Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

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)

Nr. 9

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 9 januari 2008

1. Inleiding

Met veel interesse heb ik kennis genomen van het verslag van de vaste commissie voor Justitie. Het is verheugend te constateren dat de leden van de fracties van het CDA, de ChristenUnie en de VVD het belang van de maatregelen tot bewaring van telecommunicatiegegevens onderschreven. De leden van de fractie van de PvdA gaven aan onvoldoende overtuigd te zijn van de noodzaak van de invoering van een bewaarplicht voor telecommunicatiegegevens en wensten dit wetsvoorstel te beoordelen op basis van proportionaliteit. Zij waren voorstander van implementatie van de richtlijn op het minimumniveau maar stonden open voor de argumentatie van de regering terzake. De leden van de fractie van D66 onderschreven de strekking van het voorstel, voor zover dit voorziet in het garanderen dat telecommunicatiegegevens voor een bepaalde tijd beschikbaar zijn ten behoeve van de bestrijding van ernstige criminaliteit, maar stelden evenwel vast dat een ruime kamermeerderheid een motie heeft aangenomen ter afkeuring van de aan dit wetsvoorstel ten grondslag liggende Richtlijn dataretentie (motie-Dittrich c.s., Kamerstukken II 2005/06, 23 490, nr. 407). Tot mijn spijt hadden de leden van de fractie van de SP met teleurstelling kennisgenomen van het wetsvoorstel ter implementatie van de Richtlijn dataretentie.

Graag beantwoord ik, mede namens de staatssecretaris van Economische Zaken, de gestelde vragen en reageer ik op de gemaakte opmerkingen. Daarbij hoop ik de vragen naar tevredenheid te kunnen beantwoorden en bestaande twijfels zoveel mogelijk te kunnen wegnemen. Bij de beantwoording is de volgorde van het verslag gevolgd. In een enkel geval zijn de met elkaar verband houdende vragen van twee of meer fracties samengevoegd en zijn de vragen in hun onderlinge samenhang beantwoord.

De leden van de SP-fractie riepen, onder verwijzing naar de motie van het lid Dittrich, vooraleerst in herinnering dat de richtlijn tot bewaring van

KST114314
0708tkkst31145-9
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

gegevens al eerder tot behoorlijke discussies heeft geleid in de Tweede Kamer. Zij vroegen toe te lichten op welke wijze er tegemoet is gekomen aan de bezwaren van de Kamer. Ook vroegen zij welke wijzigingen er sindsdien nog zijn doorgevoerd en daarbij de herhaalde verzekering van de toenmalige minister van Justitie aan de Kamer over de bewaartermijn te betrekken. Tenslotte vroegen deze leden om een korte beschouwing over de totstandkoming en behandeling van de richtlijn, zowel in het Europees Parlement als in de Eerste en Tweede Kamer.

