november 1950 te Rome ondertekende] Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals geïnterpreteerd in de uitspraken van het Europees Hof voor de rechten van de mens, in acht nemen. Zulke maatregelen dienen passend te zijn voor, en strikt evenredig met, het beoogde doel en noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

[...]

(22) Het verbod op het opslaan van communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers of zonder hun toestemming is niet bedoeld om de automatische, tussentijdse en tijdelijke opslag van die informatie te verbieden, voor zover deze opslag uitsluitend dient voor het doorzenden in het elektronischecommunicatienetwerk en mits de informatie niet langer wordt opgeslagen dan nodig voor het doorzenden en het beheer van het verkeer, en het vertrouwelijk karakter tijdens de opslag gewaarborgd blijft. [...]

[...]

(26) De gegevens over abonnees die in elektronischecommunicatienetwerken worden verwerkt om verbindingen tot stand te brengen en informatie over te dragen, bevatten informatie over het privéleven van natuurlijke personen en betreffen het recht op respect voor hun correspondentie of de rechtmatige belangen van rechtspersonen. Dergelijke gegevens mogen slechts worden opgeslagen voor zover dat nodig is voor het leveren van de dienst, voor facturering en voor interconnectiebetalingen, en slechts gedurende een beperkte tijd. Elke verdere verwerking van dergelijke gegevens [...] is slechts toegestaan indien de abonnee daarmee heeft ingestemd op basis van precieze en volledige informatie van de aanbieder van de openbare elektronischecommunicatiedienst over de door hem geplande verdere verwerking van de

gegevens en over het recht van de abonnee een dergelijke verwerking niet toe te staan of de toestemming daartoe in te trekken. Verkeersgegevens die worden gebruikt voor de marketing van communicatiediensten [...] moeten ook worden gewist of anoniem gemaakt [...].

[...]

(30) Systemen voor elektronischecommunicatienetwerken en -diensten moeten op dusdanige wijze worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. [...]"

15 Artikel 1 („Werkingssfeer en doelstelling") van richtlijn 2002/58 bepaalt:

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

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

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het [VWEU] vallen, zoals die bedoeld in de titels V en VI van het 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."

16 Artikel 2 („Definities") van richtlijn 2002/58 luidt:

„Tenzij anders is bepaald, zijn de definities van [richtlijn 95/46] en [richtlijn 2002/21] van toepassing.

Daarnaast wordt in deze richtlijn verstaan onder:

a) ‚gebruiker': natuurlijke persoon die gebruikmaakt van een openbare elektronischecommunicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

b) ‚verkeersgegevens': gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronischecommunicatienetwerk of voor de facturering ervan;

c) ‚locatiegegevens': gegevens die in een elektronischecommunicatienetwerk of door een elektronischecommunicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronischecommunicatiedienst wordt aangegeven;

d) ‚communicatie': informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronischecommunicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronischecommunicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

[...]"

17 Artikel 3 („Betrokken diensten") van richtlijn 2002/58 bepaalt:

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

18 In artikel 5 („Vertrouwelijk karakter van de communicatie") van die richtlijn staat:

„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 elektronischecommunicatiediensten. 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.

[...]

3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig [richtlijn 95/46], onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert."

19 Artikel 6 („Verkeersgegevens") van richtlijn 2002/58 bepaalt:

„1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronischecommunicatienetwerk 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.

3. De aanbieder van een openbare elektronischecommunicatiedienst mag ten behoeve van de marketing van elektronischecommunicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

[...]

5. De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken

om inlichtingen van klanten, opsporing van fraude en marketing van elektronischecommunicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren."

20 Artikel 9 („Andere locatiegegevens dan verkeersgegevens") van die richtlijn bepaalt in lid 1:

„Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronischecommunicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. [...]"

21 Artikel 15 („Toepassing van een aantal bepalingen van [richtlijn 95/46]") van richtlijn 2002/58 bepaalt:

„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 elektronischecommunicatiesysteem als bedoeld in artikel 13, lid 1, van [richtlijn 95/46]. 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 [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

[...]

2. Het bepaalde in hoofdstuk III van [richtlijn 95/46] inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

[...]"

Verordening 2016/679

22 In overweging 10 van verordening 2016/679 wordt verklaard:

„Teneinde natuurlijke personen een consistent en hoog beschermingsniveau te bieden en de belemmeringen voor het verkeer van persoonsgegevens binnen de Unie op te heffen, dient het niveau van bescherming van de rechten en vrijheden van natuurlijke personen op het vlak van verwerking van deze gegevens in alle lidstaten gelijkwaardig te zijn. Er moet gezorgd worden voor een in de gehele Unie coherente en homogene toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens. [...]"

23 Artikel 2 van die verordening bepaalt:

„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;

[...]

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.

[...]

4. Deze verordening laat de toepassing van [richtlijn 2000/31], en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet."

24 Artikel 4 van verordening 2016/679 luidt als volgt:

„Voor de toepassing van deze verordening wordt verstaan onder:

1) ‚persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‚de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) ‚verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

[...]"

25 Artikel 5 van die verordening bepaalt:

„1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (‚rechtmatigheid, behoorlijkheid en transparantie');

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (‚doelbinding');

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (‚minimale gegevensverwerking');

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (‚juistheid');

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (‚opslagbeperking');

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (‚integriteit en vertrouwelijkheid').

[...]"

26 Artikel 6 van verordening 2016/679 luidt als volgt:

„1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

[...]

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

[...]

3. De rechtsgrond voor de in lid 1, [onder] c) en e), bedoelde verwerking moet worden vastgesteld bij:

a) Unierecht; of

b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

Het doel van de verwerking wordt in die rechtsgrond vastgesteld [...]. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen

voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

[...]"

27 Artikel 23 van die verordening bepaalt:

„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 punten a), tot en met e) en punt g) bedoelde gevallen;

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

j) de inning van civielrechtelijke vorderingen.

2. De in lid 1 bedoelde wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste:

a) de doeleinden van de verwerking of van de categorieën van verwerking,

b) de categorieën van persoonsgegevens,

c) het toepassingsgebied van de ingevoerde beperkingen,

d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,

e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken,

f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking,

g) de risico's voor de rechten en vrijheden van de betrokkenen, en

h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking."

28 Artikel 79, lid 1, van dezelfde verordening bepaalt:

„Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, waaronder het recht uit hoofde van artikel 77 een klacht in te dienen bij een toezichthoudende autoriteit, heeft elke betrokkene het recht een doeltreffende voorziening in rechte in te stellen indien hij van mening is dat zijn rechten uit hoofde van deze verordening geschonden zijn ten gevolge van een verwerking van zijn persoonsgegevens die niet aan deze verordening voldoet."

29 In artikel 94 van verordening 2016/679 staat:

„1. [Richtlijn 95/46] wordt met ingang van 25 mei 2018 ingetrokken.

2. Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening. Verwijzingen naar de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, die bij artikel 29 van [richtlijn 95/46] is opgericht, gelden als verwijzingen naar het bij deze verordening opgerichte Europees Comité voor gegevensbescherming."

30 Artikel 95 van die verordening bepaalt:

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

Frans recht

CSI

31 Boek VIII van het deel „wetgeving" van de code de la sécurité intérieure (wetboek binnenlandse veiligheid; hierna: „CSI") bevat in de artikelen L. 801-1 tot en met L. 898-1 regels betreffende het inwinnen van inlichtingen.

32 Artikel L. 811-3 CSI bepaalt:

„Uitsluitend met het oog op de uitoefening van hun respectieve taken kunnen de gespecialiseerde inlichtingendiensten gebruikmaken van de in titel V van dit boek genoemde technieken voor het inwinnen van inlichtingen betreffende de verdediging en bevordering van de volgende fundamentele staatsbelangen:

1° de nationale onafhankelijkheid, de integriteit van het grondgebied en de landsverdediging;

2° de zwaarwegende belangen van het buitenlands beleid, de nakoming door Frankrijk van zijn Europese en internationale verplichtingen, en de voorkoming van elke vorm van buitenlandse inmenging;

3° de zwaarwegende economische, industriële en wetenschappelijke belangen van Frankrijk;

4° de voorkoming van terrorisme;

5° de voorkoming van:
a) aanvallen op de republikeinse vorm van de instituties;
b) acties die gericht zijn op het in stand houden of opnieuw oprichten van groeperingen die overeenkomstig artikel L. 212-1 zijn ontbonden;
c) collectieve gewelddadigheden die de openbare vrede ernstig ondermijnen;

6° de voorkoming van georganiseerde misdaad;

7° de voorkoming van de verspreiding van massavernietigingswapens."

33 Artikel L. 811-4 CSI luidt als volgt:

„Bij decreet vastgesteld na advies van de Conseil d'État [(hoogste bestuursrechter, Frankrijk)] en van de Commission nationale de contrôle des techniques de renseignement [(nationale commissie voor toezicht op inlichtingentechnieken)], worden de andere diensten dan de gespecialiseerde inlichtingendiensten – ressorterend onder de minister van Defensie, de minister van Binnenlandse Zaken of de minister van Justitie of onder de ministers belast met economische zaken, begrotingszaken en douanezaken – aangewezen waaraan machtiging kan worden verleend om onder de in dit boek vastgestelde voorwaarden gebruik te maken van de in titel V van dit boek genoemde technieken. Het decreet specificeert voor elke dienst de in artikel L. 811-3 vermelde doelstellingen en de technieken waarvoor machtiging kan worden verleend."

34 In artikel L. 821-1, eerste alinea, CSI staat:

„De toepassing op het nationale grondgebied van de in titel V, hoofdstukken I tot en met IV, van dit boek genoemde technieken voor het inwinnen van inlichtingen is onderworpen aan voorafgaande machtiging van de eerste minister, verleend na advies van de nationale commissie voor toezicht op inlichtingentechnieken."

35 Artikel 821-2 CSI bepaalt:

„De in artikel L. 821-1 genoemde machtiging wordt verleend op schriftelijk en met redenen omkleed verzoek van de minister van Defensie, de minister van Binnenlandse zaken, de minister van Justitie of de ministers belast met economische zaken, begrotingszaken of douanezaken. Elke minister kan deze bevoegdheid uitsluitend delegeren aan directe medewerkers die zich mogen bezighouden met vertrouwelijke kwesties in verband met de landsverdediging.

Het verzoek vermeldt:

1° de toe te passen techniek of technieken;

2° de dienst waarvoor het wordt ingediend;

3° de nagestreefde doelstelling of doelstellingen;

4° de reden of redenen voor de maatregelen;

5° de geldigheidsduur van de machtiging;

6° de persoon of de personen, de plaats of de plaatsen dan wel het voertuig of de voertuigen waarop het verzoek betrekking heeft.

Voor de toepassing van punt 6 kunnen personen van wie de identiteit onbekend is, worden aangeduid met hun identificatiekenmerken of hun hoedanigheid, en kunnen plaatsen of voertuigen worden aangeduid door verwijzing naar de personen op wie het verzoek betrekking heeft.

[...]"

36 Artikel L. 821-3, eerste alinea, CSI luidt als volgt:

„Het verzoek wordt meegedeeld aan de voorzitter of aan een van de in van artikel L. 831-1, 2° en 3°, genoemde leden van de nationale commissie voor toezicht op inlichtingentechnieken, die binnen 24 uur advies uitbrengt aan de eerste minister. Indien het verzoek wordt beoordeeld door de commissie in beperkte dan wel in volle samenstelling, wordt de eerste minister daarvan onverwijld in kennis gesteld en wordt het advies uitgebracht binnen 72 uur."

37 Artikel L. 821-4 CSI bepaalt:

„De machtiging om de in titel V, hoofdstukken I tot en met IV, van dit boek genoemde technieken toe te passen, wordt door de eerste minister verleend voor een periode van maximaal vier maanden. [...] De machtiging bevat de in artikel L. 821-2, 1° tot en met 6°, bedoelde motieven en vermeldingen. Elke machtiging kan onder dezelfde voorwaarden als genoemd in dit hoofdstuk worden verlengd.

Wanneer de machtiging wordt verleend na een negatief advies van de commissie voor toezicht op inlichtingentechnieken, worden daarin de redenen vermeld waarom dat advies niet is opgevolgd.

[...]"

38 Artikel L. 833-4 CSI, dat is opgenomen in hoofdstuk III van diezelfde titel, bepaalt:

„Hetzij uit eigen beweging, hetzij nadat bij haar een klacht is ingediend door een persoon die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem worden toegepast, gaat de commissie na of bij de toepassing van de betrokken techniek of technieken de bepalingen van dit boek in acht zijn of worden genomen. Zij stelt de indiener van de klacht ervan in kennis de noodzakelijke onderzoeken te hebben uitgevoerd, zonder de toepassing van dergelijke technieken te bevestigen of te ontkennen."

39 Artikel L. 841-1, eerste en tweede alinea, CSI luidt als volgt:

„Onverminderd de in artikel L. 854-9 van dit wetboek opgenomen bijzondere bepalingen, is de Conseil d'État bevoegd om onder de in titel VII, hoofdstuk III bis, van boek VII van de code de justice administrative [(wetboek van bestuursprocesrecht)] vastgestelde voorwaarden kennis te nemen van verzoeken betreffende de toepassing van de in titel V van de in dit boek genoemde inlichtingentechnieken.

De Conseil d'État kan worden aangezocht door:

1° eenieder die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem worden toegepast en die kan aantonen dat eerst de procedure van artikel L. 833-4 is doorlopen;

2° de commissie voor toezicht op inlichtingentechnieken, onder de in artikel L. 833-8 vastgestelde voorwaarden."

40 Boek VIII, titel V, van het deel „wetgeving" van de CSI, betreffende „aan machtiging onderworpen technieken voor het inwinnen van inlichtingen", bestaat onder meer uit hoofdstuk I („Administratieve toegang tot verbindingsgegevens"), dat de artikelen L. 851-1 tot en met 851-7 CSI omvat.

41 Artikel L. 851-1 CSI bepaalt:

„Onder de in titel II, hoofdstuk I, van dit boek vastgestelde voorwaarden kan machtiging worden verleend om bij de exploitanten van elektronischecommunicatiemiddelen, bij de in artikel L. 34-1 [CPCE] genoemde personen en bij de personen genoemd in artikel 6, lid I, punten 1 en 2, 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; JORF van 22 juni 2004, blz. 11168)] 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 nummers waarheen en waarvandaan is gebeld, de duur en datum van de communicatie.

