Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2008–2009

31 145 Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens)

F

NADERE MEMORIE VAN ANTWOORD

Ontvangen 9 april 2009

Inleiding

Graag zeg ik de leden van uw fracties dank voor hun nadere inbreng naar aanleiding van de memorie van antwoord. Het stemt tot vreugde dat de leden van de CDA-fractie de beantwoording van de gestelde vragen uitvoerig en consciëntieus noemden. Graag beantwoord ik mede namens de Staatssecretaris van Economische Zaken de vragen van de verschillende fracties die nog open zijn gebleven. In essentie gaat het hier om de implementatie van een Europese richtlijn. Het betreft hier echter tevens een veelomvattend onderwerp, waarbij beleidsmatige, juridische en technische afwegingen een rol spelen, en waarbij een goede voorbereiding essentieel is om de uitvoerbaarheid van de bewaarplicht te verzekeren. Ik ben Uw Kamer zeer erkentelijk voor de geleverde inspanningen om tot een goed inzicht te komen in alle uitvoeringsaspecten. De door de vaste commissie van justitie op 11 november 2008 georganiseerde deskundigenbijeenkomst is daarvoor naar mijn mening van groot belang. De bevindingen van de deskundigen neem ik graag ter harte, zoals uit de navolgende beantwoording mag blijken.

Met het oog op deze deskundigenbijeenkomst wilden de leden van de CDA-fractie in dit stadium van de parlementaire behandeling nog een aantal aanvullende vragen stellen. Naar aanleiding van de memorie van antwoord hielden de leden van de VVD-fractie nog enkele vragen over. Ook wensten zij nog enkele meer technische vragen te stellen, waarvan de beantwoording mede bepalend is voor de beoordeling van de effectiviteit van de wet. Tenslotte hadden ook de leden van de fracties van de PvdA en GroenLinks na lezing van de memorie van antwoord nog enkele vragen.

In deze nadere memorie van antwoord hoop ik de nadere vragen van de leden van uw fracties naar tevredenheid te kunnen beantwoorden. Bij de beantwoording is de volgorde van het nader verslag gevolgd, in een enkel

KST129808
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2009

geval zijn de met elkaar verband houdende vragen van verschillende fracties voor de beantwoording samengevoegd.

Nut en noodzaak, proportionaliteit

De leden van de CDA-fractie haalden het verslag van de expertbijeenkomst aan waaruit scherpe conclusies kunnen worden getrokken voor wat betreft de effectiviteit – en daarmee voor wat betreft nut en noodzaak – van de voorgestelde bewaarplicht van verkeersgegevens. In dit verband was het volgens deze leden in ieder geval van belang, dat het om een buitengewoon groot aantal communicaties gaat, waarin een zeer hoog percentage spam is begrepen. De aanbieder van het communicatiesysteem kan daarbij geen scheiding aanbrengen tussen spam en andere berichten. Bovendien is het aantal mogelijkheden tot omzeilen van de bewaarplicht groot. Graag vernamen de aan het woord zijnde leden de visie van de regering op de betreffende opmerkingen van de deskundigen.

Graag ga ik als volgt op deze vragen in. De lijst van de te bewaren gegevens vormt onderdeel van de Richtlijn dataretentie. De door de leden van Uw Kamer gehoorde deskundigen hebben aangegeven dat het aantal te bewaren gegevens zeer omvangrijk is. In dat verband is door de deskundigen gesproken over de verkeersgegevens van 451 miljoen communicaties per dag. Ook in het rapport van het onderzoeksbureau Verdonck, Klooster & Associates B.V. (hierna ook te noemen: VKA) is geconstateerd dat het bij de opslag en verwerking van verkeersgegevens gaat om grote hoeveelheden data. Bij het zoeken naar de in het onderzoeksrapport gepresenteerde oplossingen heeft VKA zich vergewist van de mogelijkheden die de stand der techniek biedt. Daarbij heeft VKA een inschatting gemaakt van de technische capaciteit die daarvoor nodig is. De door Uw Kamer gehoorde deskundigen hebben met zoveel woorden aangegeven dat er hardware en software technologie bestaat om de in de bijlagen A en B bij het wetsvoorstel weergegeven gegevens uit de systemen weg te schrijven, vervolgens op te slaan en te bevragen. De door VKA gehanteerde berekeningen worden door hen niet betwist en zij achten het technisch heel goed mogelijk om de gegevens te bewaren en er vervolgens zoekqueries op te draaien. Wel wijzen zij op complicaties als de gegevens real time on line bevraagd moeten kunnen worden. Ook wijzen zij erop dat er geen standaardpakketten op de markt zijn die door de serviceproviders gekocht kunnen worden en achten zij de termijnen voor de levering van de gegevens van groot belang voor de uitvoerbaarheid. In navolging van de richtlijn verplicht het wetsvoorstel tot het bewaren van de gegevens, zodat deze beschikbaar kunnen worden gesteld aan de opsporingsautoriteiten. De richtlijn, en ook het wetsvoorstel bewaarplicht telecommunicatiegegevens, strekken echter niet tot het real time on line kunnen leveren van de gegevens. Gelet op het vorenstaande deel ik de mening van de deskundigen dat het van groot belang is dat goede afspraken worden gemaakt tussen de ISP's en de behoefstellers over de wederzijdse verwachtingen en verplichtingen. Hieronder zal ik, naar aanleiding van een vraag van de PvdA-fractie, nader op dit punt ingaan. Naar aanleiding van een vraag van de VVD-fractie zal ik verderop nader ingaan op de termijnen voor de levering van de gegevens.

De leden van de CDA-fractie refereerden voorts aan het feit dat in het buitengewoon groot aantal communicaties een zeer hoog percentage spam is begrepen. De door de Kamer gehoorde deskundigen hebben hierover geen concrete cijfers genoemd. Ik erken dat in de elektronische communicatie een zeer hoog percentage aan spam is begrepen en dat dit in meerdere landen als probleem wordt ervaren. De verkeersgegevens rond spam vallen namelijk onder de lijst van gegevens van de richtlijn. Inmiddels heeft de Commissie een informeel contactcomité opgericht dat

periodiek bijeenkomt en zich buigt over de implementatie van de richtlijn in de lidstaten. Ook de telecommunicatie-industrie is in het comité vertegenwoordigd. Met de vertegenwoordigers van de sector wordt ook over de behandeling van spam gesproken. Op 22 januari jongstleden heeft in Brussel informeel overleg plaatsgevonden tussen experts over de implementatie van de Richtlijn dataretentie. Daar is onder meer gesproken over het bewaren van spam. Een van de conclusies uit dit overleg was dat veel spam de eindgebruiker niet bereikt door de toepassing van verschillende filtertechnieken door de aanbieders. Afhankelijk van de filtertechniek komt de spam al dan niet in de mailbox van de eindgebruiker. De expertbijeenkomst heeft de volgende aanbevelingen opgeleverd:

– als een e-mail die is aangemerkt als spam niettemin door de aanbieder wordt doorgestuurd naar de eindgebruiker, dient de aanbieder de data van de e-mail overeenkomstig de verplichtingen van de richtlijn te bewaren;
– als spam wordt uitgefilterd door de aanbieder op een zodanige wijze dat de overdracht van het bericht aan de bedoelde ontvanger (eindgebruiker) niet tot stand komt, dan behoeft de aanbieder de data van de e-mail niet te bewaren;
– als de aanbieder de e-mail toegankelijk maakt voor de eindgebruiker (bijvoorbeeld door dat deze het kan «ophalen» bij de aanbieder), dan wordt de aanbieder geacht de e-mail te behandelen als vallend onder de Richtlijn dataretentie, en de nationale wet- en regelgeving die daarop betrekking heeft.

De regering onderschrijft deze aanbevelingen en zal deze betrekken bij de wijze waarop uitvoering aan de richtlijn en het wetsvoorstel wordt gegeven. Tegenwoordig bieden de meeste aanbieders speciale diensten aan, in de vorm van een servicepakket, om spam te filteren zodat deze de eindgebruiker niet bereikt en ook niet meer toegankelijk is voor de eindgebruiker. In die gevallen komt geen communicatie met de eindgebruiker tot stand en behoeven de communicatiegegevens van spam dus ook niet bewaard te worden.

De leden van de CDA-fractie wezen op het grote aantal mogelijkheden tot het omzeilen van de bewaarplicht. Ook de leden van de VVD-fractie merkten op dat het wetsvoorstel niet ziet op de verkeersgegevens die betrekking hebben op vele nieuwe vormen van elektronische communicatie, zoals de verkeersgegevens van zogenaamde social networks (Hyves, Linkedin, etc.), MSN-berichtenuitwisseling en Skype (bellen via internet). Evenmin ziet de bewaarplicht op gratis mailprogramma's zoals Gmail, Hotmail e.d. Nu een belangrijke categorie verkeersgegevens buiten dit wetsvoorstel valt, kunnen vraagtekens worden geplaatst bij het nut van de bewaarplicht en dus bij de effectiviteit van de wet. De leden van deze fractie konden mijn opmerking in de memorie van antwoord, dat ik desondanks van mening blijft dat het nut van de bewaarplicht absoluut niet is verminderd, niet goed plaatsen en zij vroegen om een nadere toelichting op deze opmerking.

Het doel van het wetsvoorstel is dat zeker wordt gesteld dat gegevens over het gebruik en de gebruikers van telecommunicatie worden bewaard, zodat de opsporingsdiensten in daartoe geëigende gevallen kunnen achterhalen welke communicatie wanneer heeft plaatsgevonden en wie daar mogelijk bij betrokken waren. Het is evident dat niet in alle gevallen op basis van de beschikbare verkeersgegevens een volledig beeld kan en zal worden verkregen van de volledige communicatie die heeft plaatsgevonden. Aan de andere kant worden er dagelijks – zo hebben ook de experts bevestigd in hun antwoorden op de vragen van Uw Kamer – over honderden miljoenen communicaties per dag gegevens bewaard. Deze gegevens zijn zeer waardevol in zeer veel onderzoeken die door de opspo-

ringsdiensten worden gedaan. Daarmee staat voor mij het nut van de bewaarplicht vast.
Ik onderken dat deze categorie verkeersgegevens – namelijk verkeersgegevens die betrekking hebben op nieuwe vormen van elektronische communicatie – buiten het wetsvoorstel valt. Dat betekent echter nog niet dat deze gegevens nu of in de toekomst in daartoe geëigende gevallen niet alsnog beschikbaar komen. Zo kan uit het beeld over het gebruik van telecommunicatie, dat ontstaat aan de hand van de wel beschikbare verkeersgegevens, blijken dat een subject gebruik maakt van diensten als Hotmail, MSN of Gmail. Dat kan aanleiding zijn om die gegevens via een rechtshulpverzoek aan de autoriteiten van – in dit geval – de Verenigde Staten ten behoeve van een lopend opsporingsonderzoek op te vragen. Gegevens over het gebruik van sociale netwerksites als Hyves en LinkedIn en het gebruik van bepaalde vormen van internettelefonie als Skype vallen thans buiten het wetsvoorstel omdat het politiek draagvlak binnen de Europese Unie ontbrak om gegevens over het gebruik van internet, anders dan over de enkele internettoegang, te bewaren. Ook het Europees Parlement was hiervan geen voorstander. Dit betekent dat voor wat betreft het internetgebruik op basis van de bewaarde gegevens alleen kan worden vastgesteld wanneer toegang is verkregen tot het internet en niet welke sites vervolgens zijn bezocht, dan wel welke diensten zijn gebruikt. Indien zou blijken dat hiermee een belangrijke categorie verkeersgegevens buiten de reikwijdte van de Richtlijn dataretentie valt, dan kan dit bij de evaluatie van de richtlijn aan de orde komen en zal dit mogelijk tot voorstellen tot aanpassing van de richtlijn leiden.

De leden van de PvdA-fractie vroegen hoe mijn opmerkingen over de proportionaliteit begrepen moesten worden, namelijk dat het risico dat een ernstige strafzaak onopgelost blijft groter wordt naarmate de bewaartermijn korter wordt gesteld en dat als uit de evaluatie van de twaalf maandstermijn naar voren zou komen dat een beperkt aantal zaken onopgelost is gebleven als gevolg van het niet langer beschikbaar zijn van telecommunicatiegegevens, dit niet goed te verdedigen valt. De leden van deze fractie vroegen of hiermee feitelijk «hoe langer hoe beter» geldt, omdat iedere mogelijk onopgeloste strafzaak als gevolg van het niet meer kunnen beschikken over telecommunicatiegegevens er een teveel is. Als dat niet de inzet is – en daarbij dachten deze leden ook aan de aangehaalde cold cases – vroegen deze leden wanneer, en vooral waarom, een kritische grens wordt bereikt.

