Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

34 537 Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens)

Nr. 3

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel voorziet in aanpassing van het Wetboek van Strafvordering en de Telecommunicatiewet vanwege het arrest van het Hof van Justitie van de Europese Unie (hierna: Hof van Justitie) in de gevoegde zaken Digital Rights Ireland en Seitlinger (C-293/12 en 294/12). In dit arrest heeft het Hof van Justitie de Richtlijn 2006/24/EG[1] (hierna: richtlijn dataretentie) ongeldig verklaard. De richtlijn dataretentie voorzag in een verplichting voor aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten tot het bewaren van een bepaalde lijst van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. De richtlijn dataretentie is geïmplementeerd met de Wet bewaarplicht telecommunicatiegegevens (Stb. 2009, 333), die op 1 september 2009 in werking is getreden. In maart 2015 heeft de voorzieningenrechter van de rechtbank Den Haag in kort geding de Wet bewaarplicht telecommunicatiegegevens buiten werking gesteld.

Dit wetsvoorstel voorziet in een herziene wettelijke regeling rond de bewaarplicht voor telecommunicatiegegevens ten behoeve van de opsporing van ernstige misdrijven. Daarbij wordt voorzien in de nodige waarborgen met betrekking tot de opslag en het gebruik van, en de toegang tot, de bewaarde gegevens, die voortvloeien uit het arrest van het Hof van Justitie en het vonnis van de voorzieningenrechter.

Mede namens de Minister van Economische Zaken licht ik het wetsvoorstel in deze memorie van toelichting toe.

[1] 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 elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (Pb L 105, blz. 54).

kst-34537-3
ISSN 0921 - 7371
's-Gravenhage 2016

2. De hoofdlijnen van het wetsvoorstel

Dit wetsvoorstel voorziet in de heroverweging van de termijnen voor het bewaren van telecommunicatiegegevens ten behoeve van het algemene belang van de opsporing en vervolging van ernstige misdrijven, zodat deze worden vastgesteld op hetgeen strikt noodzakelijk is voor dat doel. Tevens worden de verschillende categorieën van te bewaren gegevens beperkt tot de gegevens die strikt noodzakelijk zijn voor de opsporing en vervolging van ernstige misdrijven. Ten slotte wordt voorgeschreven dat de telecommunicatiegegevens op het grondgebied van de Unie worden opgeslagen en verwerkt. Dit wetsvoorstel voorziet voorts in aanpassing van het Wetboek van Strafvordering. Dit betreft de beperking van de bevoegdheid van de officier van justitie tot het vorderen van verkeersgegevens. Voorgesteld wordt dat een vordering van de officier van justitie tot verstrekking van historische verkeersgegevens, die door de aanbieders op grond van de verplichting van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven, slechts kan worden gedaan na voorafgaande rechterlijke toetsing. Daarbij geldt dat de vordering een misdrijf moet betreffen dat van een zodanige ernst is dat dit in het concrete geval het vorderen van de bewaarde verkeersgegevens door de officier van justitie rechtvaardigt. Dit betreft een extra waarborg om de toegang tot de bewaarde gegevens daadwerkelijk te beperken tot hetgeen strikt noodzakelijk is voor de bestrijding van (enkel) ernstige criminaliteit. Bij dringende noodzaak kan een vordering van de officier van justitie mondeling worden gedaan, ook de machtiging van de rechter-commissaris kan dan mondeling worden gegeven. In dat geval worden vordering en machtiging binnen drie dagen op schrift gesteld.

De bewaarplicht heeft betrekking op bepaalde telecommunicatiegegevens, dit omvat verkeersgegevens en gebruikersgegevens. Gebruikersgegevens zijn gegevens die nodig zijn om de abonnee of gebruiker van een communicatiedienst te identificeren zoals naam en adres. Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie, zoals datum, tijdstip en duur van de communicatie. Hieronder vallen ook de locatiegegevens; gegevens waarmee de geografische positie van de communicatie apparatuur kan worden bepaald aan de hand van de gebruikte zendmast.
Onder de verkeersgegevens van internet vallen gegevens over de sessies. Het betreft uitsluitend het IP-adres inclusief datum en tijdstip van de log on en log off van de communicatie. De gebruikersgegevens van internet betreffen de historische NAW-gegevens (naam, adres en woonplaats) van de IP-adressen. Dit zijn uitsluitend de gegevens die nodig zijn om achteraf te kunnen vaststellen welke persoon op een bepaald moment gebruik heeft gemaakt van een specifiek IP-adres. Het surfgedrag, zoals gegevens over welke websites personen hebben bezocht, wordt niet in het kader van de bewaarplicht bewaard. Ter illustratie, de opsporing kan in een inbeslaggenomen computer waarop een website met kinderporno werd beheerd, de IP-adressen achterhalen die deze website hebben bezocht of materiaal hebben geupload of gedownload. Die informatie kan op grond van de bewaarplicht niet worden verkregen. Maar als bekend is welk IP-adres op enig moment op die website is geweest, is nog niet bekend welke persoon daarbij betrokken is: daarvoor is het nodig dat de historische NAW-gegevens beschikbaar zijn. In het systeem van het CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) zijn slechts de actuele NAW-gegevens beschikbaar, die ten hoogste vierentwintig uur oud zijn. Wanneer daartoe aanleiding bestaat, zoals in dit voorbeeld waarbij een IP-adres gekoppeld wordt aan kinderporno, kunnen die gegevens gericht bij de aanbieders van telecommunicatiediensten worden

gevorderd ten behoeve van de opsporing van ernstige strafbare feiten, en is het mogelijk slachtoffers of verdachten te identificeren.

Hierna zal van telecommunicatiegegevens worden gesproken wanneer wordt gedoeld op de gegevens die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige strafbare feiten (bewaarplicht), op basis van de Telecommunicatiewet. Er wordt van verkeersgegevens gesproken wanneer wordt gedoeld op de bevoegdheid van de officier van justitie tot het vorderen van verkeersgegevens, op basis van artikel 126n/u van het Wetboek van Strafvordering. Dit omvat de gebruikersgegevens. Er wordt van gebruikersgegevens gesproken wanneer wordt gedoeld op de bevoegdheid van de opsporingsambtenaar tot het vorderen van de NAW-gegevens, op basis van artikel 126na/ua van het Wetboek van Strafvordering.

3. De noodzaak tot aanpassing van de wettelijke regeling voor de bewaring van telecommunicatiegegevens

In het arrest van 8 april 2014 heeft het Hof van Justitie – op verzoek van het Ierse High Court en het Oostenrijkse Verfassungsgerichtshof – de geldigheid van de richtlijn dataretentie onderzocht, met name in het licht van twee door het Handvest van de grondrechten van de Europese Unie gewaarborgde grondrechten, te weten het recht op bescherming van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Uit de toetsing van de verschillende bepalingen van de richtlijn dataretentie volgt naar het oordeel van het Hof van Justitie dat de richtlijn dataretentie geen duidelijke en precieze regels stelt over de mate van aantasting van de fundamentele rechten van het Handvest van de grondrechten. Het Hof van Justitie oordeelt dat, gelet op alle overwegingen, de wetgever van de Unie met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid, van het Handvest van de grondrechten in acht had dienen te nemen.

De Wet bewaarplicht telecommunicatiegegevens zet de door het Hof van Justitie gewraakte bepalingen van de richtlijn dataretentie om in de nationale wetgeving. Op 11 maart 2015 heeft de voorzieningenrechter van de rechtbank Den Haag vonnis gewezen in een kort geding dat door een aantal partijen (Stichting Privacy First, Nederlands Juristen Comité voor Mensenrechten, Nederlandse Verenging van Strafrechtadvocaten, Nederlandse vereniging van Journalisten, BIT B.V., SpeakUP B.V. en Voys B.V.) was aangespannen tegen de Staat der Nederlanden (ECLI:NL:RBDHA:2015:2498). De voorzieningenrechter heeft de Wet bewaarplicht telecommunicatiegegevens buiten werking gesteld. De inhoud van dit vonnis is bij dit wetsvoorstel betrokken. Naar aanleiding daarvan wordt voorgesteld een extra waarborg op te nemen om de toegang tot de historische telecommunicatiegegevens, die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige strafbare feiten, daadwerkelijk te beperken tot hetgeen strikt noodzakelijk is voor de bestrijding van (enkel) ernstige criminaliteit.
Nu de richtlijn dataretentie ongeldig is verklaard, vormt de Richtlijn 2002/58/EG (e-privacyrichtlijn) het kader waarbinnen de omgang met telecommunicatiegegevens wordt geregeld. Op grond van deze richtlijn kunnen de lidstaten regels stellen voor het bewaren van telecommunicatiegegevens, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van bepaalde belangen, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Daartoe kunnen lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode voor die

doelen te bewaren. Deze maatregelen dienen in overeenstemming te zijn met het gemeenschapsrecht, met inbegrip van de beginselen, bedoeld in het Handvest van de grondrechten en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).
Zoals reeds aangegeven, heeft de voorzieningenrechter op 11 maart 2015 alle artikelen van de Wet bewaarplicht telecommunicatiegegevens buiten werking gesteld. Ter voorkoming van mogelijke onduidelijkheid over de betekenis van de buitenwerkingstelling van deze bepalingen voor dit wetsvoorstel is er daarom voor gekozen alle buiten werking gestelde artikelen van de Wet bewaarplicht telecommunicatiegegevens met inachtneming van de aanpassingen die voortvloeien uit de jurisprudentie van het Hof van Justitie, opnieuw vast te stellen. Het gaat daarbij om de artikelen dan wel de artikelleden die van belang zijn voor het antwoord op de vraag of de Nederlandse wetgeving voldoet aan de eisen van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie.

4. De noodzaak van een bewaarplicht voor de opsporing en vervolging van ernstige misdrijven

De bewaarplicht houdt in dat bedrijven die openbare telecommunicatiediensten en/of -netwerken aanbieden, de verplichting hebben bepaalde telecommunicatiegegevens te bewaren zodat deze beschikbaar blijven in het geval de gegevens nodig zijn voor een opsporingsonderzoek naar ernstige strafbare feiten. Indien er geen verplichting is voor deze aanbieders om de gegevens voor de opsporing en vervolging van ernstige misdrijven te bewaren, mogen de gegevens uitsluitend door de aanbieders worden verwerkt ten behoeve van hun bedrijfsvoering. De situatie van nu is anders dan de situatie van vóór de invoering van de bewaarplicht (met uitzondering van de telecommunicatiegegevens voor prepaid gebruikers die gedurende drie maanden werden bewaard). In 2009 was het voor aanbieders noodzakelijk om voor bedrijfsdoeleinden verkeersgegevens en internetgebruikersgegevens te bewaren; dat is nu bij veel contracten als gevolg van technologische ontwikkelingen niet meer noodzakelijk. Teruggaan naar de situatie van voor 2009 is niet mogelijk omdat de omstandigheden wezenlijk zijn veranderd. In de praktijk heeft dit bijvoorbeeld tot gevolg dat veel telecommunicatiegegevens direct nadat de communicatie heeft plaatsgevonden of kort daarna worden verwijderd of geanonimiseerd.

In een rapport van het Openbaar Ministerie en de politie (Bijlage bij Kamerstukken II 2014/15, 33 870, nr. 3) wordt het belang van de bewaring van telecommunicatiegegevens voor de opsporing van ernstige delicten onderbouwd aan de hand van circa 130 cases. De casuïstiek maakt inzichtelijk op welke wijze deze gegevens een cruciale rol spelen bij het oplossen van zaken. Zo zijn de gegevens van belang om daders en slachtoffers te identificeren, om criminele netwerken in kaart te brengen, verdachten uit te sluiten of verklaringen van verdachten te verifiëren. In het rapport wordt tevens aandacht besteed aan de omstandigheid dat minder gegevens beschikbaar zullen zijn indien de opsporing en vervolging afhankelijk zijn van de eigen bedrijfsvoering van de aanbieders.

Het afschaffen van de bewaarplicht heeft zeer verstrekkende gevolgen voor de opsporing. De gegevens die in het kader van de bewaarplicht worden bewaard zijn onmisbaar en van groot belang voor de opsporing en vervolging van ernstige misdrijven. Zonder deze gegevens wordt de opsporing van delicten die worden gepleegd op internet of via internet, zoals kinderpornografie, grooming, stalking, digitale diefstal, hacken,

digitale aanvallen, ronselen of rekruteren van personen voor de jihad ernstig belemmerd of zelfs onmogelijk gemaakt. In veel gevallen is het internetspoor, namelijk het IP-adres, het enige spoor. Zonder deze gegevens zal niet achterhaald kunnen worden wie de gebruiker van het IP-adres was.

Ook bij de opsporing van delicten die niet met behulp van internet worden gepleegd, zoals roofovervallen, verkrachtingen, ontvoeringen, moord en doodslag, zijn telecommunicatiegegevens essentieel voor het opsporingsonderzoek. In de meeste gevallen zullen historische telefonie- en internetgegevens pas dagen, weken of zelfs maanden na het plegen van het delict worden opgevraagd, omdat bij de ernstige criminaliteit dikwijls een verdachte niet direct in beeld is. Een verdachte komt in de meeste gevallen pas enige tijd na het moment van het plegen van het delict in beeld door getuigenverklaringen, forensisch onderzoek, het opvragen en onderzoeken van bewakingscamera's, onderzoek van het netwerk van het slachtoffer, de gangen van het slachtoffer in de dagen vóór het misdrijf, en dergelijke. Zonder de telefonie- en internetgegevens kan niet worden vastgesteld welke contacten het slachtoffer had of wie op of in de omgeving van de locatie van de plaats delict was als er geen getuigen zijn. Inzicht in de historische gegevens zorgt voor het uitsluiten of juist identificeren van mogelijke daders. Het zijn juist dit soort gegevens die niet meer of voor een aanzienlijk kortere periode beschikbaar zullen zijn als de opsporing en vervolging volledig afhankelijk zijn van de bedrijfsvoering van de aanbieders.

Ook in de jurisprudentie blijkt het belang van de historische telecommunicatiegegevens. In het eerdergenoemde rapport van het Openbaar Ministerie en de politie zijn een aantal voorbeelden genoemd. In een specifieke zaak heeft de rechtbank historische gegevens, mede gelet op afgelegde verklaringen van de getuigen-deskundigen, voldoende betrouwbaar geacht om als bewijs te kunnen dienen. De rechtbank neemt daarbij als uitgangspunt dat historische gegevens in beginsel een ondersteunend karakter hebben maar dat die gegevens in onderling verband beschouwd en in samenhang met andere uit het dossier blijkende feiten en omstandigheden voor de bewezenverklaring redengevend kunnen zijn.

Het belang en de noodzaak van deze gegevens voor de opsporing blijkt niet alleen uit een veelheid aan casuïstiek, maar dit is ook de conclusie van het WODC in haar evaluatie van de Wet bewaarplicht telecommunicatiegegevens (Bijlage bij Kamerstukken II 2014/15, 33 870, nr. 1). De historische telecommunicatiegegevens met betrekking tot telefonie en internet worden veelvuldig opgevraagd en geanalyseerd door de opsporing en worden gebruikt om sturing te kunnen geven aan het opsporingsonderzoek en verdachten te identificeren. Vooral voor het in kaart brengen van netwerken en het lokaliseren van een telefoon wordt vaak een beroep gedaan op telecommunicatiegegevens. Daarnaast hebben de resultaten van het WODC-onderzoek en de ervaringen uit de opsporingspraktijk laten zien dat inkorten van de bewaartermijn voor de praktijk zeer onwenselijk is. De tot nu toe geldende bewaartermijnen worden door de opsporing en vervolging als adequaat (telefonie) of zelfs te kort (internet) ervaren.

Het buiten werking stellen van de Wet bewaarplicht telecommunicatiegegevens door de voorzieningenrechter van de rechtbank Den Haag heeft reeds gevolgen voor de opsporing en vervolging van ernstige strafbare feiten. Inmiddels konden bijvoorbeeld de NAW-gegevens van het IP-adres van iemand die een kinderpornovideo had gedownload, niet meer worden

achterhaald omdat de aanbieder deze historische gegevens van het IP-adres reeds had verwijderd dan wel geanonimiseerd.

Er zijn geen alternatieven voor de bewaarplicht. Dikwijls wordt gewezen op de mogelijkheid van de bevriezing van gegevens («datapreservation»). De telecommunicatiegegevens van een gebruiker worden dan, voor zover deze op dat moment nog beschikbaar zijn, door de aanbieder bewaard nadat de officier van justitie een daartoe strekkend verzoek aan de aanbieder heeft gericht (Kamerstukken II 2007/08, 31 145, nr. 9, blz. 19). Dit biedt echter geen werkbaar alternatief voor de bewaarplicht omdat een dergelijk verzoek afhankelijk is van de wetenschap dat een strafbaar feit is gepleegd en welke telecommunicatiegegevens relevant zijn. Dat feit kan langere tijd geleden zijn gepleegd en pas later in het onderzoek kan blijken dat bepaalde gegevens relevant zijn. De opsporingsdiensten kunnen strafbare feiten niet voorspellen, en uitsluitend achteraf vaststellen dat telecommunicatiegegevens relevant zijn voor het opsporingsonderzoek. Daardoor bestaat het risico dat de gegevens niet worden bewaard, omdat de aanbieder deze niet ten behoeve van de eigen bedrijfsvoering verwerkt. Als de gegevens wel zijn bewaard bestaat het risico dat deze zijn verwijderd of geanonimiseerd, omdat de aanbieder deze niet langer ten behoeve van de eigen bedrijfsvoering verwerkt. De bewaarplicht strekt er juist toe dat de gegevens daadwerkelijk beschikbaar zijn als later blijkt dat een strafbaar feit is gepleegd. Eenzelfde bezwaar kleeft aan de mogelijkheid van een verplichting voor de aanbieder tot de verstrekking van informatie. Nog afgezien van het feit dat de huidige wetgeving reeds in een dergelijke verplichting voorziet (art. 126n/u, 126na/ua, 126ng/ug, 126zh en 126zi Sv, art. 184 Sr en art. 13.4 Tw) is deze zonder betekenis als niet gewaarborgd is dat de gegevens daadwerkelijk beschikbaar zijn. De gegevens die noodzakelijk zijn vanuit opsporingsperspectief zijn niet per definitie ook vanuit het perspectief van de bedrijfsvoering noodzakelijk om te bewaren. Dit is afhankelijk van de wijze waarop de aanbieder de eigen bedrijfsprocessen heeft ingericht. Dit verschilt per aanbieder zowel ten aanzien van de gegevens als de bewaartermijn. Tenslotte is gewezen op de alternatieve mogelijkheid om een computer in beslag te nemen, bijvoorbeeld als sprake is van verdenking van betrokkenheid bij kinderpornografische chats. De eerste vraag die dit oproept is hoe de locatie van die computer kan worden bepaald als de identificerende gegevens van de gebruiker niet langer beschikbaar zijn. Bovendien biedt dit weinig soelaas omdat, indien de IP-adressen bij onderzoek aan een inbeslaggenomen gegevensdrager bekend worden, er wel een IP-adres bekend kan zijn maar voor de koppeling van een dergelijk adres aan een gebruiker juist gegevens van de aanbieders noodzakelijk zijn.

De regering is dan ook overtuigd van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven en stelt daarom voor deze verplichting te behouden.

5. De bewaartermijn

Het Hof van Justitie overweegt dat in de richtlijn dataretentie geen onderscheid wordt gemaakt in de categorieën van gegevens en hun mogelijke betekenis voor het nagestreefde doel (par. 63). Verder is in de richtlijn niet bepaald dat de vaststelling van de bewaartermijn – die tussen de zes en vierentwintig maanden moet zijn – gebaseerd moet zijn op objectieve criteria, zodat gewaarborgd is dat deze is beperkt tot wat strikt noodzakelijk is (par. 64).