In afwijking van artikel L. 821-2 worden schriftelijke en met redenen omklede verzoeken inzake de technische gegevens betreffende de identificatie van abonnements- of verbindingsnummers voor elektronischecommunicatiediensten, of betreffende de identificatie van alle abonnements- of verbindingsnummers van een bepaalde persoon, rechtstreeks aan de commissie voor toezicht op inlichtingentechnieken doorgezonden door de individueel aangewezen en gemachtigde functionarissen van de in de artikelen L. 811-2 en L. 811-4 genoemde inlichtingendiensten. De commissie brengt haar advies uit onder de in artikel L. 821-3 vastgestelde voorwaarden.

Een onder de eerste minister ressorterende dienst is belast met het opvragen van de informatie of documenten bij de in de eerste alinea van dit artikel genoemde exploitanten en personen. De nationale commissie voor toezicht op inlichtingentechnieken heeft permanent een volledige, rechtstreekse en onmiddellijke toegang tot de verzamelde informatie of documenten.

De nadere regels voor de toepassing van dit artikel worden bepaald bij decreet, vastgesteld na advies van de Conseil d'État en van de Commission nationale de l'informatique et des libertés [(nationale commissie voor informatica en vrijheden)] en de nationale commissie voor toezicht op inlichtingentechnieken."

42 Artikel L. 851-2 CSI bepaalt:

„I. – Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kan, uitsluitend ter voorkoming van terrorisme, individueel machtiging worden verleend om op de netwerken van de in artikel L. 851-1 genoemde exploitanten en personen in real time de in ditzelfde artikel genoemde informatie of documenten op te vragen met betrekking tot een persoon die eerder is geïdentificeerd als een persoon die in verband kan worden gebracht met een dreiging. Wanneer er zwaarwegende redenen zijn om aan te nemen dat een of meer personen uit de omgeving van de persoon op wie de machtiging betrekking heeft, informatie kunnen verstrekken voor het doel waarvoor de machtiging is verleend, kan de machtiging ook individueel voor elk van die personen worden verleend.

I bis. – De eerste minister stelt na advies van de nationale commissie voor toezicht op inlichtingentechnieken het maximumaantal vast van de krachtens dit artikel verleende machtigingen die tegelijkertijd van kracht kunnen zijn. De commissie wordt in kennis gesteld van het besluit waarbij dit contingent wordt vastgesteld, van de verdeling ervan over de in artikel L. 821-2, eerste alinea, genoemde ministeries en van het aantal verleende interceptiemachtigingen.

[...]”

43 Artikel L. 851-3 CSI luidt als volgt:

„I. – Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kan, uitsluitend ter voorkoming van terrorisme, aan de in artikel L. 851-1 genoemde exploitanten en personen de verplichting worden opgelegd om op hun netwerken geautomatiseerde verwerkingen uit te voeren die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken.

Bij die geautomatiseerde verwerkingen wordt uitsluitend gebruikgemaakt van de in artikel L. 851-1 genoemde informatie of documenten. Er mogen geen andere gegevens worden opgevraagd dan die welke beantwoorden aan de ontwerpparameters, en de personen op wie de informatie of documenten betrekking hebben, mogen niet kunnen worden geïdentificeerd.

Met inachtneming van het evenredigheidsbeginsel wordt in de door de eerste minister verleende machtiging de technische reikwijdte van de toepassing van die verwerkingen gepreciseerd.

II. – De nationale commissie voor toezicht op inlichtingentechnieken brengt advies uit over het verzoek tot het verlenen van een machtiging voor geautomatiseerde verwerkingen en over de gehanteerde parameters voor het opsporen van verbindingen. Zij heeft permanent volledige en rechtstreekse toegang tot die verwerkingen en tot de opgevraagde informatie en gegevens. Zij wordt in kennis gesteld van alle wijzigingen in de verwerkingen en parameters en kan aanbevelingen doen.

De eerste machtiging voor de toepassing van geautomatiseerde verwerkingen als bedoeld in lid I van dit artikel wordt verleend voor de duur van twee maanden. De machtiging kan worden verlengd onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden inzake duur. De verlengingsaanvraag bevat een overzicht van het aantal identificatoren dat door middel van de automatische verwerking is gesignaleerd, alsook een analyse van de relevantie van die signaleringen.

III. – De in artikel L. 871-6 bepaalde voorwaarden zijn van toepassing op de materiële verrichtingen die de in artikel L. 851-1 genoemde exploitanten en personen uitvoeren met het oog op dergelijke verwerkingen.

IV. – Wanneer door middel van de in lid I van dit artikel genoemde verwerkingen gegevens worden opgespoord waaruit een terroristische dreiging zou kunnen blijken, kan de eerste minister of een van de personen aan wie deze minister zijn bevoegdheid heeft gedelegeerd, nadat de nationale commissie voor toezicht op inlichtingentechnieken overeenkomstig de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden advies heeft uitgebracht, toestemming geven om de betrokken persoon of personen te identificeren en om de betrokken gegevens op te vragen. Die gegevens worden gebruikt binnen een termijn van zestig dagen nadat zij zijn opgevraagd en worden na afloop van die termijn vernietigd, tenzij er ernstige aanwijzingen zijn voor een terroristische dreiging waarmee een of meer van de betrokken personen in verband kunnen worden gebracht.

[...]”

44 Artikel L. 851-4 CSI bepaalt:

„Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kunnen de in artikel L. 851-1 genoemde technische gegevens betreffende de locatie van de gebruikte eindapparatuur op verzoek worden opgevraagd van het netwerk en door de exploitanten in real time worden doorgezonden aan een onder de eerste minister ressorterende dienst."

45 Artikel R. 851-5 CSI, dat is opgenomen in het deel „regelgeving" van dit wetboek, luidt als volgt:

„I. – De in artikel L. 851-1 genoemde informatie of documenten zijn, met uitzondering van de inhoud van de correspondentie of de geraadpleegde informatie:

1° de informatie of de documenten genoemd in de artikelen R. 10-13 en R. 10-14 [CPCE] en in artikel 1 van [decreet nr. 2011-219];

2° de andere technische gegevens dan die welke worden genoemd onder 1°:

a) die het mogelijk maken de eindapparatuur te lokaliseren;

b) die betrekking hebben op de toegang van de eindapparatuur tot de netwerken of tot de openbare online communicatiediensten;

c) die betrekking hebben op het overbrengen van elektronische communicatie via de netwerken;

d) die betrekking hebben op de identificatie en authenticatie van een gebruiker, een verbinding, een netwerk of een openbare online communicatiedienst;

e) die betrekking hebben op de kenmerken van de eindapparatuur en op de configuratiegegevens van de op die apparatuur aanwezige software.

II. – Enkel de in lid I, onder 1°, genoemde informatie en documenten mogen worden opgevraagd overeenkomstig artikel L. 851-1. Die opvraging geschiedt niet in real time.

De in lid I, onder 2°, genoemde informatie mag uitsluitend worden opgevraagd overeenkomstig de artikelen L. 851-2 en L. 851-3, onder de voorwaarden en binnen de grenzen die in deze artikelen zijn vastgesteld, en onverminderd de toepassing van artikel R. 851-9."

CPCE

46 Artikel L. 34-1 CPCE bepaalt:

„I. – Het onderhavige artikel is van toepassing op de verwerking van persoonsgegevens in het kader van 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 het publiek online toegang tot communicatiediensten aan te bieden, wissen of anonimiseren alle verkeersgegevens, met inachtneming van het bepaalde in de leden III, IV, V en VI.

De personen die het publiek 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 de 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 elektronischecommunicatiemiddelen.

III. – Met het oog op het onderzoek, de vaststelling en de vervolging van strafbare feiten of van een niet-nakoming van de in artikel L. 336-3 van de code de la propriété intellectuelle [(wetboek intellectuele eigendom)] omschreven verplichting, of met het oog op het voorkomen van aanvallen op geautomatiseerde gegevensverwerkingssystemen als bedoeld en strafbaar gesteld in de artikelen 323-1 tot en met 323-3-1 van de code pénal [(wetboek van strafrecht)], en met als enige doel, indien nodig, de gegevens ter beschikking te kunnen stellen van de rechterlijke autoriteit of van de in artikel L. 331-12 van de code de la propriété intellectuelle bedoelde hoge autoriteit, of van de in artikel L. 2321-1 van de code de la défense [(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 en van de commissie voor informatica en vrijheden, worden binnen de in lid 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 de leden 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 de exploitanten verleende communicatiediensten en de locatie van de eindapparatuur.

Zij mogen in geen geval betrekking hebben op de inhoud van de correspondentie of van 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 [(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."

47 Artikel R. 10-13 CPCE luidt als volgt:

„I. – Overeenkomstig lid III van artikel L. 34-1 bewaren de exploitanten van elektronischecommunicatiemiddelen de volgende gegevens met het oog op het onderzoek, de vaststelling en de vervolging 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.

II. – In het geval van telefonieactiviteiten bewaart de exploitant naast de in lid II genoemde gegevens ook de gegevens aan de hand waarvan de oorsprong en de locatie van de communicatie kunnen worden bepaald.

III. – De in dit artikel genoemde gegevens worden bewaard gedurende één jaar, te rekenen vanaf de datum van registratie ervan.

IV. – De aanwijsbare en specifieke extra kosten die zijn gemaakt door exploitanten die op bevel van de rechterlijke autoriteiten gegevens hebben verstrekt die onder de in dit artikel genoemde categorieën vallen, worden gecompenseerd op de wijze als bepaald in artikel R. 213-1 van de code de procédure pénale [(wetboek van strafvordering)]."

48 Artikel R. 10-14 CPCE bepaalt:

„I. – Overeenkomstig lid IV van artikel L. 34-1 is het de exploitanten van elektronischecommunicatiemiddelen toegestaan om voor factu rerings- en betalingsdoeleinden de technische gegevens te bewaren aan de hand waarvan de gebruiker kan worden geïdentificeerd, alsmede de technische gegevens die worden genoemd in artikel R. 10-13, lid I, onder b), c) en d).

II. – In het geval van telefonieactiviteiten mogen de exploitanten behalve de in lid I genoemde gegevens ook de technische gegevens bewaren aan de hand waarvan de locatie van de communicatie kan worden bepaald en de ontvanger of de ontvangers van de communicatie kunnen worden geïdentificeerd, alsmede de voor de facturering benodigde gegevens.

III. – De in de leden I en II van dit artikel genoemde gegevens mogen slechts worden bewaard indien zij nodig zijn voor de facturering en voor de betaling van de geleverde diensten. Zij mogen niet langer worden bewaard dan strikt noodzakelijk is voor dat doel, en in geen geval langer dan één jaar.

IV. – Ten behoeve van de veiligheid van de netwerken en de faciliteiten mogen de exploitanten gedurende een periode van maximaal drie maanden de volgende gegevens bewaren:

a) gegevens aan de hand waarvan de bron van de communicatie kan worden geïdentificeerd;

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

c) technische gegevens aan de hand waarvan de ontvanger of ontvangers van de communicatie kunnen worden geïdentificeerd;

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

LCEN

49 Artikel 6 van loi n° 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; JORF van 22 juni 2004, blz. 11168; hierna: „LCEN") bepaalt:

„I. – 1. Personen van wie de activiteit erin bestaat het publiek online toegang te verlenen tot communicatiediensten, stellen hun abonnees ervan in kennis dat er technische middelen bestaan om de toegang tot bepaalde diensten te beperken of om bepaalde diensten te selecteren, en bieden hun abonnees ten minste een van die middelen aan.

[...]

2. Natuurlijke of rechtspersonen die, zelfs gratis, zorgen voor de opslag van signalen, geschriften, beelden, geluiden of berichten van om het even welke aard die door de afnemers van openbare online communicatiediensten worden aangeleverd, om deze via deze diensten ter beschikking te stellen van het publiek, kunnen niet civielrechtelijk aansprakelijk worden gesteld voor de activiteiten of de op verzoek van een afnemer van die diensten opgeslagen informatie, indien zij niet daadwerkelijk kennis hadden van het onwettige karakter daarvan of van feiten of informatie waaruit dat onwettige karakter duidelijk bleek, of indien zij, zodra zij daadwerkelijk van het bovenbedoelde kennis hadden, prompt hebben gehandeld om die gegevens te verwijderen of de toegang daartoe onmogelijk te maken.

[...]

II. – De in lid I, punten 1 en 2, genoemde personen beheren en bewaren de gegevens zodanig dat het mogelijk is eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of een deel van de inhoud van de diensten waarvan zij aanbieder zijn.

Zij verstrekken aan de personen die een openbare online communicatiedienst verlenen, technische middelen die hen in staat stellen om aan de in lid III genoemde identificatievoorwaarden te voldoen.

De rechterlijke autoriteit kan de in lid I, punten 1 en 2, genoemde dienstverleners verzoeken om de in de eerste alinea bedoelde gegevens mee te delen.

De artikelen 226-17, 226-21 en 226-22 van de code pénal zijn van toepassing op de verwerking van die gegevens.

Bij decreet vastgesteld na advies van de Conseil d'État en van de nationale commissie voor informatica en vrijheden, worden de in de eerste alinea bedoelde gegevens gedefinieerd en wordt vastgesteld hoelang en op welke wijze zij worden bewaard.

[...]"

Decreet nr. 2011-219

50 Hoofdstuk I van decreet nr. 2011-219, dat is vastgesteld op grond van artikel 6, lid II, laatste alinea, LCEN, bevat de artikelen 1 tot en met 4 van dit decreet.