Mijn opmerkingen over de proportionaliteit moeten worden begrepen in het kader van de gewenste duur van de bewaartermijn. De richtlijn biedt de lidstaten op dit punt de nodige ruimte, omdat de richtlijn voorschrijft dat de bewaartermijn ten minste zes maanden en ten hoogste twee jaar is. Tijdens de behandeling van het wetsvoorstel in de Tweede Kamer is door verschillende fracties gevraagd naar de noodzaak van een langere bewaartermijn dan het minimum van zes maanden. In dat verband werd ook gevraagd naar het te verwachten aantal zaken, waarin na verloop van zes, twaalf of achttien maanden behoefte zou bestaan aan verkeersgegevens ten behoeve van het opsporingsonderzoek. Naar mijn mening kan een dergelijke discussie echter niet alleen worden gevoerd uitsluitend op basis van cijfers of statistieken. Want het gaat daarbij niet alleen om een kwantitatieve maar ook om een kwalitatieve vraag. Ik heb aangegeven niet te verwachten dat de opsporingsdiensten straks in een groot aantal gevallen een beroep zullen doen op oudere gegevens. De realiteit is wel dat juist bij zeer ernstige misdrijven waarvan het onderzoek laat op gang komt of waarvan na enige tijd blijkt dat het onderzoek op een dwaalspoor is geweest en pas in een later stadium belangrijke aanwijzingen of aanknopingspunten beschikbaar komen op basis waarvan gericht gevraagd kan worden naar communicatiegegevens van bepaalde

personen, verkeersgegevens een belangrijke rol kunnen vervullen. De betekenis van die gegevens is niet alleen gelegen in de mogelijkheid van de bewijsvoering maar ook in de bepaling van de verdere richting van het onderzoek. Daarbij merk ik nog op dat niet alleen de opsporing maar ook de in het onderzoek betrokken personen zelf belang kunnen hebben bij dergelijke gegevens omdat hieruit ook juist hun onschuld kan blijken. De bijlage van de brief aan de Tweede Kamer van 14 februari 2005 (Kamerstukken II 2004/05, 23 490, nr. 360) bevat daarvan reeds voorbeelden. Weliswaar staat niet vast dat zeer frequent gebruik gemaakt zal worden van gegevens die in plaats van zes maanden twaalf of achttien maanden worden bewaard, maar ik ben er van doordrongen dat hoe sneller de gegevens vernietigd worden, hoe groter het risico is dat ernstige strafzaken onopgelost blijven. In de nota naar aanleiding van het verslag heb ik voorbeelden gegeven van gevallen waarin in een later stadium behoefte bestond aan verkeersgegevens (Kamerstukken II, 2007/08, 31 145, nr. 9, blz. 15). In strafzaken die ouder zijn gaat het haast per definitie om gegevens die ouder zijn. Ook in cold cases zullen verdachten in beeld kunnen komen die eerder buiten beeld waren geraakt. Als alle gegevens dan weg zijn, wordt de kans dat ernstige criminaliteit ook op langere termijn onopgelost blijft des te groter. Het is mijns inziens dan ook duidelijk dat een bewaartermijn van achttien maanden meer mogelijkheden biedt dan een termijn van een jaar. Politie en justitie hebben in hun adviezen verzocht om een bewaartermijn van twee jaar, dit betreft inderdaad de maximale termijn van de richtlijn.
Met de duur van de bewaartermijn is echter niet alleen het belang van de opsporing van strafbare feiten in het geding. Ook het belang van de bescherming van de persoonlijke levenssfeer speelt een belangrijke rol, evenals de lasten voor het bedrijfsleven. Daarbij merk ik op dat de toegang tot de bewaarde gegevens op grond van het Wetboek van Strafvordering slechts in bepaalde gevallen is toegestaan in het belang van de opsporing van strafbare feiten. Ik meen dat het belang dat strafbare feiten worden opgelost kan opwegen tegen een bewaarplicht van een jaar. Ook meen ik dat het belang dat strafbare feiten worden opgelost opweegt tegen de kosten die zijn verbonden aan het gedurende een periode van een jaar bewaren van telecommunicatiegegevens, temeer nu geldt dat de opslagkosten gedurende de afgelopen jaren sterk zijn gedaald. Hieronder zal, in antwoorden op de vragen van de leden van de fractie van GroenLinks, hierop nog worden teruggekomen. Alle belangen afwegend en alle omstandigheden in aanmerking nemend meen ik dat de kritische grens bij een bewaartermijn van een jaar zeker niet bereikt is. Daarbij merk ik nog op dat ik er geen voorstander van ben om op dit terrein bij voorbaat definitieve grenzen te stellen. Ik meen dat de evaluaties meer inzicht kunnen geven in het belang van de gegevens in concrete onderzoeken en daarmee ook in de optimale duur van de bewaartermijn. De evaluatie van de richtlijn moet voor 15 september 2010 zijn afgerond. De Wet bewaarplicht telecommunicatiegegevens zal, naar aanleiding van het amendement van het lid Anker, drie jaar na de inwerkingtreding worden geëvalueerd (Kamerstukken II 2007/08, 31 145, nr. 14).

De leden van de PvdA-fractie vroegen om een reactie op de analyse en antwoorden van de door Uw Kamer geraadpleegde experts. Tevens vroegen zij of de mogelijkheden van «de techniek» op pagina 3 van de memorie van antwoord niet te optimistisch worden voorgesteld. Tenslotte vroegen zij of de kans dat de mogelijkheden in hun tegendeel gaan verkeren niet groter wordt, naarmate de termijn waarover die gegevens worden opgeslagen langer wordt, en zo nee, waarom niet.

In antwoord op de gestelde vragen meen ik dat de analyse en antwoorden van de door de Kamer geraadpleegde experts veel waardering verdienen. Zij hebben helder in beeld gebracht waar de problemen liggen ten aanzien

van de bewaarplicht. Met name ten aanzien van de ISP's is helder uiteengezet welke punten aandacht behoeven. In het bijzonder hebben de experts gewezen op het feit dat elke ISP anders is en dat dat ook geldt voor de door hen gebruikte systemen. In dat verband neem ik ter harte dat het van belang is om ten aanzien van de uitvoering van de bewaarplicht in nauw overleg met de ISP's een uniforme aanpak te bespreken. Met enkele grote aanbieders is overleg over de uitvoering reeds in gang gezet in een daartoe ingerichte overlegstructuur. Op het niveau van service level agreements worden gedetailleerde afspraken gemaakt. Vanwege het zeer grote aantal kleine ISP's en het feit dat deze niet georganiseerd zijn is het lastig deze als groep te benaderen voor het maken van afspraken. Om deze ISP's toch te kunnen bereiken heb ik het onderzoeksbureau VKA inmiddels opdracht verstrekt om deze ISP's op een geordende wijze in beeld te brengen met het oogmerk deze als groepen te kunnen benaderen voor het maken van afspraken op maat.
Over de vraag of de mogelijkheden van de techniek in hun tegendeel gaan verkeren naarmate de bewaartermijn langer wordt meen ik dat een goede balans moet worden gevonden tussen enerzijds het maatschappelijke belang van de bestrijding van criminaliteit en anderzijds de bescherming van de persoonlijke levenssfeer en beperking van de lasten voor het bedrijfsleven. Daar waar de techniek de overheid in staat stelt in bepaalde omstandigheden en ten behoeve van de bescherming van bepaalde gerechtvaardigde belangen toegang te verkrijgen tot informatie over de gedragingen van burgers, biedt diezelfde techniek tevens de mogelijkheid om de toegang te beperken tot uitsluitend de gegevens die voor het beschermen van die belangen noodzakelijk zijn. Daarbij merk ik nog op dat het hier gaat om technische gegevens die doorgaans verspreid zijn opgeslagen in de systemen van de aanbieders en die als zodanig weinig betekenis hebben voor derden. Het risico van beperking van de persoonlijke levenssfeer van de betrokkenen is vooral gelegen in het risico dat de gegevens een beeld geven van hun communicatiegedrag. Op dit punt bestaat er weinig onderscheid met de gespecificeerde rekening die door de telecommunicatieaanbieders als extra dienstverlening wordt aangeboden. Daarnaast bestaat een risico in de koppeling van de gegevens aan strafbare gedragingen van personen. Eenzelfde risico is echter eveneens aan de orde bij de bevraging van kentekengegevens door de politie. Het Wetboek van Strafvordering kent strikte voorwaarden waaronder opsporingsambtenaren kennis kunnen nemen van gegevens van derden. Het voorgaande neemt niet weg dat de betrokkenen recht hebben op een buitengewoon zorgvuldige verwerking van de gegevens over hun communicatie.
De Wet bescherming persoonsgegevens en de Telecommunicatiewet verplichten den aanbieders tot bescherming en beveiliging van persoonsgegevens (art. 11.2 Tw). In navolging van eerdere richtlijnen op het gebied van telecommunicatie bevat de Richtlijn dataretentie voorschriften op het gebied van de beveiliging van de gegevens. Dit is uitgewerkt in het ontwerpbesluit beveiliging gegevens telecommunicatie, dat voor advies aan de Raad van State is voorgelegd. Dit ontwerpbesluit is een aanvulling en aanpassing van het bestaande Besluit beveiliging gegevens aftappen telecommunicatie en geeft strikte regels over de beveiliging van de bewaarde gegevens door de aanbieders. Deze regels hebben betrekking op de fysieke beveiliging van gegevens, het opstellen van een beveiligingsplan, de screening van personeel dat toegang heeft tot de gegevens en de vernietiging van de gegevens. Dit conceptbesluit is ter kennisneming bij deze nadere memorie van antwoord gevoegd. Mede met het oog op de geldende regels voor de beveiliging van de gegevens voor de aanbieders van telecommunicatiediensten, zoals die onder meer tot uitdrukking komen in het Besluit beveiliging gegevens telecommunicatie, meen ik dat het buiten iedere redelijke twijfel is dat de mogelijkheden, tot het langer bewaren van gegevens niet in hun nadeel kunnen

verkeren.

De leden van de fractie van GroenLinks zetten ernstige vraagtekens bij de noodzakelijkheid en proportionaliteit van de voorgestelde maatregel. Zij wezen erop dat met de bewaarplicht namelijk ongericht informatie wordt verzameld over iedereen, verdacht of onverdacht, en dat de regering niet alleen de gegevens van verdachte personen wil kunnen opvragen, maar de gegevensbestanden ook wil kunnen doorzoeken op risicoprofielen, het zogenoemde «*dataminen*». Hierdoor kan het Openbaar Ministerie volgens deze leden gevoelige gegevens in handen krijgen van onverdachte personen, waar het nooit opsporingsbevoegdheden voor zou hebben gekregen. Zij wezen erop dat in de memorie van antwoord wel wordt aangegeven dat er alleen onderzoek kan worden ingesteld bij aanwijzingen voor het beramen of plegen van een terroristisch misdrijf, maar de gegevens die worden doorzocht, zien op een grote willekeurige groep mensen. Deze leden vroegen of zij dit juist zien en zo ja, of deze wijze van gegevensvergaring strookt met de criteria van noodzakelijkheid en proportionaliteit.

In antwoord op deze vragen merk ik op dat de bewaarplicht inderdaad strekt tot het opslaan van gegevens over alle personen die gebruik maken van telecommunicatie. Voor een juist begrip moet het opslaan van de gegevens echter worden onderscheiden van het gebruik van de gegevens. De toegang tot de bewaarde gegevens is beperkt tot die gevallen waarin de wet daarin voorziet. Dit betreffen de regels over het vorderen van verkeersgegevens in het Wetboek van Strafvordering. Zo kan op grond van de artikelen 126n/u Sv de officier van justitie, in geval 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. De gegevens zijn aangewezen in het Besluit vorderen gegevens telecommunicatie (Stb. 2004, 394). Daarnaast kan de officier van justitie op grond van artikel 126na Sv zogenaamde gebruikersgegevens vorderen. Er is dus geen sprake van een algemene bevoegdheid voor het Openbaar Ministerie om de gegevensbestanden te kunnen doorzoeken op risicoprofielen of anderszins zelfstandig bewerkingen op de gegevens toe te passen waardoor er sprake zou kunnen zijn van «datamining». De enige uitzondering hierop betreft de bevoegdheid van de officier van justitie om bij een verkennend onderzoek naar terroristische misdrijven, na voorafgaande schriftelijke machtiging van de rechter-commissaris, in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot een geautomatiseerd gegevensbestand schriftelijk te vorderen dit bestand, of delen daarvan, te verstrekken teneinde de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv).Vereist is dat er daadwerkelijk aanwijzingen zijn van het binnen een groep van personen beramen of plegen van terroristische misdrijven. Deze bevoegdheid dient de bestrijding van het terrorisme, en is overigens met strikte waarborgen omgeven. Zo moet een proces-verbaal worden opgemaakt waarin een beschrijving wordt gegeven van de wijze waarop de bewerking is uitgevoerd en dienen de gegevens die niet van betekenis zijn voor het onderzoek te worden vernietigd. Voorzover mij thans bekend is tot nu nog geen gebruik gemaakt van deze bevoegdheid. Daarbij merk ik op dat de vraag van de leden van deze fractie in feite geen betrekking heeft op de bewaarplicht van telecommunicatiegegevens als zodanig maar op de wenselijkheid van de toedeling van de hierboven beschreven bevoegdheid bij de bestrijding van terrorisme. De noodzakelijkheid en proportionaliteit rond deze vorm van gegevensvergaring zijn in dat verband aan de orde. De stelling dat het Openbaar Ministerie langs deze weg gevoelige gegevens in handen kan krijgen van onverdachte personen, waar het nooit opsporings-

bevoegdheden voor zou hebben gekregen, kan ik niet plaatsen. Het Wetboek van Strafvordering geeft nauwkeurig aan in welke gevallen welke bevoegdheden kunnen worden toegepast. Voor de toepassing van artikel 126hh biedt het vereiste van de schriftelijke machtiging van de rechter-commissaris voor de dergelijke toepassing van de bevoegdheid een extra waarborg.