De bewaartermijnen van ten hoogste twaalf maanden voor telefoniegegevens en zes maanden voor internetgegevens zijn strikt noodzakelijk voor het doel, te weten de opsporing en vervolging van ernstige strafbare feiten, en kunnen vanuit het oogpunt van privacybescherming niet als onevenredig worden beschouwd. Hiervoor kan ook worden gewezen op de in het eerdergenoemde rapport van het Openbaar Ministerie en de politie opgenomen casuïstiek.

Zoals in paragraaf 3 is weergegeven, volgt volgens het Hof van Justitie uit de toetsing van de verschillende bepalingen van de richtlijn dataretentie dat de richtlijn geen duidelijke en precieze regels stelt over de mate van aantasting van de fundamentele rechten van het Handvest van de grondrechten. Het Hof van Justitie heeft overwogen dat de bewaartermijn in de richtlijn dataretentie varieerde van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat werd gepreciseerd dat deze termijn op basis van objectieve criteria moest worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is. Gegeven de privacy en terughoudendheid die daarbij hoort als reactie op de uitspraak van het Hof en de voorlichting van de Afdeling advisering van de Raad van State[2] acht de regering harmonisering van de bewaartermijn, het gelijk trekken naar twaalf maanden voor zowel telefonie als internet, niet opportuun. Daarbij is uiteraard gekeken naar zowel de privacyaspecten als de noodzakelijkheid voor de opsporing. Daarom wordt voorgesteld de bewaartermijnen onveranderd te laten. Dat wil zeggen, een bewaartermijn van zes maanden voor internetgegevens en twaalf maanden voor telefoniegegevens. Om de aantasting van de persoonlijke levenssfeer in verband met de bewaring van telecommunicatiegegevens zoveel mogelijk te beperken, wordt voorgesteld dat de vordering van de historische verkeersgegevens door de officier van justitie, die op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige strafbare feiten, een misdrijf moet betreffen waarvoor voorlopige hechtenis is toegelaten en dat van een zodanige ernst is dat dit het vorderen van de bewaarde verkeersgegevens rechtvaardigt, zodat in de wet expliciet tot uitdrukking wordt gebracht dat de vordering moet voldoen aan de vereisten van proportionaliteit en subsidiariteit met betrekking tot de ernst van het delict. Hierop wordt hieronder, in paragraaf 7, nader ingegaan.

Hieronder volgt een beschrijving van een selectie uit de vele voorbeelden uit de opsporingspraktijk om het grote belang van deze gegevens voor opsporing en vervolging te illustreren en nader te onderbouwen waarom de gegevens voor een bepaalde periode beschikbaar moeten blijven.

In de zaak Robert M. zijn de historische verkeersgegevens van cruciaal belang geweest om bewijs te verzamelen voor het grootschalig misbruik, maar ook om slachtoffers en medeverdachten in beeld te krijgen. In 2011 bedroeg de bewaartermijn voor internetgegevens overigens nog twaalf maanden. Indien de bewaartermijn destijds al zes maanden was geweest had dit grote consequenties gehad voor het identificeren van de slachtoffers en medeverdachten. In deze zaak zijn naar aanleiding van de analyse van de chatgesprekken, welke op een inbeslaggenomen gegevensdrager waren aangetroffen, zogenaamde quickscans opgesteld, waarin werd beschreven welke contacten een (op dat moment al dan niet geïdentificeerde) persoon vermoedelijk met de hoofdverdachte onderhield. Van deze quickscans zijn er vervolgens zesenzeventig aan meerdere politieregio's overgedragen met het verzoek om nader onderzoek te doen. In bijna alle gevallen kon een in de chat gebruikte gebruikersnaam worden

[2] Ter informatie gevoegd bij Kamerstuk 2014/15, 33 542, nr. 16, raadpleegbaar via www.tweedekamer.nl.

gekoppeld aan een IP-adres, dat kon worden herleid tot een Nederlandse internet service provider. Door middel van het vorderen van historische gebruikersgegevens bij die aanbieders konden veel Nederlandse verdachten worden geïdentificeerd. Naar aanleiding van dit opsporingsonderzoek in Nederland zijn ook in het buitenland opsporingsonderzoeken verricht en zijn tot op heden meer dan honderdvijftig verdachten aangehouden en konden meer dan honderd kinderen uit een actuele misbruiksituatie worden bevrijd. Met uitzondering van een (zeer) beperkt aantal gevallen was een gebruikt IP-adres de enige aanwijzing die kon leiden tot de identiteit van een verdachte of een slachtoffer.

Een internationaal onderzoek naar kindermisbruik was minder succesvol. Het betrof een website waarop kinderporno werd getoond, waar hyperlinks naar andere websites stonden en waar gebruikers kinderporno konden up- of downloaden of van commentaar konden voorzien. In het internationale onderzoek was het gelukt om zeer veel IP-adressen van gebruikers van deze omgeving te achterhalen. Daaronder vielen meer dan honderd Nederlanders. Geen van deze zaken kon door politie en Openbaar Ministerie in behandeling worden genomen, omdat de bewaartermijn was verlopen en dus de enige aanknopingspunten, te weten de IP-adressen, niet meer bruikbaar waren. Andere onderzoeksmogelijkheden ontbraken.

Als de telefonie- en internetgegevens niet meer beschikbaar zijn, kunnen verdachten in zaken als de bovengenoemde niet meer opgespoord en vervolgd worden. Dit heeft niet alleen tot gevolg dat mogelijke bezitters van kinderpornografisch materiaal niet opgespoord worden, maar dat zogenaamde «groomers» niet opgespoord worden en door kunnen gaan met hun handelingen. Ook eventueel achterliggend kindermisbruik kan daardoor niet gesignaleerd worden, waardoor misbruiksituaties rond zeer jonge slachtoffers zullen kunnen voortduren.

Om een verdachte in relatie te kunnen brengen met een gepleegd delict kan het noodzakelijk zijn een beeld te vormen van zijn of haar gedragspatroon. Om dergelijke patronen te kunnen vaststellen is het noodzakelijk om, met name telefoniegegevens, over een langere periode op te vragen en dus te bewaren. Over een korte periode kan geen gedragspatroon worden vastgesteld en wordt het ook moeilijk om afwijkingen in het gedragspatroon te benoemen. Wanneer dit patroon inzichtelijk is kan worden beoordeeld of er afwijkingen zijn te benoemen die een direct verband tonen met het delict. Daarnaast kunnen, als de termijn lang genoeg is, vaste contacten worden geïdentificeerd. Dit kan van cruciaal belang zijn wanneer een verdachte binnen een groep is geïdentificeerd en nog wordt gezocht naar de overige leden. De gegevens kunnen ook voor het uitsluiten van verdachten van doorslaggevend belang zijn. Verklaringen van verdachten of getuigen kunnen worden geverifieerd en ontkracht aan de hand van historische verkeersgegevens. Het belgedrag of de locatie van de telefoon op het moment van het plegen van het delict kan het alibi van een verdachte bevestigen of ontkrachten. In een drievoudige moordzaak waarin de verklaringen van verdachten onderling sterk van elkaar afweken, is er slechts gebruik gemaakt van verklaringen als deze in belangrijke mate werden ondersteund door andere (objectieve) gegevens. De telecomanalyse heeft hierbij een cruciale rol gespeeld daar deze analyse meermalen ondersteuning of weerlegging opleverde van afgelegde verklaringen.

Ook voor zaken met betrekking tot mensenhandel is een bewaartermijn van twaalf maanden voor telefoniegegevens van groot belang. Slachtoffers van mensenhandel komen niet zelden pas na geruime tijd tot een aangifte of tot het afleggen van een verklaring bij de politie. De redenen

hiervoor zijn divers: angst voor de uitbuiters, financiële afhankelijkheid van de uitbuiters, zich niet vrij kunnen bewegen, psychische traumaverwerking of alweer in een nieuwe uitbuitingssituatie betrokken zijn geraakt. Ook voor de gevallen dat iemand pas na maanden besluit om naar de politie te gaan of aangifte te doen, is het noodzakelijk dat de historische gegevens over een voldoende lange termijn beschikbaar zijn. Als een slachtoffer zich uit een misbruiksituatie weet te ontworstelen kan door de politie een koppeling worden gemaakt met een verdachte, door de historische verkeersgegevens van het slachtoffer over een langere periode op te vragen. Zo ook in een zaak van een twintigjarig slachtoffer die via hulpverlening aan haar misbruiksituatie wist te ontsnappen. Door het opvragen en analyseren van de historische verkeersgegevens van het slachtoffer over een periode van twaalf maanden was de politie in staat om telefoonnummers te koppelen aan een verdachte. Dankzij de verkeersgegevens werden reisbewegingen van telefoontoestellen vastgesteld. Uit de analyse bleek dat het telefoontoestel van de verdachte en het telefoontoestel van het slachtoffer zich gelijktijdig naar diverse plaatsen in Nederland verplaatsten en in de nabijheid van het prostitutiegebied, dan wel sekscubs verbleven. Vastgesteld kon worden dat de telefoon van het slachtoffer op die locaties bleef en die van de verdachte dagelijks heen en weer reisde naar zijn woonplaats. Dit patroon kwam overeen met de verklaring van het slachtoffer. Uit de verkeersgegevens van de telefoons van de verdachte en het slachtoffer bleek dat zij, gedurende een langere periode, gemiddeld meer dan vijftig keer per dag telefonisch contact met elkaar hadden. Dit is een fenomeen dat bij mensenhandel vaak voorkomt en dat de mate van controle die de verdachte op het slachtoffer uitoefent bevestigt. Het behoeft geen toelichting dat de verdachte ontkent en dat dergelijke zaken veelal mede dankzij de historische verkeersgegevens kunnen leiden tot een veroordeling.

Op basis van deze voorbeelden en vele andere voorbeelden die beschikbaar zijn kan worden geconcludeerd dat er meerdere redenen zijn waarom het langer beschikbaar hebben van de telecommunicatiegegevens noodzakelijk is. Op een plaats delict worden allerlei fysieke sporen vastgelegd die richting kunnen geven naar een potentiële dader. De analyse van deze gegevens, zoals bijvoorbeeld DNA, neemt enige tijd in beslag. Pas wanneer uit deze analyses een verdachte kan worden geïdentificeerd kunnen verkeersgegevens met betrekking tot het gebruik van telecommunicatie door of met een verdachte worden gevorderd. Daarnaast komt het (met name) bij zedendelicten, mensenhandel en geweld in familiekring regelmatig voor dat slachtoffers zich om meerdere redenen (zoals angst en/of late ontdekking van het strafbare feit) laat melden bij de politie. Dit kan tot gevolg hebben dat er geen telecommunicatiegegevens meer beschikbaar zijn, waardoor zaken niet (verder) opgepakt kunnen worden. Ten slotte is het bij internationale rechtshulpverzoeken niet ongebruikelijk dat een aanzoekend land pas geruime tijd na aanvang van het eigen onderzoek een verzoek om rechtshulp richt aan de Nederlandse autoriteiten. Dit is met name het geval in terreurzaken, bij zware (georganiseerde) criminaliteit en bij onderzoeken die zich richten op het ontnemen van wederrechtelijk verkregen voordeel. Ook andersom geldt dat Nederlandse onderzoeken in toenemende mate een internationaal karakter dragen en dat rechtshulp moet worden verzocht. Dit betekent dat langer op onderzoeksresultaten moet worden gewacht en verder onderzoek naar die resultaten, waarbij het vorderen van historische verkeersgegevens aan de orde kan zijn, pas in een later stadium kan plaatsvinden.

In dit verband wijs ik ook op de Veiligheidsagenda (Kamerstukken II 2014/15, 28 684, nr. 412). In deze agenda zijn door de veiligheidspartners doelstellingen en prestaties geformuleerd rondom een aantal fenomenen, zoals bijvoorbeeld cybercriminaliteit en de aanpak van (het aanzetten tot) jihadisme/terrorisme. Bij de laatste algemene beschouwingen zijn de aanpak van cybercrime en internationale samenwerking, ook op het gebied van kinderporno en misbruik van kinderen als prioriteit bestempeld. Het behoeft geen betoog dat het realiseren van deze ambitie mede wordt bepaald door de slagkracht van de opsporing. Deze is gebaat bij mogelijkheden om telecommunicatiegegevens gedurende langere tijd te bewaren zodat deze beschikbaar zijn ten behoeve van de opsporing en vervolging van ernstige misdrijven.

Voor wat betreft het onderscheid tussen de verschillende categorieën van gegevens naar gelang het nut ervan voor het nagestreefde doel, kan worden opgemerkt dat de bewaartermijn van twaalf maanden voor telefonie- en zes maanden voor internetgegevens geldt voor de gegevens van alle personen, ongeacht de mate van hun betrokkenheid bij ernstige misdrijven. Deze gegevens worden door de aanbieders bewaard. Indien de gegevens zijn gevorderd ten behoeve van het opsporingsonderzoek naar ernstige misdrijven en relevant blijken voor de opsporing of vervolging van andere misdrijven, dan gelden andere termijnen voor de verdere verwerking van de gevorderde gegevens door de politie of het Openbaar Ministerie. Deze termijnen zijn vastgelegd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Als de gegevens op grond van de vordering van de officier van justitie door de aanbieder van de telecommunicatiedienst worden verstrekt ten behoeve van een opsporingsonderzoek, dan is het regime van de Wet politiegegevens van toepassing op de verdere verwerking van de gegevens. De gegevens kunnen worden verwerkt zolang als nodig voor het doel van het onderzoek (art. 9, vierde lid, Wpg).

Het Platform BOD'en acht het gebruiken van verkeers- en gebruikersgegevens cruciaal voor de bestrijding van ernstige misdrijven. Dit kan worden geïllustreerd met voorbeeldcasussen met name op het terrein van (fiscale) fraude. In met name toeslagonderzoeken gaat er meestal geruime tijd overheen voordat de Belastingdienst middels haar controlesysteem ontdekt dat er sprake is van fraude. In feite geldt dit ook voor BTW-onderzoeken. IP-adressen zijn van groot belang om te kunnen achterhalen vanaf welke aansluiting een document is verstuurd, of vanaf dat adres vaker frauduleuze documenten zijn verstuurd en voor het koppelen van verdachten aan andere verdachten. Enkele casussen ter illustratie zijn als bijlage bij het advies van het Platform opgenomen.

6. De te bewaren gegevens

Met de Wet bewaarplicht telecommunicatiegegevens is een lijst van gegevens vastgesteld die dienen te worden bewaard ten behoeve van de opsporing en vervolging van strafbare feiten. De lijst van de te bewaren gegevens gaat als bijlage behorende bij artikel 13.2a van de Telecommunicatiewet. Daarbij wordt onderscheid gemaakt tussen telefonie door middel van een vast of mobiel netwerk, inclusief bepaalde vormen van telefonie via internet, enerzijds en internettoegang, inclusief vormen van telefonie via internet die niet aan de wettelijke criteria voldoen, anderzijds. Bij bepaalde vormen van telefonie via internet, zoals voice over IP (VoIP), komen de functionaliteit en de gegenereerde telecommunicatiegegevens overeen met die van reguliere vaste telefonie. In dit wetsvoorstel worden deze vormen van telefonie omschreven als «internettelefonie» (art. 13.2a, eerste lid, onderdeel c, Tw). Voor de telecommunicatiegegevens van

internettelefonie geldt een bewaartermijn van twaalf maanden (Kamerstukken II 2009/10, 32 185, nrs. 3 en 6).

Naar aanleiding van het arrest van het Hof van Justitie heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden. Daarbij is onderzocht welke gegevens strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Dit heeft geleid tot aanpassing van de lijst van te bewaren telecommunicatiegegevens. Voorgesteld wordt onder meer om over te gaan tot schrapping van de gegevens met betrekking tot e-mail over internet. Tenslotte is de verplichting tot bewaring van bepaalde locatiegegevens, anders dan de locatieaanduiding bij het begin van de verbinding (de zogenaamde first Cell ID), overbodig. Dit betreft de gegevens ten behoeve van de zogenaamde bestandsanalyse die zijn aangewezen in het Besluit bijzondere vergaring nummers telecommunicatie, op basis van artikel 13.4, derde lid, van de Telecommunicatiewet. Door middel van de bestandsanalyse kan het nummer worden achterhaald bij het gebruik van een prepaidkaart. Voorgesteld wordt deze verplichting te schrappen omdat de politie inmiddels over andere methoden beschikt om de betreffende gegevens te achterhalen.

De bedoeling van de bewaarplicht voor telecommunicatiegegevens is dat gegevens beschikbaar zijn voor opsporing en vervolging waarmee de abonnee of gebruiker van telecommunicatie kan worden geïdentificeerd. In de praktijk blijken er echter, mede vanwege technische ontwikkelingen, verschillende interpretaties mogelijk van de term IP-adres als bedoeld in de bijlage, behorende bij artikel 13.2a van de Telecommunicatiewet. Voorgesteld wordt om de formulering aan te passen, zodat IP-adressen te relateren zijn aan een gebruiker of abonnee.

7. De toegang tot de bewaarde telecommunicatiegegevens

Het Hof van Justitie overweegt dat de richtlijn geen objectief criterium bevat ter beperking van het aantal personen dat wordt geautoriseerd voor de toegang, en het verdere gebruik van de gegevens, tot hetgeen strikt noodzakelijk is in het licht van de te bereiken doelen. Bovenal is de toegang van de bevoegde autoriteiten tot de bewaarde gegevens niet afhankelijk gesteld van voorafgaande toetsing door een gerecht of een onafhankelijk bestuurlijk orgaan naar aanleiding van een gemotiveerd verzoek van de aangewezen autoriteiten (par. 62).

Met inachtneming van de regeling van de eerdergenoemde e-privacyrichtlijn worden de telecommunicatiegegevens uitsluitend bewaard ten behoeve van bepaalde doeleinden van het algemeen belang. Dit betreft de opsporing en vervolging van ernstige misdrijven. Dit zijn misdrijven waarvoor voorlopige hechtenis mogelijk is. Deze misdrijven zijn opgesomd in artikel 67, eerste lid, van het Wetboek van Strafvordering.

De telecommunicatiegegevens worden door de aanbieders bewaard ten behoeve van de strafrechtelijke handhaving van de rechtsorde, meer in het bijzonder de opsporing en vervolging van ernstige misdrijven. Naar aanleiding van het arrest van het Hof van Justitie wordt voorgesteld de toegang tot de historische verkeersgegevens, die door de aanbieders op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven, afhankelijk te stellen van een voorafgaande rechterlijke toetsing, zodat kan worden verzekerd dat de gegevens uitsluitend worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat. De rechterlijke

toetsing zal worden gewaarborgd door middel van het wettelijke vereiste van een voorafgaande machtiging van de rechter-commissaris. Daarbij geldt het vereiste dat de vordering een misdrijf moet betreffen dat van een zodanige ernst is dat dit in het concrete geval het vorderen van de bewaarde verkeersgegevens rechtvaardigt. Met dit vereiste wordt in de wet geëxpliciteerd dat de vordering moet voldoen aan de vereisten van proportionaliteit en subsidiariteit met betrekking tot de ernst van het delict. Het doel van de bewaarplicht is te garanderen dat bepaalde telecommunicatiegegevens beschikbaar zijn met het oog op de bestrijding van ernstige criminaliteit. Strafbare feiten waarvoor voorlopige hechtenis is toegelaten zijn onder meer misdrijven waarop een gevangenisstraf van vier jaar of meer is gesteld. Een delict als fietsendiefstal geldt weliswaar als misdrijf waarvoor op grond van artikel 67, eerste lid, onder a, Sv voorlopige hechtenis mogelijk is, zodat een vordering van de officier van justitie tot verstrekking van de bewaarde verkeersgegevens mogelijk is, maar een bevel daartoe zal wegens de geringe ernst slechts in uitzonderlijke gevallen volgen. Het criterium van de ernst van het misdrijf vormt aldus een «ondergrens» voor het vorderen van de verkeersgegevens die door de aanbieders op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven, zodat de toegang tot de gegevens daadwerkelijk is beperkt tot hetgeen strikt noodzakelijk is voor de bestrijding van (enkel) ernstige criminaliteit. Hiermee wordt tevens uitvoering gegeven aan het arrest van het Hof van Justitie, waarin is overwogen dat de richtlijn dataretentie in het bijzonder geen objectief criterium bevatte met behulp waarvan de toegang en het gebruik van de gegevens werd beperkt tot hetgeen strikt noodzakelijk is in het licht van het nagestreefde doel (par. 62). Het staat in eerste instantie ter beoordeling van de officier van justitie of de ernst van het misdrijf het vorderen van de bewaarde verkeersgegevens rechtvaardigt. Bij de vraag of de machtiging kan worden verstrekt dient de rechter-commissaris te toetsen of aan deze voorwaarde is voldaan.