51 Artikel 1 van decreet nr. 2011-219 bepaalt:

„De in artikel 6, lid II, [LCEN] genoemde en op grond van deze bepaling te bewaren gegevens zijn:

1° voor de in artikel 6, lid I, punt 1, genoemde personen en voor elke verbinding van hun abonnees:

a) de identificator van de verbinding;

b) de door die personen aan de abonnee toegekende identificator;

c) de identificator van de voor de verbinding gebruikte eindapparatuur, wanneer deze voor die personen toegankelijk is;

d) de datum en het tijdstip van het begin en het einde van de verbinding;

e) de kenmerken van de lijn van de abonnee;

2° voor de in artikel 6, lid I, punt 2, genoemde personen en voor elke creatie:

a) de identificator van de verbinding aan de oorsprong van de communicatie;

b) de identificator die door het informatiesysteem is toegekend aan de inhoud die het voorwerp van de verrichting is;

c) de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud;

d) de aard van de verrichting;

e) de datum en het tijdstip van de verrichting;

f) de identificator die is gebruikt door de auteur van de verrichting, voor zover deze door die auteur is verstrekt;

3° voor de in artikel 6, lid I, punten 1 en 2, genoemde personen, de informatie die door een gebruiker is verstrekt bij het ondertekenen van een contract of het aanmaken van een account:

a) de identificator van de verbinding bij het aanmaken van het account;

b) de naam, achternaam of bedrijfsnaam;

c) de bijbehorende postadressen;

d) de gebruikte pseudoniemen;

e) de bijbehorende e-mail- of accountadressen;

f) de telefoonnummers;

g) het bijgewerkte wachtwoord en de bijgewerkte gegevens voor de verificatie of wijziging ervan;

4° voor de in artikel 6, lid I, punten 1 en 2, genoemde personen, wanneer voor het sluiten van het contract of het aanmaken van het account een vergoeding verschuldigd is, de volgende betalingsgegevens voor elke betalingstransactie:

a) de gebruikte betalingswijze;

b) de betalingsreferentie;

c) het bedrag;

d) de datum en het tijdstip van de transactie.

De onder 3° en 4° genoemde gegevens hoeven slechts te worden bewaard voor zover de betrokken personen deze gegevens plegen te verzamelen.”

52 Artikel 2 van decreet nr. 2011-219 luidt als volgt:

„Het bijdragen aan de creatie van inhoud omvat de volgende verrichtingen:

a) de oorspronkelijke creatie van inhoud;

b) wijzigingen van inhoud en van daarmee verband houdende gegevens;

c) verwijdering van inhoud."

53 Artikel 3 van dat decreet bepaalt:

„De bewaartermijn voor de in artikel 1 genoemde gegevens bedraagt één jaar:

a) in het geval van de onder 1° en 2° genoemde gegevens te rekenen vanaf de dag waarop de inhoud is gecreëerd, voor elke verrichting die heeft bijgedragen aan de creatie van inhoud, zoals gedefinieerd in artikel 2;

b) in het geval van de onder 3° genoemde gegevens te rekenen vanaf de dag waarop het contract is beëindigd of het account is opgeheven;

c) in het geval van de onder 4° genoemde gegevens te rekenen vanaf de datum waarop de factuur is uitgereikt of de betalingstransactie heeft plaatsgevonden, voor elke factuur of betalingstransactie."

Belgisch recht

54 Bij de wet van 29 mei 2016 zijn met name wijzigingen aangebracht in de wet van 13 juni 2005 betreffende de elektronische communicatie (*Belgisch Staatsblad*, 20 juni 2005, blz. 28070; hierna: „wet van 13 juni 2005"), het Wetboek van strafvordering en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (*Belgisch Staatsblad*, 18 december 1998, blz. 40312; hierna: „wet van 30 november 1998").

55 Artikel 126 van de wet van 13 juni 2005, zoals gewijzigd bij de wet van 29 mei 2016, bepaalt:

„§ 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dienen de aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegang, van e-mail via het internet, de operatoren die openbare elektronischecommunicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken, de in paragraaf 3 bedoelde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

De verplichting om de in paragraaf 3 bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:

1° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren van openbare elektronischecommunicatiediensten of van een openbaar netwerk voor elektronische communicatie, of

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

§ 2. Enkel de volgende overheden mogen op eenvoudig verzoek van de in paragraaf 1, eerste lid, bedoelde aanbieders en operatoren gegevens ontvangen die worden bewaard krachtens dit artikel om de doeleinden en volgens de hieronder opgesomde voorwaarden:

1° de gerechtelijke autoriteiten, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken, voor de uitvoering van de in de artikelen 46bis en 88bis van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen;

2° de inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren van gegevens zoals bedoeld in de artikelen 16/2, 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te vervullen en volgens de voorwaarden vastgelegd in die wet;

3° elke officier van gerechtelijke politie van het [Belgisch Instituut voor postdiensten en telecommunicatie (hierna: „Instituut")], met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en dit artikel;

4° de hulpdiensten die hulp ter plaatse bieden, wanneer ze naar aanleiding van een noodoproep, van de betrokken aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen met behulp van de databank beoogd in artikel 107, § 2, derde lid, of onvolledige of onjuiste gegevens krijgen. Enkel de identificatiegegevens van de oproeper mogen worden gevraagd en uiterlijk binnen 24 uur na de oproep;

5° de officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood, opsporing van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is. Enkel de gegevens die zijn beoogd in paragraaf 3, eerste en tweede lid, met betrekking tot de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan het verzoek om de gegevens te krijgen, mogen worden gevraagd aan de operator of de aanbieder in kwestie via een door de Koning aangewezen politiedienst;

6° de Ombudsdienst voor telecommunicatie, met het oog op de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronischecommunicatienetwerk of -dienst, conform de voorwaarden beoogd in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd.

De aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de in paragraaf 3 bedoelde gegevens onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en uitsluitend aan de in deze paragraaf bedoelde autoriteiten kunnen worden meegedeeld.

Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden.

§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin het tweede en derde lid specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf maanden bewaard vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister [die bevoegd is voor elektronische communicatie], en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de te bewaren gegevens per type van categorie bedoeld in het eerste tot derde lid alsook de vereisten waaraan deze gegevens moeten beantwoorden.

[...]"

Hoofdgedingen en prejudiciële vragen

Zaak C-511/18

56 Bij verzoekschriften die op 30 november 2015 en 16 maart 2016 zijn ingediend en die in de procedure in het hoofdgeding zijn gevoegd, hebben La Quadrature du Net, French Data Network, de Fédération des fournisseurs d'accès à Internet associatifs en Igwan.net bij de Conseil d'État nietigverklaring gevorderd van decreten nr. 2015-1185, nr. 2015-1211, nr. 2015-1639 en nr. 2016-67, met name omdat zij deze decreten in strijd achten met de Franse grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: „EVRM") en de richtlijnen 2000/31 en 2002/58, gelezen in het licht van de artikelen 7, 8 en 47 van het Handvest.

57 Wat in het bijzonder de middelen inzake schending van richtlijn 2000/31 betreft, merkt de verwijzende rechter op dat artikel L. 851-3 CSI aan exploitanten van elektronischecommunicatiemiddelen en technische dienstverleners de verplichting oplegt om „op hun netwerken geautomatiseerde verwerkingen uit te voeren 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 is volgens de verwijzende rechter bedoeld om gedurende een beperkte periode van alle door die exploitanten en dienstverleners verwerkte verbindingsgegevens de gegevens op te vragen die in verband kunnen worden gebracht met een dergelijk ernstig misdrijf. De verwijzende rechter meent dan ook dat artikel L 851-3 CSI, dat niet voorziet in een algemene verplichting om actief toezicht uit te oefenen, niet in strijd is met artikel 15 van richtlijn 2000/31.

58 Wat de middelen inzake schending van richtlijn 2002/58 betreft, is de verwijzende rechter van mening dat met name uit de bepalingen van deze richtlijn en uit het arrest van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970; hierna: „arrest Tele2"), volgt dat nationale bepalingen waarbij aan aanbieders van elektronischecommunicatiediensten verplichtingen worden opgelegd, zoals een verplichting tot algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens van hun gebruikers en abonnees voor de in artikel 15, lid 1, van die richtlijn genoemde doeleinden, waaronder de bescherming van de nationale veiligheid, de landsverdediging en de openbare veiligheid, binnen de werkingssfeer van die richtlijn vallen voor zover zij de activiteit van die aanbieders regelen. Volgens de verwijzende rechter geldt hetzelfde voor bepalingen die de toegang van de nationale autoriteiten tot de betrokken gegevens en het gebruik ervan regelen.

59 De verwijzende rechter leidt daaruit af dat zowel de uit artikel L. 851-1 CSI voortvloeiende bewaarplicht als de in de artikelen L.851-1, L.851-2 en L.851-4 van dat wetboek geregelde administratieve toegang tot die gegevens, ook in real time, binnen de werkingssfeer van richtlijn 2002/58 valt. Volgens de verwijzende rechter geldt hetzelfde voor artikel L. 851-3 CSI, dat weliswaar aan de betrokken aanbieders geen algemene bewaarplicht oplegt, maar wel van hen verlangt dat zij op hun netwerken geautomatiseerde verwerkingen uitvoeren die erop gericht zijn verbindingen op te sporen die kunnen wijzen op een terroristische dreiging.

60 De verwijzende rechter is daarentegen van mening dat richtlijn 2002/58 niet van toepassing is op de bestreden bepalingen van de CSI die betrekking hebben op technieken voor het inwinnen van inlichtingen die rechtstreeks door de staat worden toegepast en die niet de activiteiten van aanbieders van elektronischecommunicatiediensten regelen door aan deze aanbieders specifieke verplichtingen op te leggen. Die bepalingen kunnen volgens de verwijzende rechter dus niet worden geacht uitvoering te geven aan het Unierecht, zodat de middelen volgens welke die bepalingen in strijd zijn met richtlijn 2002/58, niet met succes kunnen worden aangevoerd.

61 Met het oog op de beslechting van de geschillen over de rechtmatigheid van decreten nr. 2015-1185, nr. 2015-2011, nr. 2015-1639 en nr. 2016-67 in het licht van richtlijn 2002/58, voor zover deze zijn vastgesteld ter uitvoering van de artikelen L. 851-1 tot en met 851-4 CSI, moeten volgens de verwijzende rechter dan ook drie vragen betreffende de uitlegging van het Unierecht worden beantwoord.

62 Wat de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 betreft, vraagt de verwijzende rechter zich in de eerste plaats af of een op grond van de artikelen L. 851-1 en R. 851-5 CSI aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot algemene en ongedifferentieerde bewaring, met name gelet op de waarborgen en controles waarmee de administratieve toegang tot verbindingsgegevens en het gebruik van die gegevens zijn omgeven, niet moet worden beschouwd als een inmenging die haar rechtvaardiging vindt in het door artikel 6 van het Handvest gewaarborgde recht op veiligheid en in de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 VEU uitsluitend op de lidstaten rust.

63 Wat in de tweede plaats de andere verplichtingen betreft die aan aanbieders van elektronischecommunicatiediensten kunnen worden opgelegd, merkt de verwijzende rechter op dat op grond van artikel L. 851-2 CSI de in artikel L. 851-1 van dit wetboek bedoelde informatie of documenten uitsluitend ter voorkoming van terrorisme kunnen worden opgevraagd bij dezelfde personen. Deze opvraging, die slechts betrekking heeft op een of meer personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging, wordt in real time uitgevoerd. Dit geldt volgende verwijzende rechter ook voor artikel L. 851-4 CSI, op grond waarvan exploitanten enkel technische gegevens over de locatie van de eindapparatuur in real time mogen doorgeven. Die technieken regelen voor verschillende doeleinden en op verschillende manieren de administratieve toegang in real time tot de op grond van de CPCE en de LCEN bewaarde gegevens, zonder dat aan de betrokken aanbieders een extra bewaarplicht wordt opgelegd naast wat noodzakelijk is voor de facturering en de levering van hun diensten. Ook artikel L. 851-3 CSI, dat voorziet in een verplichting voor de betrokken aanbieders om op hun netwerken een geautomatiseerde analyse van de verbindingen uit te voeren, impliceert volgens de verwijzende rechter geen algemene en ongedifferentieerde gegevensbewaring.

64 De verwijzende rechter is van oordeel dat in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, met name door terreurgevaar, zowel de algemene en ongedifferentieerde bewaring als de toegang in real time tot de verbindingsgegevens een ongekend operationeel nut opleveren. Dankzij de algemene en ongedifferentieerde bewaring kunnen de inlichtingendiensten immers toegang krijgen tot de communicatiegegevens van een persoon voordat de redenen zijn vastgesteld om aan te nemen dat die persoon een bedreiging vormt voor de openbare veiligheid, de landsverdediging of de staatsveiligheid, en dankzij de toegang in real time tot de verbindingsgegevens kan het gedrag van personen die een onmiddellijke bedreiging voor de openbare orde kunnen vormen, met een hoog niveau van alertheid in de gaten worden gehouden.

65 Voorts maakt de in artikel L. 851-3 CSI genoemde techniek het volgens de verwijzende rechter mogelijk om aan de hand van daartoe nauwkeurig vastgestelde criteria personen op te sporen van wie het gedrag, gelet op hun communicatiemethoden, een terroristische dreiging aan het licht kan brengen.

66 Wat in de derde plaats de toegang van de bevoegde autoriteiten tot de bewaarde gegevens betreft, vraagt de verwijzende rechter zich af of richtlijn 2002/58, gelezen in het licht van het Handvest, aldus moet 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 een dergelijke kennisgeving het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, dan wel of dergelijke procedures als regelmatig kunnen worden beschouwd gelet op alle andere procedurele waarborgen waarin het nationale recht voorziet, wanneer deze waarborgen de doeltreffendheid van het recht op beroep garanderen.

67 Met betrekking tot die andere procedurele waarborgen merkt de verwijzende rechter met name op dat eenieder die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem zijn toegepast, zich kan wenden tot een speciale formatie van de Conseil d'État, die tot taak heeft om aan de hand van de in het kader van een niet-contradictoire procedure aan hem verstrekte informatie na te gaan of jegens de verzoeker een techniek is toegepast, en zo ja, of daarbij de bepalingen van boek VIII CSI in acht zijn genomen. De bevoegdheden waarover die formatie bij de beoordeling van de ingediende verzoeken beschikt, waarborgen volgens de verwijzende rechter de doeltreffendheid van de door haar uitgevoerde rechterlijke toetsing. Zo is die formatie bevoegd om de verzoeken te onderzoeken, alle onrechtmatigheden die zij vaststelt ambtshalve op te werpen, en de autoriteiten te gelasten alle passende maatregelen te nemen om een einde te maken aan de vastgestelde onrechtmatigheden. Voorts is het de taak van de nationale commissie voor toezicht op inlichtingentechnieken om na te gaan of de technieken voor het inwinnen van inlichtingen op het nationale grondgebied worden toegepast in overeenstemming met de vereisten die voortvloeien uit de CSI. De omstandigheid dat de in het hoofdgeding aan de orde zijnde wettelijke bepalingen niet voorschrijven dat personen jegens wie surveillancemaatregelen worden toegepast, daarover worden geïnformeerd, levert volgens de verwijzende rechter dan ook op zichzelf geen buitensporige aantasting op van het recht op eerbiediging van het privéleven.