De leden van de GroenLinks-fractie merkten verder op dat ongerichte zoekacties in de enorme gegevensbestanden zoeken is naar de bekende speld in een hooiberg: relevante gegevens voor de opsporing kan het bijna niet opleveren. Bovendien weerspraken meerdere onderzoeken volgens hen de stelling van de regering, dat de beschikbaarheid van verkeersdata aanwijsbaar invloed heeft op het percentage opgeloste misdaden. Verdachten die uiteindelijk worden veroordeeld, werden vaak ook al om andere redenen gevolgd. De verkeersdata die een rol kunnen spelen bij de opsporing, zijn praktisch nooit ouder dan drie maanden. Een langere bewaarplicht heeft voor een strafrechtelijk onderzoek dan ook nauwelijks enige meerwaarde. De mate van meerwaarde die de bewaarplicht heeft, bepaalt volgens de leden van GroenLinks mede de toets of de inbreuk op het privé-leven geoorloofd is. De leden van deze fractie vroegen of de regering het met deze redenering eens is. Ook vroegen zij hoe de regering onderbouwt dat de bewaarplicht wel iets wezenlijks toevoegt aan de huidige opsporingsmogelijkheden, en in zodanige mate dat het de inbreuk op de privacy rechtvaardigt.

In antwoord op deze vraag merk ik allereerst op dat de verkeersgegevens worden gezocht aan de hand van een nummer van een gebruiker van telecommunicatie. Zoals ik ook hierboven uitéén heb gezet, is er geen sprake van ongerichte zoekacties in enorme gegevensbestanden. Voor wat betreft de meerwaarde van de bewaarplicht deel ik de mening van de leden van deze fractie, dat een langere bewaarplicht voor een strafrechtelijk onderzoek nauwelijks enige meerwaarde heeft, bepaald niet. Uit de ervaringen van politie en justitie en ook uit de onderzoeken die hiernaar zijn verricht blijkt heel anders, namelijk dat een langere bewaarperiode wel degelijk van belang is voor het strafrechtelijk onderzoek. De politie heeft aangedrongen op een lange bewaartermijn ten behoeve van de opsporing van ernstige criminaliteit en zich uitgesproken voor een bewaartermijn van vierentwintig maanden. In zijn advies heeft de Raad van Hoofdcommissarissen gemeld dat binnen de tactische opsporing een bewaartermijn van vierentwintig maanden als minimaal wordt ervaren. In het onderzoek naar de moord op Theo van Gogh werden de opsporingsmogelijkheden volgens de Raad beperkt doordat de verkeersgegevens, ouder dan zes maanden, waren vernietigd. In de nota naar aanleiding van het verslag heb ik verschillende voorbeelden gegeven van zaken waarin een langere beschikbaarheid van verkeersgegevens van essentieel belang waren voor het welslagen van de opsporing en vervolging in ernstige zaken (Kamerstukken II 2007/09, 31 345, nr. 9, blz. 15). In zijn advies over het wetsvoorstel heeft het Openbaar Ministerie aangegeven dat de door de onderzoekers van de Erasmus universiteit aanbevolen bewaartermijn van een jaar als een minimum moet worden beschouwd. Het College heeft er op gewezen dat het rapport van de Erasmus Universiteit zich voornamelijk richt op het opsporingsonderzoek. Ook tijdens het onderzoek ter terechtzitting kan het echter noodzakelijk zijn te beschikken over de bewaarde gegevens. Het onderzoek ter terechtzitting zal in een later stadium aanvangen, zeker in het geval van grootschalige opsporingsonderzoeken die langere tijd hebben gelopen. Daarbij kan het ook in het belang van de verdachte zelf zijn om te kunnen beschikken over verkeersgegevens, omdat uit de gegevens zijn onschuld kan blijken. Als men zich realiseert dat ook de rechter in hoger beroep nader onderzoek kan gelasten dan is het volgens het College duidelijk dat de toentertijd voorge-

stelde bewaartermijn van achttien maanden niets te lang zal zijn. De onderzoekers van de Erasmus Universiteit Rotterdam hebben in hun onderzoek, dat is verricht van februari tot mei 2005, geconstateerd dat er behoefte is aan een ruimere bewaartermijn met het oog op complexere opsporingsonderzoeken op regionaal en nationaal niveau, onderzoeken waarbij internationale samenwerking nodig is, en de zogenaamde cold cases, waarbij het onderzoek op dood spoor is geraakt. Daarbij kwam naar voren dat de behoefte aan verkeersgegevens pas later blijkt, bijvoorbeeld in het geval van vermissing van personen. Het kan ook voorkomen dat een onderzoek reeds langer loopt maar dat tijdens het onderzoek andere inzichten ontstaan over de toedracht of de betrokken personen, bijvoorbeeld als nieuwe getuigen worden gevonden of nieuwe sporen worden aangetroffen. Tevens hebben de onderzoekers geconcludeerd dat een langere bewaartermijn kan leiden tot meer afgewogen, beperktere bevraging van verkeersgegevens omdat minder gegevens opgevraagd zullen worden uit vrees dat zij op een later moment vernietigd zullen zijn die achteraf bezien niet relevant waren voor het onderzoek. Al met al concludeer ik dat verkeersgegevens van groot belang zijn voor het opsporingsonderzoek naar ernstige vormen van criminaliteit en dat de bewaarplicht iets wezenlijks toevoegt aan de bestaande opsporingsmogelijkheden, en wel zodanig dat dit een mogelijke beperking van de persoonlijke levenssfeer rechtvaardigt. Het recht op de bescherming van de persoonlijke levenssfeer, voortvloeiend uit de artikelen 8 van het EVRM en artikel 10 van de Grondwet, is slechts in beperkte mate in het geding. Over de inhoud van communicatie wordt niets vastgelegd. De gegevens zijn technisch van aard en worden doorgaans verspreid opgeslagen in de systemen van de aanbieders. Verkeersgegevens zijn niet erg veelzeggend zolang deze niet kunnen worden gekoppeld aan gedragingen van personen. Een beperking van de persoonlijke levenssfeer is vooral aan de orde bij de raadpleging van de gegevens. Het opvragen van verkeersgegevens bij de aanbieders is reeds langere tijd een gebruikelijke handelwijze binnen de opsporing. Hiervoor gelden strikte wettelijke vereisten. Op dit punt brengt de bewaarplicht geen verandering. De consequenties van de wettelijke bewaarplicht voor de bescherming van de persoonlijke levenssfeer mogen naar mijn mening dan ook niet worden overtrokken. Hieronder, bij de beantwoording van de vragen van de CDA-fractie over de jurisprudentie van het Europese Hof met betrekking tot artikel 8 EVRM, zal ik hierop nader ingaan.

De leden van de GroenLinks-fractie merkten op dat ook om andere redenen de effectiviteit van de wet allerminst is gegarandeerd omdat de bewaarplicht simpel te omzeilen valt door gebruik te maken van een buitenlandse provider. Daarnaast is de communicatie via Skype niet vast te leggen, en valt bedrijfsmail, MSN-verkeer en twitteren (dit laatste deels) buiten de bewaarplicht. Nu de communicatietechnologie zich razendsnel ontwikkelt, heeft zelfs een niet al te snuggere boef, die zijn zaakjes buiten het vizier van de opsporingsdiensten wil houden, volgens deze leden nog een ruime keuze aan communicatiemiddelen. Zij vroegen of de regering weet wat het percentage verkeersgegevens is dat buiten de bewaarplicht valt en of de regering de indruk van de leden van GroenLinks deelt dat dit percentage nog verder zal groeien. Tevens vroegen zij of de regering de wet nog voldoende effectief acht, gelet op deze enorme omvang van data die buiten de reikwijdte van de wet vallen, en zo ja, op welke wijze. Tenslotte vroegen zij of de regering op mogelijkheden zint om het groeiende aantal verkeersgegevens dat buiten de reikwijdte van de wet valt in te dammen, en zo ja, op welke wijze.

De regering beschikt niet over cijfers over het percentage verkeersgegevens dat buiten de bewaarplicht valt. Het ligt echter in de lijn der verwachting dat het gebruik van diensten als Hotmail aanzienlijk is en mogelijk zal

groeien. Daarmee zal ook het volume aan verkeersgegevens, dat buiten de werkingssfeer van de bewaarplicht valt, toenemen. Ondanks het gebruik van deze diensten is het nut van de toepassing van strafvorderlijke bevoegdheden met betrekking tot telecommunicatie via de mobiele telefoon en de internetvoorzieningen die de traditionele e-mail benutten, waarbij dus gebruik wordt gemaakt van Nederlandse aanbieders, echter absoluut niet verminderd. Dat sommige aanbieders van e-maildiensten zelf niet als aanbieder in de zin van de Telecommunicatiewet kunnen worden aangemerkt, waardoor minder gegevens beschikbaar zijn voor politie en justitie, is een beperking die inherent is aan de Richtlijn dataretentie en het onderhavige wetsvoorstel. Ik heb de Tweede Kamer toegezegd te onderzoeken hoe dit gat, waar nodig via internationale samenwerking, kan worden gedicht. Hierbij kan ook worden gedacht aan de eerdergenoemde evaluatie van de Richtlijn dataretentie door de Commissie, die volgend jaar zal worden afgerond. In antwoord op vragen van de fractie van de VVD en het CDA ben ik in het voorgaande reeds ingegaan op de effectiviteit van de regeling. In het uiterste geval kan, indien de verkregen informatie onvoldoende richting kan geven aan het opsporingsonderzoek onder omstandigheden en indien daar aanleiding voor is, door de rechter-commissaris een machtiging worden gegeven voor het zetten van een tap op de internettoegang. In dat geval worden alle verkeersgegevens voor de duur van de tap ondervangen.
De leden van Groen Links wezen er nog op dat ICT-experts verwachten dat 98 procent van de bewaarde gegevens uit spam zal bestaan en vroegen in dat verband wat het nut is van de opslag van die data. Hierboven heb ik, naar aanleiding van een gelijkluidende vraag van de leden van de CDA-fractie, aangegeven dat op Europees niveau aan de orde is hoe kan worden omgegaan met de verkeersgegevens van spam. Een belangrijke aanbeveling van de deskundigen, die ik onderschrijf, is dat als spam op een zodanige manier wordt gefilterd dat de overdracht van het bericht aan de gebruiker niet tot stand komt, de verkeersgegevens van de e-mail niet hoeven te worden bewaard. Ik verwijs voor het overige graag naar de eerdere beantwoording. Omdat de meeste aanbieders spam filteren voordat het de eindgebruiker bereikt, en veel klanten inmiddels gebruik maken van deze mogelijkheid, zal de hoeveelheid spam die uiteindelijk de eindgebruiker bereikt aanzienlijk minder worden.

Betrouwbaarheid identiteit/gegevens

De leden van de VVD-fractie achtten het een gegeven dat het heel gemakkelijk is om via iemand anders identiteit te communiceren. Volgens hen kost het niet veel inspanning om berichten zodanig te versleutelen, dat het voor een buitenstaander niet mogelijk is de identiteitsgegevens te achterhalen. Dit heeft naar hun oordeel ook belangrijke consequenties voor de betrouwbaarheid van het strafrechtelijk onderzoek en mogelijk bewijsmateriaal. Zij vroegen hoe ik kan waarborgen dat de gegenereerde verkeersgegevens desondanks toch betrouwbaar zijn. De leden van de fractie van GroenLinks stelden een soortgelijke vraag en wezen op het risico voor de privacy.