Het criterium van het belang van het onderzoek heeft eveneens betrekking op de proportionaliteit en subsidiariteit. Dit betreft echter niet de noodzakelijkheid van de vordering vanuit het perspectief van de ernst van het delict maar vanuit het perspectief van het onderzoek. Dit criterium kan strekken tot beperking van de reikwijdte van de bevraging in de tijd. Dit wil zeggen dat de rechter-commissaris zal kunnen toetsen of het belang van het onderzoek noopt tot de raadpleging van alle gegevens die met betrekking tot de gevorderde periode beschikbaar zijn. Gaat het bijvoorbeeld om telefoniegegevens waarvoor een bewaartermijn van twaalf maanden geldt, dan zal de rechter-commissaris kunnen beoordelen in hoeverre het onderzoeksbelang, in het licht van het feitencomplex en de tijdstippen waarop die feiten zijn gepleegd, vereist dat gegevens worden gevorderd die gedurende een langere periode zijn opgeslagen, voorafgaand aan de vordering. Als bijvoorbeeld in februari 2015 een diefstal met geweld is gepleegd dan zal de officier van justitie, als hij in maart 2016 de bewaarde telecommunicatiegegevens vordert met betrekking tot een persoon die wordt verdacht van betrokkenheid bij dat delict, moeten kunnen motiveren over welke periode binnen de bewaartermijn van twaalf maanden de bewaarde gegevens worden gevorderd. Het is aan de rechter-commissaris om deze motivering te toetsen.

Aanvullende criteria om de rechter-commissaris houvast te bieden bij de beoordeling of met de vordering tot verstrekking van verkeersgegevens wordt voldaan aan de vereisten van proportionaliteit en subsidiariteit met betrekking tot de ernst van het misdrijf acht ik niet nodig. Zo zal bijvoorbeeld een nadere inkadering aan de hand van een lijst van bepaalde delicten of categorieën van delicten niet alleen een tamelijk arbitraire

afweging weerspiegelen maar bovendien het risico van onvolledigheid in zich bergen. Hier komt bij dat de wettelijke regeling reeds de nodige criteria bevat om te komen tot een adequate toetsing van de vordering tot verstrekking van de bewaarde verkeersgegevens. Tot die waarborgen behoren criteria als een feit waarvoor voorlopige hechtenis mogelijk is en het belang van het onderzoek. Met dit wetsvoorstel wordt daaraan toegevoegd het vereiste van een voorafgaande toetsing door een rechter-commissaris. Met het aanvullend opnemen van het criterium van de rechtvaardiging van de ernst van het misdrijf wordt gewaarborgd dat de rechterlijke toetsing ook de ernst van het misdrijf in het concrete geval omvat. Het meer aanvullend opnemen van concrete criteria voor de beoordeling van de vereisten van proportionaliteit en subsidiariteit is minder goed te realiseren omdat de afweging in het concrete geval afhangt van een samenstel van factoren als de aard en ernst van het strafbare feit, de omstandigheden waaronder het feit is gepleegd en de betrokkenheid van slachtoffers, mede bezien in hun onderlinge verband. Dit laat zich niet eenvoudig in harde criteria vertalen, en kan beter worden overgelaten aan de rechterlijke oordeelsvorming. Met het aanvullend formuleren of vaststellen van criteria voor deze specifieke bevoegdheid zou ook worden afgeweken van de regeling van de toetsing van de inzet van dwangmiddelen en bijzondere opsporingsbevoegdheden door de rechter-commissaris. Zo brengt de toepassing van de bevoegdheid tot het aftappen en opnemen van telecommunicatie (art. 126m en 126t Sv) een meer ingrijpende inbreuk op de persoonlijke levenssfeer van betrokkenen met zich mee dan de toepassing van de bevoegdheid van het vorderen van verkeersgegevens. Niettemin wordt de toetsing van de proportionaliteit en subsidiariteit bij de toetsing van een bevel tot het aftappen en opnemen van telecommunicatie overgelaten aan het oordeel van de rechter-commissaris. Ook bij een vordering van de officier van justitie tot het verstrekken van verkeersgegevens moet de rechter-commissaris bij uitstek in staat worden geacht om de rechtmatigheid van een dergelijke vordering in het concrete geval te beoordelen.

Het College van procureurs-generaal en de politie maken bezwaar tegen de voorafgaande machtiging van een rechter-commissaris en adviseren deze te schrappen. Het College vraagt zich af of het arrest noodzaakt tot de inzet van de rechter-commissaris en meent dat de toetsing door de rechter-commissaris geen bijzondere meerwaarde oplevert waar het gaat om de beoordeling van de rechtmatigheid van de vordering van de officier van justitie tot verstrekking van historische verkeersgegevens. Dit past niet goed in het wettelijke systeem van strafvordering, nu het vereiste van een voorafgaande machtiging van de rechter-commissaris niet geldt voor andere bijzondere opsporingsbevoegdheden die een meer ingrijpende inbreuk op de persoonlijke levenssfeer met zich meebrengen dan het vorderen van telecommunicatiegegevens. Voorts wijzen het College en de politie op de gevolgen voor de werkbelasting van de kabinetten-RC; gelet op de huidige belasting van die kabinetten zal de voorgestelde toetsing ongetwijfeld tot grote vertragingen leiden.
Ook de NVvR verzoekt af te zien van deze wijziging. In de visie van de NVvR volgt uit de uitspraken van het Hof van Justitie niet (zonder meer) dat de officier van justitie als toetsende autoriteit binnen het huidige wettelijk kader niet zou voldoen. Bovendien koerst deze wijziging aan op een systeembreuk en vermag de NVvR niet in te zien waarom een minder ingrijpende bevoegdheid tot het vorderen van verkeersgegevens aan de rechter-commissaris zou moeten worden toegekend. Daarnaast voorziet de NVvR een grote toename van het aantal vorderingen bij de rechter-commissaris die, bij gelijkblijvende bezetting, zullen leiden tot vertragingen binnen het kabinet-RC.
Het Platform BOD'en acht het verwonderlijk dat voor zo'n relatief lichte inbreuk de toets door de rechter-commissaris wordt geïntroduceerd, en

wijst op de administratieve lastenverzwaring voor het Openbaar Ministerie en de kabinetten-RC. Ook vormt dit volgens het Platform BOD'en een breuk met het huidige toetsingskader.
De Raad voor de rechtspraak acht voorafgaande rechterlijke toetsing wenselijk vanuit het oogpunt van de bescherming van de grondrechten. De Raad verwacht wel dat het wetsvoorstel gevolgen heeft voor de werklast van de rechtbanken. De Raad verwacht dat het aantal vorderingen bij de rechter-commissaris structureel zal toenemen met jaarlijks ongeveer 42.000 extra vorderingen. Dit zorgt voor extra kosten van ongeveer twee miljoen euro per jaar.

Naar aanleiding van deze adviezen kan worden opgemerkt dat de voorzieningenrechter in het vonnis van 11 maart 2015 heeft geoordeeld dat het Hof van Justitie als een zwaarwegend bezwaar beschouwt dat de toegang tot de bewaarde gegevens niet is onderworpen aan een voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie. Dit kan worden afgeleid uit het gebruik van het woord «bovenal» («above all») onder paragraaf 62 van het arrest. Het Openbaar Ministerie kan naar het oordeel van de voorzieningenrechter niet als een onafhankelijke administratieve instantie worden aangemerkt (par. 3.12.). Een voorafgaande toetsing door een rechter-commissaris ligt dan in de rede. Door de toegang tot de bewaarde gegevens afhankelijk te stellen van een voorafgaande rechterlijke toetsing wordt nog meer gewaarborgd dat de gegevens slechts worden gevorderd in de gevallen waarin daartoe voldoende aanleiding bestaat en dat daarmee de privacy van burgers afdoende wordt beschermd. De rechterlijke toetsing is ingegeven doordat sprake is van opslag van bepaalde telecommunicatiegegevensgegevens van alle klanten, die door de aanbieders zijn verzameld en die aanwijzingen kunnen geven over het privéleven van de betrokkenen, en deze gegevens gedurende een bepaalde periode beschikbaar zijn met het oog op de opsporing en vervolging van ernstige strafbare feiten. In deze situatie vloeit de inbreuk op de privacy niet zozeer voort uit de vordering jegens een individuele gebruiker, maar uit de opslag van de telecommunicatiegegevens van alle klanten met het oog op de opsporing en vervolging van ernstige strafbare feiten. Er is in zoverre sprake van een verandering in het systeem dat een dergelijke algemene opslag van gegevens ten behoeve van de toepassing van de bevoegdheden tot het vorderen van gegevens bij derden tot nu toe niet aan de orde is. Deze toetsing zal echter zwaarwegende financiële en organisatorische gevolgen hebben voor de politie, het Openbaar Ministerie en de zittende magistratuur. Op deze consequenties wordt elders in deze toelichting ingegaan.

De gegevens worden bewaard door de telecombedrijven en kunnen alleen in een individuele zaak, als aan de voorwaarden van het Wetboek van Strafvordering is voldaan, worden gevorderd. Derhalve is voor de toegang tot de gegevens altijd een concrete vordering vereist, gebaseerd op een concreet strafrechtelijk onderzoek en een concrete verdenking, en wordt uitsluitend toegang verkregen tot de specifiek gevorderde gegevens. De bewaartermijn is voor de gegevens met betrekking tot telefonie over een vast of mobiel netwerk en via het internet vastgesteld op twaalf maanden, voorafgaand aan de datum van de vordering. Voor de gegevens in verband met internettoegang en bepaalde vormen van internettelefonie is de bewaartermijn vastgesteld op zes maanden, voorafgaand aan de datum van de vordering.

Voor het vorderen van gegevens van derden geldt dat de mogelijkheid wordt geboden van een mondelinge vordering. Daarbij geldt het vereiste van de dringende noodzaak. In het geval van een mondelinge vordering stelt de opsporingsambtenaar of de officier van justitie de vordering

achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht. Op basis van de geldende wettelijke regels kan een vordering aan een aanbieder van een communicatiedienst tot het verstrekken van andere gegevens dan verkeersgegevens mondeling worden gedaan (art. 126ng en 126ug Sv). Ook voor het vorderen van gegevens bij anderen dan de aanbieders (art. 126nc en 126nd Sv) geldt dat deze vordering mondeling kan worden gedaan. Voor een vordering tot het verstrekken van verkeersgegevens is dit echter niet mogelijk. Dit is in de praktijk minder goed werkbaar en de behoefte bestaat aan de mogelijkheid van een mondelinge vordering tot verstrekking van verkeersgegevens ingeval van dringende noodzaak. Daarom was in het conceptwetsvoorstel Computercriminaliteit III voorgesteld om expliciet de mogelijkheid te bieden van een mondelinge vordering van verkeersgegevens. Vanwege de inhoudelijke samenhang wordt voorgesteld de in dat conceptwetsvoorstel voorgestelde regeling voor het mondeling vorderen van verkeersgegevens op te nemen in het onderhavige wetsvoorstel. De betreffende onderdelen zijn in het wetsvoorstel Computercriminaliteit III geschrapt (Kamerstukken II 2015/16, 34 372, nr. 2). In de thans voorgestelde regeling is rekening gehouden met het vereiste van een machtiging van de rechter-commissaris voor het vorderen van historische verkeersgegevens, die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven. In aansluiting op de regeling van het vorderen van gegevens bij derden wordt voorgesteld dat de machtiging van de rechter-commissaris, bij dringende noodzaak, ook mondeling kan worden gegeven.

8. Gegevensbescherming en gegevens beveiliging (de bescherming en beveiliging van de bewaarde gegevens)

Het Hof van Justitie overweegt dat de richtlijn niet voorschrijft dat de betrokken gegevens op het grondgebied van de Unie worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk voorgeschreven door artikel 8, derde lid, van het Handvest van de grondrechten (par. 68).

Naar aanleiding hiervan wordt voorgesteld de Telecommunicatiewet aan te passen. Voorgeschreven wordt dat de te bewaren gegevens worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie. Doordat de gegevens worden bewaard op het grondgebied van de Unie is ten volle gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk voorgeschreven in het Handvest van de grondrechten (art. 8, derde lid, Handvest).

Het Besluit beveiliging gegevens telecommunicatie (Bbgt) schrijft voor dat beveiligingsmaatregelen moeten worden genomen. Deze maatregelen hebben betrekking op de beveiliging en de toegang tot de gegevens. Zo moeten de gegevens die de aanbieders sinds 2009 moeten bewaren, zoveel mogelijk binnen één ruimte worden geconcentreerd die deugdelijk fysiek is beveiligd. De toegang tot deze ruimte is uitsluitend toegestaan aan daartoe geautoriseerde personen voor zover dit voor hun functie noodzakelijk is. Personeel dat in aanraking komt met de gegevens tekent een geheimhoudingsverklaring.

9. Controle en verantwoording

De bewaarplicht voor telecommunicatiegegevens dient het algemene belang van de criminaliteitsbestrijding, meer in het bijzonder de opsporing en vervolging van ernstige misdrijven. Hierbij is echter eveneens de privacybescherming aan de orde; de bewaarde gegevens kunnen inzicht verschaffen in bepaalde aspecten van het privéleven van burgers. Dit betreft in het bijzonder hun contacten met andere personen en hun geografische verplaatsingen. Zoals ook in de brief over de privacybescherming van burgers in onze informatiemaatschappij (Kamerstukken II 2014/2015, 32 761, nr. 83) aan de orde is gekomen, worden veiligheid en privacy vaak als uitersten gezien, alsof het een keuze betreft tussen het één of het ander. Zij liggen naar mijn overtuiging echter voor een belangrijk deel in elkaars verlengde, het gaat steeds om de bescherming van burgers tegen aantastingen van hun persoonlijke veiligheid en vrijheid. Dit geldt in het bijzonder voor de bewaarplicht voor telecommunicatiegegevens. Niet alleen het slachtoffer van een strafbaar feit is er zeer bij gebaat dat informatie beschikbaar is die kan bijdragen aan de opsporing of vervolging van de daders, het is ook in het belang van de samenleving dat de veiligheid van de burgers kan worden gewaarborgd. De afweging omtrent het gebruik van die informatie mag dan ook niet worden geplaatst uitsluitend in het perspectief van de aantasting van de persoonlijke levenssfeer. De toegang tot en het gebruik van die informatie kan tevens bijdragen aan de bescherming van de persoonlijke veiligheid en vrijheden van anderen en de beveiliging van de samenleving tegen criminaliteit. De wettelijke regeling moet een balans weerspiegelen tussen de betrokken belangen, namelijk het algemene belang van de bescherming van de veiligheid van de samenleving enerzijds en het belang van de bescherming van de persoonlijke levenssfeer van de burger anderzijds. De garanties en waarborgen voor een zorgvuldige toepassing van de regels betreffende de toegang tot en het gebruik van de gegevens, de bewaartermijn en de bescherming en beveiliging van de gegevens dienen ervoor te zorgen dat de inmenging in haar totaliteit evenredig is.

Vanuit de Kamer is door verschillende fracties de behoefte geuit aan robuuster inzicht in de privacywaarborgen voor, en de meerwaarde van, het opslaan van telecommunicatiegegevens (Algemeen Overleg over de evaluatie van de Wet bewaarplicht telecommunicatie- en internetgegevens, gehouden op 25 maart 2015, Kamerstukken II 2014/15, 33 870, nr. 4). Dit betreft concrete vragen, zoals bij welke misdaden of bij welke zaken er veel gebruik is gemaakt van de bewaarde telecommunicatiegegevens, welk percentage van de bevraagde gegevens tot succes heeft geleid en waarom de gegevens die de aanbieders ten behoeve van hun eigen bedrijfsvoering verwerken, niet voldoende zijn voor de opsporing en vervolging van ernstige misdrijven. Het belang van transparantie over het gebruik van verkeersgegevens in de opsporing, mede tegen de achtergrond van de bescherming van de privacy, acht ik essentieel. De wens tot transparantie wordt tegelijkertijd begrensd omdat over de wijze van toepassing in concrete gevallen, de wijze waarop aan de hand van de verkeersgegevens richting kan worden verkregen in de opsporing uiteraard geen mededelingen kunnen worden gedaan. Zulks heb ik ook aan Uw Kamer meegedeeld. Ook heb ik erop gewezen dat inzicht verschaffen in de effectiviteit van een specifiek opsporingsmiddel niet kan, omdat het middel in samenhang met andere opsporingsmiddelen wordt ingezet. Een cijfermatig inzicht in de effectiviteit van dataretentie is niet mogelijk, maar meer cijfermatig inzicht in het gebruik van de dataretentiegegevens door de opsporing wel.

Tegen deze achtergrond heb ik, rekening houdend met de bestaande structuren op het gebied van rechterlijke toetsing, toezicht en controle, gezocht naar mogelijkheden tot intensivering van de controle en verantwoording van het gebruik van historische verkeersgegevens ten behoeve van de opsporing en vervolging. Hieronder worden eerst de bestaande structuren geschetst, waarna aanvullend de maatregelen ter intensivering van het toezicht aan de orde komen.

9.1. Controle en rechterlijke toetsing

Het Agentschap Telecom (AT) van het Ministerie van Economische Zaken, de Autoriteit Persoonsgegevens (AP, voorheen het College Bescherming persoonsgegevens), het College van procureurs-generaal en de procureur-generaal bij de Hoge Raad vervullen verschillende rollen ten aanzien van het toezicht of de controle op de bewaarplicht en de toegang tot de gegevens door de opsporing. In dit wetsvoorstel wordt aan deze bestaande structuur een extra waarborg toegevoegd in de zin van een toets door de rechter-commissaris.

De verzameling en opslag van telecommunicatiegegevens door de aanbieders van openbare telecommunicatienetwerken en -diensten valt onder de reikwijdte van de Telecommunicatiewet en – voor zover het persoonsgegevens betreft – de Wet bescherming persoonsgegevens (Wbp). Op basis van die wetten gelden strikte regels voor de verwerking en beveiliging van de gegevens door de aanbieders. Op de naleving van die regels wordt toezicht uitgeoefend door AT en door de AP. De verdere verwerking van de geraadpleegde telecommunicatiegegevens ten behoeve van opsporing en vervolging valt onder het regime van de Wet politiegegevens (Wpg) respectievelijk de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze privacywetten zijn specifiek van toepassing op de verwerking van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Het toezicht op de naleving van deze wetten door de opsporingsdiensten en het Openbaar Ministerie wordt eveneens door de AP uitgeoefend.

Het Openbaar Ministerie heeft in het kader van de strafrechtelijke handhaving van de rechtsorde als taak een – onpartijdige en niet vooringenomen – bijdrage te leveren aan de waarheidsvinding en behoort in te staan voor de rechtmatigheid van opsporing en vervolging (Kamerstukken II 1996/97, 25 392, nr. 3, blz. 3). Het College van procureurs-generaal staat aan het hoofd van het Openbaar Ministerie en waakt voor een richtige opsporing van strafbare feiten (art. 140 Sv). Het College van procureurs-generaal oefent toezicht uit over de uitoefening van de taken en bevoegdheden van het Openbaar Ministerie, en is bevoegd daartoe aanwijzingen te geven aan hoofden van de parketten of de individuele leden van het Openbaar Ministerie. Dit toezicht omvat de opsporing van strafbare feiten, en daarmee de toepassing van de wettelijke bevoegdheden rond het vorderen van gegevens bij derden door de officier van justitie, al dan niet met tussenkomst van een rechter-commissaris.