68 In deze omstandigheden heeft de Conseil d'État de behandeling van de zaak geschorst en 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, of kunnen dergelijke procedures als regelmatig worden beschouwd gelet op alle andere bestaande procedurele waarborgen, wanneer deze waarborgen de doeltreffendheid van het recht op beroep garanderen?"

Zaak C-512/18

69 Bij een op 1 september 2015 ingediend verzoekschrift hebben French Data Network, La Quadrature du Net en de Fédération des fournisseurs d'accès à Internet associatifs bij de Conseil d'État nietigverklaring gevorderd van het stilzwijgende besluit van de eerste minister tot afwijzing van hun verzoek tot intrekking van artikel R. 10-13 CPCE en decreet nr. 2011-219, met name wegens strijdigheid met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 van het Handvest. Privacy International en het Center for Democracy and Technology zijn toegelaten tot interventie in het hoofdgeding.

70 Met betrekking tot artikel R. 10-13 CPCE en de daarin neergelegde verplichting tot algemene en ongedifferentieerde bewaring van communicatiegegevens merkt de verwijzende rechter – die vergelijkbare overwegingen formuleert als in zaak C-511/18 – op dat een dergelijke bewaring de gerechtelijke autoriteit in staat stelt toegang te krijgen tot gegevens inzake de communicatie van een persoon nog voordat deze ervan wordt verdacht een strafbaar feit te hebben gepleegd, zodat die bewaring ongekend nuttig is voor het onderzoeken, vaststellen en vervolgen van strafbare feiten.

71 Wat decreet nr. 2011-219 betreft, is de verwijzende rechter van mening dat artikel 6, punt II, LCEN, waarbij uitsluitend voor gegevens inzake de creatie van inhoud een bewaarplicht wordt opgelegd, niet binnen de werkingssfeer valt van richtlijn 2002/58, die immers volgens artikel 3, lid 1, ervan enkel van toepassing is op de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Unie, maar binnen de werkingssfeer van richtlijn 2000/31.

72 Volgens de verwijzende rechter volgt evenwel uit artikel 15, leden 1 en 2, van richtlijn 2000/31 dat deze richtlijn geen principieel verbod stelt op het bewaren van gegevens inzake de creatie van inhoud waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Naar het oordeel van de verwijzende rechter rijst dan ook de vraag of de artikelen 12, 14 en 15 van richtlijn 2002/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij een lidstaat toestaan een nationale regeling in te voeren als die van artikel 6, lid II, LCEN, op grond waarvan de betrokken personen verplicht zijn om de 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, opdat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken teneinde de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven.

73 In deze omstandigheden heeft de Conseil d'État de behandeling van de zaak geschorst en 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?"

Zaak C-520/18

74 Bij verzoekschriften die op 10 januari, 16 januari, 17 januari en 18 januari 2017 zijn ingediend en die in de procedure in het hoofdgeding zijn gevoegd, hebben de Ordre des barreaux francophones et germanophone, de Académie Fiscale ASBL en UA, de Liga voor Mensenrechten VZW en de Ligue des Droits de l'Homme ASBL, alsmede VZ, WY en XX bij het Grondwettelijk Hof (België) beroepen tot vernietiging van de wet van 29 mei 2016 ingesteld, omdat deze wet in hun ogen in strijd is met de artikelen 10 en 11 van de Belgische grondwet, gelezen in samenhang met de artikelen 5, 6 tot en met 11, 14, 15, 17 en 18 EVRM, met de artikelen 7, 8, 11 en 47 en artikel 52, lid 1, van het Handvest, met artikel 17 van het op 16 december 1966 door de Algemene Vergadering van de Verenigde Naties aangenomen en op 23 maart 1976 in werking getreden Internationaal Verdrag inzake burgerrechten en politieke rechten, met de algemene beginselen van rechtszekerheid, evenredigheid en zelfbeschikking op informatiegebied, en met artikel 5, lid 4, VEU.

75 Verzoekers in het hoofdgeding voeren ter ondersteuning van hun beroepen in wezen aan dat de wet van 29 mei 2016 met name onrechtmatig is omdat zij de grenzen van het strikt noodzakelijke overschrijdt en onvoldoende waarborgen biedt op het vlak van bescherming. Zij stellen in het bijzonder dat noch de in de wet opgenomen bepalingen betreffende de bewaring van gegevens, noch die welke de toegang van de autoriteiten tot de bewaarde gegevens regelen, voldoen aan de vereisten die voortvloeien uit het arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238; hierna: „Arrest Digital Rights"), en het arrest van 21 december 2016, Tele2 (C-203/15 en C-698/15, EU:C:2016:970). Volgens verzoekers houden die bepalingen in het hoofdgeding namelijk het risico in dat persoonlijkheidsprofielen worden opgesteld waarvan de bevoegde autoriteiten misbruik zouden kunnen maken, en voorzien zij niet in een passend niveau van beveiliging en bescherming van de bewaarde gegevens. Verzoekers in het hoofdgeding stellen tot slot dat de betrokken wet ook van toepassing is op personen voor wie het beroepsgeheim of een vertrouwelijkheidsplicht geldt, en betrekking heeft op communicatiegegevens die gevoelige persoonsgegevens zijn, terwijl zij niet voorziet in bijzondere waarborgen om deze gegevens te beschermen.

76 De verwijzende rechter merkt op dat de gegevens die op grond van de wet van 29 mei 2016 moeten worden bewaard door de aanbieders van telefoniediensten, ook via internet, van internettoegang en van e-mail via het internet, en door de exploitanten van openbare elektronischecommunicatienetwerken, identiek zijn aan die welke worden genoemd in richtlijn 2006/24/EG 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), zonder dat enig onderscheid wordt gemaakt naargelang van de betrokken personen of naargelang van het nagestreefde doel. Met betrekking tot dit laatste punt wijst de verwijzende rechter erop dat de wetgever met de wet van 29 mei 2016 niet alleen terrorisme en kinderpornografie heeft willen bestrijden, maar het ook mogelijk heeft willen maken de bewaarde gegevens te gebruiken in zeer veel verschillende situaties in het kader van strafrechtelijke onderzoeken. De verwijzende rechter stelt bovendien vast dat uit de memorie van toelichting van die wet blijkt dat de nationale wetgever invoering van een gerichte en gedifferentieerde bewaarplicht in het licht van de nagestreefde doelstelling niet mogelijk heeft geacht en ervoor heeft gekozen om de algemene en ongedifferentieerde bewaarplicht met strikte waarborgen te omgeven, zowel op het vlak van de bewaring van de gegevens als op het vlak van de toegang ertoe, teneinde de inmenging in het recht op bescherming van de persoonlijke levenssfeer tot een minimum te beperken.

77 De verwijzende rechter voegt daaraan toe dat artikel 126, lid 2, 1° en 2°, van de wet van 13 juni 2005, zoals gewijzigd bij de wet van 29 mei 2016, de voorwaarden bepaalt waaronder de gerechtelijke autoriteiten respectievelijk de inlichtingen- en veiligheidsdiensten toegang kunnen krijgen tot de bewaarde gegevens, zodat het onderzoek of die wet in overeenstemming is met de vereisten die voortvloeien uit het Unierecht, moet worden opgeschort totdat het Hof uitspraak zal hebben gedaan in twee bij hem aanhangige prejudiciële procedures die gaan over een dergelijke toegang.

78 De verwijzende rechter merkt tot slot op dat de wet van 29 mei 2016 een effectief strafrechtelijk onderzoek naar en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk beoogt te maken en het daarnaast mogelijk wil maken om de pleger van een dergelijk misdrijf te identificeren, ook wanneer wordt gebruikgemaakt van elektronischecommunicatiemiddelen. Tijdens de bij de verwijzende rechter aanhangige procedure zou in dit verband zijn gewezen op de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM. Die verplichtingen zouden volgens de verwijzende rechter ook kunnen voortvloeien uit de overeenkomstige bepalingen van het Handvest, wat gevolgen zou kunnen hebben voor de uitlegging van artikel 15, lid 1, van richtlijn 2002/58.

79 In deze omstandigheden heeft het Grondwettelijk Hof de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

„1) Dient artikel 15, lid 1, van [richtlijn 2002/58], in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van [het Handvest], en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7 en 8 en artikel 52, lid 1, van [het Handvest], in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronischecommunicatiediensten om de verkeers- en locatiegegevens in de zin van [richtlijn 2002/58] die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronischecommunicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van [verordening 2016/679] en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe?

2) Dient artikel 15, lid 1, van [richtlijn 2002/58], gelezen in samenhang met de artikelen 4, 7, 8 en 11 en artikel 52, lid 1, van [het Handvest], in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronischecommunicatiediensten om de verkeers- en locatiegegevens in de zin van [richtlijn 2002/58] die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en [7] van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronischecommunicatiemiddelen?

3) Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van [de wet van 29 mei 2016] tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden?”

Procedure bij het Hof

80 Bij beslissing van de president van het Hof van 25 september 2018 zijn de zaken C-511/18 en C-512/18 gevoegd voor de schriftelijke en de mondelinge behandeling alsmede voor het arrest. Bij beslissing van de president van het Hof van 9 juli 2020 is zaak C-520/18 bij deze zaken gevoegd voor het arrest.

Prejudiciële vragen

Eerste vraag in de zaken C-511/18 en C-512/18 en eerste en tweede vraag in zaak C-520/18

81 Met de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18, die samen moeten worden onderzocht, wensen de verwijzende rechters in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58 aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die voor de in deze bepaling genoemde doeleinden aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt.

Inleidende opmerkingen

82 Uit de dossiers waarover het Hof beschikt blijkt dat de in de hoofdgedingen aan de orde zijnde regelingen zich uitstrekken tot alle elektronischecommunicatiemiddelen en tot alle gebruikers van die middelen, zonder dat daarbij enig onderscheid of enige uitzondering wordt gemaakt. Verder gaat het bij de gegevens die aanbieders van elektronischecommunicatiediensten op grond van die regelingen dienen te bewaren, met name om de gegevens die nodig zijn om de bron en de bestemming van een communicatie op te sporen, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte communicatiemateriaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren in het bijzonder de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, en het IP-adres voor de internetdiensten. De inhoud van de communicatie behoort daarentegen niet tot die gegevens.

83 De gegevens die op grond van de in de hoofdgedingen aan de orde zijnde nationale regelingen een jaar lang moeten worden bewaard, maken het dus in het bijzonder mogelijk om na te gaan met wie en met welk middel de gebruiker van een elektronisch communicatiemiddel heeft gecommuniceerd, om de datum, het tijdstip en de duur van de communicatie en de internetverbindingen te bepalen, alsook de plaats waarvandaan die communicatie en die verbindingen tot stand zijn gebracht, en om de eindapparatuur te lokaliseren, zonder dat er noodzakelijkerwijs informatie is overgebracht. Verder kan aan de hand van die gegevens worden achterhaald hoe vaak de gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd. Tot slot lijkt in het geval van de in de zaken C-511/18 en C-512/18 aan de orde zijnde nationale regeling, die ook geldt voor gegevens betreffende het overbrengen van elektronische communicatie via netwerken, ook de aard van de online geraadpleegde informatie te kunnen worden bepaald.

84 Met betrekking tot de nagestreefde doelstellingen moet worden opgemerkt dat de in de zaken C-511/18 en C-512/18 aan de orde zijnde regelingen onder meer gericht zijn op het opsporen, vaststellen en vervolgen van strafbare feiten in het algemeen, het waarborgen van de nationale onafhankelijkheid, de integriteit van het grondgebied en de landsverdediging, de bescherming van de zwaarwegende belangen van het buitenlands beleid, de nakoming door Frankrijk van zijn Europese en internationale verplichtingen, de bescherming van de zwaarwegende economische, industriële en wetenschappelijke belangen van Frankrijk, en de voorkoming van terrorisme, van aanvallen op de republikeinse vorm van de instituties en van collectieve gewelddadigheden die de openbare vrede

ernstig ondermijnen. De in zaak C-520/18 centraal staande regeling heeft onder meer het opsporen, onderzoeken en vervolgen van strafbare feiten alsmede het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en de openbare veiligheid tot doel.

85 De verwijzende rechters vragen zich in het bijzonder af welke gevolgen het in artikel 6 van het Handvest verankerde recht op veiligheid kan hebben voor de uitlegging van artikel 15, lid 1, van richtlijn 2002/58. Ook vragen zij zich af of de inmenging die de door de betrokken nationale regelingen voorgeschreven gegevensbewaring vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten als gerechtvaardigd kan worden beschouwd wegens het bestaan van regels die de toegang van de nationale autoriteiten tot de bewaarde gegevens beperken. De Conseil d'État is bovendien van mening dat die vraag ook moet worden beoordeeld in het licht van artikel 4, lid 2, VEU, aangezien zij rijst in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid. Het Grondwettelijk Hof benadrukt op zijn beurt dat de in zaak C-520/18 aan de orde zijnde nationale regeling ook uitvoering geeft aan de uit de artikelen 4 en 7 van het Handvest voortvloeiende positieve verplichting om te voorzien in een wettelijk kader dat een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt.

86 Zowel de Conseil d'État als het Grondwettelijk Hof gaat ervan uit dat de in de hoofdgedingen aan de orde zijnde nationale regelingen betreffende de bewaring van verkeers- en locatiegegevens en de toegang van de nationale autoriteiten tot die gegevens voor in artikel 15, lid 1, van richtlijn 2002/58 genoemde doeleinden, zoals de bescherming van de nationale veiligheid, binnen de werkingssfeer van deze richtlijn vallen. Bepaalde partijen in de hoofdgedingen en enkele van de lidstaten die schriftelijke opmerkingen hebben ingediend bij het Hof, zijn op dit punt echter een andere mening toegedaan, met name als het gaat om de uitlegging van artikel 1, lid 3, van richtlijn 2002/58. Daarom moet om te beginnen worden onderzocht of de betrokken regelingen binnen de werkingssfeer van deze richtlijn vallen.