In antwoord op de gestelde vragen merk ik op dat er inderdaad verschillenende manieren zijn om bij de communicatie via het internet een andere identiteit aan te nemen of gegevens te versleutelen. Zo kan de zender bijvoorbeeld eenvoudig de naam in de header veranderen. Ook is het, voor terzake deskundige personen, mogelijk de communicatieprotocollen te manipuleren waardoor de kennelijke afzender niet de werkelijke afzender blijkt te zijn. De ontvangende eindgebruiker zal niet eenvoudig een valse van een echte identiteit kunnen onderscheiden. Een en ander betekent echter niet dat de verkeersgegevens zelf zijn aangetast. De e-mailserver van de gebruiker legt vast dat er vanaf het account van de

zender een bericht is uitgegaan. Uitgangspunt bij de bewaarplicht is dat de loggegevens van de e-mailserver worden bewaard en niet de headers van de e-mailberichten. Niet de gegevens in de header, maar de gegevens in de logfiles van de e-mailserver zijn dus relevant. Wanneer naast deze loggegevens ook de e-mail zelf voor de opsporings beschikbaar is, is het mogelijk om na te gaan of de gegevens van het account stroken met de valse naam in de header.
Naar aanleiding van de vragen van deze fracties wijs ik er op dat het meeste van het door de opsporingsautoriteiten gebruikte opsporingsmateriaal in zijn oorsprong nooit voor dat doel bedoeld is. Het door de dief gebruikte gereedschap om zich toegang te verschaffen tot een ruimte laat zogenaamde werktuigsporen na die uniek kunnen zijn voor het gebruikte gereedschap. Vergelijking van de achtergelaten sporen met het gebruikte gereedschap kan de politie naar de dader leiden. Ook kunnen op deze wijze door vergelijking van sporen uit verschillende zaken, deze met elkaar in verband worden gebracht. Zo is bijvoorbeeld autolak bedoeld om een auto te beschermen tegen roest en ter verfraaiing. Met de laksporen, die op de plaats van een delict zijn aangetroffen, kan de auto waar deze laksporen van afkomstig zijn worden geïdentificeerd. Een eigen interpretatie van het materiaal door de politie is nodig. Eén van de kenmerken van het rechercheren is het verzamelen van informatie uit meerdere bronnen om aan de hand daarvan de betrouwbaarheid te beoordelen. De essentie van het opsporingsonderzoek is dat de betrouwbaarheid van gegevens wordt geverifieerd, ook met het oog op de bewijsvoering. Ingeval twijfel ontstaat aan de betrouwbaarheid van gegevens ligt het voor de hand dat aanvullend onderzoek wordt verricht om die twijfel te kunnen wegnemen. Dat is voor het rechercheren op verkeersgegevens van internetcommunicatie niet anders. Verkeersgegevens zijn op zichzelf niet onbetrouwbaar. Het zoeken naar een IP-adres zal een reeks van connecties kunnen opleveren met hetzelfde tijdskenmerk waaruit een selectie gemaakt kan worden van mogelijke contractanten, die vervolgens weer gebruikt kan worden voor verder onderzoek met andere gegevens.

Artikel 8 EVRM

De leden van de CDA-fractie merkten op dat het wetsvoorstel beoogt de inhoud van de communicatie buiten de bewaarplicht te houden maar dat de experts hebben aangegeven dat verkeers- en locatiegegevens – in ieder geval door de aanwezigheid van headers – lang niet altijd zijn te scheiden van de inhoud van het bericht. Zij vroegen of daarmee niet vaststaat dat het in de praktijk onmogelijk zal zijn bij het bewaren van verkeersgegevens aan een inbreuk op art. 8 EVRM te ontkomen. In dit verband wezen zij nog op het Copland-arrest en het Malone-arrest, waarin is beslist dat verkeersgegevens van gesprekken en andere elektronische communicatie onder de bescherming vallen van artikel 8 EVRM.

In antwoord op de gestelde vragen merk ik op dat door mij tot nu toe nooit is betwist of weersproken dat verkeersgegevens van gesprekken en andere elektronische communicatie onder de bescherming van artikel 8 EVRM vallen. In de brief aan de Tweede Kamer van 14 februari 2005 (Kamerstukken II 2004/2005, 23 490, nr. 360, blz. 4/5), de memorie van toelichting en de nota naar aanleiding van het verslag heb ik aangegeven dat het bewaren van verkeersgegevens aan het recht op bescherming van de persoonlijke levenssfeer raakt. In de zaak Malone (NJ 1988, 534) heeft het Europese Hof voor de Rechten van de Mens (EHRM) geoordeeld dat het aftappen van telefoongesprekken een schending van artikel 8 EVRM opleverde. Wil een dergelijke inmenging gerechtvaardigd zijn ingevolge artikel 8, tweede lid, van het EVRM dan moet deze allereerst bij de wet zijn voorzien. De desbetreffende rechtsnorm moet voldoende toegankelijk zijn en met voldoende precisie geformuleerd, zodanig dat deze een voldoende

indicatie bevat van de omstandigheden waarin en de voorwaarden waaronder de overheid tot deze inmenging mag overgaan, en de rechtssubjecten een adequate bescherming tegen willekeurige inmenging biedt. In de zaak Copland (NJ 2007, 617) heeft het Hof geoordeeld dat de term «private correspondence» in artikel 8 niet alleen op de inhoud van communicatie betrekking heeft, maar ook op de verkeersgegevens over gesprekken en andere elektronische communicaties. In casu was deze inbreuk op het privé-leven volgens het Hof niet in overeenstemming met de wet, nu er in het Verenigd Koninkrijk in de desbetreffende periode geen nationaal recht was dat regels stelde met betrekking tot de omstandigheden waaronder werkgevers het telefoon-, e-mail- en internetgebruik van werknemers mochten monitoren.
Het recht op eerbiediging van de persoonlijke levenssfeer wordt beschermd, niet alleen in het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950 (artikel 8), maar ook in de Nederlandse Grondwet (artikel 10, eerste lid). 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 belang van het voorkomen van wanordelijkheden en strafbare feiten. Onder het doelcriterium «het voorkomen van strafbare feiten» is, zo blijkt uit de rechtspraak van het Europese Hof voor de Rechten van de Mens, de strafvorderlijke afwikkeling van strafbare feiten, waaronder de opsporing daarvan, begrepen. Uit de jurisprudentie van het EHRM vloeit voort dat de inmenging door enig openbaar gezag in de privacyrechten moet voldoen aan vereisten inzake noodzakelijkheid en evenredigheid, en derhalve specifieke, expliciete en legitieme doeleinden moet dienen en moet plaatsvinden op adequate en relevante wijze, en niet buitensporig mag zijn in verhouding tot het doel van de inmenging. Bij de eerdergenoemde gelegenheden heb ik uiteengezet waarom de voorgestelde wettelijke regeling van de bewaarplicht voldoet aan de eisen van artikel 8 EVRM en artikel 10 van de Grondwet. De eis dat de inmenging «bij wet is voorzien» houdt in dat in het nationale recht is voorzien in een wettelijke regeling die voor de burger voldoende kenbaar en voorzienbaar is. De bewaarplicht en de lijst van de te bewaren gegevens worden bij wet in formele zin vastgelegd. De verplichtingen van de aanbieders op het gebied van de beveiliging van de gegevens worden bij algemene maatregel van bestuur geregeld, maar het begrip «law», zoals geïnterpreteerd door de Straatsburgse jurisprudentie vereist niet dat er sprake is van een uitputtende regeling in een wet in formele zin. Naar mijn mening voldoet de voorgestelde regeling aan de eisen van voorzienbaarheid en van waarborgen tegen willekeur en misbruik. Bij de eis dat de inmenging noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid. De bewaarplicht vloeit echter voort uit een Europese richtlijn en de bewaartermijn valt binnen de kaders van die richtlijn. Verkeersgegevens zijn van groot belang voor de opsporing en vervolging van ernstige misdrijven. De wettelijke bewaarplicht stelt zeker dat die gegevens daadwerkelijk beschikbaar zijn, biedt een wettelijke grondslag voor de opsporingsinstanties om de aanbieders op de verstrekking van die gegevens aan te spreken en geeft de aanbieders helderheid over de reikwijdte van hun verplichtingen jegens politie en justitie. Ik zie dan ook geen reden waarom de voorgestelde regeling niet zou voldoen aan de vereisten op het gebied van de bescherming van de persoonlijke levenssfeer, zoals die voortvloeien uit artikel 8 EVRM en artikel 10 van de Grondwet. Daarbij merk ik nog op dat er geen sprake is van een verplichting tot het bewaren van de headers van internetberichten. De aanbieder is gehouden de gegevens te bewaren van de lijst van de bijlage bij het wetsvoorstel, dit betreft onder meer de verkeersgegevens rond de gebruikersidentificatie van de ontvanger van internetcommunicatie. De gegevens die daarvoor worden

gebruikt zijn de verkeersgegevens die in de logging van de e-mail servers worden vastgelegd. Daartoe behoren echter niet de headers. Doorgaans kunnen de identificatie van de verzender en de ontvanger van e-mailberichten uit deze verkeersgegevens worden afgeleid. In die gevallen waarin dit niet het geval zou zijn resteert de mogelijkheid van een internettap.
Het recht op de bescherming van de persoonlijke levenssfeer is geen absoluut recht. Beperking van dit recht is mogelijk, mits gerechtvaardigd met het oog op de betrokken belangen en omgeven met de nodige waarborgen om die beperking zo gering mogelijk te doen zijn. Naast het belang van de persoonlijke levenssfeer van de burger is ook het belang van zijn veiligheid met het oog op het voorkomen en vervolgen van strafbare feiten aan de orde. De burger verwacht van de overheid dat deze de veiligheid in de samenleving beschermt en doet wat in haar vermogen ligt om daders van strafbare feiten aan te houden en te bestraffen. Dit belang van de veiligheid is sterk gediend met de bewaring van verkeersgegevens. Daar tegenover staat dat de beperking van de persoonlijke levenssfeer slechts in geringe mate aan de orde is omdat het niet gaat om de inhoud van gesprekken en de gegevens slechts in bepaalde gevallen door opsporingsambtenaren bij de aanbieders opgevraagd mogen worden ten behoeve van de opsporing van ernstige misdrijven. Ik ben dan ook van mening dat de mogelijke beperking van het recht op bescherming van de persoonlijke levenssfeer die de bewaarplicht met zich meebrengt, geen ééndimensionale afweging verdient maar in het perspectief moet worden gezien van alle belangen die daarbij aan de orde zijn, alsmede de mate waarin dit recht wordt beperkt en de getroffen waarborgen om deze beperking zo gering mogelijk te doen zijn. Met de voorgestelde regeling wordt naar mijn oordeel ruimschoots gebleven binnen de grenzen die door artikel 8 van het EVRM worden gesteld.

Kosten providers

De leden van de CDA-fractie wezen erop dat voor de «verantwoording» met betrekking tot de kosten van de bewaarplicht in de stukken veelvuldig verwezen wordt naar het VKA-rapport (Verdonck, Klooster en Associates) van 9 oktober 2006. Dit rapport besluit met de mededeling, dat «er met de uitkomsten van de beoordeling in de hand wel degelijk van mening kan worden verschild» en houdt de aanbeveling in om een vervolgonderzoek uit te voeren. Zij vroegen of aan deze aanbeveling gevolg gegeven is en zo ja, wat daarvan de conclusies zijn.

Graag ga ik als volgt op deze vragen in. Het onderzoeksbureau VKA heeft in het onderzoek naar de nationale implementatie van de Richtlijn dataretentie verschillende modaliteiten onderzocht voor de opslag van de te bewaren gegevens. In de memorie van toelichting is op dit onderzoek ingegaan (Kamerstukken II, 2006/07, 31 145, nr. 3, blz. 15). In het rapport van dit onderzoek zijn een aantal modellen of scenario's uitgewerkt die kunnen worden gebruikt voor de opslag en de bevraging van de te bewaren telecommunicatiegegevens. In het overleg met de aanbieders is duidelijk geworden dat de optie met de hoogste score in het rapport van VKA, centrale opslag en directe toegang, niet tot de haalbare opties behoorde. Decentrale opslag en beantwoording door de aanbieder was op dat moment in feite het enig haalbare alternatief. Dit betreft de bestaande situatie. In het wetsvoorstel is dan ook van deze situatie uit gegaan. De aanbeveling van VKA zag er op om na keuze voor een implementatieoptie op basis van de ingeslagen richting een vervolgonderzoek uit te voeren naar onder meer het technisch ontwerp en de organisatorische uitvoering. Nu voor de implementatie van de bewaarplicht van de bestaande situatie is uitgegaan ligt een vervolgonderzoek echter niet in de rede.

De leden van de VVD-fractie vroegen hoe de motie-De Wit (Kamerstukken II, 2007/08, 31 145, nr. 15) wordt uitgevoerd, namelijk door te differentiëren naar de omvang van het percentage informatiebevragingen en taplasten waarmee aanbieders van openbare telecommunicatiediensten en/of netwerken jaarlijks worden geconfronteerd. De afspraken die nu worden gemaakt of reeds zijn gemaakt, zijn met de grote aanbieders gemaakt. Met de kleinere aanbieders moet nog overeenstemming worden bereikt. Zij vroegen of ik bereid ben om een andere lijn te kiezen dan te differentiëren naar de omvang van het percentage informatiebevragingen en taplasten en of ik kan aangeven of ik daarbij ook rekening houdt met de kosten van de aanschaf van extra capaciteit en software, het treffen van procedures en maatregelen en het treffen van beveiligingsmaatregelen. Verder vroegen deze leden of zij het goed hadden begrepen dat geen afspraken worden gemaakt met vertegenwoordigers van de internetsector en of ik bereid ben alsnog afspraken te maken met vertegenwoordigers van de internetsector, waarbij rekening wordt gehouden met de kosten van de aanschaf van extra capaciteit en software, het treffen van procedures en maatregelen en het treffen van beveiligingsmaatregelen.