Ten slotte kan worden gewezen op de taak van de procureur-generaal bij de Hoge Raad. Deze is bevoegd, indien naar zijn oordeel het Openbaar Ministerie bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert, de Minister van Veiligheid en Justitie daarvan in kennis te stellen (art. 122 Wet RO). Het is aan de procureur-generaal gelaten om invulling te geven aan zijn toezichthoudende taak op grond van artikel 122 Wet RO. Inmiddels heeft de procureur-generaal bij de Hoge Raad besloten aan deze toezichthoudende taak meer inhoud te geven door middel van thematische onderzoeken naar de wijze waarop het Openbaar Ministerie zijn taken uitvoert. Dit heeft inmiddels geleid tot

het rapport «Beschikt en Gewogen; over de naleving van de wet door het Openbaar Ministerie bij het uitvaardigen van strafbeschikkingen», dat op 15 februari 2015 door mij aan Uw Kamer is aangeboden (Kamerstukken II 2014/15, 29 279, nr. 225).

In dit wetsvoorstel wordt voorgesteld de toegang tot en het gebruik van de bewaarde gegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten tevens te onderwerpen aan een voorafgaande rechterlijke toetsing. De rechter-commissaris beoordeelt vooraf of de vordering op goede gronden wordt gedaan. Deze toetsing omvat de rechtmatigheid van de vordering van de gegevens, inclusief de proportionaliteit en subsidiariteit van de vordering. De rechtmatigheid van de toegang tot en het gebruik van de bewaarde gegevens kan daarnaast in voorkomende gevallen op de terechtzitting aan de orde worden gesteld. De rechterlijke controle is gericht op individuele gevallen, wanneer in concreet opsporingsonderzoek of een concrete strafzaak de behoefte bestaat aan toegang tot de bewaarde gegevens ten behoeve van de opsporing of vervolging van een ernstig strafbaar feit.

9.2. Informatieverschaffing over de betekenis van de bewaarplicht

In aanvulling op de bestaande voorzieningen op het gebied van controle en rechterlijke toetsing zal het College van procureurs-generaal bezien of en hoe periodiek inzicht kan worden gegeven in de betekenis van de gevorderde telecommunicatiegegevens voor de opsporing en de vervolging, zoals de aard van de strafbare feiten, het aantal strafzaken waarin telecommunicatiegegevens van betekenis zijn geweest en het aantal vorderingen tot verstrekking van telecommunicatiegegevens. De politie en het Openbaar Ministerie zijn samen met het WODC aan het bekijken welke gegevens uit de beschikbare systemen een betrouwbaar beeld kunnen geven van het gebruik van de gegevens door de opsporing. Deze cijfers zullen, evenals de tapstatistieken en het aantal CIOT-bevragingen, jaarlijks in het jaarverslag van het Ministerie van Veiligheid en Justitie worden gepubliceerd.

Hierboven is gewezen op de toezichthoudende bevoegdheden van AT, de AP en de procureur-generaal bij de Hoge Raad. De inhoud van de rapportage van het College van procureurs-generaal kan voor deze instanties aanleiding vormen tot aanvullende activiteiten op het gebied van het toezicht, op basis van hun wettelijke bevoegdheden.

9.3. Aanvullend toezicht door de procureur-generaal bij de Hoge Raad

Op grond van zijn wettelijke bevoegdheid kan de procureur-generaal bij de Hoge Raad aanvullend toezicht uitoefenen op het Openbaar Ministerie. Het doet mij genoegen dat de procureur-generaal zich bereid heeft getoond op grond van die bevoegdheid in de toekomst onderzoek te verrichten naar de naleving van de voorschriften van het Wetboek van Strafvordering met betrekking tot historische telecommunicatiegegevens door het Openbaar Ministerie. Het toezicht van de procureur-generaal bij de Hoge Raad zal zijn gericht op de rechtmatigheid van de toepassing van die voorschriften. Het zal geen betrekking hebben op de vraag of terecht een machtiging tot het opvragen van historische telecommunicatiegegevens is gevorderd, omdat die vraag wordt beantwoord door de rechter-commissaris bij het al dan niet verlenen van een machtiging. Dat betekent dat het onderzoek zich zal beperken tot de naleving van de voorschriften die betrekking hebben op het gebruik van de verstrekte verkeersgegevens, zoals de kennisgeving van de vordering aan de betrokkene (notificatieplicht), de vernietiging van de gegevens nadat de zaak is geëindigd en het gebruik van de verkregen gegevens in een ander

strafrechtelijk onderzoek (art. 126bb, 126cc en 26dd Sv). De rapportage zal, zoals in alle gevallen van een onderzoek ex. artikel 122 Wet RO door de procureur-generaal, aan de Kamer worden aangeboden.

Het doen van een onderzoek ex. artikel 122 Wet RO is pas mogelijk als voldoende strafzaken beschikbaar zijn waarin de wettelijke voorschriften zijn toegepast en hebben geleid tot een onherroepelijke beslissing ter afdoening.

10. De bescherming van de persoonlijke levenssfeer

Het wetsvoorstel strekt tot de bewaring van bepaalde categorieën van telecommunicatiegegevens ten behoeve van het opsporen en vervolgen van ernstige misdrijven. Dit betreft verkeersgegevens alsmede de hiermee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren (gebruikersgegevens). Aan de hand van dergelijke gegevens kan inzicht worden verkregen in de gedragingen van personen. Zoals in paragraaf 2 aan de orde is gekomen, kan dit betrekking hebben op bijvoorbeeld de telecommunicatiediensten die door een bepaalde persoon worden gebruikt, de aansluitnummers waarmee verbinding is geweest en de duur van die verbinding. Deze gegevens raken aan de persoonlijke levenssfeer. Zowel het bewaren als het vorderen van de telecommunicatiegegevens betreffen een inmenging op de persoonlijke levenssfeer, hiervoor kan ook worden gewezen op het vonnis van de voorzieningenrechter van 11 maart 2015 (paragraaf 3).

Het grondrecht op bescherming van de persoonlijke levenssfeer vindt zowel in het nationale als in het internationale recht bescherming. In de Grondwet is bepaald dat ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Beperking van dit recht dient een basis te hebben in een wet in formele zin (art. 10 Gw). Voor wat betreft het internationale recht zijn het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en het Handvest van de grondrechten van de Europese Unie van belang. Het wetsvoorstel valt namelijk binnen het toepassingsgebied van het recht van de Europese Unie en daarmee onder de werkingssfeer van het Handvest van de grondrechten. Aanknopingspunten hiervoor worden gevormd door de e-privacyrichtlijn en het vrij verkeer van diensten. Hiervoor kan worden verwezen naar de eerdergenoemde voorlichting van de Afdeling advisering van de Raad van State over het arrest van het Hof van Justitie.

Op grond van het Handvest heeft eenieder recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie (art. 7 Handvest). Ook heeft eenieder recht op bescherming van de hem betreffende persoonsgegevens. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan (art. 8 Handvest). Deze rechten vertonen grote overeenkomst met artikel 8 van het EVRM, op grond waarvan een ieder het recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Geen inmenging van enig openbaar gezag in de uitoefening van dit recht is toegestaan dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van, onder meer, de nationale veiligheid, de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten. De in het Handvest gewaarborgde rechten zijn onderworpen aan een vergelijkbare beperkingssystematiek. Op grond van artikel 52, eerste lid, van het Handvest kunnen de reikwijdte en uitlegging

van die rechten beperkt worden op voorwaarde dat deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van de in het Handvest gewaarborgde fundamentele rechten eerbiedigen, noodzakelijk zijn en daadwerkelijk beantwoorden aan de door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden, en daarbij het evenredigheidsbeginsel in acht nemen. Om te kunnen voldoen aan de door het evenredigheidsbeginsel gestelde grenzen, moet een inbreuk op de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten duidelijke en precieze regels bevatten over de omvang van de inbreuk, minimale vereisten opleggen zodat de personen van wie de gegevens worden bewaard over voldoende garanties beschikken dat hun persoonsgegevens worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens, en nauwkeurig worden omkaderd door bepalingen die kunnen waarborgen dat de inbreuk daadwerkelijk beperkt is tot het strikt noodzakelijke. In de eerdergenoemde voorlichting heeft de Afdeling advisering van de Raad van State een aantal voorwaarden geformuleerd waaraan een Europese regeling die de aanbieders verplicht om verkeers- en locatiegegevens te bewaren met het oog op de opsporing en vervolging van ernstige criminaliteit, zal moeten voldoen. Voor de reactie van het kabinet op die voorwaarden wordt verwezen naar de brief van 17 november 2014 (Kamerstukken II 2014/15, 33 542, nr. 16).

Met het voorliggende wetsvoorstel wordt beoogd te komen tot aanvulling van de Telecommunicatiewet en het Wetboek van Strafvordering, zodat met de wettelijke regeling voor de bewaarplicht van telecommunicatiegegevens wordt tegemoet gekomen aan de eisen die daaraan op grond van de Europese grondrechten op het gebied van de bescherming van de persoonlijke levenssfeer, zoals die in het Handvest van de grondrechten en het EVRM zijn vastgelegd, kunnen worden gesteld.

«Voorzien bij wet»

Met de Wet bewaarplicht telecommunicatiegegevens is reeds in een wettelijke regeling voorzien. Doordat de verplichting tot het bewaren van bepaalde categorieën van gegevens, de bewaartermijnen en de lijst van de te bewaren gegevens in de wet zijn vastgelegd is de regeling voldoende precies geformuleerd, zodat de burger vooraf kan weten onder welke voorwaarden de gegevens worden bewaard. Hiermee wordt tegemoet gekomen aan het vereiste van de voorzienbaarheid.

«Legitiem doel»

De voorgestelde bewaarplicht heeft tot doel bij te dragen aan de voorkoming, opsporing en vervolging van strafbare feiten, waaronder terrorisme. Telecommunicatiegegevens zijn van groot belang voor het opsporingsonderzoek naar ernstige vormen van criminaliteit. Dit is hiervoor, in paragraaf 4, reeds aan de orde gekomen. Dit wordt door het Hof van Justitie in het arrest van 8 april 2014 ook onderkend (par. 41–44). Zo wijst het Hof van Justitie op artikel 6 van het Handvest dat eenieder niet alleen recht heeft op vrijheid, maar ook op veiligheid. De door de richtlijn voorgeschreven bewaring van gegevens beantwoordt volgens het Hof van Justitie daadwerkelijk aan een doel van algemeen belang. Ook het EHRM onderkent de «detection and, therefore, prevention of crime» als een legitiem doel (S and Marper v United Kingdom [2008] ECHR 1581, § 100).

«Noodzakelijk en effectief»

Bij de eis dat de inmenging in het privacyrecht noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid («margin of appreciation»). De eis van noodzakelijkheid houdt in dat bezien moet worden of de voorgestelde maatregel nodig is voor de strafrechtelijke handhaving van de rechtsorde. Daarbij gaat het om een toetsing aan de eisen van proportionaliteit en subsidiariteit.
De bewaarplicht is noodzakelijk en effectief; bepaalde vormen van criminaliteit zijn nagenoeg uitsluitend op te sporen door het gebruik van historische telecommunicatiegegevens.

De Autoriteit Persoonsgegevens wijst erop dat in het arrest van het Hof van Justitie veel aandacht wordt besteed aan de proportionaliteitstoets. Dit betreft de evenredigheid tussen middel en het doel, in relatie tot de inbreuk op de grondrechten van burgers. Op grond van het wetsvoorstel dienen de telecommunicatieaanbieders de telecommunicatiegegevens van alle klanten te bewaren, ook de gegevens van klanten waarbij in het geheel geen aanwijzingen bestaan dat hun gedrag verband houdt met zware criminaliteit of de bedreiging van de openbare veiligheid. Het feit dat de bewaarplicht niet wordt ingekaderd maakt dat de inbreuk op de artikelen 7 en 8 van het Handvest naar het oordeel van de AP te groot is, en dat de maatregel niet voldoet aan het proportionaliteitsvereiste van artikel 8 EVRM. De AP stelt vast dat de instandhouding van een algemene bewaarplicht strijdig is met de Europese grondrechten en dat de conclusies van het Hof van Justitie nopen tot heroverweging van het uitgangspunt van een algemene bewaarplicht voor telecommunicatiegegevens van iedere Nederlander, en daarmee van het wetsvoorstel. De AP concludeert dat het door de regering beoogde onderscheid tot het bewaren van gegevens en het gebruik ervan niet leidt tot beëindiging van de geconstateerde onevenredigheid en daarmee onrechtmatigheid van een algemene bewaarplicht voor telecommunicatiegegevens. Telecomaanbieder XS4ALL wijst erop dat het wetsvoorstel voorbij gaat aan het meest fundamentele en grootste bezwaar van het Hof van Justitie, namelijk de verplichting tot langdurige opslag van de verkeersgegevens van alle burgers. Een dergelijke algemene opslag van persoonsgegevens leidt tot een ongekende, voortdurende en doordringende controle van de communicatie en activiteiten in het dagelijks leven van iedereen. De bewaring moet daarom beperkt worden tot gegevens die betrekking hebben op een bepaalde periode en/of een geografische zone en/of een kring van bepaalde personen. Het belang bij opsporing en vervolging – hoe wezenlijk ook – weegt niet op tegen de vergaande inbreuk op de rechten van burgers die de bewaringsmaatregel met zich meebrengt. Ook Bits of Freedom voert soortgelijke argumenten aan en acht ongerichte surveillance, en zeker op deze gigantische schaal, ongepast in een democratische rechtsstaat.
Deze adviezen raken aan hetgeen de Afdeling advisering van de Raad van State hierover in de voorlichting heeft opgemerkt. In de kabinetsreactie is hierop reeds nader ingegaan (par. 5.3.1.).

De opvatting die aan de genoemde adviezen ten grondslag lijkt te liggen, dat de instandhouding van een algemene bewaarplicht (en het enkel bewaren van de telecommunicatiegegevens) reeds strijdig is met de Europese grondrechten, is niet goed verenigbaar met het arrest van het Hof van Justitie. Het doel van de richtlijn dataretentie is destijds geweest dat gegevens toegankelijk zijn voor het geval die nodig zijn voor de bestrijding van zware criminaliteit. De toegang tot deze gegevens moest niet enkel en alleen afhankelijk zijn van de omstandigheid of de aanbieder de gegevens voor zijn bedrijfsvoering bewaarde. De selectie van

gegevens kan pas later plaatsvinden, omdat vooraf niet mogelijk is te bepalen welke gegevens van belang kunnen zijn voor de bestrijding van zware criminaliteit. Het Hof van Justitie keurt in het arrest deze grondgedachte van de richtlijn niet af. Het is, gezien de omvangrijke bewaarplicht, het ontbreken van allerlei waarborgen ten aanzien van de bewaring van de gegevens en de toegang tot de gegevens dat voor het Hof van Justitie maakt dat een dergelijke bewaarplicht onevenredig is. Dit kan worden afgeleid uit het oordeel van het Hof dat gelet op alle overwegingen («Having regard to all the foregoing considerations») de wetgever van de Unie met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid, van het Handvest van de grondrechten in acht had dienen te nemen (par. 69). In het vonnis van de voorzieningenrechter van 11 maart 2015 wordt op soortgelijke gronden overwogen dat uit het arrest van het Hof niet kan worden afgeleid dat een dergelijke ruime bewaarplicht hoe dan ook niet evenredig is ten opzichte van het beoogde doel (par. 3.7.). Daarbij wordt overwogen dat een beperking van de gegevens die moeten worden opgeslagen tot de gegevens van verdachte burgers, niet goed denkbaar is met het oog op het doel van de Wet bewaarplicht telecommunicatiegegevens, de doeltreffende opsporing van zware criminaliteit. In geval van een first offender kan immers niet reeds op voorhand een onderscheid worden gemaakt tussen verdachte en niet-verdachte burgers. Daarnaast worden de gegevens ook gebruikt om slachtoffers te kunnen identificeren, bijvoorbeeld in het geval van grooming of kinderporno. De noodzaak voor het bieden van waarborgen en garanties ten aanzien van de toegang tot die gegevens is evenwel des te groter nu het gaat om een zeer ruime inmenging, zodat daaraan hoge eisen dienen te worden gesteld (par. 3.8.). Bij deze overwegingen sluit ik mij graag aan.

Ook de jurisprudentie van het EHRM geeft geen steun aan de opvatting dat een dergelijke gegevensopslag niet is toegestaan. De eerdergenoemde zaak van S. en Marper tegen het Verenigd Koninkrijk betrof een verzoek tot vernietiging van vingerafdrukken en DNA-profielen, nadat vrijspraak was gevolgd respectievelijk de vervolging was gestaakt. Bij de beoordeling van de proportionaliteit en evenredigheid van de maatregel beoordeelde het Hof de publieke en individuele belangen (par. 118). Daarbij werden verschillende omstandigheden geformuleerd op grond waarvan de gegevensopslag van niet-veroordeelde personen toelaatbaar zou kunnen zijn (par. 119). Dit betrof de omstandigheid dat: het materiaal kon worden bewaard ongeacht de ernst of zwaarte van het delict (1), de vingerafdrukken en profielen konden worden afgenomen en bewaard van iedere persoon, ongeacht de leeftijd en voor ieder delict (2), de bewaring niet beperkt was in tijd en gegevens werden bewaard ongeacht de aard of ernst van het strafbare feit waarvan de persoon werd verdacht (3), er voor de persoon die was vrijgesproken slechts beperkte mogelijkheden waren, tot verwijdering of vernietiging van de gegevens (4), er in het bijzonder geen onafhankelijk toezicht was op de rechtmatigheid van de bewaring (5). Op basis van deze omstandigheden kwam het Hof, na afweging van de belangen, tot het oordeel dat er sprake was van een schending van artikel 8 EVRM (par. 125). Uit deze uitspraak kan worden afgeleid dat het EHRM de bewaring van gegevens van niet-verdachte burgers op zichzelf niet in strijd acht met artikel 8 EVRM maar verschillende criteria formuleert die in hun onderlinge samenhang in de beoordeling worden betrokken. Dit blijkt ook uit de verwijzing naar de situatie in andere landen (par. 112: «The Court cannot, however, disregard the fact that, nothwithstanding the advantages provided by comprehensive extension of the DNA-database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life»). Te

dien aanzien vertoont de jurisprudentie van het EHRM in de zaak Marper gelijkenis met die van het Hof van Justitie over de richtlijn dataretentie.

De zaak M.K. tegen Frankrijk (appl. no. 19522/09, 18 april 2013) betrof de bewaring van vingerafdrukken van een persoon, ook nadat de vervolging was gestaakt. De bewaarperiode was maximaal vijfentwintig jaar, en de opslag was niet beperkt tot gevallen van verdenking van ernstige strafbare feiten. Onder verwijzing naar de zaak Marper overwoog het Hof dat de noodzaak van waarborgen des te groter is in het geval van geautomatiseerde verwerking van persoonsgegevens, niet in het minst als de gegevens worden gebruikt voor politiedoeleinden. De nationale wetgeving dient in het bijzonder te verzekeren dat dergelijke gegevens relevant zijn en niet buitensporig in relatie tot de doelen waarvoor ze worden opgeslagen, en bewaard in een vorm die de identificatie van de betrokkene niet langer toelaat dan noodzakelijk voor het doel waarvoor de gegeven zijn opgeslagen. De nationale wet dient ook in adequate waarborgen te voorzien tegen misbruik en oneigenlijk gebruik van de bewaarde gegevens (par. 32.). In de context van deze zaak is het Hof in het bijzonder bezorgd over het risico van stigmatisering, nu niet-veroordeelde personen gelijk worden behandeld als veroordeelde personen. Naar aanleiding van dit arrest kan worden opgemerkt dat de afwegingen rond de bewaarplicht voor telecommunicatiegegevens anders zijn, in die zin dat het geen vingerafdrukken van personen betreft maar bepaalde telecommunicatiegegevens van burgers, dat daarbij beperkte bewaartermijnen aan de orde zijn en dat daarbij geen onderscheid wordt gemaakt tussen niet-veroordeelde en veroordeelde personen. Bovendien worden de gegevens niet bij de politie opgeslagen maar bij een derde partij, waarbij de gegevens in individuele gevallen kunnen worden gevorderd ten behoeve van de opsporing en vervolging van ernstige strafbare feiten.