Werkingssfeer van richtlijn 2002/58

87 La Quadrature du Net, de Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International en het Center for Democracy and Technology voeren in wezen aan dat uit de rechtspraak van het Hof betreffende de werkingssfeer van richtlijn 2002/58 volgt dat deze richtlijn zowel van toepassing is op de bewaring van de gegevens als op de toegang, al dan niet in real time, tot de bewaarde gegevens. Die partijen zijn namelijk van mening dat, aangezien de doelstelling van bescherming van de nationale veiligheid expliciet vermeld staat in artikel 15, lid 1, van richtlijn 2002/58, het nastreven van die doelstelling niet ertoe leidt dat deze richtlijn niet van toepassing is. Het door de verwijzende rechters genoemde artikel 4, lid 2, VEU doet in hun ogen niet aan dit oordeel af.

88 Met betrekking tot de inlichtingenmaatregelen die door de bevoegde Franse autoriteiten rechtstreeks worden toegepast zonder dat de activiteiten van aanbieders van elektronischecommunicatiediensten worden geregeld doordat hun specifieke verplichtingen worden opgelegd, merkt het Center for Democracy and Technology op dat die maatregelen noodzakelijkerwijs binnen de werkingssfeer van richtlijn 2002/58 en het Handvest vallen, aangezien daarmee wordt afgeweken van het door artikel 5 van deze richtlijn gewaarborgde vertrouwelijkheidsbeginsel. Die maatregelen moeten volgens die partijen dan ook voldoen aan de vereisten die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58.

89 De regering van het Verenigd Koninkrijk, de Franse, de Tsjechische en de Estse regering, Ierland en de Cypriotische, de Hongaarse, de Poolse en de Zweedse regering stellen daarentegen in wezen dat richtlijn 2002/58 niet van toepassing is op nationale regelingen als die van de hoofdgedingen, aangezien deze tot doel hebben de nationale veiligheid te waarborgen. Die regeringen zijn van mening dat de activiteiten van de inlichtingendiensten behoren tot de essentiële functies van de lidstaten, daar

zij verband houden met de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid en de territoriale integriteit, en dus onder de exclusieve bevoegdheid van de lidstaten vallen, zoals met name uit artikel 4, lid 2, derde zin, VEU volgt.

90 Die regeringen alsmede Ierland verwijzen bovendien naar artikel 1, lid 3, van richtlijn 2002/58, dat volgens hen activiteiten die verband houden met openbare veiligheid, defensie en staatsveiligheid van de werkingssfeer van deze richtlijn uitsluit, zulks in navolging van artikel 3, lid 2, eerste streepje, van richtlijn 95/46. Zij baseren zich in dit verband op de uitlegging die aan laatstgenoemde bepaling is gegeven in het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346).

91 In dit verband zij erop gewezen dat richtlijn 2002/58 volgens artikel 1, lid 1, onder meer de nationale regelgeving harmoniseert 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.

92 Volgens artikel 1, lid 3, van die richtlijn zijn van de werkingssfeer ervan uitgesloten de „activiteiten van de staat" op de aldaar bedoelde gebieden, waaronder de activiteiten van de staat op strafrechtelijk gebied en die welke verband houden met openbare veiligheid, defensie en staatsveiligheid, met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid. De in die bepaling als voorbeeld genoemde activiteiten zijn in alle gevallen specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien (arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 32 en aldaar aangehaalde rechtspraak).

93 Voorts bepaalt artikel 3 van richtlijn 2002/58 dat deze richtlijn van toepassing is op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Unie, met inbegrip van de openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen (hierna: „elektronischecommunicatiediensten"). Bijgevolg moet worden aangenomen dat deze richtlijn de activiteiten van de aanbieders van dergelijke diensten regelt (arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 33 en aldaar aangehaalde rechtspraak).

94 Op grond van artikel 15, lid 1, van richtlijn 2002/58 kunnen de lidstaten in dat kader met inachtneming van de in deze bepaling geformuleerde voorwaarden „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" (arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 71).

95 Artikel 15, lid 1, van richtlijn 2002/58 vooronderstelt noodzakelijkerwijs dat de daarin bedoelde nationale wettelijke maatregelen binnen de werkingssfeer van deze richtlijn vallen, aangezien deze richtlijn uitdrukkelijk bepaalt dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de in de richtlijn geformuleerde voorwaarden. Bovendien regelen die maatregelen de activiteit van aanbieders van elektronischecommunicatiediensten voor de in die bepaling vermelde doeleinden (arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 34 en aldaar aangehaalde rechtspraak).

96 Met name op grond van deze overwegingen heeft het Hof geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met artikel 3 van deze richtlijn, aldus moet worden uitgelegd dat binnen de werkingssfeer van deze richtlijn niet alleen wettelijke maatregelen vallen die aanbieders van elektronischecommunicatiediensten de verplichting opleggen om verkeers- en locatiegegevens te bewaren, maar ook wettelijke maatregelen die hun de verplichting opleggen om de bevoegde nationale autoriteiten toegang tot die gegevens te verlenen. Dergelijke wettelijke maatregelen impliceren immers noodzakelijkerwijs dat die aanbieders die gegevens verwerken, en kunnen, voor zover zij de activiteiten

van die aanbieders regelen, niet worden gelijkgesteld met de in artikel 1, lid 3, van richtlijn 2002/58 bedoelde specifieke activiteiten van staten (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punten 35 en 37 en aldaar aangehaalde rechtspraak).

97 Bovendien zou, gelet op de overwegingen in punt 95 van het onderhavige arrest en op de algemene opzet van richtlijn 2002/58, een uitlegging van deze richtlijn volgens welke de in artikel 15, lid 1, ervan bedoelde wettelijke maatregelen van de werkingssfeer van de richtlijn zijn uitgesloten omdat de doelstellingen die dergelijke maatregelen moeten nastreven, grotendeels overeenstemmen met de doelstellingen van de in artikel 1, lid 3, van diezelfde richtlijn bedoelde activiteiten, artikel 15, lid 1, elk nuttig effect ontnemen (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 72 en 73).

98 Bijgevolg kan het begrip „activiteiten" in artikel 1, lid 3, van richtlijn 2002/58, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 75 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6), niet aldus worden uitgelegd dat daaronder ook de in artikel 15, lid 1, van die richtlijn bedoelde wettelijke maatregelen vallen.

99 Artikel 4, lid 2, VEU, waaraan de in punt 89 van het onderhavige arrest genoemde regeringen hebben gerefereerd, kan niet afdoen aan deze conclusie. Volgens vaste rechtspraak van het Hof staat het immers weliswaar aan de lidstaten om hun wezenlijke veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te verzekeren, maar kan het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, niet ertoe leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen [zie in die zin arresten van 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punt 38 en aldaar aangehaalde rechtspraak; 20 maart 2018, Commissie/Oostenrijk (Staatsdrukkerij), C-187/16, EU:C:2018:194, punten 75 en 76, en 2 april 2020, Commissie/Polen, Hongarije en Tsjechië (Tijdelijk herplaatsingsmechanisme voor aanvragers van internationale bescherming), C-715/17, C-718/17 en C-719/17, EU:C:2020:257, punten 143 en 170].

100 Het is juist dat het Hof in het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346, punten 56-59), heeft geoordeeld dat de doorgifte van persoonsgegevens door luchtvaarmaatschappijen aan overheidsdiensten van een derde land met het oog op het voorkomen en bestrijden van terrorisme en andere ernstige misdrijven, ingevolge artikel 3, lid 2, eerste streepje, van richtlijn 95/46 niet binnen de werkingssfeer van deze richtlijn viel, aangezien die doorgifte geschiedde binnen een door de overheid ingesteld kader dat betrekking had op de openbare veiligheid.

101 Gelet op de overwegingen in de punten 93, 95 en 96 van het onderhavige arrest, kan die rechtspraak echter niet worden toegepast op de uitlegging van artikel 1, lid 3, van richtlijn 2002/58. Zoals de advocaat-generaal in wezen heeft opgemerkt in de punten 70 tot en met 72 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6), sloot artikel 3, lid 2, eerste streepje, van richtlijn 95/46, waarop die rechtspraak betrekking heeft, „verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat" immers in het algemeen van de werkingssfeer van deze richtlijn uit, zonder onderscheid te maken naar de persoon die de gegevensverwerkingshandeling uitvoerde. In het kader van de uitlegging van artikel 1, lid 3, van richtlijn 2002/58 moet dat onderscheid echter wel worden gemaakt. Zoals uit de punten 94 tot en met 97 van het onderhavige arrest blijkt, valt immers elke verwerking van persoonsgegevens door aanbieders van elektronischecommunicatiediensten binnen de werkingssfeer van die richtlijn, inclusief de verwerking die het gevolg is van door de overheid aan die aanbieders opgelegde verplichtingen, terwijl laatstgenoemde verwerking eventueel onder de uitzondering kon vallen van artikel 3, lid 2, eerste streepje, van richtlijn 95/46, gelet op de ruimere formulering van deze bepaling, die zag op elke verwerking die betrekking had op de openbare veiligheid, de defensie of de veiligheid van de staat, ongeacht de persoon die de handeling uitvoerde.

102 Bovendien moet worden opgemerkt dat richtlijn 95/46, die aan de orde was in de zaak die heeft geleid tot het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346), overeenkomstig artikel 94, lid 1, van verordening 2016/679 met ingang van 25 mei 2018 is ingetrokken en vervangen door deze verordening. Verordening 2016/679 is volgens artikel 2, lid 2, onder d), weliswaar niet van toepassing op verwerkingen die „door de bevoegde autoriteiten" worden verricht met het oog op onder meer de voorkoming en de opsporing van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, maar uit artikel 23, lid 1, onder d) en h), van deze verordening blijkt dat verwerkingen van persoonsgegevens die voor diezelfde doeleinden worden verricht door particulieren, binnen de werkingssfeer van deze verordening vallen. Hieruit volgt dat bovenstaande uitlegging van artikel 1, lid 3, artikel 3 en artikel 15, lid 1, van richtlijn 2002/58 in overeenstemming is met de afbakening van de werkingssfeer van verordening 2016/679, die door deze richtlijn wordt aangevuld en gespecificeerd.

103 Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronischecommunicatiediensten, wordt de bescherming van de gegevens van de betrokken personen niet beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (PB 2016, L 119, blz. 89), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM.

104 Uit het voorgaande volgt dat een nationale regeling die, zoals de in de hoofdgedingen aan de orde zijnde regelingen, ten behoeve van de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot bewaring van verkeers- en locatiegegevens oplegt, binnen de werkingssfeer van richtlijn 2002/58 valt.

Uitlegging van artikel 15, lid 1, van richtlijn 2002/58

105 Vooraf zij eraan herinnerd dat volgens vaste rechtspraak bij de uitlegging van een Unierechtelijke bepaling niet alleen rekening moet worden gehouden met de bewoordingen ervan, maar ook met de context van die bepaling, de doelstellingen van de regeling waarvan zij deel uitmaakt en, met name, de ontstaansgeschiedenis van die regeling (zie in die zin arrest van 17 april 2018, Egenberger, C-414/16, EU:C:2018:257, punt 44).

106 Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen „zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie".

107 Daartoe legt artikel 5, lid 1, van richtlijn 2002/58 het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert het met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd.

108 Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 86 en aldaar aangehaalde rechtspraak).

109 Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.

110 Artikel 15, lid 1, van richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

111 De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104).

112 Met betrekking tot de doelstellingen die een beperking van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste zin, van deze richtlijn gegeven opsomming van doelstellingen exhaustief is, zodat een op grond van die bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet berusten op een van die doelstellingen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 52 en aldaar aangehaalde rechtspraak).

113 Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in

voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

114 Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie volgens artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, Connolly/Commissie, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).

115 In dit verband dient te worden gepreciseerd dat de bewaring van verkeers- en locatiegegevens als zodanig behalve een uitzondering op het in artikel 5, lid 1, van richtlijn 2002/58 gestelde verbod op de opslag van die gegevens door anderen dan de gebruikers, ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens vormt, waarbij niet van belang is of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak; zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 30 januari 2020, Breyer tegen Duitsland, CE:ECHR:2020:0130JUD005000112, § 81].

116 Het is ook irrelevant of de bewaarde gegevens vervolgens al dan niet worden gebruikt (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 16 februari 2000, Amann tegen Zwisterland, CE:ECHR:2000:0216JUD002779895, § 69, en 13 februari 2020, Trjakovski en Chipovski tegen Noord-Macedonië, CE:ECHR:2020:0213JUD005320513, § 51), aangezien de toegang tot die gegevens, ongeacht het latere gebruik ervan, op zichzelf al een inmenging vormt in de in het voorgaande punt genoemde grondrechten [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126].

117 Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, Digital Rights, C-293/12 en C-594/12, EU:C:2014:238, punt 27, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 99).

118 De bewaring van verkeers- en locatiegegevens voor politiële doeleinden kan dus om te beginnen op zichzelf afbreuk doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen (zie in die zin

arresten van 8 april 2014, Digital Rights, C-293/12 en C-594/12, EU:C:2014:238, punt 28, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 101). Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn.

119 Bovendien is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene en ongedifferentieerde bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

120 Het feit dat het de lidstaten op grond van artikel 15, lid 1, van richtlijn 2002/58 is toegestaan om te voorzien in de in punt 110 van het onderhavige arrest bedoelde uitzonderingen, heeft ermee te maken dat de in de artikelen 7, 8 en 11 van het Handvest verankerde rechten geen absolute gelding hebben, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

121 Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, 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.

122 Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 in het licht van het Handvest moet derhalve ook rekening worden gehouden met het belang van de door de artikelen 3, 4, 6 en 7 van het Handvest gewaarborgde rechten en met dat van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van ernstige criminaliteit, die bijdragen tot de bescherming van de rechten en vrijheden van anderen.

123 Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punt 47; 28 juli 2016, JZ, C-294/16 PPU, EU:C:2016:610, punt 48, en 19 september 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, punt 42 en aldaar aangehaalde rechtspraak).