Naar aanleiding van de gestelde vragen merk ik het volgende op. Ook in de deskundigenbijeenkomst in Uw Kamer is de aandacht gevestigd op de kosten van implementatie van het wetsvoorstel, in het bijzonder voor de kleinere internetaanbieders. Ik neem de door de experts naar voren gebrachte punten zeer serieus en hoop dat daar op zodanige wijze mee kan worden omgegaan dat de richtlijn volledig wordt geimplementeerd zonder dat de aanbieders daardoor onevenredig worden belast, ook in vergelijking met de andere lidstaten. Een aantal lidstaten hanteert een soortgelijke vergoedingssysteem als Nederland, dat wil zeggen dat de aanbieders alle investeringslasten dragen maar dat er een vergoedingsregeling geldt voor de bevraging van de bewaarde gegevens door politie en justitie. Sommige lidstaten vergoeden in het geheel geen kosten van de aanbieders. Op basis van de vergoedingssystematiek, geregeld in de Regeling kosten aftappen en gegevensverstrekking (Staatscourant 31 maart 2005, nr. 62,blz. 16) zijn er sinds eind oktober 2008 in Nederland afspraken gemaakt tussen de overheid en een aantal aanbieders over de kwaliteit van de informatieverstrekking rond het aftappen van telecommunicatie en het bewaren en verstrekken van verkeersgegevens. Afspraken zijn nu, gelet op de omvang van het aantal bevragingen, eerst gemaakt met de grote aanbieders. De afspraken zullen worden uitgewerkt in zogenaamde service level agreements. Onderdeel van de afspraken vormt de wijze van vergoeding van de door de aanbieders gemaakte kosten om aan de verzoeken tot aftappen en gegevensverstrekking te voldoen, binnen de kaders van de geldende regelingen. Ten aanzien van de kleine aanbieders wordt op dit moment onderzocht of een vergelijkbare, maar wel een op deze groep aanbieders toegesneden overeenkomst kan worden opgesteld. Inmiddels is een onderzoek (quick scan) gestart om inzicht te verkrijgen in groepen van aanbieders, met name internetaanbieders, en de mate waarin die als groep benaderd kan worden, teneinde ook met hen tot vergoedingsarrangementen te komen. De Nationale Beheersorganisatie voor Internet Providers (NBIP) is een voorbeeld van een organisatie die diensten in het kader van de uitvoering van tapbevelen uitvoert voor enkele tientallen kleinere aanbieders. Het bedrijf overweegt om ook diensten aan te bieden rond de implementatie van de bewaarplicht van verkeersgegevens. Voor de echt kleine internetaanbieders die niet zijn aangesloten bij een bedrijf als het NBIP, geldt maatwerk op individueel niveau. Nu de kans bestaat dat deze groep van aanbieders slechts sporadisch bevraagd wordt, rechtvaardigt dit een ander kwaliteitsniveau voor de te leveren diensten dan voor de groep van grote aanbieders.
Tijdens de door de vaste commissie van Uw Kamer georganiseerde deskundigenbijeenkomst is tevens het belang onderstreept van goede

afspraken met de internetaanbieders over wat politie en justitie van hen verwachten en wat zij van politie en justitie kunnen verwachten. Dit betreft een mede door de fractie van het CDA aan de orde gesteld punt van aandacht. Thans vindt periodiek overleg plaats tussen de vertegenwoordigers van politie en justitie en vertegenwoordigers van de aanbieders van telecommunicatiediensten en internet service providers. Dit betreft het Telecommunicatie Aanbieders Coördinatie Overleg (TACO), onder voorzitterschap van de landelijk officier van justitie voor telecommunicatie. In dit overlegorgaan wordt informatie uitgewisseld tussen de betrokken partijen over de toepassing van hoofdstuk 13 van de Telecommunicatiewet (bevoegd aftappen). In dit overleg kunnen ook nadere afspraken worden gemaakt over de wijze waarop aan de wettelijke verplichtingen invulling wordt gegeven. Het is bijvoorbeeld niet de bedoeling dat de aanbieders in opdracht van politie en justitie allerlei zoekslagen op de gegevens toepassen waardoor er sprake zou zijn van «datamining». Ook kunnen nadere afspraken worden gemaakt over de termijnen waarbinnen de gegevens geleverd worden. De wet bevat op dit punt geen harde verplichtingen. In die afspraken kan rekening worden gehouden met de bedrijfsvoering van de aanbieders, zodat de kleinere aanbieders, die jaarlijks minder verzoeken tot verstrekking ontvangen en minder ver zijn met de automatisering van hun gegevensverwerking, daarvoor meer tijd krijgen. Naar ik hoop is hiermee de vraag van de leden van de VVD-fractie over de motie-De Wit naar tevredenheid beantwoord.

De leden van de VVD-fractie merkten op dat het, om een goede inschatting te kunnen maken van de kosten die providers moeten maken om aan de bewaarplicht te voldoen, relevant is om te weten wat onder het begrip «onverwijld» van het voorgestelde artikel 13.4 sub b lid 1 moet worden verstaan. Als gegevens binnen enkele uren opgeleverd moeten worden, dan vereist dat een veel complexere en zwaardere systematiek van gegevensontsluiting en brengt dat dus meer kosten met zich mee dan wanneer een aanbieder daarvoor enkele dagen de tijd krijgt. Deze leden vroegen wat ik onder «onverwijld» versta. Ook de leden van de CDA-fractie vroegen hoe het begrip «onverwijld» in het voorgestelde artikel 13.4, eerste lid, van de Telecommunicatiewet moet worden opgevat.

De richtlijn bevat de verplichting voor de lidstaten om ervoor te zorgen dat de gegevens op zodanige wijze worden bewaard dat deze onverwijld aan de bevoegde autoriteiten kunnen worden meegedeeld wanneer daarom wordt verzocht. Zoals ook in de memorie van toelichting is aangegeven, voorziet de Telecommunicatiewet niet in een termijn waarbinnen de gegevens door de aanbieders aan de bevoegde autoriteiten moeten worden aangeleverd (Kamerstukken II, 2006/07, 31 145, nr. 3, blz. 16 en 50). Wel zijn er inmiddels afspraken gemaakt tussen de betrokken partijen die erin voorzien dat verkeersgegevens in beginsel binnen vijf dagen worden geleverd. De termijnen waarbinnen de gegevens voor de opsporing beschikbaar komen verschillen naar de aard van de gegevens en zijn mede afhankelijk van de inrichting van de bedrijfsvoering en de staat van de techniek bij de betreffende aanbieder. In noodgevallen kan de aanbieder worden verzocht verkeersgegevens zo spoedig mogelijk te leveren. Het wetsvoorstel biedt de mogelijkheid om zonodig nadere regels te stellen over de termijnen waarbinnen de gegevens beschikbaar worden gesteld. Omdat de huidige praktijk een uiteenlopend beeld geeft en aan het stellen van termijnen aanzienlijke lasten voor de aanbieders verbonden kunnen zijn zie ik vooralsnog geen reden om hierover nadere regels te stellen, in aanvulling op de thans geldende afspraken op operationeel niveau. Daarbij merk ik op dat het mijn streven is de uitwisseling van gegevens tussen de aanbieders en de opsporingsdiensten zoveel mogelijk geautomatiseerd te laten verlopen. Dat bevordert niet alleen de

snelheid maar ook de uniformiteit en kwaliteit van die uitwisseling. Dit betekent echter niet dat ik de aanbieders, in het bijzonder de kleinere aanbieders van telecommunicatiediensten, bij voorbaat wil dwingen tot het treffen van kostbare voorzieningen op het terrein van de ICT. Juist voor die aanbieders, die naar verwachting jaarlijks een gering aantal verzoeken tot verstrekking van telecommunicatiegegevens zullen ontvangen, kan een langere verstrekkingstermijn vanuit bedrijfseconomisch oogpunt van groot belang zijn, omdat hiermee de nodige flexibiliteit kan worden geboden ten aanzien van de wijze waarop de gegevens uit de systemen opgehaald worden. Als zou blijken dat nadere afspraken nodig zijn over de termijnen waarbinnen de bewaarde gegevens door de aanbieders geleverd worden, dan zal daarbij naar mijn mening ook rekening gehouden moeten worden met de situatie bij de kleinere aanbieders van telecommunicatiediensten. Uitgangspunt zal dan zijn dat de termijn zodanig ruim is dat de aanbieders daardoor niet worden gedwongen tot het treffen van kostbare maatregelen op het gebied van de informatievoorziening, uitsluitend ten behoeve van de verstrekking van de bewaarde gegevens aan de opsporingsdiensten.

De leden van de VVD-fractie wezen erop dat het voor de inschatting van de consequenties van het wetsvoorstel voor providers ook belangrijk is om duidelijkheid te hebben over het type vragen dat gesteld zal worden. Zo maakt het volgens deze leden voor internetproviders nogal uit of bijvoorbeeld vragen gesteld worden naar verkeersgegevens van communicatie tussen bepaalde personen op een bepaald tijdstip of naar verkeersgegevens van communicatie tussen bepaalde personen gedurende een bepaalde periode. Zij vroegen of ik bereid ben om afspraken te maken met de telecom- en internetproviders over het type vragen dat gesteld zal worden, zodat de providers op basis daarvan hun opslagsystematiek sterker kunnen sturen en kosten zouden kunnen beheersen.

Ik onderschrijf van harte het belang van goede afspraken tussen de aanbieders en politie en justitie over het type vragen dat gesteld gaat worden. De Richtlijn dataretentie bevat verplichtingen die door de lidstaten geïmplementeerd moeten worden en de ruimte voor de lidstaten beperken. Niettemin kan de uitvoerbaarheid zeer gediend zijn met goede afspraken tussen de betrokken partijen over de wijze waarop aan de wettelijke verplichtingen invulling gegeven wordt. Op grond van de wet zijn de aanbieders – ook de internetaanbieders – reeds verplicht om telecommunicatiegegevens te leveren over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker. Dit betreft het vorderen van verkeersgegevens, op grond van de artikelen 126n/u van het Wetboek van Strafvordering. De te verstrekken gegevens zijn opgesomd in het eerdergenoemde Besluit vorderen gegevens telecommunicatie. Hierbij gaat het om gegevens over het gebruik van telecommunicatie door een bepaalde persoon over een bepaalde periode. De verkeersgegevens worden gezocht aan de hand van een nummer van de gebruiker van telecommunicatie. Het gaat niet om het opzoeken van communicatie tussen personen. Niet is voorzien in de mogelijkheid dat de aanbieders in opdracht van politie of justitie zelfstandig bewerkingen op de gegevens toepassen waardoor er sprake zou kunnen zijn van «datamining». Daarnaast zijn de aanbieders gehouden gegevens te verstrekken terzake van de personalia (naam, adres, postcode en woonplaats), nummer en soort dienst van een gebruiker. Dit betreft het vorderen van gebruikersgegevens, op grond van de artikelen 126na/ua van het Wetboek van Strafvordering. Ook de internetaanbieders zijn aan deze verplichtingen gebonden. Op dit punt brengt de bewaarplicht dus geen verandering in de bestaande situatie. Wel zal de bewaarplicht kunnen leiden tot meer verzoeken om verstrekking van gegevens dan voorheen, omdat de gegevens daadwerkelijk beschikbaar zijn – de

aanbieder is niet meer verplicht tot vernietiging van de gegevens zodra deze voor zijn eigen bedrijfsvoering niet meer van belang zijn – en omdat de gegevens gedurende een langere periode beschikbaar zijn. Thans vindt periodiek overleg plaats tussen de vertegenwoordigers van politie en justitie en vertegenwoordigers van de aanbieders van telecommunicatiediensten en internet service providers. Het eerdergenoemde Telecommunicatie Aanbieders Coördinatie Overleg kan goed dienen als platform voor het maken van aanvullende afspraken over de uitvoering van de bewaarplicht en de toepassing van strafvorderlijke bevoegdheden, indien daaraan behoefte bestaat. In ieder geval ben ik zeker bereid om aanvullend de nodige afspraken te maken met de internetaanbieders.

De leden van de GroenLinks-fractie vroegen of het juist is dat de kosten voor de implementatie van de wet voor de komende vijf jaar tussen de 133 miljoen en 157 miljoen euro bedragen, en of de regering bereid is de bedrijven tegemoet te komen bij het dragen van deze kosten. Ook vroegen deze leden in hoeverre de regering deze kosten acceptabel acht, gelet op het gemak waarmee mensen de bewaarplicht kunnen omzeilen. Voorts vroegen deze leden hoe ver de regering is met het formuleren en uitdenken van het soort data dat ze wil kunnen opvragen, om zo een uniforme en werkbare implementatie door de bedrijven te kunnen doorvoeren en of de regering het denkbaar acht dat de implementatiekosten voor de communicatietechnieken die onder de bewaarplicht vallen, tot gevolg hebben dat de andere communicatietechnieken nog meer benut zullen worden.