Ook uit Brunet tegen Frankrijk (appl.no. 21010/10, 18 september 2014) volgt niet dat het bewaren van gegevens van niet-verdachte burgers op voorhand is uitgesloten. In deze zaak werd geklaagd over de registratie van persoonsgegevens van een persoon tegen wie de vervolging was gestaakt in een «recorded crime database». Het EHRM erkende dat dit een ingrijpende inbreuk betrof nu het ging om persoonsgegevens die werden opgeslagen in een systeem dat werd gebruikt voor onderzoek naar misdrijven. Daarbij merkte het EHRM op dat een bewaartermijn van twintig jaar in het bijzonder lang is, afgezet tegen het ontbreken van een veroordeling van betrokkene of verdere vervolging. Vervolgens beoordeelde het EHRM de lengte van de bewaartermijn in het licht van de mogelijkheid om te kunnen verzoeken om verwijdering van de opgeslagen gegevens uit het systeem. Een dergelijke beoordeling illustreert dat het EHRM hecht aan een redelijke bewaartermijn en aan waarborgen omtrent de opslag en het gebruik van de gegevens, in het bijzonder wanneer het gaat om niet-veroordeelde personen.

De Wet bewaarplicht telecommunicatiegegevens bevat reeds de nodige garanties en waarborgen voor een zorgvuldige gegevensverwerking. Deze garanties en waarborgen hebben betrekking op de toegang tot de gegevens, de bescherming en beveiliging van de gegevens en de rechten van de betrokkene. Nu het gaat om een zeer ruime inmenging is de noodzaak voor het bieden van waarborgen en garanties ten aanzien van de toegang tot die gegevens evenwel des te groter. Daarom worden in dit conceptwetsvoorstel aanvullende maatregelen voorgesteld. Deze hebben betrekking op een verdere beperking van de toegang tot de gegevens, zodat de toegang is beperkt tot gevallen waarin daadwerkelijk sprake is van ernstige criminaliteit, en de opslag van de gegevens in de EU. Met de aanvullende maatregelen van het voorliggende conceptwetsvoorstel is de inmenging in de artikelen 7 en 8 van het Handvest naar mijn oordeel

voldoende nauwkeurig omkaderd door bepalingen die waarborgen dat deze daadwerkelijk beperkt is tot het strikt noodzakelijke.

– Waarborgen omtrent de toegang tot de gegevens

De toegang tot de gegevens is geregeld in het Wetboek van Strafvordering. De toegang tot verkeersgegevens is beperkt tot de daartoe aangewezen autoriteit, de officier van justitie. Vereist is een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren dan wel aanwijzingen van een terroristisch misdrijf. Met dit wetsvoorstel wordt beoogd te waarborgen dat de toegang van de bevoegde nationale autoriteiten tot de historische verkeersgegevens, die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige strafbare feiten, en het latere gebruik ervan met het oog op het voorkomen, opsporen en vervolgen van strafbare feiten is beperkt tot inbreuken die voldoende ernstig geacht kunnen worden om de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten te rechtvaardigen. Daartoe wordt voorgesteld aanvullend in de wet het vereiste op te nemen dat in het concrete geval sprake is van een misdrijf van een zodanige ernst dat dit het vorderen van de bewaarde verkeersgegevens rechtvaardigt. Tenslotte wordt voorgesteld te voorzien in een voorafgaande rechterlijke toetsing van de toegang tot de verkeersgegevens, op grond van een gemotiveerde vordering van de officier van justitie. Met deze extra waarborgen wordt de toegang tot de verkeersgegevens daadwerkelijk beperkt tot hetgeen strikt noodzakelijk is voor de bestrijding van ernstige criminaliteit. Met het vereiste van de voorafgaande toetsing door een rechter-commissaris wordt tegemoet gekomen aan het arrest van het Hof van Justitie (par. 60/62).

– Waarborgen omtrent de bewaring van de gegevens

De wettelijke regeling bevat de nodige waarborgen tegen misbruik of onzorgvuldig gebruik van de bewaarde gegevens. Deze waarborgen hebben betrekking op de gegevensbescherming en de gegevensveiligheid. Dit omvat de wettelijke verplichting om de bewaarde gegevens aan het einde van de bewaartermijn onverwijld te vernietigen. Deze waarborgen zijn uitgewerkt in het Besluit beveiliging gegevens telecommunicatie. Hiervoor kan worden verwezen naar de eerdergenoemde kabinetsreactie (par. 5.3.4.).
Met de verplichting tot de opslag en verwerking van de bewaarde telecommunicatiegegevens in Nederland of in een andere lidstaat van de Europese Unie wordt ten volle gewaarborgd dat een onafhankelijke autoriteit op basis van het Unierecht toezicht houdt op de inachtneming van de vereisten inzake bescherming en beveiliging. Met dit vereiste wordt tegemoet gekomen aan het arrest van het Hof van Justitie (par. 68).

Ten slotte heeft de betrokkene op grond van de Wet bescherming persoonsgegevens het recht op kennisneming en correctie. Dit wil zeggen dat de betrokkene zich tot de aanbieder kan wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt (art. 35 Wbp). Na kennisneming kan de betrokkene de aanbieder verzoeken de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de bewaring onvolledig of niet terzake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt (art. 36 Wbp).

11. Vrij verkeer van diensten en notificatie

Het wetsvoorstel voorziet in een verplichting voor de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten om bepaalde telecommunicatiegegevens te bewaren ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. De juridische en technische verschillen tussen de bepalingen op het gebied van het bewaren van gegevens ten behoeve van het voorkomen, opsporen en vervolgen van strafbare feiten in de lidstaten kunnen de werking van de interne markt voor elektronische communicatie belemmeren, omdat de aanbieders kunnen worden geconfronteerd met uiteenlopende voorschriften wat betreft de categorieën te bewaren telecommunicatiegegevens, de bewaringsvoorwaarden en de bewaringstermijnen. De voorgestelde maatregel heeft tot gevolg dat de aanbieders over apparatuur moeten beschikken en personeel in dienst hebben om aan de bewaarplicht te kunnen voldoen. Dit raakt aan het vrije verkeer van diensten binnen de Europese Unie.

Nu de richtlijn dataretentie ongeldig is verklaard en de Europese Commissie heeft aangegeven niet met een nieuw voorstel te zullen komen, is de betreffende materie niet geharmoniseerd en zijn de lidstaten bevoegd binnen de overige Europeesrechtelijke kaders maatregelen vast te stellen. Daarbij is met name artikel 15, eerste lid, van de eerdergenoemde Richtlijn 2002/58/EG relevant. Dit artikel biedt de lidstaten de mogelijkheid om wettelijke maatregelen te 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 die richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale veiligheid, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie».

In de eerdergenoemde voorlichting aan de Minister van Veiligheid van Justitie heeft de Raad van State erop gewezen dat het Hof in het arrest Pfleger (C-390/12, 30 april 2014, ECLI:EU:C:2014:281) heeft geconcludeerd dat wanneer een lidstaat zich beroept op dwingende vereisten van algemeen belang ter rechtvaardiging van een regeling die de uitoefening van de vrijheid van dienstverlening kan belemmeren, deze door het Unierecht geboden rechtvaardigingsgrond moet worden uitgelegd in het licht van de algemene rechtsbeginselen van het Unierecht en met name in het licht van de inmiddels in het Handvest neergelegde grondrechten. Hieruit vloeit volgende Raad van State voort dat nationale wetgeving op het gebied van een bewaarplicht voor telecommunicatiegegevens moet voldoen aan het bepaalde in de artikelen 7 en 8 van het Handvest van de grondrechten.

Zoals in paragraaf 10 reeds aan de orde is gekomen, kunnen de reikwijdte en uitlegging van de in de artikelen 7 en 8 van het Handvest neergelegde rechten worden beperkt op voorwaarde dat deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van de in het Handvest gewaarborgde fundamentele rechten eerbiedigen, noodzakelijk zijn en daadwerkelijk beantwoorden aan de door de Unie erkende doelstellingen van

algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden, en daarbij het evenredigheidsbeginsel in acht nemen. In die paragraaf is toegelicht dat met de voorgestelde wettelijke regeling voor de bewaarplicht van telecommunicatiegegevens tegemoet wordt gekomen aan de eisen op het gebied van de bescherming van de persoonlijke levenssfeer, zoals die in het Handvest van de grondrechten en het EVRM zijn vastgelegd.

Vanwege de nauwe raakvlakken van de inhoud van dit wetsvoorstel met het vrije verkeer van diensten is tevens de vraag aan de orde in hoeverre het wetsvoorstel in aanmerking komt voor notificatie bij de Commissie. Dit betreft de toepassing van de (zogenoemde) Notificatierichtlijn en de Dienstenrichtlijn.

De Notificatierichtlijn

De Notificatierichtlijn reguleert technische voorschriften met betrekking tot producten en diensten, met het oog op een goede werking van de interne markt. De procedure is voor het eerst gecodificeerd in Richtlijn 98/34/EG van 22 juni 1998 en gewijzigd bij Richtlijn 98/48/EG van 20 juli 1998, voornamelijk om het toepassingsgebied uit te breiden naar diensten van de informatiemaatschappij. De procedure is onlangs voor de tweede keer gecodificeerd in Richtlijn (EU) 2015/1535.
De richtlijn is van toepassing op alle ontwerpen voor technische voorschriften, zoals technische specificaties en voorschriften die vervaardiging, invoer, verhandeling of gebruik van een product verbieden of die verlening of gebruik van een dienst of de vestiging als dienstverlener verbieden. Onder het begrip «technisch voorschrift» moet tevens «een regel betreffende diensten» worden verstaan (art. 1, onder f). Onder het begrip dienst wordt verstaan elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht (art. 1, onder b).

De richtlijn voorziet in een kennisgevings- of notificatieplicht, zodat de technische voorschriften kunnen worden onderzocht die lidstaten voornemens zijn te introduceren voor producten (op het gebied van industrie, landbouw en visserij) en voor diensten van de informatiemaatschappij voordat ze worden vastgesteld (art. 5, eerste lid).

Een dienst van de informatiemaatschappij in de zin van de richtlijn is elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht (art. 1, onder b).
Langs elektronische weg ziet op het aspect dat het aanbieden van de dienst plaatsvindt middels «elektronische apparatuur voor de verwerking en de opslag van gegevens (met inbegrip van digitale compressie), en die geheel via draden, radio, optische middelen of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen». Voor het criterium «op afstand» is vereist dat een dienst wordt geleverd zonder dat de partijen gelijktijdig aanwezig zijn (zie bijlage I bij de Notificatierichtlijn, «indicatieve lijst van diensten die niet onder art. 1, eerste lid, punt b, tweede alinea, vallen» onder 1). Indien bijvoorbeeld een reis wordt geboekt bij een reisbureau met behulp van elektronische middelen, is er geen sprake van een dienst van de informatiemaatschappij omdat partijen gelijktijdig aanwezig zijn. Indien de afnemer van de dienst deze reis echter zelf vanuit huis boekt via internet dan is wel sprake van een dienst van de informatiemaatschappij. Tevens is vereist dat het een dienst betreft die op individueel verzoek van een afnemer van diensten wordt verricht. Daarvan

is sprake indien een dienst op individueel verzoek via de transmissie van gegevens wordt geleverd (art. 1, onder b, onder punt iii).

Verder is relevant dat de richtlijn niet geldt voor, onder meer, regels betreffende zaken die vallen onder een regeling van de Unie inzake telecommunicatiediensten, zoals bedoeld in Richtlijn 2002/21/EG van het Europees Parlement en de Raad (art. 1, derde lid).

Dit wetsvoorstel heeft geen betrekking op regels over diensten die via elektronische weg worden aangeboden, maar op het bewaren van bepaalde telecommunicatiegegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. In feite ziet het voorstel op regels betreffende het openbare elektronische communicatienetwerk waarlangs diensten van de informatiemaatschappij worden aangeboden en verricht.

Er is voorts geen sprake van regels die betrekking hebben op een dienst «op individueel verzoek van een afnemer», waarbij een dienst op individueel verzoek van een afnemer via de transmissie van gegevens wordt geleverd. In de door de Europese Commissie opgestelde «Leidraad bij de informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de informatiemaatschappij» is over dit element opgenomen:

Dit is het element van interactiviteit dat diensten van de informatiemaatschappij kenmerkt en onderscheidt van andere diensten die worden verstuurd zonder dat hiervoor een verzoek van de afnemer noodzakelijk is. (....) Voorbeelden van diensten die wel onder de richtlijn vallen, zijn algemene online informatiediensten (kranten, databanken enz.), bewakingsactiviteiten op afstand, interactief telewinkelen, elektronische post, online vluchtreserveringen, online professionele dienstverlening (bijvoorbeeld toegang tot databanken, diagnostieken).

Hiervoor kan ook worden gewezen op bovengenoemde bijlage I van de richtlijn inzake de «indicatieve lijst van diensten die niet als diensten van de informatiemaatschappij worden beschouwd» (art. 1, onder b van de Notificatierichtlijn). In de bijlage is onder categorie 3 «diensten die niet op individueel verzoek van een afnemer van diensten worden geleverd». Daar wordt aangegeven dat het gaat om «diensten die via de verzending van gegevens zonder individuele oproep worden verricht en bestemd zijn voor gelijktijdige ontvangst door een onbepaald aantal ontvangers (point-to-multipoint-transmissie»). Onder deze categorie is bijvoorbeeld de uitzondering «televisieomroepdiensten (waaronder near-video-on-demand)» opgenomen. In dit verband kan worden gewezen op het arrest van het Hof van Justitie van de EU van 2 juni 2005, Mediakabel BV tegen Commissariaat voor de Media, waarin het begrip dienst van de informatiemaatschappij en het onderdeel «op individueel verzoek van de afnemer» aan de orde kwam. In deze zaak ging het om het aanbieden van een selectie van films aan alle abonnees, waarbij de films met behulp van een persoonlijke sleutel toegankelijk waren op door de aanbieder vastgestelde uitzendtijdstippen. Het Hof gaf aan dat deze dienst weliswaar voldoet aan de criteria op afstand en via elektronische weg, maar aan het derde criterium «op individueel verzoek van de afnemer» niet werd voldaan. De dienst moest volgens het Hof worden beschouwd als een dienst op basis van «point-to-multipoint» en niet als een dienst die op individueel verzoek van een afnemer wordt verstrekt (r.o. 38–39). Ook bij het aanbieden van openbare telecommunicatienetwerken en diensten is sprake van «point-to-multipoint» waarbij de infrastructuur niet op individueel verzoek van een afnemer wordt onderhouden. Ook de maatregelen voor het bewaren van gegevens maken onderdeel uit van het aanbieden van het netwerk en aldus is het bewaren van gegevens op

grond van dit wetsvoorstel evenmin een dienst die op individueel verzoek van een afnemer wordt verricht.

Bovendien kan nog worden opgemerkt dat de regels onder de uitzondering van artikel 1, derde lid, van de Notificatierichtlijn vallen, omdat sprake is van regels betreffende zaken die vallen onder een regeling van de Unie inzake telecommunicatiediensten, zoals bedoeld in Richtlijn 2002/21/EG van het Europees Parlement en de Raad. Richtlijn 2002/21/EG betreft de kaderrichtlijn betreffende telecommunicatie. De uitzondering voor regels inzake telecommunicatie omvat meer dan alleen de regels inzake de implementatie van Richtlijn 2002/21, maar regels die vallen onder het begrip telecommunicatie zoals bedoeld in de voornoemde richtlijn. De uitzondering van artikel 1, derde lid, zou namelijk overbodig zijn indien deze slechts zou zien op regels die zijn opgenomen in de richtlijn. Maatregelen die implementatie van EU-richtlijnen betreffen hoeven uiteraard niet genotificeerd te worden op grond van artikel 7, eerste lid, van de richtlijn. In de bovengenoemde Leidraad van de Commissie wordt over deze uitzondering aangegeven dat de reden voor deze specifieke uitsluiting is dat een groot aantal zaken op het gebied van telecommunicatiediensten reeds zijn geharmoniseerd en onderdeel vormt van een reeds bestaand en voldoende gedefinieerd communautair regelgevingskader.

Op grond van het voorgaande kan worden geconcludeerd dat er geen sprake is van een dienst van de informatiemaatschappij maar van een reguliere dienst, zodat de Notificatierichtlijn niet van toepassing is. Vervolgens is de vraag aan de orde in hoeverre de Dienstenrichtlijn van toepassing is.

De Dienstenrichtlijn

De Dienstenrichtlijn beoogt het wegnemen van handelsbelemmeringen bij diensten in de EU, door het vereenvoudigen van administratieve procedures voor dienstverleners, het versterken van de rechten van consumenten en bedrijven, en het aanmoedigen van samenwerking tussen EU-landen. De richtlijn heeft betrekking op een groot aantal diensten, waaronder detail- en groothandel van goederen en diensten, de activiteiten van de meest gereglementeerde beroepen zoals juridische en belastingadviseurs, architecten en ingenieurs, bouwdiensten, bedrijfsgerelateerde diensten zoals onderhoud van kantoren, management consultancy en evenementorganisatie, en toerisme en de vrijetijdssector. De richtlijn voorziet in een kennisgevings- of notificatieplicht aan de Europese Commissie voor eisen die worden gesteld aan de verrichting van diensten en de vestiging van dienstenverrichters (art. 15, zevende lid en art. 39, vijfde lid jo. art. 16).

Bepaalde diensten zijn uitgezonderd van de werkingssfeer van de Dienstenrichtlijn. Dit betreft (onder meer) elektronische -communicatiediensten en -netwerken en bijbehorende faciliteiten en diensten, wat de aangelegenheden betreft die vallen onder (onder meer) de Richtlijn 2002/58/EG (art. 2, tweede lid). In overweging 20 van de richtlijn is over deze uitzondering verduidelijkt dat het niet alleen om zaken gaat die specifiek in de richtlijnen geregeld worden, maar ook op die zaken waarvoor de lidstaten in die richtlijnen expliciet de mogelijkheid wordt gelaten bepaalde maatregelen op nationaal niveau te nemen.

In artikel 15, eerste lid, van Richtlijn 2002/58/EG wordt de lidstaten expliciet de mogelijkheid geboden om wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Deze maatregelen dienen in overeenstemming

te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

Dit wetsvoorstel bevat verplichtingen voor de aanbieders van openbare telecommunicatiediensten en/of netwerken tot het bewaren van bepaalde telecommunicatiegegevens, binnen het kader van artikel 15 van Richtlijn 2002/58/EG. De Dienstenrichtlijn is hierop dus niet van toepassing zodat getoetst dient te worden aan het primaire EU-recht, namelijk het vrij verkeer van diensten van artikel 56 VWEU. Het voorstel bevat geen eisen in de zin van één van de andere vrijheden van het Verdrag. Ingevolge vaste jurisprudentie van het Hof van Justitie van de EU dienen nationale maatregelen die de uitoefening van de in het Verdrag gewaarborgde fundamentele vrijheden kunnen belemmeren of minder aantrekkelijk kunnen maken, aan vier voorwaarden voldoen: zij moeten zonder discriminatie worden toegepast, zij moeten hun rechtvaardiging vinden in dwingende redenen van algemeen belang, zij moeten geschikt zijn om de verwezenlijking van het nagestreefde doel te waarborgen, en zij mogen niet verder gaan dan nodig is voor het bereiken van dat doel (zie onder meer de zaak Gebhard van 30 november 1996, C- 55/94 en de zaak Pfleger, r.o. 43 reeds aangehaald).

De maatregelen in het wetsvoorstel vormen een gerechtvaardigde belemmering op het vrij verkeer van diensten in de zin van artikel 56 VWEU.