124 Voorts zij eraan herinnerd dat artikel 52, lid 3, van het Handvest beoogt te zorgen voor de nodige samenhang tussen de in het Handvest vervatte rechten en de daarmee corresponderende, door het EVRM gewaarborgde rechten, zonder de autonomie van het Unierecht en van het Hof van Justitie van de Europese Unie aan te tasten. Bijgevolg dient bij de uitlegging van het Handvest rekening te worden gehouden met de overeenkomstige rechten van het EVRM, die het minimale beschermingsniveau bepalen [zie in die zin arresten van 12 februari 2019, TC, C-492/18 PPU, EU:C:2019:108, punt 57, en 21 mei 2019, Commissie/Hongarije (Vruchtgebruik op landbouwgrond), C-235/17, EU:C:2019:432, punt 72 en aldaar aangehaalde rechtspraak].

125 Artikel 5 EVRM, waarin het „recht op vrijheid" en het „recht op veiligheid" zijn verankerd, beoogt volgens de rechtspraak van het EHRM eenieder te beschermen tegen willekeurige en ongerechtvaardigde vrijheidsontneming (zie in die zin EHRM, 18 maart 2008, Ladent tegen Polen, CE:ECHR:2008:0318JUD001103603, §§ 45 en 46; 29 maart 2010, Medvedyev e.a. tegen Frankrijk, CE:ECHR:2010:0329JUD000339403, §§ 76 en 77, en 13 december 2012, El-Masri tegen „The former

Yugoslav Republic of Macedonia", CE:ECHR:2012:1213JUD003963009, § 239). Die bepaling ziet echter op vrijheidsontneming door overheidsinstanties, zodat artikel 6 van het Handvest niet aldus kan worden uitgelegd dat het de overheid een verplichting oplegt om specifieke maatregelen te nemen teneinde bepaalde strafbare handelingen tegen te gaan.

126 Wat daarentegen in het bijzonder de door het Grondwettelijk Hof genoemde effectieve bestrijding betreft van strafbare handelingen waarvan met name minderjarigen en andere kwetsbare personen het slachtoffer zijn, moet worden beklemtoond dat uit artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter bescherming van het privéleven en het familie- en gezinsleven [zie in die zin arrest van 18 juni 2020, Commissie/Hongarije (Transparantie van verenigingen), C-78/18, EU:C:2020:476, punt 123 en aldaar aangehaalde rechtspraak van het EHRM). Dergelijke verplichtingen kunnen ook uit dat artikel voortvloeien ten aanzien van de bescherming van iemands woning en communicatie, en uit de artikelen 3 en 4 van het Handvest ten aanzien van de bescherming van iemands lichamelijke en geestelijke integriteit en het verbod op folteringen en onmenselijke en vernederende behandelingen.

127 Gelet op die verschillende positieve verplichtingen is het noodzakelijk de diverse op het spel staande belangen en rechten met elkaar te verzoenen.

128 Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, Osman tegen Verenigd Koninkrijk, CE:ECHR:1998:1028JUD002345294, §§ 115 en 116; 4 maart 2004, M.C. tegen Bulgarije, CE:ECHR:2003:1204JUD003927298, § 151; 24 juni 2004, Von Hannover tegen Duitsland, CE:ECHR:2004:0624JUD005932000, §§ 57 en 58, en 2 december 2008, K.U. tegen Finland, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 en 49).

129 Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel „in een democratische samenleving noodzakelijk, redelijk en proportioneel is" in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel „strikt" evenredig moet zijn aan het nagestreefde doel.

130 In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, Volker und Markus Schecke en Eifert,

C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].

131 Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 55 en aldaar aangehaalde rechtspraak).

132 Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

133 Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 191 en aldaar aangehaalde rechtspraak, en arrest van 3 oktober 2019, A e.a., C-70/18, EU:C:2019:823, punt 63].

– Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid

134 Het Hof heeft zich in zijn arresten betreffende de uitlegging van richtlijn 2002/58 nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid, waaraan is gerefereerd door de verwijzende rechters en de regeringen die opmerkingen hebben ingediend.

135 In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.

136 Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van – zelfs ernstige –

criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich – zelfs ernstige – spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.

137 In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronischecommunicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen gedurende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

138 Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk. Het valt weliswaar niet uit te sluiten dat het aan aanbieders van elektronischecommunicatiemiddelen opgelegde bevel tot bewaring van die gegevens kan worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode. Een dergelijke gegevensbewaring moet bovendien zijn onderworpen aan beperkingen en zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens van de betrokken personen doeltreffend worden beschermd tegen het risico van misbruik. Die bewaring mag derhalve geen stelselmatig karakter hebben.

139 Gelet op de ernst van de inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten die een dergelijke algemene en ongedifferentieerde bewaring van gegevens met zich brengt, dient te worden gewaarborgd dat de toepassing van die maatregel daadwerkelijk beperkt blijft tot situaties waarin de nationale veiligheid ernstig wordt bedreigd, zoals de in de punten 135 en 136 van het onderhavige arrest bedoelde situaties. Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

– Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

140 Als het gaat om de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, kunnen overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, zoals die welke voortvloeien uit de bewaring van verkeers- en

locatiegegevens. De doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, kan derhalve enkel niet-ernstige inmengingen in die grondrechten rechtvaardigen [zie in die zin arresten van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 102, en 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punten 56 en 57; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 149].

141 Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 107).

142 Gezien het gevoelige karakter van de informatie die verkeers- en locatiegegevens kunnen prijsgeven, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op het in punt 118 van het onderhavige arrest bedoelde ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest verankerde grondrechten, en op de ernst van de inmenging die een dergelijke bewaring met zich brengt, is het in een democratische samenleving dan ook van belang dat deze bewaring, zoals het bij richtlijn 2002/58 ingevoerde stelsel eist, de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend.

143 Voorts heeft het Hof benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel. Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat die personen zich – zelfs maar indirect – in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen, wat in strijd is met het in punt 133 van het onderhavige arrest in herinnering gebrachte vereiste. Zij is 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 die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid (zie in die zin arresten van 8 april 2014, Digital Rights, C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 105).

144 Zoals het Hof reeds heeft geoordeeld, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit (zie in die zin arresten van 8 april 2014, Digital Rights, C-293/12 en C-594/12, EU:C:2014:238, punt 59, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 106).

145 Zelfs de positieve verplichtingen die, naargelang van het geval, voor de lidstaten kunnen voortvloeien uit de artikelen 3, 4 en 7 van het Handvest en, zoals in de punten 126 en 128 van het onderhavige arrest is opgemerkt, betrekking hebben op de invoering van regels die een effectieve bestrijding van strafbare feiten mogelijk maken, kunnen geen inmengingen rechtvaardigen die zo ernstig zijn als de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van vrijwel de

gehele bevolking die een regeling die voorziet in de bewaring van verkeers- en locatiegegevens met zich brengt, zonder dat de gegevens van de betrokken personen, althans indirect, een verband met het nagestreefde doel aan het licht kunnen brengen.

146 Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, a fortiori, bescherming van de nationale veiligheid – gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd – de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.

147 Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 108).

148 De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111).

149 In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zij die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150 Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151 Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

– Wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

152 Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153 Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben.

154 Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder c), van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (PB 2011, L 335, blz. 1).

155 In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt, en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

156 Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de

bescherming van de nationale veiligheid, die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel. Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.

157 Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als „ernstig” worden aangemerkt (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punten 59 en 60).

158 Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 62).

159 Gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, moet in deze omstandigheden om de in de punten 131 en 158 van het onderhavige arrest uiteengezette redenen worden geoordeeld dat, ook al bestaat er geen verband tussen alle gebruikers van elektronischecommunicatiemiddelen en de nagestreefde doelstellingen, artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 2, van het Handvest, zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronischecommunicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers van elektronischecommunicatiemiddelen gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.

– Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit

160 Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die richtlijn moeten worden verwerkt en opgeslagen.

161 Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen

wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162 In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen – nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

163 In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164 Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165 In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of

gepleegd. Bovendien moet aan de bevoegde autoriteiten toegang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin richtlijn 2002/58 is uitgelegd (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 118-121 en aldaar aangehaalde rechtspraak).

166 Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167 In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58.

168 Gelet op een en ander moet op de eerste vraag in de zaken C-511/18 en C-512/18 en op de eerste en de tweede vraag in zaak C-520/18 worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

– die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

Tweede en derde vraag in zaak C-511/18

169 Met de tweede en de derde vraag in zaak C-511/18 wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die aan aanbieders van elektronischecommunicatiediensten de verplichting oplegt om op hun netwerken maatregelen toe te passen die het mogelijk maken om, ten eerste, verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, maar die niet bepaalt dat de betrokken personen over die verwerkingen en opvragingen moeten worden geïnformeerd.

170 De verwijzende rechter wijst erop dat de in de artikelen L. 851-2 tot en met L. 851-4 CSI genoemde technieken voor het inwinnen van inlichtingen voor aanbieders van elektronischecommunicatiediensten geen specifieke verplichting tot bewaring van verkeers- en locatiegegevens impliceren. Wat in het bijzonder de in artikel L. 851-3 CSI bedoelde geautomatiseerde analyse betreft, merkt die rechter op dat deze verwerking bedoeld is om aan de hand van daartoe vastgestelde criteria verbindingen op te sporen die kunnen wijzen op een terroristische dreiging. Met betrekking tot de in artikel L. 851-2 CSI bedoelde opvraging in real time stelt de verwijzende rechter vast dat deze slechts betrekking heeft op een of meer personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging. Volgens de verwijzende rechter kunnen die twee technieken uitsluitend worden toegepast ter voorkoming van terrorisme en betreffen zij de in de artikelen L. 851-1 en R. 851-5 CSI bedoelde gegevens.

171 Om te beginnen dient te worden gepreciseerd dat het feit dat volgens artikel L. 851-3 CSI de in deze bepaling geregelde geautomatiseerde analyse het op zichzelf niet mogelijk maakt om de gebruikers te identificeren van wie de gegevens aan die analyse worden onderworpen, niet aan de kwalificatie van die gegevens als „persoonsgegevens” in de weg staat. Aangezien de procedure van punt IV van diezelfde bepaling het mogelijk maakt om de persoon of de personen op wie de gegevens betrekking hebben waarvan de geautomatiseerde analyse een mogelijke terroristische dreiging aan het licht heeft gebracht, in een later stadium te identificeren, blijven immers alle personen op wier gegevens die

analyse worden toegepast, aan de hand van die gegevens identificeerbaar. Volgens de in artikel 4, punt 1, van verordening 2016/679 opgenomen definitie van het begrip „persoonsgegevens" omvat dit begrip onder meer informatie over een identificeerbare persoon.

Geautomatiseerde analyse van verkeers- en locatiegegevens

172 Uit artikel L. 851-3 CSI blijkt dat de in deze bepaling geregelde geautomatiseerde analyse in wezen erop neerkomt dat aanbieders van elektronischecommunicatiediensten op verzoek van de bevoegde nationale autoriteiten en in overeenstemming met de door die autoriteiten vastgestelde parameters alle door hen bewaarde verkeers- en locatiegegevens filteren. Dit betekent dat van alle gegevens van de gebruikers van elektronischecommunicatiemiddelen wordt nagegaan of zij met die parameters corresponderen. Derhalve moet worden aangenomen dat een dergelijke geautomatiseerde analyse inhoudt dat aanbieders van elektronischecommunicatiediensten in opdracht van de bevoegde autoriteit overgaan tot een algemene en ongedifferentieerde verwerking van alle verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen, in die zin dat die gegevens via een geautomatiseerd procedé worden gebruikt in de zin van artikel 4, punt 2, van verordening 2016/679. Die verwerking staat los van de latere, op grond van artikel L. 851-3, lid IV, CSI toegestane opvraging van de gegevens betreffende de personen die na de geautomatiseerde analyse zijn geïdentificeerd.

173 Een nationale regeling die een dergelijke geautomatiseerde analyse van verkeers- en locatiegegevens toestaat, wijkt af van de in artikel 5 van richtlijn 2002/58 neergelegde principeverplichting om de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens te waarborgen. Een dergelijke regeling vormt ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. Tot slot kan zo'n regeling een ontmoedigend effect hebben op de uitoefening van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting.

174 Voorts is de inmenging die het gevolg is van een geautomatiseerde analyse van verkeers- en locatiegegevens als aan de orde in het hoofdgeding bijzonder ernstig, daar zij op algemene en ongedifferentieerde wijze de gegevens betreft van personen die gebruikmaken van elektronischecommunicatiemiddelen. Dit geldt te meer nu de gegevens die aan de geautomatiseerde analyse worden onderworpen, zoals uit de in het hoofdgeding aan de orde zijnde nationale regeling blijkt, de aard van de online geraadpleegde informatie kunnen onthullen. Bovendien vindt een dergelijke geautomatiseerde analyse algemeen plaats bij alle personen die gebruikmaken van elektronischecommunicatiemiddelen, dat wil zeggen ook bij personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met terroristische activiteiten.

175 Wat de rechtvaardiging van een dergelijke inmenging betreft, moet worden gepreciseerd dat het in artikel 52, lid 1, van het Handvest geformuleerde vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 175 en aldaar aangehaalde rechtspraak).

176 Om te voldoen aan het in de punten 130 en 131 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, moet een nationale regeling die de toegang van de bevoegde autoriteiten tot de bewaarde verkeers- en locatiegegevens regelt, bovendien in overeenstemming zijn met de vereisten die voortvloeien uit de in punt 132 van het onderhavige arrest aangehaalde rechtspraak. Met name mag een dergelijke regeling zich er niet toe beperken te eisen dat de autoriteiten toegang tot de gegevens wordt verleend voor het doel dat met

die regeling wordt nagestreefd, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].

177 In dit verband zij eraan herinnerd dat de bijzonder ernstige inmenging die het gevolg is van een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, zoals besproken in de punten 134 tot en met 139 van het onderhavige arrest, en de bijzonder ernstige inmenging die de geautomatiseerde analyse van die gegevens met zich brengt, slechts aan het evenredigheidsvereiste kunnen voldoen in situaties waarin een lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en op voorwaarde dat de duur van die bewaring tot het strikt noodzakelijke wordt beperkt.

178 In situaties als bedoeld in het voorgaande punt kan een geautomatiseerde analyse van de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen, gedurende een periode die niet langer is dan strikt noodzakelijk, gelet op de vereisten die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, als gerechtvaardigd worden beschouwd.