In antwoord op de gestelde vragen kan ik het volgende melden. Uit het onderzoek van VKA is gebleken dat bij een bewaartermijn van 12 maanden en decentrale opslag voor een periode van 5 jaar de investeringskosten voor de telecommunicatieaanbieders circa 75 miljoen euro zullen bedragen en dat de exploitatiekosten over die periode zullen oplopen van 12 miljoen tot in totaal circa 20 miljoen euro per jaar. Er is hierbij uitgegaan van een verwachte toename in het bevragingsvolume. Hierbij is gerekend naar het prijspeil van begin 2006. Inmiddels zijn de kosten voor geheugenopslag zeer sterk gedaald en zullen de kosten voor opslag de komende jaren naar verwachting verder gaan dalen. De verwachting is dan ook gerechtvaardigd dat de kosten voor investeringen en exploitatiekosten (over een periode van 5 jaar) beneden de 157 miljoen euro zullen blijven. Hierboven is, naar aanleiding van vragen van de fractie van de VVD aan de orde gekomen dat er een vergoedingssystematiek geldt, op basis van de Regeling kosten aftappen en gegevensverstrekking. Zoals hierboven opgemerkt zijn hierover inmiddels aanvullende afspraken gemaakt met een aantal grote telecommunicatieaanbieders. De kosten gemoeid met een algehele invoering van de bewaarplicht blijven daarmee acceptabel, zeker gelet op het belang van de opsporing en vervolging van ernstige misdrijven dat daarbij aan de orde is. Dat kwaadwillenden de bewaarplicht kunnen omzeilen acht ik daarbij niet van doorslaggevend belang. Er zullen altijd methoden of middelen gebruikt worden die de opsporing kunnen bemoeilijken. De dief kan handschoenen aantrekken en de bankrover zal bij voorkeur een motorvoertuig gebruiken dat op naam staat van een derde. Dat betekent echter niet dat het afnemen van vingerafdrukken of het opvragen van kentekens bij voorbaat zinloos is. Ook in die gevallen waarin gebruik wordt gemaakt van anonimiseringsdiensten of van versleutelde berichtgeving leveren verkeersgegevens nuttige inzichten op over het verkeer dat heeft plaatsgevonden. In het voorgaande is, in antwoord op vragen van de leden van de fracties van de VVD en het CDA reeds ingegaan op de vraag in hoeverre volledige onttrekking van het gebruik van telecommunicatiediensten aan het oog van de opsporing mogelijk is. Er lopen altijd wel sporen naar personen in de directe omgeving van de

verdachte, zoals slachtoffers of betrokkenen, die geen inspanningen doen om de bewaarplicht bewust te omzeilen. Ik acht de kosten – mede gegeven de noodzaak van implementatie van de EU-richtlijn – ook in dit licht acceptabel.
Voor wat betreft het soort data die bewaard moeten worden, geldt dat de gegevens die moeten worden bewaard en opgevraagd kunnen worden, in artikel 5 van de Richtlijn dataretentie zijn vastgelegd. Deze lijst van gegevens, die voor alle lidstaten geldt, is opgenomen in de bijlage bij het wetsvoorstel. Daarmee worden deze gegevens wettelijk vastgelegd, zodat de aanbieders weten welke gegevens bewaard moeten worden. Deze lijst zal in ieder geval ongewijzigd blijven tot aan de evaluatie van de richtlijn.
Tenslotte is het naar mijn oordeel niet de verwachting dat, vanwege de implementatiekosten voor communicatietechnieken die onder de bewaarplicht vallen, andere communicatietechnieken nog meer benut zullen gaan worden. Zoals hierboven uiteengezet, zullen deze kosten naar verwachting niet een zodanig beslag leggen op de middelen van de aanbieders dat deze zich uitsluitend daardoor zullen laten leiden bij het maken van bedrijfseconomische keuzes.

Concurrentiepositie

Het was de leden van de CDA-fractie opgevallen dat de vergoeding van de met de bewaarplicht samenhangende kosten, die de overheid voor haar rekening neemt, ook niet over de gehele EU op gelijke wijze plaatsvindt. Zo worden in het Verenigd Koninkrijk alle benodigde investeringen door de overheid vergoed, terwijl dit in Nederland bij lange na niet het geval blijkt te zijn. Zij vroegen of de regering de vrees deelt dat een dergelijke aanpak zal leiden tot een ongunstige marktpositie van Nederlandse providers aangezien zij met een flink concurrentienadeel zullen worden geconfronteerd. De leden van de VVD-fractie merkten op dat ik de vraag van deze fractie naar het effect van de bewaarplicht op de concurrentiepositie van met name kleinere providers niet beantwoord had. Graag zouden zij mijn visie op dit punt vernemen. Ook vroegen zij of ik kan aangeven wat in andere lidstaten het effect van de bewaarplicht op de concurrentieverhoudingen is.

De vrees voor verstoring van de concurrentieverhoudingen binnen de EU acht ik niet gewettigd. Alle als openbare aanbieders aangemerkte partijen die in Nederland actief zijn, dus klein en groot, kunnen een beroep doen op de vergoedingsregeling van artikel 13.6 van de Telecommunicatiewet. Die regeling geldt ongeacht de herkomst van de aanbieder. Voor alle aanbieders onderling geldt binnen Nederland na de invoering van de bewaarplicht dan nog steeds een gelijk speelveld. De extra kosten voor de aanbieders, die voortvloeien uit de verplichtingen rond de bewaarplicht, zijn ook in relatie tot de omzet van de aanbieders beperkt. Volgens berekeningen van VKA, waarbij is uitgegaan van automatisering, bedragen de kosten voor kleine bedrijven met een gemiddeld aantal van duizend accounts ongeveer 2% van de totale kosten. Ten tijde van het onderzoek heeft VKA gerekend met een aantal van ongeveer 255 kleine bedrijven. Per bedrijf zouden de investeringskosten dan ongeveer € 5 900.– bedragen, over een periode van vijf jaar. Daarbij dient bedacht te worden dat ICT-toepassingen steeds goedkoper worden terwijl deze berekeningen enkele jaren geleden gemaakt zijn. Niet alleen de kosten van de bewaarplicht zijn van invloed op de concurrentieverhoudingen maar tevens andere factoren met betrekking tot de bedrijfsvoering van de aanbieders, zoals de efficiency, personeelslasten en dergelijke.
Voor wat betreft de vergoeding van de kosten van de aanbieders geldt dat de situatie in Nederland voor de aanbieders niet ongunstiger is dan die in de ons omringende landen. Duitsland kent een vergelijkbaar vergoedingssysteem als Nederland. De investeringskosten komen voor rekening van

de aanbieders. In afzonderlijke gevallen kan aan de aanbieders een vergoeding worden verstrekt op grond van de zogenaamde Justitievergoedings- en schadeloosstellingswet. Thans geldt in Duitsland een vergoeding van € 17,– per uur voor de verstrekking van verkeersgegevens, waarbij ervan wordt uitgegaan dat ieder verzoek om verstrekking één uur verwerkingstijd met zich meebrengt. Dit bedrag ligt lager dan de Nederlandse norm van € 27,– per uur (Staatscourant 31 maart 2005, nr. 62, blz. 16). Overigens is een aanpassing van deze regeling in voorbereiding, ter vereenvoudiging van de kostenberekening envergoeding.
In België staan in een bijlage van een Koninklijk Besluit uit 2003 de vergoedingen weergegeven die worden vergoed aan «de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten voor hun medewerking» aan een vordering. Naast de vergoedingen vastgelegd volgens het Koninklijk Besluit is er echter ook sprake van onderling overeengekomen vergoedingen tussen justitie en de aanbieders in België. Beide soorten vergoedingen voorzien in een tarief per vordering en in een tarief per dag en zijn, afhankelijk van de soort vordering, aanzienlijk hoger dan de vergoeding opgenomen in het Nederlandse Regeling kosten aftappen en gegevensverstrekking. De investeringskosten worden niet vergoed. Op dit moment wordt in België echter gewerkt aan de vervanging van het Koninklijk Besluit uit 2003 waarbij zal worden uitgegaan van lagere bedragen.
Alle aanbieders in het Verenigd Koninkrijk hebben een medewerkingsplicht voor aftappen en informatieverzoeken. De verplichting om ook structurele voorzieningen (permanent capability) te hebben voor deze diensten geldt alleen voor die aanbieders die door de overheid zijn aangewezen. Bij aanbieders die geen structurele voorziening hebben, regelt de overheid de tap via een mobiele tapinstallatie. De kosten voor de aanbieders die een structurele voorziening moeten hebben worden door de overheid volledig vergoed. Aanpassing in deze systemen wordt formeel alleen vergoed als de aanpassing noodzakelijk is door wijzigingen bij de overheid. In andere gevallen dient de aanbieder zelf de lasten te dragen. De kosten worden gecheckt door een onafhankelijk bureau op noodzaak en proportionaliteit.
Bij ministerieel besluit van de Franse Minister de l'économie, des finances et de l'industrie, van 22 augustus 2006, zijn de tarieven vastgesteld die door de Franse overheid vergoed worden aan de aanbieders van elektronische communicatie voor de levering van communicatiegegevens (verkeersgegevens). In dit besluit wordt op zeer gedetailleerd niveau weergeven welke de tarieven zijn voor elk type van bevraging. Onderscheid wordt gemaakt naar bevragingen voor vaste telefonie, mobiele telefonie en internet. Binnen deze categorieën gelden subcategorieën voor persoonsgegevens, verkeersgegevens en abonnementsgegevens. Daarbinnen gelden tarieven die zijn vastgesteld naar de te verrichten prestatie door de aanbieder. Tevens wordt onderscheid gemaakt in tarieven voor informatie die langs elektronische weg kan worden afgedaan en informatie die schriftelijk moet worden afgedaan. Dit laatste is duurder. Voor het vragen van gebruikersgegevens op basis van een bekend nummer wordt € 6,50,– vergoed. Voor het bevragen van verkeersgegevens over een periode van een maand wordt een bedrag van € 17,50,– in rekening gebracht. De investeringskosten die de aanbieders moeten maken om aan de bevragingen te kunnen voldoen worden niet door de Franse overheid vergoed.
Ondanks dat er binnen de Europese Unie geen eenduidige regeling geldt, rechtvaardigt de situatie in de ons omringende lidstaten – gelet op het voorgaande – mijns inziens niet de conclusie dat er sprake is van een minder gunstige situatie voor de aanbieders die in Nederland actief zijn. Daarbij merk ik nog op dat in een aantal lidstaten in het geheel geen kosten worden vergoed. Voorbeelden daarvan zijn Spanje, Ierland, Hongarije en Polen. Mede gelet op de betrekkelijk geringe meerkosten van de

bewaarplicht voor de bedrijfsvoering van de aanbieders zie ik dan ook geen aanleiding voor de vrees dat de bewaarplicht tot een concurrentienadeel voor de Nederlandse aanbieders zal leiden.

Geheimhoudingsverklaring

De aan het woord zijnde leden wezen op de geheimhoudingsverklaring, die op de website van het Ministerie van Justitie is gepubliceerd, waarin een passage is opgenomen dat ten aanzien van medewerkers en derden die werkzaamheden uitvoeren voor het CIOT een verklaring van geen bezwaar moet worden verstrekt door de AIVD. Een dergelijke geheimhoudingsverklaring vormt onderdeel van een service level agreement (SLA) die tussen de aanbieders van informatiesystemen en het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) wordt gesloten. Ook voor het geval dat er geen SLA tussen de aanbieder en het CIOT tot stand komt, dient de aanbieder een geheimhoudingsverklaring te ondertekenen. De reden daarvoor is dat het CIOT (en daarmee ook haar informatiesysteem bij het Ministerie van Justitie) is geclassificeerd als Staatsgeheim/Geheim. Zij vroegen zich af of de genoemde classificatie en het AIVD toezicht betekenen dat de Wet politiegegevens cum annexis niet van toepassing is op de bewaring van de opgeslagen gegevens en de noodzakelijke bewerking c.q. verwerking daarvan.

In antwoord op de gestelde vragen merk ik op dat het wetsvoorstel bewaarplicht telecommunicatiegegevens ervan uit gaat dat de aanbieders de te bewaren gegevens zelf opslaan en dat deze gegevens, ingeval van een vordering van een autoriteit die is belast met het onderzoeken, opsporen en vervolgen van strafbare feiten, voor dat doel ter beschikking worden gesteld. De gegevensverwerking door de aanbieders in het kader van het aanbieden van openbare telecommunicatienetwerken en openbare telecommunicatiediensten valt onder de reikwijdte van de Wet bescherming persoonsgegevens (WBP). In aanvulling op de regels van die wet worden in de Telecommunicatiewet specifieke regels gegeven over de verwerking van persoonsgegevens door de aanbieders. Deze regels zijn van toepassing op de te bewaren telecommunicatiegegevens. Aanvullend bevat het Besluit beveiliging gegevens telecommunicatie regels voor de beveiliging van de bewaarde gegevens. Onderdeel daarvan vormt de verplichting voor de aanbieder om ervoor zorg te dragen dat de personen, die medewerking verlenen aan de verstrekking van de gegevens, tenminste een verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële documentatie en de verklaringen omtrent het gedrag hebben overlegd (artikel 4, tweede lid, Bbgt). Zodra de bewaarde gegevens worden verstrekt aan de politie dan is de Wet politiegegevens van toepassing op de verdere verwerking van de verstrekte gegevens.