Voor wat betreft de algemene beginselen van het Gemeenschapsrecht waarnaar Richtlijn 2002/58/EG verwijst, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2 VEU kan overigens worden verwezen naar paragraaf 10 van deze toelichting. Tevens is de maatregel non-discriminatoir nu de betreffende gegevens worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie. Hierdoor kunnen telecommunicatiediensten gebruik maken van opslagfaciliteiten in de hele EU zonder dat er een bevoordeling is van Nederlandse telecommunicatiediensten. Bovendien is de maatregel geschikt om het doel van de opsporing en vervolging van ernstige misdrijven te bereiken waarbij zoals in paragraaf 10 is toegelicht, de maatregel niet verder gaat dan strikt noodzakelijk.

Geconcludeerd moet worden dat de regels die in het onderhavige wetsvoorstel zijn opgenomen niet genotificeerd hoeven te worden onder de Notificatierichtlijn, dan wel de Dienstenrichtlijn. Ook voor het overige zijn de maatregelen in overeenstemming met de regels van het Unierecht, waaronder Richtlijn 2002/58/EG en het vrij verkeer van diensten.

12. Bedrijfseffecten

Het wetsvoorstel zal gevolgen hebben voor de administratieve lasten van politie, Openbaar Ministerie en rechtspraak. Dit houdt vooraleerst verband met de voorgestelde rechterlijke toetsing, voorafgaand aan de toegang tot de bewaarde gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven.
In samenwerking met de politie en het Openbaar Ministerie is een impactanalyse uitgevoerd naar de effecten van het wetsvoorstel op de bedrijfsvoering van deze instanties. In het advies van de Raad voor de rechtspraak wordt aandacht besteed aan de gevolgen van de invoering van de toetsing door de rechter-commissaris voor de rechtspraak.

Voor de bedrijfsvoering bij politie en Openbaar Ministerie zal de invoering van een machtiging van de rechter-commissaris ertoe leiden dat de

bewerkingstijd per vordering toeneemt. Dit komt doordat het procesverbaal moet worden uitgebreid, er bij het Openbaar Ministerie een extra werkstap bijkomt (het opmaken van de vordering tot machtiging) en er meer afstemming nodig is. Per vordering wordt een extra bewerkingstijd verwacht van 15–35 minuten per vordering. Als het aantal vorderingen gelijk blijft aan de huidige situatie zal naar schatting 9–21 extra fte (€ 0,6–€ 1,5 miljoen per jaar) nodig zijn om de bijgekomen administratieve lasten te dragen. Blijft het aantal vorderingen stijgen met ca. 10% per jaar – zoals in de afgelopen jaren – dan zal het komend jaar 11–25 extra fte (€ 0,8–€ 1,8 miljoen per jaar) nodig zijn. In het scenario dat verkeersgegevens een toenemende rol gaan spelen in de opsporing, zal het komende jaar 12–30 extra fte (€ 0,9–€ 2,1 miljoen per jaar) nodig zijn voor de extra administratieve lasten die er door het wetsvoorstel bijkomen. Deze extra capaciteit zal verdeeld moeten worden over politie en Openbaar Ministerie.
Wat betreft de gevolgen voor de rechtspraak wijst de Nederlandse Vereniging voor Rechtspraak erop dat de voorgestelde regeling van de toets door de rechter-commissaris onmiskenbaar zal leiden tot een grote toename van het aantal vorderingen dat bij de rechter-commissaris zal worden ingediend. Vertragingen in de gang van zaken bij het kabinet van de rechter-commissaris zullen bij een gelijkblijvende bezetting onvermijdelijk zijn. De impactanalyse die voor politie en Openbaar Ministerie is opgesteld geeft aan dat de wachttijd op de machtiging van de rechtercommissaris door het grote aantal vorderingen – bij gelijke capaciteit van het rechtercommissariaat – inderdaad sterk zal toenemen. De Raad voor de rechtspraak heeft in zijn consultatie-advies één en ander gekwantificeerd. De Raad meent dat het wetsvoorstel gevolgen heeft voor de rechtbanken. Men verwacht dat het aantal vorderingen bij de rechtercommissaris structureel toeneemt met ongeveer 42.000 extra vorderingen. De behandeltijd van de extra vorderingen wordt geschat op circa vijftien minuten per vordering. In geval van spoed gaat hier een mondeling verzoek aan vooraf. De behandeling van spoedvorderingen bedraagt gemiddeld 20 minuten per vordering. Bij elkaar zal dit, aldus de Raad voor de rechtspraak, zorgen voor extra kosten van ongeveer € 2 miljoen euro per jaar.

Het wetsvoorstel zal tevens gevolgen kunnen hebben voor de bedrijfsvoering van de in Nederland opererende internet- en telecomaanbieders. In opdracht van het Ministerie van Economische Zaken is een onderzoek uitgevoerd naar de bedrijfseffecten bij de aanbieders. De vijf grote aanbieders hebben aan het onderzoek meegewerkt. Daarnaast is een steekproef getrokken uit de circa vijfhonderd middelgrote of kleine aanbieders. Vier van de tien benaderde middelgrote of kleine aanbieders hebben hun medewerking verleend. Uit dat onderzoek blijkt dat dataretentie de aanbieders ongeveer 40 miljoen per drie jaar kost, dat is 0,07% van de omzet. Op basis van de gegevens uit het onderzoek kan worden berekend dat dit neerkomt op circa één euro per abonnee per jaar. Gelet op de betrekkelijk geringe meerkosten van de bewaarplicht voor de bedrijfsvoering van de aanbieders zie ik geen aanleiding voor de vrees dat de bewaarplicht tot een concurrentienadeel voor de aanbieders zal leiden.

Hieraan kan worden toegevoegd dat er in Nederland een stelsel is tot vergoeding aan de aanbieders voor het geven van opvolging aan een verzoek op grond van het Wetboek van Strafvordering. De vergoeding geschied conform artikel 13, tweede lid, van de Telecommunicatiewet. De aanbieders ontvangen geen vergoeding voor het bewaren van de gegevens maar een vergoeding voor het voldoen aan een strafrechtelijke vordering, kortom het leveren van de gevorderde gegevens. Met dit wetsvoorstel wordt dit stelsel niet gewijzigd.

Naast het onderzoek naar de bedrijfseffecten van het wetsvoorstel voor de aanbieders heeft het Ministerie van Economische Zaken de onderzoekers de opdracht gegeven een vergelijking te maken met enkele andere Europese landen. Daarbij is onder andere gekeken naar het vergoedingenbeleid en in hoeverre in andere Europese landen de kleinere aanbieders worden ontzien. In het onderzoek zijn zeven andere Europese landen betrokken, te weten het Verenigd Koninkrijk, België, Frankrijk, Duitsland, Zweden, Polen en Spanje.
Uit de onderzoeksgegevens blijkt dat alleen het Verenigd Koninkrijk een uitzondering maakt ten aanzien van de kleinere aanbieders. De overige landen uit het onderzoek hanteren een generieke bewaarplicht. Uit de analyse van het vergoedingenbeleid blijkt dat zes landen (inclusief Nederland) vergoeden voor het leveren van de gegevens. Twee landen vergoeden in het geheel niet en in geen enkel land ontvangen aanbieders een vergoeding voor het bewaren van de gegevens.

13. De adviezen over het wetsvoorstel[3]

Het wetsvoorstel is in consultatie gegeven aan het College van procureurs-generaal, de korpschef van de politie, de Raad voor de rechtspraak (Rvdr), de Nederlandse Vereniging voor Rechtspraak (NVvR), de Nederlandse Orde van Advocaten (NOvA), de Autoriteit Persoonsgegevens, de Business Communication Providers Alliance, Nederland ICT, NL kabel en de marktpartijen vertegenwoordigd in het zogenaamde Platform 13-samenwerkingsverband. Daarnaast is het wetsvoorstel op internet gepubliceerd en is een ieder in de gelegenheid gesteld hierop te reageren. Dit heeft ruim zeventig reacties opgeleverd.
Hieronder worden de inhoud van de adviezen en de reacties naar aanleiding van de internetconsultatie op hooflijnen besproken. De voorstellen op deelterreinen komen elders in deze toelichting aan de orde.

Het College van procureurs-generaal is verheugd dat het belang van dataretentie door de wetgever wordt onderkend en wil graag duidelijk maken dat bijvoorbeeld het vervolgonderzoek in de zaak Robert M., dat heeft geleid tot de aanhouding van meer dan honderdvijftig verdachten en de bevrijding van meer dan honderd kinderen uit een actuele misbruiksituatie, vrijwel onmogelijk was geweest indien de bewaartermijn voor internetgegevens destijds zes maanden was geweest. Er moet ernstig rekening mee worden gehouden dat de bevrijding van meer dan honderd kinderen uit de misbruiksituatie dan ook niet mogelijk zou zijn geweest. Daarbij vestigt het College met nadruk de aandacht op het belang van de slachtoffers. Juist bij vormen van criminaliteit die een enorme persoonlijke impact op slachtoffers hebben, zoals stalking en bepaalde zedendelicten, hangen een succesvolle opsporing en vervolging grotendeels af van het beschikbaar hebben van verkeersgegevens.

Het College en de politie vragen zich af waarom in het conceptwetsvoorstel is gekozen voor de differentiatie in de bewaartermijnen, waardoor gegevens met betrekking tot telefonie slechts in geval van een strafbedreiging van acht jaar of meer gedurende de volledige bewaartermijn van twaalf maanden kunnen worden gevorderd. Het College en de politie achten het voorgestelde onderscheid niet bevorderlijk voor een zorgvuldig strafvorderlijk onderzoek, omdat het onderscheid tussen een delict waar vier jaar of een delict waar acht jaar gevangenisstraf op is gesteld in veel gevallen in het beginstadium van het onderzoek niet goed is te maken. De voorgestelde constructie is een vreemde eend in de bijt van het systeem van strafvordering, nu een drempel van een gevangenisstraf van acht jaar of meer alleen aan de orde is bij het binnentreden van

[3] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

een woning met het oog op het opnemen van vertrouwelijke communicatie (direct afluisteren). Vanuit het oogpunt van de inmenging in de persoonlijke levenssfeer betreft dit een andersoortige bevoegdheid. Het College is voorts geen voorstander van de differentiatie omdat het in het geval van een strafrechtelijk onderzoek in veel gevallen zal worden gekeken of de verdenking voor een zwaarder delict mogelijk is teneinde over een langere periode gegevens te kunnen vorderen. De differentiatie komt ook de NVvR onwenselijk voor. Er zijn ernstige strafbare feiten aan te wijzen met een grote maatschappelijke impact, waarvan de maximale strafbedreiging lager is dan zes jaar. Gedacht kan worden aan delicten als gewoonteheling, seriematige ladingdiefstallen, ramkraken en gewoontewitwassen. In dergelijke onderzoeken zou de opsporing worden bemoeilijkt door de thans voorgestelde verkorte termijn van zes maanden. De NVvR adviseert van de voorgestelde regeling af te zien.

Aan deze adviezen is gevolg gegeven. Uit de eerdergenoemde impactanalyse blijkt dat voor misdrijven waarin telecommunicatiegegevens een bepalende rol kunnen spelen, zoals diefstal, mensensmokkel, mishandeling met voorbedachte rade, grooming, stalking, oplichting of bedreiging, straks in plaats van twaalf maanden nog maar zes maanden telefoniegegevens beschikbaar zijn. Aangezien van dit soort misdrijven vaak pas na geruime tijd aangifte wordt gedaan en/of een verdachte in beeld is, zullen belangrijke gegevens voor het onderzoek niet langer beschikbaar zijn. De verwachting is dat het aantal vorderingen van verkeersgegevens niet zal afnemen door de beperktere toegang. Er zal enkel een verschuiving plaatsvinden in de termijn waarvoor de telefoniegegevens opgevraagd worden. Vanwege de voorgestelde differentiatie zal in de processen en systemen van politie en Openbaar Ministerie een extra onderscheid gemaakt moeten worden naar misdrijven waarvoor zes maanden telefoniegegevens mogen worden opgevraagd versus misdrijven waarvoor twaalf maanden dergelijke gegevens mogen worden opgevraagd. Dit leidt tot extra complexiteit die het risico op fouten in het proces sterk vergroot.
In reactie op deze adviezen wordt voorts opgemerkt dat, met de introductie van het vereiste dat de ernst van het misdrijf het vorderen van de bewaarde telecommunicatiegegevens rechtvaardigt, de noodzaak van de toetsing van de zwaarte van het delict in het concrete geval in de wet wordt vastgelegd. Daarmee wordt de beoordeling van de proportionaliteit en de subsidiariteit van de vordering in het concrete geval wettelijk geëxpliciteerd. In combinatie met het vereiste van een voorafgaande machtiging van de rechter-commissaris wordt hiermee in adequate waarborgen voorzien om de toegang tot de gegevens daadwerkelijk te beperken tot hetgeen strikt noodzakelijk is voor de bestrijding van (enkel) ernstige criminaliteit. De toetsing van de rechter-commissaris betreffende de proportionaliteit en subsidiariteit van de vordering omvat niet alleen de concrete ernst van het delict, maar ook het onderzoeksbelang. De toetsing kan daarmee tevens betrekking hebben op de periode waarover de gegevens worden gevorderd, in relatie tot de ernst van het feit en de periode tussen de datum van het plegen van het feit en de datum van het vorderen van de gegevens. Dit is in paragraaf 7 nader toegelicht. In het licht van de toetsing van de proportionaliteit en subsidiariteit van de vordering tot verstrekking van de bewaarde gegevens door de rechter-commissaris en de door het Openbaar Ministerie en de politie ingebrachte bezwaren tegen de differentiatie in de toegang tot de bewaarde gegevens ligt handhaving van die differentiatie minder in de rede. Daarom is ervoor gekozen de differentiatie te schrappen.

De AP leest in het arrest van het Hof van Justitie een aanwijzing dat notificatie aan betrokkenen dat hun telecommunicatiegegevens zijn opgevraagd, een bijdrage levert aan de proportionaliteit van de

maatregel. Zonder deugdelijk notificatiesysteem kan bij iedereen in Nederland het gevoel ontstaan dat zij bespied worden. De AP vraagt zich af hoe zich dit verhoudt tot de voorgenomen afschaffing van de notificatieplicht, zoals voorgesteld in het wetsontwerp tot versterking van het presterend vermogen van de politie (Kamerstukken 33 747). In reactie hierop kan worden opgemerkt dat het Hof van Justitie, onder verwijzing naar het oordeel van de advocaat-generaal, opmerkt dat het feit dat gegevens worden bewaard en gebruikt zonder dat de abonnee of gebruiker wordt geïnformeerd bij de betrokkenen het gevoel kan oproepen dat hun privéleven onderwerp is van voortdurend toezicht (par. 37). De voorgestelde regeling strekt er echter niet toe dat iedereen wordt bespied. De bevoegdheid van het vorderen van verkeersgegevens kan slechts worden uitgeoefend indien sprake is van een concrete verdenking van een ernstig strafbaar feit, waarvoor voorlopige hechtenis kan worden opgelegd. De situatie rond de bewaarplicht is op dat punt niet afwijkend van die wanneer op grond van de bestaande wettelijke bevoegdheden persoonsgegevens van derden worden gevorderd, bijvoorbeeld bij banken of autoverhuurbedrijven.
Verder wijst de AP erop dat bij de evaluatiebepaling (art. 13.9 Tw) een concrete invulling ontbreekt van de minimumvereisten waaraan het verslag aan de Staten-Generaal zou moeten voldoen. In het WODC-rapport wordt geadviseerd meer inzicht te bieden door de vorderingen zodanig te registreren dat zichtbaar wordt over hoeveel personen er jaarlijks telecommunicatiegegevens worden opgevraagd, in hoeveel zaken dit gebeurt en voor welke soort zaken deze gegevens worden opgevraagd. Het ontbreken van transparantie op dit punt staat democratische controle op de effectiviteit van de uitoefening van de bevoegdheden in de weg en biedt ook geen inzicht aan burgers over de inzet van dit instrument. Naar aanleiding van dit advies wordt opgemerkt dat gebleken is dat het niet goed mogelijk is om het belang van de bewaarplicht voor de opsporing van ernstige criminaliteit aan de hand van cijfermateriaal te kwantitatief te onderbouwen. Zoals eerder reeds aan de orde is gekomen, hebben Openbaar Ministerie en politie inmiddels een rapportage opgesteld over nut en noodzaak van de bewaarplicht voor telecommunicatiegegevens. In aanvulling op de gegevens van deze rapportage zal ik mij inspannen om de Kamer nader te informeren over het gebruik van de gegevens ten behoeve van de criminaliteitsbestrijding. Dit is hierboven, in paragraaf 9, reeds aan de orde gekomen.
Aanvullend merkt de AP op dat de voorgestelde wetsaanpassing niet tegemoet komt aan een ander kritiekpunt van het Hof, te weten dat de richtlijn geen uitzonderingen bevat voor de communicatie van mensen met een beroepsgeheim. In het advies van XS4ALL wordt hierop ook gewezen (par. 22). Naar aanleiding van deze adviezen wordt opgemerkt dat de regeling van het verschoningsrecht in het Wetboek van Strafvordering reeds in voldoende waarborgen voorziet ter bescherming van de positie van professionele verschoningsgerechtigden. Opneming van een wettelijke uitzonderingspositie voor professionele verschoningsgerechtigden voor de toegang tot opgeslagen telecommunicatiegegevens past niet in het wettelijke stelsel.

Uit het arrest van het Hof van de Europese Unie van 8 april 2014 kan worden afgeleid dat het Hof bij de beoordeling van de rechtmatigheid van de voormalige richtlijn dataretentie, gewicht toekent aan het feit dat in die richtlijn geen uitzondering wordt gemaakt voor professioneel verschoningsgerechtigden (punt 58). Het is een van de factoren die meeweegt. Dit moet worden bezien tegen de achtergrond dat de inbreuk op het recht op privacy groter is wanneer het gaat om communicatie met professioneel verschoningsgerechtigden. Dit betekent evenwel niet zonder meer dat in deze regeling moet worden voorzien in een wettelijke uitzonderingspositie voor verschoningsgerechtigden.

In de huidige wettelijke regeling van de bijzondere opsporingsbevoegdheden (Titels IVA en V) is geen beperking of verbod opgenomen voor de inzet van een bijzondere opsporingsbevoegdheid, zoals de stelselmatige observatie (art. 126g/o Sv), de infiltratie (art. 126h/p Sv) of het aftappen en opnemen van telecommunicatie (art. 126m/s Sv), jegens een verschoningsgerechtigde. Opneming van een wettelijke uitzondering voor het vorderen van verkeersgegevens vormt een inbreuk op dit systeem. In het Wetboek van Strafvordering is vastgelegd dat de zogenaamde professionele verschoningsgerechtigden zich kunnen verschonen van geven van getuigenis of het beantwoorden van bepaalde vragen (art. 218 Sv). Dit betreft personen die uit hoofde van hun stand, hun beroep of hun ambt tot geheimhouding verplicht zijn, zoals de advocaat, de notaris en de arts. Het recht van artikel 218 Sv. is beperkt tot «hetgeen waarvan de wetenschap aan hen als zodanig is toevertrouwd». De grondslag van het professionele verschoningsrecht moet volgens de Hoge Raad worden gevonden in een in Nederland algemeen erkend rechtsbeginsel dat meebrengt dat bij zodanige vertrouwenspersonen het maatschappelijk belang dat de waarheid in rechte aan het licht komt, moet wijken voor het maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking van het besprokene om bijstand en advies tot hen moet kunnen wenden (Hoge Raad 1 maart 1985, NJ 1986, 173). Van belang is dat de toegang tot personen met een maatschappelijke functie wordt gegarandeerd, nu op die personen een beroep kan worden gedaan zonder dat gevreesd hoeft te worden voor openbaarmaking van datgene wat hen in die hoedanigheid bekend wordt. Het wetboek vrijwaart de verschoningsgerechtigde niet van onderzoek; het beschermt vooral de mededelingen die onder het verschoningsrecht vallen. Dit uitgangspunt van de wetgever is ingegeven door de afweging van het belang van de waarheidsvinding tegen het belang dat een ieder zich zonder vrees tot een geheimhouder moet kunnen wenden.