179 Om te garanderen dat de toepassing van een dergelijke maatregel daadwerkelijk beperkt blijft tot hetgeen strikt noodzakelijk is ter bescherming van de nationale veiligheid en, meer bepaald, ter voorkoming van terrorisme, is het echter, overeenkomstig hetgeen is vastgesteld in punt 139 van het onderhavige arrest, van wezenlijk belang dat de beslissing waarbij de geautomatiseerde analyse wordt toegestaan, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of zich een situatie voordoet die die maatregel rechtvaardigt, en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

180 In dit verband dient te worden gepreciseerd dat de vooraf vastgestelde modellen en criteria waarop dit type gegevensverwerking is gebaseerd, ten eerste specifiek en betrouwbaar moeten zijn, zodat zij tot resultaten leiden waarmee die personen worden geïdentificeerd op wie een redelijk vermoeden van deelneming aan terrorisme kan rusten, en ten tweede niet mogen discrimineren [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 172].

181 Voorts zij eraan herinnerd dat elke geautomatiseerde analyse aan de hand van modellen en criteria die ervan uitgaan dat de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, de gezondheid of het seksueel gedrag van een persoon op zichzelf en los van het individuele gedrag van die persoon relevant zouden kunnen zijn in het licht van het voorkomen van terrorisme, in strijd zou zijn met de door de artikelen 7 en 8 juncto artikel 21 van het Handvest gewaarborgde rechten. De modellen en criteria die vooraf worden vastgesteld ten behoeve van een geautomatiseerde analyse die tot doel heeft terroristische activiteiten die een ernstige bedreiging vormen voor de nationale veiligheid, te voorkomen, kunnen dus niet alleen op die gevoelige gegevens zijn gebaseerd [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 165].

182 Aangezien geautomatiseerde analyses van verkeers- en locatiegegevens noodzakelijkerwijs een zekere foutenmarge bevatten, moet bovendien elk positief resultaat van een geautomatiseerde verwerking nog eens individueel – met niet-geautomatiseerde middelen – worden onderzocht alvorens een individuele maatregel wordt genomen die nadelige gevolgen heeft voor de betrokken personen, zoals de latere opvraging in real time van de betrokken gegevens. Een dergelijke maatregel mag namelijk niet uitsluitend op het resultaat van een geautomatiseerde verwerking worden gebaseerd. Om te garanderen dat de vooraf vastgestelde modellen en criteria, het gebruik dat daarvan wordt gemaakt en de gehanteerde databases in de praktijk niet discrimineren en beperkt blijven tot hetgeen strikt noodzakelijk is in het licht van de doelstelling terroristische activiteiten die een ernstige bedreiging opleveren voor de nationale veiligheid, te voorkomen, moet ook regelmatig worden onderzocht of die

vooraf vastgestelde modellen en criteria en de gebruikte databases betrouwbaar en up-to-date zijn [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 173 en 174].

Opvraging in real time van verkeers- en locatiegegevens

183 Voor de in artikel L. 851-2 CSI geregelde opvraging in real time van verkeers- en locatiegegevens kan individueel machtiging worden verleend voor zover het gaat om „een persoon die eerder in verband is gebracht met een [terroristische] dreiging". In diezelfde bepaling staat dat „[w]anneer er zwaarwegende redenen zijn om aan te nemen dat een of meer personen uit de omgeving van de persoon op wie de machtiging betrekking heeft, informatie kunnen verstrekken voor het doel waarvoor de machtiging is verleend, [...] de machtiging ook individueel voor elk van die personen [kan] worden verleend".

184 De gegevens waarop een dergelijke maatregel betrekking heeft, stellen de bevoegde nationale autoriteiten in staat om voor de duur van de machtiging continu en in real time in de gaten te houden met wie, met welke middelen en hoelang de betrokken personen communiceren, alsook waar zij verblijven en waarheen zij zich verplaatsen. Ook lijkt uit die gegevens de aard van de online geraadpleegde informatie te kunnen worden afgeleid. Zoals uit punt 117 van het onderhavige arrest blijkt, kunnen uit die gegevens, in hun geheel genomen, zeer precieze conclusies worden getrokken over het privéleven van de betrokken personen, en kan aan de hand van die gegevens het profiel van deze personen worden bepaald, informatie die vanuit het oogpunt van het recht op eerbiediging van het privéleven even gevoelig is als de inhoud zelf van de communicatie.

185 Met betrekking tot de in artikel L. 851-4 CSI geregelde opvraging in real time van gegevens moet worden opgemerkt dat op grond van deze bepaling technische gegevens betreffende de locatie van de eindapparatuur kunnen worden opgevraagd en in real time kunnen worden doorgezonden aan een onder de eerste minister ressorterende dienst. Dergelijke gegevens stellen de bevoegde dienst in staat om voor de duur van de machtiging continu en in real time de locatie te bepalen van gebruikte eindapparatuur, zoals mobiele telefoons.

186 Een nationale regeling die een dergelijke opvraging in real time van gegevens toestaat, wijkt – net zoals nationale wetgeving die de geautomatiseerde analyse van gegevens toestaat – af van de in artikel 5 van richtlijn 2002/58 neergelegde principeverplichting om de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens te waarborgen. Zij vormt derhalve ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten en kan een ontmoedigend effect hebben op de uitoefening van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting.

187 Benadrukt dient te worden dat de inmenging die de opvraging in real time van gegevens aan de hand waarvan een eindapparaat kan worden gelokaliseerd, met zich brengt, bijzonder ernstig is, aangezien die gegevens de bevoegde nationale autoriteiten in staat stellen om de verplaatsingen van gebruikers van mobiele telefoons nauwkeurig en permanent te volgen. Aangezien dergelijke gegevens dus als bijzonder gevoelig moeten worden beschouwd, dient de realtimetoegang van de bevoegde autoriteiten tot die gegevens te worden onderscheiden van de toegang daartoe die niet in real time plaatsvindt. De eerste soort toegang is ingrijpender omdat deze het mogelijk maakt om vrijwel alle gangen van de betrokken gebruikers na te gaan (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 8 februari 2018, Ben Faiza tegen Frankrijk, CE:ECHR:2018:0208JUD003144612, § 74). Die inmenging gaat nog verder wanneer de opvraging in real time zich ook uitstrekt tot de verkeersgegevens van de betrokken personen.

188 De doelstelling van voorkoming van terrorisme die met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan weliswaar wegens het belang ervan de inmenging rechtvaardigen die de opvraging in real time van verkeers- en locatiegegevens met zich brengt, maar

een dergelijke maatregel kan, gelet op het bijzonder ingrijpende karakter ervan, slechts worden toegepast met betrekking tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten. De gegevens van niet tot deze categorie behorende personen kunnen uitsluitend openstaan voor niet-realtime-toegang, die overeenkomstig de rechtspraak van het Hof slechts kan worden verleend in bijzondere situaties, zoals die waarin terroristische activiteiten aan de orde zijn, en wanneer op grond van objectieve factoren kan worden geoordeeld dat deze gegevens in het concrete geval daadwerkelijk tot de bestrijding van terrorisme zouden kunnen bijdragen (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).

189 Bovendien moet een beslissing waarbij machtiging wordt verleend voor de opvraging in real time van verkeers- en locatiegegevens, gebaseerd zijn op objectieve, in de nationale wetgeving vastgestelde criteria. Die wetgeving moet overeenkomstig de in punt 176 van het onderhavige arrest aangehaalde rechtspraak in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een dergelijke opvraging kan worden toegestaan, en bepalen dat, zoals in het voorgaande punt is gepreciseerd, deze maatregel slechts kan worden toegepast met betrekking tot personen die in verband kunnen worden gebracht met de doelstelling van voorkoming van terrorisme. Om te garanderen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toepassing van de maatregel waarbij machtiging wordt verleend voor de opvraging in real time van gegevens, is onderworpen aan voorafgaande rechterlijke toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij die instantie of autoriteit zich met name ervan dient te vergewissen dat die opvraging slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 120). In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

Informatieverstrekking aan de personen van wie de gegevens zijn opgevraagd of geanalyseerd

190 Het is van belang dat de bevoegde nationale autoriteiten die in real time verkeers- en locatiegegevens opvragen, de betrokken personen in het kader van de toepasselijke nationale procedures daarover informeren zodra deze informatieverstrekking geen gevaar meer kan opleveren voor de taken die zij moeten uitvoeren. Deze informatieverstrekking is immers noodzakelijk om die personen in staat te stellen hun uit de artikelen 7 en 8 van het Handvest voortvloeiende rechten uit te oefenen, inzage te vragen in de persoonsgegevens die in real time zijn opgevraagd, en in voorkomend geval rectificatie of vernietiging van die gegevens te verlangen, alsook overeenkomstig artikel 47, eerste alinea, van het Handvest een doeltreffende voorziening in rechte in te stellen. Dat recht van beroep wordt overigens uitdrukkelijk gewaarborgd door artikel 15, lid 2, van richtlijn 2002/58, gelezen in samenhang met artikel 79, lid 1, van verordening 2016/679 [zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 121 en aldaar aangehaalde rechtspraak, en advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017 2017, EU:C:2017:592, punten 219 en 220].

191 Wat de in het kader van een geautomatiseerde analyse van verkeers- en locatiegegevens te verstrekken informatie betreft, moet worden opgemerkt dat de bevoegde nationale autoriteit verplicht is om algemene inlichtingen inzake die analyse te publiceren, maar de betrokken personen niet individueel hoeft in te lichten. Wanneer die gegevens beantwoorden aan de parameters die zijn bepaald in de maatregel waarbij machtiging is verleend voor de geautomatiseerde analyse, en die autoriteit de betrokken persoon identificeert met als doel om de op hem of haar betrekking hebbende gegevens nader te analyseren, is het daarentegen wel noodzakelijk om die persoon individueel te informeren. Een dergelijke informatieverstrekking mag evenwel pas geschieden zodra dit geen gevaar meer kan opleveren voor de door die autoriteit uit te voeren taken [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 222-224].

192 Gelet op een en ander moet op de tweede en de derde vraag in zaak C-511/18 worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer

– die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer

– het in real time opvragen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

Tweede vraag in zaak C-512/18

193 Met de tweede vraag in zaak C-512/18 wenst de verwijzende rechter in wezen te vernemen of de bepalingen van richtlijn 2000/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij zich verzetten tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

194 De verwijzende rechter, die van mening is dat dergelijke diensten binnen de werkingssfeer van richtlijn 2000/31 en niet binnen die van richtlijn 2002/58 vallen, stelt zich op het standpunt dat artikel 15, leden 1 en 2, van richtlijn 2000/31, gelezen in samenhang met de artikelen 12 en 14 van deze richtlijn, als zodanig geen principieel verbod op het bewaren van gegevens inzake de creatie van inhoud invoert waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Hij vraagt zich niettemin af of dit standpunt aanvaardbaar is, gelet op de noodzaak om de in de artikelen 6 tot en met 8 en 11 van het Handvest verankerde grondrechten te eerbiedigen.

195 De verwijzende rechter verduidelijkt voorts dat zijn vraag ziet op de bewaarplicht die is neergelegd in artikel 6 LCEN, gelezen in samenhang met decreet nr. 2011-219. Tot de gegevens die de betrokken aanbieders van diensten uit dien hoofde dienen te bewaren, behoren onder meer de gegevens betreffende de burgerlijke identiteit van de personen die van die diensten hebben gebruikgemaakt, zoals hun naam, voornaam, hun bijbehorende postadressen, hun bijbehorende e-mail- of accountadressen, hun wachtwoorden en, wanneer het ondertekenen van het contract of het aanmaken van het account plaatsvindt tegen betaling, de gebruikte betaalsoort, de betalingsreferentie, het bedrag en de datum en het tijdstip van de transactie.

196 Tot de te bewaren gegevens behoren ook de identificatoren van de abonnees, van de verbindingen en van de gebruikte eindapparatuur, de aan de inhoud toegekende identificatoren, de datum en het tijdstip van het begin en het einde van de verbindingen en verrichtingen, en de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud. De bewaartermijn voor die gegevens bedraagt één jaar en er kan om toegang tot die gegevens worden verzocht in het kader van strafrechtelijke en civielrechtelijke procedures, om de regels inzake civielrechtelijke of strafrechtelijke aansprakelijkheid te doen naleven, en in het kader van maatregelen voor het inwinnen van inlichtingen waarop artikel L. 851-1 CSI van toepassing is.

197 In dit verband moet worden opgemerkt dat richtlijn 2000/31 volgens artikel 1, lid 2, bepaalde nationale bepalingen nader tot elkaar brengt die van toepassing zijn op de diensten van de informatiemaatschappij in de zin van artikel 2, onder a).

198 Tot die diensten behoren onder meer die welke op individueel verzoek van een afnemer van diensten en gewoonlijk tegen vergoeding worden verricht via elektronische apparatuur voor de verwerking en de opslag van gegevens op afstand, zoals diensten waarbij toegang wordt verschaft tot het internet of tot een communicatienetwerk, en opslagdiensten (zie in die zin arresten van 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punt 40; 16 februari 2012, SABAM, C-360/10, EU:C:2012:85, punt 34; 15 september 2016, Mc Fadden, C-484/14, EU:C:2016:689, punt 55, en 7 augustus 2018, SNB-REACT, C-521/17, EU:C:2018:639, punt 42 en aldaar aangehaalde rechtspraak).

199 Artikel 1, lid 5, van richtlijn 2000/31 bepaalt evenwel dat deze richtlijn niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder richtlijnen 95/46 en 97/66 vallen. Dienaangaande blijkt uit de overwegingen 14 en 15 van richtlijn 2000/31 dat de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij uitsluitend wordt beheerst door richtlijnen 95/46 en 97/66. Laatstgenoemde richtlijn stelt ter waarborging van de vertrouwelijkheid van communicatie in artikel 5 een verbod op iedere vorm van onderschepping of bewaking van berichten.

200 Vragen die verband houden met de bescherming van het vertrouwelijke karakter van communicatie en van persoonsgegevens moeten derhalve worden beoordeeld aan de hand van richtlijn 2002/58 en verordening 2016/679, die in de plaats zijn gekomen van, respectievelijk, richtlijn 97/66 en richtlijn 95/46, waarbij moet worden aangetekend dat de bescherming die richtlijn 2000/31 beoogt te verzekeren, hoe dan ook geen afbreuk mag doen aan de vereisten die voortvloeien uit richtlijn 2002/58 en verordening 2016/679 (zie in die zin arrest van 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punt 57).