In geval van een vordering van actuele gebruikersgegevens (naam. adres, woonplaats, nummer en soort dienst) verlopen de vordering en de beschikbaarstelling door tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) dat in Den Haag gevestigd is. Dit is geregeld in het Besluit verstrekking gegevens telecommunicatie, dat op 1 september 2004 in werking is getreden. Het CIOT-informatiesysteem, dat is beschreven op de website van het Ministerie van Justitie, fungeert als intermediair tussen aanvragers en aanbieders. Zelf heeft het CIOT geen inzage in de gegevens en het slaat zelf ook geen gegevens over gebruikers van telecommunicatie op. De intermediairfunctie van het CIOT heeft dan ook geen invloed op de regels die op de verwerking van de gegevens door de opsporingsdiensten van toepassing zijn. Die zijn hierboven beschreven, waarbij geldt dat de Wet politiegegevens op die verdere verwerking van toepassing is. De geheimhoudingsverklaring heeft uitsluitend betrekking op gegevens over de bedrijfsvoering van de aanbieders

en de opbouw en werking van het CIOT-systeem. Deze gegevens lenen zich niet voor openbaarmaking.

Bewaartermijn

De leden van de VVD-fractie merkten op dat in het voorgestelde artikel 13.2a, derde lid, van het wetsvoorstel bewaarplicht telecommunicatiegegevens wordt bepaald dat de verkeersgegevens een periode van 12 maanden moeten worden bewaard, gerekend vanaf de datum van de communicatie. Zij vroegen welk moment dan leidend is, het moment waarop de communicatie is gestart of het moment waarop de communicatie afgerond is.

De Richtlijn dataretentie verplicht de lidstaten ertoe bepaalde gegevens gedurende ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie te bewaren (artikel 6). Deze verplichting wordt met het voorgestelde artikel 13.2a, eerste lid, van het wetsvoorstel geïmplementeerd. Een redelijke wetstoepassing brengt naar mijn mening met zich mee dat voor de bewaarperiode in beginsel wordt gerekend vanaf de datum waarop de communicatie wordt gestart. Deze datum zal doorgaans dezelfde zijn als die waarop de communicatie is afgerond, zodat er in de praktijk weinig tot geen verschil is. De gegevens rond een telefoongesprek, dat wordt gevoerd vanaf 13 maart 2009 tot de ochtend van 14 maart 2009, moeten bij een bewaartermijn van twaalf maanden worden bewaard tot 13 maart 2010. In het ontwerpbesluit beveiliging gegevens telecommunicatie, dat inmiddels voor consultatie is voorgelegd aan de Raad van State, is vastgelegd dat de aanbieder de bewaarde gegevens uiterlijk binnen acht dagen na afloop van de bewaartermijn vernietigt. De vernietigingstermijn van acht dagen brengt dus nog enige speling in de daadwerkelijke beschikbaarheid van de gegevens na afloop van de bewaartermijn met zich mee. Voor gegevens over internettoegang ligt dit enigszins anders omdat niet uitgesloten is dat een internetsessie langere tijd duurt, en zich over verschillende dagen uitstrekt. Tijdens de bijeenkomst hebben ook de deskundigen op dit aspect gewezen. De richtlijn houdt hiermee rekening omdat voorgeschreven wordt dat gegevens worden bewaard die nodig zijn om de datum, het tijdstip en de duur van een communicatie te bepalen (artikel 5, eerste lid, onderdeel c, onder punt 2). In het geval van internettoegang, e-mail over het internet en internettelefonie betreft dit de datum en het tijdstip van de log-in en log-off van een internetsessie gebaseerd op een bepaalde tijdzone, samen met het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen, en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker (onder i). Bij e-mail over het internet en internettelefonie betreft dit de datum en tijdstip van de log-in en log-off van een e-maildienst over het internet of internettelefonie gebaseerd op een bepaalde tijdzone (punt ii). In de bijlage behorende bij artikel 13.2a van het wetsvoorstel is dit terug te vinden in punt B, onderdelen d. en e. Van belang is dat in deze gevallen twee data worden bewaard, namelijk de datum van het begin van de log-in en die van de log-off.

De leden van de PvdA-fractie wezen erop dat in de memorie van antwoord wordt aangegeven dat de gemiddelde doorlooptijd in strafzaken in 2005 zeven en een halve maand bedroeg, terwijl de meer complexe en ernstiger zaken vaak een langere doorlooptijd kennen. Zij vroegen of met doorlooptijd wordt bedoeld de periode tussen het gepleegde feit en de sluiting van het GVO. Ook vroegen zij waarom de doorlooptijd van ernstiger, maar niet per se meer complexe zaken (eveneens) langer is, en wat is in dit verband onder «langer» moet worden verstaan.

Op deze vraag kan ik antwoorden dat met de gemiddelde doorlooptijd in strafzaken wordt gedoeld op de periode die ligt tussen het moment van inschrijving bij de rechtbank en het moment van afdoening door de rechter. In 2007 bedroeg de gemiddelde doorlooptijd bij de meervoudige (straf) kamer 248 dagen. (bron: Criminaliteit en rechtshandhaving 2007, WODC). De door het WODC gepubliceerde statistieken laten zien dat er weliswaar niet een direct verband is te leggen tussen de doorlooptijd en de ernst of de complexiteit van de zaak maar wel dat bij een aantal ernstige zaken, zoals seksuele misdrijven waaronder verkrachting en dood en lichamelijk letsel door schuld, en meer complexe zaken zoals valsheidmisdrijven de doorlooptijd kan oplopen tot meer dan een jaar. Als gerekend wordt vanaf het moment van het plegen van het misdrijf, dan is de doorlooptijd uiteraard navenant langer.

Hofuitspraak rechtsgrondslag richtlijn

De leden van de CDA-fractie wezen erop dat de rechtsgrondslag van de richtlijn bij het Europese Hof van Justitie van de Europese Gemeenschappen in Luxemburg is aangevochten. Zij legden de vraag voor of het niet in de rede ligt deze uitspraak af te wachten om te voorkomen, dat er misschien een implementatiewet in werking zal zijn, terwijl de aan die wet ten grondslag liggende richtlijn is vernietigd.

In antwoord op deze vraag kan het volgende worden opgemerkt. Op voorstel van de Commissie heeft de Raad op 15 maart 2006 de Richtlijn dataretentie vastgesteld. De Commissie was van mening dat artikel 95 EG, dat de vaststelling mogelijk maakt van maatregelen die de instelling en de werking van de interne markt betreffen (eerste pijler) de juiste rechtsgrondslag was voor de aan de marktdeelnemers opgelegde verplichtingen de gegevens een bepaalde tijd te bewaren. Nadat de richtlijn door de Raad was aangenomen verzocht Ierland, ondersteund door Slowakije, het Hof van Justitie om nietigverklaring van de richtlijn, omdat deze niet op de juiste rechtsgrondslag zou zijn vastgesteld (zaak C-301/06). Ierland was van oordeel dat het «zwaartepunt» van de richtlijn niet zozeer de interne markt is, maar het onderzoeken, opsporen en vervolgen van strafbare feiten. De maatregelen zouden dan ook moeten worden vastgesteld opgrond van de bepalingen van het EU-Verdrag betreffende de politiële en justitiële samenwerking in strafzaken (derde pijler).
In zijn arrest van 10 februari 2009 heeft het Hof geoordeeld dat de Richtlijn dataretentie terecht is vastgesteld op grond van het EG-Verdrag, aangezien zij vooral betrekking hebben op de interne markt. Het Hof wijst erop dat verschillende lidstaten maatregelen hadden getroffen op het gebied van de bewaarplicht. Die situatie rechtvaardigde dat de gemeenschapswetgever het doel van de bescherming van de interne markt nastreefde door de vaststelling van geharmoniseerde regels. Het Hof merkt voorts op dat met de Richtlijn dataretentie de bepaling van de privacyrichtlijn werden gewijzigd, die zelf op artikel 95 EG is gebaseerd. Wijziging van een bestaande richtlijn, die tot het acquis communautaire behoort, kan niet worden gebaseerd op het EU-Verdrag zonder schending van artikel 47 EU. Tenslotte stelt het Hof vast dat de maatregelen beperkt zijn tot de activiteiten van de aanbieders van diensten en geen betrekking hebben op de toegang tot gegevens noch het gebruik daarvan door de politiële of justitiële autoriteiten van de lidstaten. Het Hof concludeert dan ook dat de richtlijn overwegend betrekking heeft op de werking van de interne markt. Met deze uitspraak volgt het Hof de conclusie van Advocaat-Generaal Y. Bot. Deze had in zijn advies van 14 oktober 2008 reeds geconcludeerd dat de richtlijn terecht in het kader van de communautaire pijler is vastgesteld en dat het beroep van Ierland verworpen zou moeten worden.
Met dit arrest is de gekozen rechtsgrondslag voor de Europese bewaarplicht, namelijk een richtlijn onder de eerste pijler, onweersproken vast

komen te staan. Hieruit vloeit voort dat de richtlijn geldig is, inclusief de implementatiedatum. Zoals Uw Kamer bekend is diende de richtlijn uiterlijk 15 september 2007 te zijn geïmplementeerd (artikel 15, eerste lid). Voor internetcommunicatie (internettoegang, internettelefonie en e-mail) geldt dat de lidstaten de mogelijkheid hebben de toepassing van de richtlijn op de bewaring van communicaties uit te stellen voor een periode van ten hoogste 18 maanden (artikel 15, derde lid). Nederland heeft van deze mogelijkheid gebruik gemaakt, zodat de richtlijn voor deze gegevens uiterlijk op 15 maart 2009 moet worden toegepast.[1]

Implementatie in de overige lidstaten

De leden van de PvdA-fractie riepen in herinnering dat ik had gemeld dat Nederland met een bewaartermijn van twaalf maanden aansluit bij de keuze in een aantal andere lidstaten zoals Frankrijk, het Verenigd Koninkrijk, België, Spanje en Denemarken. De leden van deze fractie vroegen of met het woord «zoals», is bedoeld dat nog andere lidstaten voor deze termijn geopteerd hebben, en zo ja welke. Verder vroegen zijn in welke lidstaten de minimumtermijn van zes maanden is aangehouden en of er voor de overzichtelijkheid een staatje kan worden gegeven waaruit blijkt:
a) welke lidstaten de richtlijn geïmplementeerd hebben en welke nog niet en van deze eerste
b) de gekozen bewaartermijn per lidstaat?

Naar aanleiding van deze vragen is hieronder een overzicht opgenomen van de omzetting van de Richtlijn dataretentie in de lidstaten:

Lidstaat	Bewaartermijn die aan de Commissie is gemeld
1. België	12 maanden
2. Bulgarije	12 maanden
3. Tsjechië	12/6 maanden
4. Denemarken	12 maanden
5. Duitsland	6 maanden
6. Estland	12 maanden
7. Ierland	Geen bericht
8. Griekenland	Geen bericht
9. Spanje	12 maanden
10. Frankrijk	12 maanden
11. Italië	24 maanden
12. Cyprus	6 maanden
13. Letland	18 maanden
14. Litouwen	6 maanden
15. Luxemburg	6 maanden
16. Hongarije	Niet bekend
17. Malta	12/6 maanden
18. Nederland	Geen bericht
19. Oostenrijk	Geen bericht
20. Polen	24 maanden
21. Portugal	12 maanden
22. Roemenië	12 maanden
23. Slovenië	24 maanden
24. Slowakije	6 maanden
25. Finland	12 maanden
26. Zweden	Geen bericht
27. Verenigd Koninkrijk	12 maanden

Uit dit overzicht[2] blijkt dat naast België, Denemarken, Frankrijk, Spanje en het Verenigd Koninkrijk ook Bulgarije, Estland, Finland, Malta, Portugal, Roemenië en Tsjechië (telefoniegegevens) hebben gekozen voor een bewaartermijn van twaalf maanden. Het Verenigd Koninkrijk kende een systeem van gegevensbewaring op basis van vrijwilligheid maar heeft dat inmiddels vervangen door een verplichting, de bewaartermijn voor internetgegevens zal worden verhoogd van zes naar twaalf maanden. Duitsland, Cyprus, Litouwen, Luxemburg, Malta (internetgegevens) en Slowa-

[1] De Nederlandse tekst spreekt ten onrechte van een periode van 18 maanden, te rekenen vanaf 15 maart 2009. Dit betreft echter een vertaalfout, die inmiddels is gecorrigeerd (PbEU 2009, L 50/32).
[2] Bron: Europese Commissie.

kije en Tsjechië (internetgegevens) hebben gekozen voor een bewaartermijn van zes maanden. De bewaartermijn van Hongarije is niet bekend. Tenslotte hebben vijf lidstaten, waaronder Nederland, de Richtlijn dataretentie nog niet geïmplementeerd. Deze lidstaten hebben dus nog geen bewaartermijn aan de commissie gemeld.