Dit klemt temeer daar niet zonder meer kan worden gezegd dat verkeersgegevens betrekking hebben op hetgeen een geheimhouder en een cliënt uitwisselen. Gegevens betreffende het telecommunicatieverkeer van de geheimhouder kunnen namelijk geen betrekking hebben op «hetgeen waarvan de wetenschap aan hen als zodanig is toevertrouwd» (art. 218 Sv). Dit is ook in de jurisprudentie erkend (Hoge Raad 20 september 2011, ECLI: NL:HR:2011:BP6016). De regeling van de bescherming van het verschoningsrecht bij de toepassing van bijzondere opsporingsbevoegdheden is gericht op mededelingen gedaan door of aan een professioneel geheimhouder (art. 126aa, tweede lid, Sv). Verkeersgegevens betreffen geen mededelingen door of aan een geheimhouder.

Het voorgaande betekent bepaald niet dat er een vrijbrief is om de bewaarde verkeersgegevens van de communicatie van een verschoningsgerechtigde te vorderen. Met het vereiste van een voorafgaande machtiging van de rechter-commissaris voor de vordering van de bewaarde telecommunicatiegegevens bij een aanbieder is een voorafgaande rechterlijke toetsing ter zake gewaarborgd. Deze toetsing strekt zich ook uit over de positie van een professioneel geheimhouder, waarbij rekening moet worden gehouden met de rechtspraak van het Hof van de Europese Unie. Hiermee wordt gewaarborgd dat een ongerechtvaardigde inzet van deze bevoegdheid om de bewaarde verkeersgegevens over een professioneel verschoningsgerechtigde te verkrijgen, wordt voorkomen. Dit is ook in lijn met de inzet van andere bijzondere opsporingsbevoegdheden, waarbij de rechter-commissaris beslist over de voeging bij de processtukken van processen-verbaal of andere voorwerpen die mededelingen bevatten gedaan door of aan een professioneel verschoningsgerechtigde.

De adviezen die volgen uit de internetconsultatie zijn vrijwel alle negatief. De respondenten zijn tegen de bewaarplicht vanwege de schending van de persoonlijke levenssfeer, de strijdigheid met het Europese recht, de lasten voor de aanbieders, en het gebrek aan effectiviteit van de bewaarplicht. Uit de daarbij gehanteerde kwalificaties (totalitaire staat, iedere burger is verdachte, dit past niet in een democratische rechtsstaat, politiestaat, 1984) kan worden afgeleid dat er in bepaalde maatschappelijke geledingen weinig begrip is voor het doel van de bewaarplicht en de aard en inhoud van de te bewaren gegevens. Het doel van de bewaarplicht is om de samenleving veiliger te maken, daarbij is een ieder gebaat. Het is hiervoor noodzakelijk om bepaalde telecommunicatiegegevens te bewaren. Naar aanleiding van deze adviezen is in de toelichting verhelderd om welke gegevens het precies gaat. Hiervoor wordt verwezen naar paragraaf 2.

ARTIKELSGEWIJS DEEL

Artikel I

Wijziging van de Telecommunicatiewet

Onderdeel A

De aanleiding voor het vervallen van de artikelen 13.2a, 13.4, eerste, derde en vierde lid, 13.5, 13.9, 13.10 en 18.7, tweede lid, is in paragraaf 3 van deze toelichting reeds aan de orde gekomen. Met dit wetsvoorstel wordt een aantal onderdelen van de Wet bewaarplicht telecommunicatiegegevens niet alleen opnieuw vastgesteld maar ook gewijzigd. Dit betreft de artikelen 13.2a, derde lid, 13.4, eerste en derde lid, 13.5, derde lid, 18.7, tweede lid, en de bijlage behorende bij artikel 13.2a van de Telecommunicatiewet. Met dit wetsvoorstel wordt een aantal andere onderdelen van die wet opnieuw vastgesteld. Dit betreft de artikelen 13.2a, eerste, tweede en vierde lid, 13.4, tweede en vierde lid, en 13.5, eerste, tweede en vierde lid. Tenslotte wordt artikel 13.10 vernummerd tot artikel 13.9 en opnieuw vastgesteld.

Onderdeel B

Artikel 13.2a

Eerste lid

Dit lid wordt opnieuw vastgesteld. Daarnaast is een nieuw onderdeel c ingevoegd, dat een omschrijving bevat van het begrip «internettelefonie». Hiermee wordt gedoeld op vormen van telefonie via internet. Zoals in het kader van de eerdere wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang en internettelefonie reeds aan de orde is gekomen (Kamerstukken II 2009/10, 32 185, nr. 3), werkt telefonie via internet (zoals voice over IP, ofwel VoIP) in het gebruik hetzelfde als telefonie over een vast netwerk. Het is een alternatief voor vaste telefonie. Dat wil zeggen dat de functionaliteit en de gegenereerde verkeersgegevens overeen komen met die van reguliere vaste telefonie. In dit wetsvoorstel worden deze vormen van telefonie via internet omschreven als «internettelefonie» (art. 13.2a, eerste lid, onderdeel c). Voor de verkeersgegevens van deze vormen van telefonie geldt een bewaartermijn van twaalf maanden (Kamerstukken II 2009/10, 32 185, nr. 3 en nr. 6, blz. 3 respectievelijk blz. 4).

Criteria die daarvoor gelden zijn:
– De VoIP diensten maken gebruik van het reguliere E.164 nummerplan;
– De verkeersgegevens gegenereerd door betreffende VoIP platformen komen voor een groot deel overeen met verkeersgegevens gegenereerd door traditionele geschakelde telefooncentrales;
– De VoIP diensten worden gebruikt als alternatief voor een reguliere circuit geschakelde dienst met gelijksoortige kwaliteitskaders, te weten klanten zijn over het algemeen vierentwintig uur per dag en zeven dagen per week aangemeld bij het platform en klanten zijn vanwege het nummerplan hard gekoppeld aan de modem op eigen locatie.

Tweede en vierde lid

Deze leden worden opnieuw vastgesteld.

Derde lid

Dit lid wordt opnieuw vastgesteld, waarbij de tekst wordt gewijzigd. De voorgestelde wijziging vloeit voort uit de wijziging van de aanpassing van de lijst van de te bewaren gegevens, waarbij onderscheid wordt gemaakt tussen telefonie door middel van een vast of mobiel netwerk en bepaalde vormen van telefonie via het internet enerzijds en internettoegang en andere vormen van telefonie via het internet anderzijds. In het algemeen deel van deze toelichting is aan de orde gekomen dat bepaalde vormen van internettelefonie qua functionaliteit en de gegenereerde telecommunicatiegegevens in zodanige mate overeen komen met reguliere vaste telefonie dat voor deze vormen de bewaartermijn van twaalf maanden geldt (paragraaf 6). Met de voorgestelde wijziging wordt dit onderscheid in dit lid tot uitdrukking gebracht.

Onderdeel C

Artikel 13.4

Eerste lid

Dit lid wordt opnieuw vastgesteld, waarbij de tekst wordt gewijzigd. De voorgestelde wijziging betreft het herstel van een omissie. Met de Wet bewaarplicht telecommunicatiegegevens is dit artikel gewijzigd, waarbij de vorderingsbevoegdheden op grond van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten in één bepaling zijn samengebracht. De verplichting voor de aanbieders op basis van het eerste lid betreft de vordering of het verzoek tot verstrekking van verkeersgegevens. Dit betreft een vordering op grond van artikel 126n, 126u of 126zh Sv. De verplichting voor de aanbieders op grond van het tweede lid betreft de vordering of het verzoek tot verstrekking van gebruikersgegevens. Dit betreft een vordering op grond van artikel 126na, 126ua of 126zi Sv. Thans wordt in het eerste lid echter ook verwezen naar de vordering tot verstrekking van gebruikersgegevens. Dat is niet alleen verwarrend maar bovendien overbodig omdat de vordering tot verstrekking van verkeersgegevens ook de gebruikersgegevens omvat. Daarom wordt voorgesteld in dit lid de verwijzingen naar de vordering van gebruikersgegevens te schrappen. Dit impliceert schrapping van de verwijzing naar de artikelen 126na en 126ua Sv.

Tevens wordt voorgesteld een verwijzing naar artikel 126zh Sv in te voegen. Dit betreft de bevoegdheid van de officier van justitie tot het vorderen van verkeersgegevens, ingeval van aanwijzingen van een terroristisch misdrijf. De verplichting van de aanbieders om aan een

degelijke vordering te voldoen is ten onrechte niet in dit lid opgenomen. Met de voorgestelde wijziging wordt deze omissie hersteld.

Tweede lid

Dit lid wordt opnieuw vastgesteld.

Derde lid

Dit lid wordt opnieuw vastgesteld, waarbij de tekst wordt gewijzigd. De voorgestelde wijziging betreft een technische wijziging. In artikel 13.4, derde lid, van de Telecommunicatiewet is een beperkte bewaarplicht opgenomen, ten behoeve van de zogenaamde bestandsanalyse. Deze analyse houdt in dat als de aanbieder niet kan voldoen aan zijn verplichting om op vordering van een bevoegde autoriteit gegevens over een gebruiker van telecommunicatie te verstrekken, hij deze gegevens door middel van een analyse van zijn bestanden achterhaalt. Dit doet zich voor als de gegevens over een gebruiker van telecommunicatie niet bij de aanbieder zijn geregistreerd, zoals bij prepaid mobiele telefonie. De bestandsanalyse is, als alternatief voor een registratieplicht van prepaid cardhouders, nodig om gebruikers van vooruitbetaalde diensten te kunnen identificeren in het belang van het opsporingsonderzoek naar strafbare feiten. Deze bestandsanalyse is uitgewerkt in het Besluit bijzondere vergaring nummergegevens (Stb. 2002, 31). Met de Wet bewaarplicht telecommunicatiegegevens is de bewaartermijn voor de in het Besluit bijzondere vergaring nummergegevens aangewezen gegevens verhoogd van drie maanden naar twaalf maanden.

Voor zowel de bewaarplicht als de bestandsanalyse moeten de aanbieders dezelfde gegevens bewaren. Schrapping van de tweede volzin van dit lid levert meer duidelijkheid over de verplichtingen van de aanbieder. Dit betreft specifiek de beperking tot de zogenaamde «first Cell ID», en niet tevens de «last Cell ID».

Vierde lid

Dit lid wordt opnieuw vastgesteld.

Onderdeel D

Artikel 13.5

Eerste, tweede en vierde lid

Deze leden worden opnieuw vastgesteld.

Derde lid, onderdeel c

Dit lid wordt opnieuw vastgesteld, waarbij de tekst wordt gewijzigd. Op het gebied van de gegevensbescherming en gegevensbeveiliging zijn verschillende regels van toepassing op de gegevensverwerking door de aanbieders. Deze regels houden in de eerste plaats verband met de Wet bescherming persoonsgegevens. De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Ook de gegevensverwerking door de aanbieders in het kader van het aanbieden van openbare telecommunicatienetwerken en openbare telecommunicatiediensten valt onder de reikwijdte van deze wet. De Wbp bevat bepalingen omtrent de voorwaarden voor gegevens-

verwerking, doelbinding en de verdere verwerking van gegevens, de bewaartermijnen, de rechten van de betrokkene, rechtsbescherming en het toezicht. De verantwoordelijke dient de nodige maatregelen te treffen opdat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verder verwerkt, juist en nauwkeurig zijn (art. 11, tweede lid, Wbp). Ook is de verantwoordelijke verplicht passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige gegevensverwerking (art. 13 Wbp).

In aanvulling op de regels van de Wet bescherming persoonsgegevens worden in de Telecommunicatiewet specifieke regels gesteld voor de verwerking van persoonsgegevens door de aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. Dit houdt verband met de implementatie van de e-privacyrichtlijn. In deze richtlijn worden de beginselen van Richtlijn nr. 95/46/EG (Privacyrichtlijn) omgezet in specifieke voorschriften voor de verwerking van persoonsgegevens in de sector elektronische communicatie van de Europese Unie. Anders dan de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de verwerking van gegevens betreffende natuurlijke personen, strekt de reikwijdte van de bepalingen van de richtlijn betreffende privacy en elektronische communicatie zich in beginsel ook uit tot rechtspersonen. De richtlijn privacy en elektronische communicatie is grotendeels geïmplementeerd in hoofdstuk 11 van de Telecommunicatiewet en de daarop berustende uitvoeringsregelgeving. Deze regels hebben onder meer betrekking op de doeleinden met het oog waarop de aanbieders verkeersgegevens kunnen verwerken, de duur van de gegevensverwerking, de veiligheid en de verstrekking van informatie over de gegevensverwerking aan de abonnee of gebruiker. De aanbieders zijn verplicht passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de aangeboden netwerken en diensten (art.11.3 Tw).

In aanvulling op de regels van de Wet bescherming persoonsgegevens en de Telecommunicatiewet worden in het eerdergenoemde Bbgt nadere regels gesteld terzake van de bescherming en beveiliging van de te bewaren gegevens. Deze regels betreffen de technische en organisatorische maatregelen die de aanbieder moet treffen om de gegevens te beveiligen tegen vernietiging, verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking en om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen.

Met de verplichting om de te bewaren gegevens op het grondgebied van de Europese Unie op te slaan en te verwerken kan ten volle worden gewaarborgd dat de Minister van Economische Zaken toezicht kan houden op de bescherming en beveiliging van de opgeslagen gegevens, met inachtneming van de bevoegdheden van de Autoriteit Persoonsgegevens terzake. Dit toezicht wordt uitgeoefend door het Agentschap Telecom. In de gevallen waarin de gegevens in een andere lidstaat worden opgeslagen, kan het AT een beroep doen op de toezichthoudende autoriteit van die lidstaat. Op grond van de Privacyrichtlijn moeten de autoriteiten van de lidstaten elkaar bij de vervulling van hun taken wederzijds bijstaan om te waarborgen dat de beschermingsvoorschriften in de Europese Unie ten volle worden geëerbiedigd (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, Publicatieblad Nr. L 281). Daartoe werken de toezichthoudende autoriteiten onderling samen voor zover zulks noodzakelijk is voor de uitvoering

van hun taken, met name door de uitwisseling van alle nuttige inlichtingen (art. 28, zesde lid, Privacyrichtlijn). Deze bijstand wordt vereenvoudigd doordat de Nederlandse regels voor de bescherming en de beveiliging van de gegevens voor een belangrijk deel gelijk zijn aan, dan wel de implementatie vormen van, Europese normen op dit gebied.

Onderdeel E

Artikel 13.9

Dit artikel betreft de vaststelling van Bijlage behorende bij artikel 13.2a van de wet. Vanwege de voorgestelde schrapping van de evaluatiebepaling, wordt het huidige artikel 13.10 vernummerd tot artikel 13.9. Deze bepaling wordt opnieuw vastgesteld.
Nu het Hof van Justitie de richtlijn dataretentie met terugwerkende kracht ongeldig heeft verklaard ligt schrapping van de evaluatiebepaling in de rede omdat daarin wordt verwezen naar de richtlijn dataretentie. In plaats daarvan wordt een nieuwe evaluatiebepaling voorgesteld (Artikel III).

Onderdeel F

Artikel 18.7

Tweede lid

Dit lid wordt opnieuw vastgesteld waarbij de tekst wordt gewijzigd. De voorgestelde wijziging heeft betrekking op het volgende. De door Onze Minister aangewezen ambtenaren zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Telecommunicatiewet met betrekking tot bevoegd aftappen en het bewaren van gegevens, als bedoeld in hoofdstuk 13 van de Telecommunicatiewet (art. 15, eerste lid, Tw). Daartoe is de Minister van Economische Zaken bevoegd alle informatie te vorderen voor zover dat nodig is voor de vervulling van zijn taak (art. 18.7 Tw). De telecommunicatiegegevens die door de aanbieders worden bewaard op grond van artikel 13.2a van die wet zijn hiervan echter uitgezonderd, voor zover deze gegevens niet ten dienste van de eigen bedrijfsvoering worden verwerkt (Kamerstukken II 2006/07, 31 145, nr. 3, blz. 55).

Aldus bestaat het toezicht op de beveiliging en vernietiging van gegevens die nodig zijn voor de opsporing op dit moment uit systeemtoezicht. Dat wil zeggen dat de toezichthouders aan de hand van een beschrijving die de aanbieder geeft van zijn bedrijfsvoeringsprocessen, beoordelen of die aanbieder voldoende maatregelen heeft genomen om de beveiliging en vernietiging van deze gegevens te waarborgen. Deze aanpak betekent dat de toezichthouders niet feitelijk kunnen vaststellen welke gegevens de aanbieder bewaart, hoe deze worden bewaard, hoe ze worden beveiligd en wanneer en hoe ze worden vernietigd. Daarvoor is noodzakelijk dat de toezichthouders bevoegd zijn om deze gegevens daadwerkelijk in te kunnen zien als bewijs voor de mate waarin de aanbieder gegevens verwijdert en als bewijs voor het beveiligingsniveau. In het eerdergenoemde onderzoek naar de evaluatie van de Wet bewaarplicht telecommunicatiegegevens door het WODC wordt daarover het volgende gemeld:

«Het AT heeft enkel de mogelijkheid om toe te zien op de juiste uitvoering van bedrijfsprocessen en beschikt niet over de instrumenten die nodig zijn om op de inhoud van de bewaarde en geleverde gegevens toe te kunnen zien. Het AT heeft niet de bevoegdheid om de daadwerkelijke output van verkeers- en locatiegegevens van verschillende aanbieders in te zien. Hiermee mist het Agentschap een instrument om dit aspect van het

toezicht goed uit te kunnen voeren. Wanneer een overheid besluit privacygevoelige informatie van burgers op te slaan en te bewaren, hoort daar een solide en effectief toezicht bij. Het verdient daarom aanbeveling om de rol van de toezichthouder op dit vlak te verbeteren.»

Gelet hierop wordt voorgesteld dit artikel te wijzigen om de toezichthouders in staat te stellen om gegevens feitelijk in te zien. Met de voorgestelde wijziging wordt de bescherming van de privacy van personen op wie deze gegevens betrekking hebben, vergroot. Immers diegene is er bij gebaat dat de toezichthouder feitelijk kan onderzoeken of de verwerking, beveiliging en vernietiging van gegevens plaats heeft conform de wettelijke voorschriften.

Door de Minister van Economische Zaken aangewezen toezichthouders van het Agentschap Telecom zien op grond van artikel 15.1, eerste lid, onderdeel i, van de Telecommunicatiewet toe op de beveiliging en vernietiging van de gegevens die op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard door de aanbieders. In het Besluit aanwijzing toezichthouders Telecommunicatiewet zijn de ambtenaren met de functienamen inspecteur/medewerker toezicht, senior inspecteur van de afdeling Toezicht van Agentschap Telecom belast met het toezicht. Andere ambtenaren die zijn belast met het toezicht op de naleving van het bij of krachtens andere hoofdstukken van de Telecommunicatiewet bepaalde (die aldus geen toezicht houden op de zogenoemde bewaarplicht) hebben geen toegang tot deze gegevens. Hiertoe strekt de clausulering «voor zover dit nodig is voor het toezicht op de naleving van het bepaalde bij of krachtens hoofdstuk 13».

De AP heeft opgemerkt dat niet alleen het AT toezicht houdt op het bepaalde bij of krachtens hoofdstuk 13, maar ook de AP, voor zover het gaat om de verwerking van persoonsgegevens. De zinsnede «Andere toezichthouders (die aldus geen toezicht houden op de zogenoemde bewaarplicht) hebben geen toegang tot deze gegevens», lijkt het toezicht door de AP uit te sluiten. Aanvullend merkt de AP op dat in de richtlijn dataretentie was bepaald dat de toezichthoudende instanties volledig onafhankelijk zijn bij de uitoefening van de (...) bedoelde taak. Daarvan is naar het oordeel van de AP in het Nederlandse voorstel geen sprake, nu deze taak is toebedeeld aan een agentschap onder directe verantwoordelijkheid van de Minister van Economische Zaken. Het Hof van Justitie benadrukt volgens de AP het belang van onafhankelijk toezicht (par. 68). Daarbij wordt ook verwezen naar de voorlichting van de Raad van State, waarin is vermeld dat ten volle moet zijn gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de beveiliging en bescherming van de opgeslagen gegevens.