201 De bewaarplicht die de in punt 195 van het onderhavige arrest bedoelde nationale regeling oplegt aan aanbieders die het publiek online toegang geven tot communicatiediensten en aanbieders van opslagdiensten, en die betrekking heeft op de met die diensten verband houdende persoonsgegevens, moet dus worden getoetst aan richtlijn 2002/58 of verordening 2016/679, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 141 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6).

202 Afhankelijk van de vraag of de levering van de diensten waarop die nationale regeling betrekking heeft, al dan niet onder richtlijn 2002/58 valt, zal die levering derhalve ofwel worden beheerst door deze richtlijn, in het bijzonder door artikel 15, lid 1, ervan, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, ofwel door verordening 2016/679, in het bijzonder door artikel 23, lid 1, van deze verordening, gelezen in het licht van dezelfde bepalingen van het Handvest.

203 Zoals de Europese Commissie in haar schriftelijke opmerkingen heeft gesteld, valt in casu niet uit te sluiten dat sommige van de diensten waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling betrekking heeft, elektronischecommunicatiediensten in de zin van richtlijn 2002/58 zijn, hetgeen de verwijzende rechter dient na te gaan.

204 In dit verband moet worden opgemerkt dat richtlijn 2002/58 van toepassing is op elektronischecommunicatiediensten die voldoen aan de voorwaarden die vermeld staan in artikel 2, onder c), van richtlijn 2002/21, waarnaar artikel 2 van richtlijn 2002/58 verwijst en waarin een elektronischecommunicatiedienst wordt gedefinieerd als „een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt". Wat de door richtlijn 2000/31 bestreken diensten van de informatiemaatschappij als bedoeld in de punten 197 en 198 van het onderhavige arrest betreft, deze diensten zijn elektronischecommunicatiediensten indien zij geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken. (zie in die zin arrest van 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punten 47 en 48).

205 Internettoegangsdiensten, waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling van toepassing lijkt te zijn, zijn derhalve elektronischecommunicatiediensten in de zin van richtlijn 2002/21, zoals in overweging 10 van deze richtlijn wordt bevestigd (zie in die zin arrest van 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punt 37). Dit geldt ook voor webgebaseerde e-maildiensten, die mogelijk eveneens onder die nationale regeling vallen, aangezien die diensten technisch gezien kunnen worden beschouwd als diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken (zie in die zin arrest van 13 juni 2019, Google, C-193/18, EU:C:2019:498, punten 35 en 38).

206 Wat de vereisten betreft die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zij verwezen naar alle vaststellingen en beoordelingen in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18.

207 Wat de uit verordening 2016/679 voortvloeiende vereisten betreft, zij eraan herinnerd dat deze verordening, zoals blijkt uit overweging 10 ervan, met name een consistent en hoog niveau van bescherming van natuurlijke personen binnen de Unie beoogt te waarborgen en daartoe een coherente en homogene toepassing van de regels inzake bescherming van de grondrechten van deze personen in verband met de verwerking van persoonsgegevens binnen de gehele Unie wil verzekeren (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 101).

208 Daartoe moeten bij elke verwerking van persoonsgegevens, behoudens de op grond van artikel 23 van verordening 2016/679 toegestane uitzonderingen, de in hoofdstuk II van deze verordening neergelegde beginselen inzake verwerking van persoonsgegevens en de in hoofdstuk III van deze verordening geregelde rechten van de betrokkene worden geëerbiedigd. In het bijzonder moet elke verwerking van persoonsgegevens ten eerste in overeenstemming zijn met de in artikel 5 van verordening 2016/679 geformuleerde beginselen, en ten tweede voldoen aan de in artikel 6 van deze verordening opgesomde rechtmatigheidsvoorwaarden (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 30 mei 2013, Worten, C-342/12, EU:C:2013:355, punt 33 en aldaar aangehaalde rechtspraak).

209 Wat meer bepaald artikel 23, lid 1, van verordening 2016/679 betreft, moet worden opgemerkt dat deze bepaling – net als artikel 15, lid 1, van richtlijn 2002/58 – de lidstaten de mogelijkheid biedt om met het oog op de erin genoemde doelstellingen via wetgevingsmaatregelen de reikwijdte van de erin bedoelde verplichtingen en rechten te beperken, „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" het nagestreefde doel. Elke op die grondslag vastgestelde wettelijke maatregel moet met name voldoen aan de specifieke vereisten die zijn geformuleerd in artikel 23, lid 2, van verordening 2016/679.

210 Artikel 23, leden 1 en 2, van verordening 2016/679 kan derhalve niet aldus worden uitgelegd dat het de lidstaten de bevoegdheid kan verlenen om afbreuk te doen aan de eerbiediging van de persoonlijke levenssfeer, in strijd met artikel 7 van het Handvest, of aan de andere door het Handvest geboden waarborgen (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 20 mei 2003, arrest van 20 mei 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 en C-139/01, EU:C:2003:294, punt 91). Net zoals geldt voor artikel 15, lid 1, van richtlijn 2002/58, is het met name zo dat de bevoegdheid die artikel 23, lid 1, van verordening 2016/679 de lidstaten verleent, slechts kan worden uitgeoefend in overeenstemming met het evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 7 november 2013, IPI, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

211 Bijgevolg gelden de vaststellingen die zijn gedaan in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en van de eerste en de tweede vraag in zaak C-520/18, en de beoordelingen die in dat kader zijn verricht, mutatis mutandis voor artikel 23 van verordening 2016/679.

212 Gelet op een en ander moet op de tweede vraag in zaak C-512/18 worden geantwoord dat richtlijn 2000/31 aldus moet worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58 of verordening 2016/679. Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

Derde vraag in zaak C-520/18

213 Met de derde vraag in zaak C-520/18 wenst de verwijzende rechter in wezen te vernemen of een nationale rechterlijke instantie een bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd van een onwettigverklaring te beperken wanneer hij op grond van dit recht een nationale wettelijke regeling die ten behoeve van onder meer de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, onwettig dient te verklaren omdat zij onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

214 Het beginsel van het primaat van het Unierecht houdt in dat dit recht voorrang heeft op het recht van de lidstaten. Dit beginsel verplicht dus alle instanties van de lidstaten om volle werking te verlenen aan de verschillende normen van de Unie, aangezien het recht van de lidstaten niet kan afdoen aan de werking die op het grondgebied van die staten aan deze verschillende normen is verleend [arrest van 15 juli 1964, Costa, 6/64, EU:C:1964:66, blz. 1219 en 1220, en 19 november 2019, A. K. e.a. (Onafhankelijkheid van de tuchtkamer van de Sąd Najwyższy), C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punten 157 en 158 en aldaar aangehaalde rechtspraak].

215 Het voorrangsbeginsel brengt mee dat, indien de nationale regelgeving niet in overeenstemming met de vereisten van het Unierecht kan worden uitgelegd, de nationale rechter die in het kader van zijn bevoegdheid is belast met de toepassing van de bepalingen van het Unierecht, verplicht is de volle werking van deze bepalingen te verzekeren en daarbij zo nodig, op eigen gezag, elke, zelfs latere, strijdige bepaling van de nationale wettelijke regeling buiten toepassing te laten, zonder dat hij de voorafgaande opheffing hiervan via de wetgeving of enige andere constitutionele procedure hoeft te vragen of af te wachten [arresten van 22 juni 2010, Melki en Abdeli, C-188/10 en C-189/10, EU:C:2010:363, punt 43 en aldaar aangehaalde rechtspraak; 24 juni 2019, Popławski, C-573/17, EU:C:2019:530, punt 58, en 19 november 2019, A. K. e.a. (Onafhankelijkheid van de tuchtkamer van de Sąd Najwyższy), C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punt 160].

216 Enkel het Hof kan, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting toestaan van het effect dat een regel van het Unierecht op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan. Een dergelijke beperking in de tijd van de werking van de door het Hof aan het Unierecht gegeven uitlegging kan slechts worden vastgesteld in het arrest waarin de gevraagde uitlegging wordt gegeven [zie in die zin arresten van 23 oktober 2012, Nelson e.a., C-581/10 en C-629/10, EU:C:2012:657, punten 89 en 91; 23 april 2020, Herst, C-401/18, EU:C:2020:295, punten 56 en 57, en 25 juni 2020, A e.a. (Windturbines in Aalter en Nevele), C-24/19, EU:C:2020:503, punt 84 en aldaar aangehaalde rechtspraak].

217 Aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn (zie in die zin arrest van 29 juli 2019, Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punt 177 en aldaar aangehaalde rechtspraak).

218 Het Hof heeft evenwel in een zaak waarin het draaide om de rechtmatigheid van maatregelen die waren vastgesteld in strijd met de Unierechtelijke verplichting om een voorafgaande beoordeling te verrichten van de gevolgen van een project voor het milieu of voor een beschermd gebied, geoordeeld dat een nationale rechterlijke instantie, indien het nationale recht dat toestaat, bij wijze van uitzondering de gevolgen van dergelijke maatregelen kan handhaven indien deze handhaving wordt gerechtvaardigd door dwingende redenen die verband houden met de noodzaak om het reële en ernstige risico af te wenden dat de elektriciteitsbevoorrading van de betrokken lidstaat wordt onderbroken, en aan dit risico niet het hoofd zou kunnen worden geboden met andere middelen en alternatieven, met name in het kader van de interne markt, met dien verstande dat die handhaving niet langer kan duren dan strikt noodzakelijk is om een einde te maken aan die onrechtmatigheid (zie in die zin arrest van 29 juli 2019, Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punten 175, 176, 179 en 181).

219 Anders dan de niet-nakoming van een procedurele verplichting als de voorafgaande beoordeling van de gevolgen van een project op het specifieke terrein van de milieubescherming, kan een schending van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, niet worden geregulariseerd via een procedure die vergelijkbaar is met die waaraan in het voorgaande punt wordt gerefereerd. Handhaving van de gevolgen van een nationale wettelijke regeling als in het hoofdgeding aan de orde is, zou immers betekenen dat die regeling aan aanbieders van elektronischecommunicatiediensten verplichtingen blijft opleggen die in strijd zijn met het Unierecht en leiden tot een ernstige inmenging in de grondrechten van de personen van wie de gegevens zijn bewaard.

220 Hieruit volgt dat de verwijzende rechter geen bepaling van zijn nationale recht mag toepassen die hem machtigt om de werking in de tijd te beperken van een door hem op grond van dit recht uit te spreken onwettigverklaring van de in het hoofdgeding aan de orde zijnde nationale wettelijke regeling.

221 VZ, WY en XX stellen in hun bij het Hof ingediende schriftelijke opmerkingen dat de derde vraag impliciet maar noodzakelijkerwijs de vraag opwerpt of het Unierecht zich ertegen verzet dat in het kader van een strafrechtelijke procedure wordt gebruikgemaakt van informatie en bewijzen die zijn verkregen door middel van een met dit recht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

222 Om de verwijzende rechter een nuttig antwoord te verstrekken, zij er in dit verband aan herinnerd dat het bij de huidige stand van het Unierecht uitsluitend een zaak van het nationale recht is om de regels vast te stellen met betrekking tot de aanvaarding en de beoordeling van door middel van een dergelijke met het Unierecht strijdige gegevensbewaring verkregen informatie en bewijzen in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van ernstige strafbare feiten.

223 Het is immers vaste rechtspraak dat het bij gebreke van Unieregelgeving ter zake krachtens het beginsel van procedurele autonomie een aangelegenheid van de interne rechtsorde van elke lidstaat is om de procedureregels vast te stellen voor rechtsvorderingen die ertoe strekken de rechten die de justitiabelen aan het Unierecht ontlenen, te beschermen, op voorwaarde evenwel dat die regels niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (zie in die zin arresten van 6 oktober 2015, Târşia, C-69/14, EU:C:2015:662, punten 26 en 27; 24 oktober 2018, XC e.a., C-234/17, EU:C:2018:853, punten 21 en 22 en aldaar aangehaalde rechtspraak, en 19 december 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, punt 33).

224 Wat het gelijkwaardigheidsbeginsel betreft, staat het aan de nationale rechter bij wie een strafrechtelijke procedure is aangebracht die gebaseerd is op informatie of bewijzen die in strijd met de uit richtlijn 2002/58 voortvloeiende vereisten zijn verkregen, om na te gaan of het op die procedure van toepassing zijnde nationale recht minder gunstige regels bevat voor de aanvaarding en het gebruik van dergelijke informatie en bewijzen dan voor de aanvaarding en het gebruik van informatie en bewijzen die zijn verkregen in strijd met het interne recht.

225 Met betrekking tot het doeltreffendheidsbeginsel moet worden opgemerkt dat nationale regels inzake de aanvaarding en het gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dat doel kan naar nationaal recht niet alleen worden bereikt door middel van een verbod op het gebruik van dergelijke informatie en bewijzen, maar ook door middel van nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting.

226 Uit de rechtspraak van het Hof volgt dat bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, met name moet worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben (zie in die zin arrest van 10 april 2003, Steffensen, C-276/01, EU:C:2003:228, punten 76 en 77). Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en dat bewijsmiddel uitsluiten om die schending te voorkomen (zie in die zin arrest van 10 april 2003, Steffensen, C-276/01, EU:C:2003:228, punten 78 en 79).

227 Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een

strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

228 Gelet op een en ander moet op de derde vraag in zaak C-520/18 worden geantwoord dat een nationale rechterlijke instantie geen bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

Kosten

229 Ten aanzien van de partijen in het hoofdgeding is de procedure als een aldaar gerezen incident te beschouwen, zodat de verwijzende rechter over de kosten heeft te beslissen. De door anderen wegens indiening van hun opmerkingen bij het Hof gemaakte kosten komen niet voor vergoeding in aanmerking.

Het Hof (Grote kamer) verklaart voor recht:

1) **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), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van 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 het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen**

   – **die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan**

aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

– **die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;**

– **die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;**

– **die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en**

– **die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,**

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

2) **Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer**

– **die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer**

– **het in real time opvragen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke**

maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

3) **Richtlijn 2000/31/EG 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") moet aldus worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, of door verordening (EU) 2016/679 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/EG (algemene verordening gegevensbescherming). Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.**

4) **Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.**

ondertekeningen