De leden van de GroenLinks-fractie vroegen of de gebrekkige effectiviteit van de richtlijn, vanwege de territoriale beperkingen, een rol heeft gespeeld bij de onderhandelingen over de richtlijn, en zo ja op welke wijze. Zij vroegen tevens of de lidstaten expliciet als standpunt hebben ingenomen dat ze zich bewust waren van de beperkingen, maar de richtlijn niettemin relevant vonden.

Het antwoord op de gesteld vragen is dat de lidstaten juist regels op Europees niveau wilden vaststellen, omdat de aanbieders anders geconfronteerd zouden worden met verschillende bewaartermijnen in de verschillende lidstaten. Daarmee zou ook de strafrechtelijke samenwerking worden bemoeilijkt. De richtlijn werd door de lidstaten dus zeker relevant gevonden. Met hun vraag over de territoriale beperking doelen de leden van de GroenLinks-fractie er kennelijk op dat de aanbieders van diensten, die niet in de Europese Unie gevestigd zijn, buiten de reikwijdte van de richtlijn vallen. Dit element, dat voor iedere Europese richtlijn geldt, heeft tijdens de onderhandelingen over de richtlijn geen rol van betekenis gespeeld. De richtlijn is van toepassing op aanbieders indien deze actief hun diensten aanbieden in de lidstaten van de Gemeenschap. Daardoor valt het overgrote deel van de aanbieders van telecommunicatiediensten onder de reikwijdte van de richtlijn. Voor die gevallen waarin een aanbieder buiten de Europese Unie gevestigd is en geen actieve diensten binnen de Unie aanbiedt, kan de netwerkaanbieder worden aangesproken op de verplichtingen die uit de Richtlijn dataretentie voortvloeien. Ik meen dan ook dat het territoriale aspect geen goed argument is om af te zien van regelgeving op Europees niveau.

De leden van de GroenLinks-fractie vroegen voorts of de gebrekkige effectiviteit ook een onderwerp van discussie is geweest tijdens het implementatieproces in andere lidstaten, en zo ja in welke mate, en wat hiervan de uitkomst was. De leden van deze fractie vroegen tevens of er een contactcomité van nationale ambtenaren bestaat die de implementatie bespreken met de Commissie en zo ja, of daar de effectiviteit aan de orde is, en zo ja, welke oplossingen hiervoor worden aangedragen.

In reactie op de gestelde vragen kan ik antwoorden dat – voorzover mij thans bekend – de gebrekkige effectiviteit van de richtlijn als zodanig geen onderwerp van discussie is geweest in andere lidstaten. Wel is mij bekend dat in enkele lidstaten discussie is geweest over de implementatie van de verplichtingen van de richtlijn maar dit betrof andere aspecten dan de effectiviteit van de regeling. Oostenrijk heeft vertraging ondervonden bij de implementatie omdat dit land een Grondwettelijk vastgelegde verplichting kent om alle kosten van de aanbieders in verband met de opslag en verstrekking van telecommunicatiegegevens te vergoeden. Dit heeft geleid tot langdurige onderhandelingen met de aanbieders. Ierland is vertraagd vanwege langlopende onderhandelingen met de internetaanbieders over hun verplichtingen. Bovendien bleek de keuze voor opneming van de verplichtingen in lagere regelgeving niet juist, daardoor was het nodig alsnog een wetsvoorstel op te stellen en in procedure te brengen. Zweden is vertraagd vanwege de politieke gevoeligheid van dit onderwerp. Een speciale onderzoekscommissie heeft inmiddels een rapport uitgebracht, op basis van de bevindingen zal een wetsvoorstel worden opgesteld. In Griekenland heeft een werkgroep een ontwerp voor een wet inzake de bewaring van telefoniegegevens opgesteld, voor inter-

netgegevens zal binnen afzienbare termijn een voorstel volgen. Zoals Uw Kamer bekend is de Duitse wetgeving inmiddels aan het Bundesverfassungsgericht voorgelegd. Dit betreft de gevallen waarin, en de voorwaarden waaronder, op grond van het Duitse Wetboek van Strafvordering toegang kan worden verkregen tot de bewaarde gegevens. Nu het Hof van Justitie zich heeft uitgesproken over de rechtsgrondslag van de richtlijn wordt het vonnis van het hoogste Duitse rechtscollege binnen afzienbare termijn verwacht.
Tot nu toe heeft de Commissie enkele conferenties georganiseerd over de bewaring van verkeersgegevens. Tijdens de conferentie van maart 2007 is gesignaleerd dat er belangrijke vraagstukken zijn met betrekking tot de toepassing van de richtlijn, in het bijzonder voor internetgegevens. De Commissie heeft een informele groep van deskundigen opgericht om die vraagstukken uit te werken, bestaande uit de in Overweging 14 van de richtlijn genoemde partijen. Daarnaast heeft de Commissie een informeel contactcomité opgericht dat periodiek bijeenkomt en zich buigt over de implementatie van de richtlijn in de lidstaten. De lidstaten en de telecommunicatie-industrie zijn in het comité vertegenwoordigd, de participatie in de vergaderingen is echter afhankelijk van de onderwerpen. Tussen de Commissie en de lidstaten wordt gesproken over de verstrekking van statistische gegevens aan de Commissie (artikel 10), de vergoeding van de kosten en de gecentraliseerde opslag van gegevens binnen de Europese Unie. Met de vertegenwoordigers van de sector telecommunicatie wordt gesproken over de behandeling van spam, de toepassing van de richtlijn op web mail diensten, de implicaties van internettelefonie door middel van VoIP (Voice over Internet Protocol) en de ontwikkeling van de ETSI-standaard voor de levering van de gegevens door de aanbieders. Daarbij is niet gebleken van bijzondere problemen rond de implementatie van de richtlijn. Wel is er door de industrie op gewezen dat verschillen in business model en systeemarchitectuur kunnen leiden tot verschillen in de set van gegevens die bewaard kan worden. In sommige systemen worden vrijwel dezelfde gegevens bewaard als bij telefonie terwijl bij peer-to-peer systemen vrijwel geen gegevens bewaard worden. Ook het gebruikte business model kan tot verschillen leiden in de beschikbare gegevens. Daarom zou de bewaarplicht voor VoIP zorgvuldig moeten worden geanalyseerd en besproken met de aanbieders, zodat de vereisten niet alleen betrekking hebben op de te bewaren gegevens maar ook op de betreffende situatie (welk type dienst, welke netwerktoegang e.d.). Tijdens de laatste bijeenkomst van het contactcomité, gehouden op 22 januari jongstleden, zijn deze documenten door de industrie gepresenteerd en toegelicht. Tijdens deze bijeenkomst heeft de Nederlandse delegatie melding gemaakt van de hoorzitting in de Eerste Kamer en gewezen op de belangrijkste bevindingen van de door de Eerste Kamer gehoorde deskundigen over de bewaring van internetgegevens. De Nederlandse delegatie heeft aangegeven geïnteresseerd te zijn in de ervaringen op dit gebied in de andere lidstaten en de Commissie opgeroepen aan deze bevindingen aandacht te besteden in het kader van de evaluatie van de richtlijn, die in september 2010 moet zijn afgerond. In reactie hierop is door vertegenwoordigers van de Commissie aangegeven dat de door Nederland ingebrachte bevindingen serieus genomen zullen worden en de andere lidstaten opgeroepen hun bevindingen op dit terrein aan de Commissie te melden, zodat daarmee rekening gehouden kan worden bij de evaluatie van de richtlijn.

De vraag van de leden van de PvdA-fractie of ik, nu inmiddels meer lidstaten de richtlijn hebben geïmplementeerd, een actuele stand van zaken kan geven wat betreft de bewaartermijnen die alle lidstaten hanteren is hierboven, met het overzicht van de omzetting van de richtlijn dataretentie in de lidstaten, reeds beantwoord.

Tenslotte

Tenslotte hadden de leden van de CDA-fractie enkele vragen over de uitleg van in het wetsvoorstel voorkomende begrippen of situaties. Naar aanleiding van die vragen merk ik het volgende op:

– Op de vraag of de verwijzing in artikel 13.2b van de Telecommunicatiewet naar artikel 126 hh Sv betekent dat aanbieders verplicht zijn om hun gehele bewaarde databestand – of een willekeurig door de Officier van Justitie naar eigen goedvinden te specificeren deel daarvan – in zodanige staat te houden, dat zij deze gegevens op eerste verzoek kunnen verstrekken kan ik als volgt antwoorden. De verplichting van artikel 13.2b van de Telecommunicatiewet vormt een zogenaamde spiegelbepaling voor de bevoegdheden van het Wetboek van Strafvordering met betrekking tot telecommunicatie. De bevoegdheid van artikel 126hh van het Wetboek van Strafvordering staat los van de bewaarplicht en is opgenomen ten behoeve van de opsporing en vervolging van terroristische misdrijven. Ingeval van een verkennend onderzoek naar terroristische misdrijven kan de officier van justitie, na een voorafgaande machtiging van de rechter-commissaris, in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot een geautomatiseerd gegevensbestand schriftelijk vorderen dit bestand, of delen daarvan, te verstrekken, teneinde de hierin opgenomen gegevens te doen bewerken. Vereist is dat uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd. Dit betreft een bevoegdheid waarvan verkeersgegevens niet zijn uitgezonderd. Deze bevoegdheid kan daarom ook worden uitgeoefend jegens aanbieders van telecommunicatiediensten of -netwerken. Dit betekent echter niet dat de aanbieders verplicht zijn om hun gehele gegevensbestand bij voorbaat in zodanige staat te houden dat zij deze gegevens op eerste verzoek kunnen verstrekken. Een dergelijke verplichting vloeit niet voort uit artikel 126hh van het Wetboek van Strafvordering noch uit artikel 13.2b van de Telecommunicatiewet.

– Op de vraag hoe het begrip «onverwijld» in het voorgestelde art. 13.4, eerste lid, van het wetsvoorstel bewaarplicht telecommunicatiegegevens moet worden opgevat ben ik hiervoor, naar aanleiding van een vraag van de leden van de VVD-fractie, reeds nader ingegaan. Ik verwijs dan ook naar het antwoord op die vraag.

– Op de vraag wat het relevante moment van de communicatie is, dat kan dienen om het einde van de bewaartermijn aan te geven ben ik hiervoor, naar aanleiding van een vraag van de leden van de VVD-fractie, eveneens reeds nader ingegaan. Ik verwijs dan ook naar het antwoord op die vraag.

– Op de vraag welke de relevante beheerscriteria zijn voor het opslaan van de in bijlage B genoemde gegevens kan ik het volgende antwoorden. De relevante beheerscriteria, zoals die tijdens de expertbijeenkomst aan de orde waren, hebben deels betrekking op de kwaliteit van de gegevensopslag. Dit betreft aspecten als de volledigheid van de opslag en het uitvalpercentage. Daarnaast hebben deze criteria betrekking op de beveiliging van de bewaarde gegevens. Voor wat betreft de kwaliteit van de gegevensopslag stellen de richtlijn dataretentie, en daarmee ook het wetsvoorstel, geen andere normen dan dat de bewaarde gegevens dezelfde kwaliteit hebben als de gegevens in het netwerk (art. 13.5, derde lid, onderdeel a). De zorg voor de volledigheid van de gegevensopslag betreft voornamelijk een verantwoordelijkheid van de aanbieders zelf, omdat zij anders niet aan hun

verplichtingen zullen kunnen voldoen. Voor wat betreft de beveiliging van de bewaarde gegevens biedt de wet de mogelijkheid om bij algemene maatregel van bestuur regels te stellen met betrekking tot de te nemen maatregelen in verband met de beveiliging van, de toegang tot, en de vernietiging van de gegevens (artikel 13.4 Tw). In het ontwerpbesluit beveiliging gegevens telecommunicatie, dat inmiddels voor advies is voorgelegd aan de Raad van State, worden strikte regels gesteld over de fysieke beveiliging van de bewaarde gegevens, het opstellen van een beveiligingsplan, de screening van personeel dat toegang heeft tot de bewaarde gegevens en de vernietiging van de gegevens. Dit ontwerpbesluit vormt een aanpassing van het bestaande Besluit beveiliging gegevens aftappen telecommunicatie (Staatsblad 2003, 472).Zoals eerder naar aanleiding van vragen van de PvdA-fractie al is opgemerkt, is het conceptbesluit[1] ter informatie bij deze memorie gevoegd.

Naar ik hoop zijn met het voorgaande alle nadere vragen die door de leden van de aan het woord zijnde fracties waren gesteld, naar tevredenheid beantwoord.

De minister van Justitie,
E. M. H. Hirsch Ballin

[1] Ter inzage gelegd op de afdeling Inhoudelijke Ondersteuning onder griffie nr. 143 760.