Naar aanleiding van dit advies kan worden opgemerkt dat destijds, in het toenmalige wetsvoorstel bewaarplicht telecommunicatiegegevens (Kamerstukken 2006/07, 31 145, nr. 2), is voorgesteld het toezicht op de naleving van het bij of krachtens dit wetsvoorstel bepaalde op te dragen aan de Minister van Economische Zaken, met inachtneming van de bevoegdheden van de Autoriteit Persoonsgegevens terzake. Die keuze was ingegeven door de situatie dat de Minister van Economische Zaken reeds toezicht hield op de naleving van de aftapverplichtingen die voortvloeien uit hoofdstuk 13. De toezichthoudende taak van de Minister van Economische Zaken doet echter op geen enkele wijze afbreuk aan de toezichtbevoegdheden die de Autoriteit Persoonsgegevens heeft met betrekking tot het gebruik van gegevens die zijn aan te merken als persoonsgegevens. De Wet bescherming persoonsgegevens is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van

persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (art. 2, eerste lid, Wbp). De verwerking van persoonsgegevens door de aanbieders, op grond van de Telecommunicatiewet, is hiervan niet uitgesloten. Op grond van de Wbp heeft de AP tot taak toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens die wet bepaalde (art. 51 Wbp). De AP heeft de bevoegdheid om eigen onderzoek te verrichten, ongeacht de rol van andere toezichthouders. Deze bevoegdheid heeft ook betrekking op de telecommunicatiegegevens die aan te merken zijn als persoonsgegevens, en die door de aanbieders worden verwerkt op grond van hoofdstuk 13 van de Telecommunicatiewet. Op grond van de artikelen 5:16 en 5:17 Awb kan de AP toegang verkrijgen tot de verkeers- en locatiegegevens die door de aanbieders op grond van artikel 13.2a TW worden bewaard. Naar aanleiding van het advies van de AP is de zinsnede over de andere toezichthouders aangepast. Verhelderd is dat deze betrekking heeft op de ambtenaren die zijn belast met het toezicht op de naleving van het bij of krachtens andere hoofdstukken van de Telecommunicatiewet bepaalde, en dus niet op het toezicht op de naleving van de Wet bescherming persoonsgegevens.

Onderdeel G

De bijlage wordt opnieuw vastgesteld en gewijzigd. De voorgestelde wijziging betreft de aanpassing van de lijst van de te bewaren gegevens. Voorgesteld wordt om de volgende gegevens te schrappen uit de bijlage behorende bij artikel 13.2a van de Telecommunicatiewet:

– enhanced media service (EMS) en multimedia service (MMS) in de definitie van telefoondienst onder a;
– e-mail over internet onder B;
– internettelefonie onder B en de daarmee samenhangende toegewezen gebruikersidentificatie(s) en de gebruikersidentificatie of telefoonnummer van de beoogde ontvanger(s) van een internettelefoonoproep onder B, sub a;
– datum en tijdstip van de log-in en log-off van een e-maildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone onder B, sub e;
– het inbellende nummer voor een inbelverbinding onder B, sub g;
– de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie onder B, sub h.

Voorgesteld wordt om in de lijst van de te bewaren verkeersgegevens tot uitdrukking te brengen dat bepaalde vormen van telefonie via internet ook tot telefonie behoren, zodat voor de betreffende gegevens een bewaartermijn geldt van twaalf maanden. Hiervoor kan worden verwezen naar de toelichting op artikel 13.2a, eerste lid.
Voor de verkeersgegevens van spraakdiensten die gebruik maken van het internet en niet over deze functionaliteiten beschikken, geldt een bewaartermijn van zes maanden.

Verder blijken in de praktijk verschillende interpretaties van de term IP-adres, als bedoeld in de bijlage behorende bij artikel 13.2a, te bestaan. De bedoeling van de Wet bewaarplicht telecommunicatiegegevens is dat gegevens beschikbaar zijn voor opsporing en vervolging waarmee de abonnee of gebruiker van telecommunicatie kan worden geïdentificeerd. De unieke identificatie van een individuele abonnee of gebruiker noopt tot aanpassing van de te bewaren gegevens. Als de term IP-adres te beperkt wordt uitgelegd, betekent dit dat slechts het interne of publieke IP-adres wordt opgeslagen zonder de daaraan gerelateerde gegevens zoals de poortnummers. Een poortnummer is een extra label dat gebruikt kan worden om een specifieke koppeling met het IP-adres te maken. Poort-

nummers worden onder andere beschreven in de zogenoemde network address translator (rfc 2663). Een enkel intern of publiek IP-adres is door de technologische ontwikkelingen ten aanzien van internet niet langer tot een individuele gebruiker te herleiden, maar tot bijvoorbeeld meerdere gebruikers in de hele straat of wijk waar het signaal vandaan komt of een groep gebruikers van mobiel internet. Dit strookt niet met het doel van de wet.
Voorgesteld wordt om de formulering aan te passen zodat expliciet tot uitdrukking komt dat naast een IP-adres direct aan de gebruiker gekoppeld ook aanvullende IP-adressen, die voor het in stand houden van de verbinding door de aanbieder van de communicatiedienst via het internet noodzakelijk zijn, inclusief de datum en het tijdstip van de betreffende sessie, in combinatie met de daaraan gerelateerde poortnummers moeten worden opgeslagen. Onder «sessie» wordt verstaan de periode tussen het moment van uitgifte van de unieke combinatie van IP-adres en poortnummer en het moment dat hetzij het IP-adres, hetzij het poortnummer, dan wel de unieke combinatie van IP-adres en poortnummer weer wordt vrijgegeven. Op deze manier wordt gewaarborgd dat IP-adressen, conform het doel van de wet, te relateren zijn aan een gebruiker of abonnee. Dit betekent ook dat de opsporing gerichter kan plaatsvinden, hetgeen tot een beperktere inbreuk op de privacy leidt. Immers, als gericht gezocht kan worden naar een abonnee of gebruiker hoeven andere gebruikers van hetzelfde IP-adres niet in beeld te worden gebracht. Het is niet zo dat als er andere technieken dan bijvoorbeeld poortnummers worden gebruikt, deze technieken zijn uitgesloten. Het doel is immers een individuele gebruiker te herleiden.

KPN constateert dat de eis dat aanbieders steeds de mogelijkheid moeten hebben om eindgebruikers aan (externe) IP-adressen te relateren kan leiden tot complexe, tijdrovende en kostbare aanpassingen van systemen. Met de voorgestelde formulering wordt een zeer technologie-afhankelijke verplichting opgelegd waarvan de praktische omvang niet voorzien kan worden. KPN acht deze aanpassing dan ook niet proportioneel en adviseert te kiezen voor een systeem waarbij een doel wordt beschreven dat in overleg tussen aanbieders en behoeftestellers – en op kosten van de laatste – kan worden ingevuld. Daarbij dient een adequate implementatietermijn te worden toegepast. In reactie hierop kan worden opgemerkt dat met de voorgestelde bepaling niet wordt beoogd een techniekafhankelijke verplichting op te leggen. Essentieel is dat de gebruiker uniek identificeerbaar is. Het is aan de aanbieder om in de hiervoor benodigde technische voorzieningen te voorzien.

T-Mobile kent op dit moment per device en SIM een routeerbaar (uniek) IP-adres toe en vraagt zich af de aanname juist is dat er geen opslag van poortnummers meer nodig is. Voor zover dit zou betekenen dat de gebruiker uniek identificeerbaar is, doordat het publieke IP-adres wordt vastgelegd waarmee de gebruiker het internet op gaat, is deze aanname inderdaad juist.

Artikel II

Wijziging van het Wetboek van Strafvordering

Onderdeel A

Artikel 126n Sv

Derde lid

Dit lid bevat een specifieke bepaling voor het vorderen van historische verkeersgegevens, die door de aanbieders op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven. Deze bepaling vormt een bijzondere regeling ten opzichte van de regeling voor het vorderen van verkeersgegevens, opgenomen in het eerste lid. Op grond van die regeling kan de officier van justitie, ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker.

Met de voorgestelde bepaling worden nadere eisen gesteld aan het vorderen van historische verkeersgegevens, die door de aanbieders op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven. De nadere eisen betreffen de toegang tot de bewaarde verkeersgegevens en de voorafgaande machtiging van de rechter-commissaris. Het moet gaan om een misdrijf waarvoor voorlopige hechtenis mogelijk is en dat van een zodanig ernst is dat dit het vorderen van de bewaarde gegevens rechtvaardigt. Hiermee worden de vereisten van proportionaliteit en subsidiariteit in de wet expliciet tot uitdrukking gebracht.

Met de verwijzing naar de gegevens, als bedoeld in het eerste lid, tweede volzin, onder a, wordt gedoeld op de zogenaamde historische verkeersgegevens. Dit betreft de verkeersgegevens die door de aanbieder zijn verwerkt ten tijde van de vordering tot verstrekking van de gegevens. De gegevens die op grond van dit lid kunnen worden gevorderd, zijn beperkt tot de gegevens die in de bijlage behorende bij de Telecommunicatiewet zijn aangewezen en op grond daarvan worden bewaard gedurende de termijn, bedoeld in artikel 13.2a van de Telecommunicatiewet. Van de historische verkeersgegevens kunnen worden onderscheiden de gegevens die na het tijdstip van de vordering worden verwerkt, de zogenaamde toekomstige verkeersgegevens. De vordering van toekomstige verkeersgegevens valt onder het eerste lid, tweede volzin, onder b. De gegevens die kunnen worden gevorderd, zijn limitatief opgesomd in het Besluit vorderen gegevens telecommunicatie (Stb. 2004, 394).

De vordering van de officier van justitie op grond van dit lid, kan uitsluitend worden gericht tot de aanbieder die gehouden is tot de bewaring van de gegevens, op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet. Deze kring van aanbieders is kleiner dan de kring van aanbieders, bedoeld in artikel 126la van het Wetboek van Strafvordering. Laatstgenoemde kring van aanbieders omvat tevens niet-openbare bedrijfsnetwerken, communicatie faciliterende webdiensten en sociale netwerksites. Deze aanbieders dienen in beginsel uitvoering te geven aan vorderingen van politie en justitie maar de verplichting tot bewaring van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven, op grond van artikel 13.2a, tweede lid, van de Wet bewaarplicht telecommunicatiegegevens, is op hen uitdrukkelijk niet van toepassing.

De vordering van de officier van justitie op grond van dit lid, kan uitsluitend worden gedaan na een voorafgaande machtiging van de rechter-commissaris. Op basis van de door de officier van justitie aan te voeren feiten en omstandigheden kan de rechter-commissaris besluiten tot de afgifte van een machtiging tot het vorderen van de bewaarde verkeersgegevens. Daarbij toetst de rechter-commissaris de wettelijke voorwaarden voor de vordering, zoals de aard en ernst van de verdenking, de ernst van het strafbare feit waarvoor de gegevens worden gevorderd, de periode waarover de gegevens worden gevorderd en de proportionaliteit en subsidiariteit van de vordering. Voorgesteld wordt dat artikel 126l, zevende lid, Sv van overeenkomstige toepassing is zodat de machtiging bij dringende noodzaak, ingeval van spoed, mondeling kan worden gegeven. De rechter-commissaris stelt in dat geval de machtiging binnen drie dagen op schrift.

Vierde lid

Met de Wet vorderen gegevens zijn specifieke bevoegdheden voor het vorderen van gegevens opgenomen in de zevende en achtste afdeling van Titel IVA van het Wetboek van Strafvordering. In deze gevallen wordt de mogelijkheid geboden van een mondelinge vordering. In het geval van een mondelinge vordering stelt de opsporingsambtenaar of de officier van justitie de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht (art. 126nc, vijfde lid, 126nd, vierde lid, 126ne, eerste lid, 126nf, vierde lid, 126ng, vijfde lid, 126uc, tweede lid, 126ud, tweede lid, 126ue, tweede lid, 126uf, tweede lid, 126ug, vijfde lid, Sv).
Op basis van de geldende wettelijke regels is de situatie ontstaan dat een vordering aan een aanbieder van een communicatiedienst tot het verstrekken van andere gegevens dan verkeersgegevens, op grond van de artikelen 126ng en 126ug Sv, mondeling kan worden gedaan. Voor een vordering tot het verstrekken van verkeersgegevens is dit echter niet mogelijk. Dit is in de praktijk niet goed werkbaar. Daarom wordt voorgesteld om voor de bevoegdheid van het vorderen van verkeersgegevens door de officier van justitie expliciet de mogelijkheid te bieden van een mondelinge vordering van verkeersgegevens. In het geval van een mondelinge vordering stelt de officier van justitie de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.

Vijfde lid

Dit lid bevat de gegevens die in de vordering van de officier van justitie aan de rechter-commissaris moeten worden vermeld. Dit betreft de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon over wie gegevens worden gevorderd en de gegevens die worden gevorderd. Ook het misdrijf en de feiten en omstandigheden waaruit blijkt dat aan de wettelijke voorwaarden is voldaan, worden opgenomen in de vordering. De officier van justitie zal in de vordering tevens de periode opnemen waarover de gegevens worden gevorderd.

Zesde en achtste lid (nieuw)

Door de invoeging van het nieuwe derde lid kent de bepaling van artikel 126n Sv twee verschillende soorten vorderingen. Enerzijds de vordering van de officier van justitie aan de aanbieder en anderzijds de vordering van de officier van justitie aan de rechter-commissaris, waarin de officier vraagt om een machtiging. Door middel van de voorgestelde wijzigingen in het nieuwe zesde en achtste lid wordt verduidelijkt dat het in deze leden gaat om de vordering aan de aanbieder.

Zevende lid (nieuw)

Door de invoeging van het nieuwe derde lid bestaan ten aanzien van het vorderen van verkeersgegevens bij een aanbieder een drietal opties. Allereerst blijft ook, op grond van het eerste lid, de mogelijkheid bestaan dat de officier van justitie historische verkeersgegevens vordert zonder machtiging van de rechter-commissaris. Dit zijn historische gegevens die niet zijn bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet of worden gevorderd bij een aanbieder die niet valt onder de reikwijdte van de Telecommunicatiewet. Daarnaast de optie dat de officier van justitie, met machtiging van de rechter-commissaris, historische verkeersgegevens vordert als bedoeld in het derde lid. Tot slot de optie dat de officier van justitie toekomstige verkeersgegevens vordert bij de aanbieder, op grond van het eerste lid.

Het zevende lid (nieuw) stelt eisen aan het proces-verbaal dat de officier van justitie van de vordering opmaakt. Dit ziet alleen op de vordering van toekomstige verkeersgegevens en de vordering van historische verkeersgegevens die niet zijn bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet (opties 2 en 3 als hierboven omschreven). Ten aanzien van de historische verkeersgegevens is aan de opsomming toegevoegd de periode waarover de vordering zich uitstrekt. Dat vereiste bestond reeds ten aanzien van de toekomstige verkeersgegevens.

Dit lid geldt derhalve niet voor de vordering van historische verkeersgegevens, bedoeld in het derde lid. Dit vanwege het nieuwe vijfde lid.

Onderdeel B

Artikel 126na

Eerste en derde lid

Dit artikel betreft de bevoegdheid tot het vorderen van gegevens ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Deze gegevens worden ook aangeduid als gebruikersgegevens. Ook voor de vordering van gebruikersgegevens geldt dat de wettelijke bevoegdheid niet voorziet in de mogelijkheid van een mondelinge vordering van deze gegevens. Hiermee wordt afgeweken van het stelsel van het vorderen van gegevens, in de zevende en achtste afdeling van Titel IVA van het Wetboek van Strafvordering, waarin wel in een dergelijke mogelijkheid wordt voorzien. Hiervoor kan ook worden verwezen naar de toelichting op artikel II, onderdeel A. In het geval van een mondelinge vordering stelt de opsporingsambtenaar de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht. De wijziging in artikel 126na, vierde lid, Sv betreft een wijziging van technische aard die voortvloeit uit de vernummering van het derde tot en met zesde lid van artikel 126n Sv.

Onderdeel C

Artikel 126u

Derde lid

Dit lid bevat een specifieke bepaling voor het vorderen van historische verkeersgegevens, die door de aanbieders worden bewaard ten behoeve van het onderzoek naar georganiseerde criminaliteit.

Deze bepaling vormt een bijzondere regeling ten opzichte van de regeling voor het vorderen van verkeersgegevens, opgenomen in het eerste lid. De regeling vormt onderdeel van Titel V van het Wetboek van Strafvordering, waarin bijzondere opsporingsbevoegdheden zijn opgenomen die kunnen worden ingezet bij het onderzoek naar een georganiseerd verband waarin ernstige misdrijven worden beraamd of gepleegd. Op grond van de regeling kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker, indien uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven waarvoor voorlopige hechtenis is toegelaten worden beraamd of gepleegd die, gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren.

De vordering van de officier van justitie kan, ten aanzien van historische gegevens die door de aanbieders zijn bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet, uitsluitend worden gegeven na een voorafgaande machtiging van de rechter-commissaris. Voor het overige wordt verwezen naar de toelichting bij artikel 126n Sv (Artikel II, onderdeel A).

Onderdeel D

Artikel 126ua

Eerste en derde lid

Dit betreft deels een wijziging van technische aard die voortvloeit uit de vernummering van het derde tot en met zesde lid van artikel 126u Sv tot het zesde tot en met negende lid, van artikel 126u Sv. De wijziging in het eerste lid maakt het mogelijk dat ook de vordering van gebruikersgegevens in Titel V mondeling kan worden gedaan.

Onderdeel E

Artikel 126zh

Tweede lid

In Titel VB van het Eerste Boek van het Wetboek van Strafvordering zijn bijzondere bevoegdheden tot opsporing van terroristische misdrijven opgenomen. In artikel 126zh, tweede lid, Sv is de bevoegdheid van de officier van justitie opgenomen om, in geval van aanwijzingen van een terroristisch misdrijf, een vordering te doen tot het verstrekken van verkeersgegevens. Met de voorgestelde wijziging van dit artikel wordt onder meer de mogelijkheid geboden van een mondelinge vordering van dergelijke gegevens (126n, vierde lid, Sv). Tevens worden het nieuwe derde en vijfde lid van artikel 126n Sv van overeenkomstige toepassing verklaard. Dit betreft de regeling ten aanzien van het vorderen van historische verkeersgegevens die door de aanbieders zijn bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet. Hiervoor kan worden verwezen naar de toelichting op artikel 126n Sv (artikel II, onderdeel A).

Onderdeel F

Artikel 126ii

Tweede lid

De voorgestelde wijziging van dit lid betreft een wijziging van technische aard die voortvloeit uit de vernummering van het derde tot en met zesde lid van artikel 126n Sv tot het zesde tot en met negende lid.

Onderdeel G

Artikel 577be

Tweede en vierde lid

Dit artikel geeft de officier van justitie de bevoegdheid tot het vorderen van verkeersgegevens in het belang van een onderzoek naar het vermogen van de veroordeelde. De voorgestelde wijziging van artikel 126n Sv (Artikel II, onderdeel A) strekt tot aanpassing van deze bepaling. In het tweede lid betreft dit de verwijzing naar het voorgestelde zesde en negende lid van artikel 126n Sv (thans het derde en zesde lid) en in het vierde lid betreft dit de mogelijkheid van een mondelinge vordering tot verstrekking van verkeersgegevens.

Artikel IV

Dit betreft de evaluatiebepaling. Voor de formulering van deze bepaling is aangesloten bij de aanwijzingen voor de regelgeving (aanwijzing 164). Inmiddels heeft de eerste evaluatie van de bewaarplicht voor telecommunicatiegegevens plaatsgevonden, en is het rapport van de evaluatie aangeboden aan de Tweede Kamer (Kamerstukken II 2013/14, 33 870, nr. 1).

De Minister van Veiligheid en Justitie,
G.A. van der Steur