Graag reageer ik als volgt op deze vragen, waarbij ik, voor een goed begrip, begin met de laatste vraag over de totstandkoming en behandeling van de Richtlijn dataretentie. In de Verklaring betreffende de bestrijding van terrorisme, die op 25 maart 2004 door de Europese Raad is aangenomen, werd de Raad de opdracht gegeven om maatregelen te bestuderen voor het opstellen van voorschriften voor het bewaren van verkeersgegevens door telecommunicatieaanbieders, zodat deze voor 1 juni 2005 zouden kunnen worden aangenomen. In vervolg op deze Verklaring heeft een viertal lidstaten – Frankrijk, het Verenigd Koninkrijk, Ierland en Zweden – in het voorjaar van 2004 het initiatief genomen voor een ontwerp-kaderbesluit inzake de bewaring van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. In dat voorstel werd voorzien in een bewaartermijn van minimaal twaalf en maximaal zesendertig maanden. Wel konden de lidstaten van deze termijn afwijken voor SMS-, EMS- en MMS-gegevens en internetprotocollen. Naar aanleiding van dat voorstel is op 14 juli 2004 aan de Kamer een fiche gezonden waarin de achtergrond en inhoud van het ontwerp-kaderbesluit zijn toegelicht (Kamerstukken II 2003/04, 22 112, nr. 331). Daarbij is aangegeven dat het Nederlandse standpunt ten aanzien van een bewaarplicht voor telecommunicatiegegevens in beginsel positief was, maar dat de nodige aandacht moest worden geschonken aan de wijze waarop deze verplichting werd ingevuld.
Tijdens de onderhandelingen heeft de Commissie bezwaar gemaakt tegen de keuze voor een ontwerp-kaderbesluit, onder de reikwijdte van Titel VI VEU (derde pijler), en aangegeven dat een rechtsgrondslag voor een verplichting voor de telecommunicatieaanbieders, tot bewaring van gegevens gedurende een bepaalde periode, uitsluitend kon worden gevonden onder de reikwijdte van het EG-Verdrag (eerste pijler). Dit vanwege het feit dat onder het Gemeenschapsrecht reeds verplichtingen aan de aanbieders waren opgelegd met betrekking tot de betreffende gegevens. In deze opvatting werd de Commissie gesteund door de Juridische Dienst van het Raadssecretariaat en de Juridische Dienst van het Europees Parlement. De Commissie gaf vervolgens aan bereid te zijn met een initiatief te komen, gebaseerd op artikel 95 van het EG-Verdrag. In de brief aan de Eerste Kamer van 12 april 2005 is vermeld dat een dergelijk initiatief op zijn merites zou worden beoordeeld. Verder is opgemerkt dat, gelet op de discussie over het ontwerp-kaderbesluit in de verschillende maatschappelijke geledingen tot nu toe en de effecten daarvan voor de Europese burgers, een grotere mate van betrokkenheid van het Europees Parlement slechts als positief kon worden beoordeeld (Kamerstukken I 2004/05, 23 490, AM).
Ter voorbereiding van de JBZ-Raad van 2 en 3 juni 2005 is uw Kamer bericht dat Nederland, vanwege het advies van de Juridische Dienst van de Raad, niet afwijzend stond ten opzichte van splitsing van het ontwerp-kaderbesluit. Aangegeven is dat, in afwachting van een voorstel van de Commissie voor een richtlijn, het overleg in de Raad over de inhoud van het ontwerp-kaderbesluit diende te worden voortgezet, zodat met de uitkomsten daarvan rekening zou kunnen worden gehouden bij de behandeling van het voorstel voor een richtlijn (Kamerstukken 2004/05 23 490, AO en nr. 370). In het AO ter voorbereiding van die Raad is door de leden Vendrik, Albayrak en Van der Laan een tweetal moties ingediend (Kamer-

stukken II 2004/05, 23 490, nrs. 372 en 373). In de door de Tweede Kamer aangenomen motie nr. 372 werd de regering verzocht in de JBZ-Raad te bewerkstelligen dat overleg over het initiatiefvoorstel inzake de bewaarplicht van verkeersgegevens telecommunicatie pas zou worden voortgezet op het moment dat de resultaten van het onderzoek van de Erasmus Universiteit Rotterdam door de Kamer besproken zouden zijn. Daarnaast werd de regering verzocht zich rond dit onderwerp te onthouden van welke instemming dan ook in de JBZ-Raad. Naar aanleiding van de motie nr. 372 is door mijn ambtsvoorganger in de JBZ-Raad aangegeven dat het Nederlandse parlement hem geen ruimte gaf om zich op enigerlei wijze te binden aan de inhoud van het voorstel voor een ontwerp-kaderbesluit en eerst het voorstel van de Commissie te willen afwachten (Kamerstukken II 2004/05, 23 490, nr. 377). In september 2005 heeft de Commissie het voorstel voor een richtlijn inzake de bewaarplicht van verkeersgegevens gepresenteerd (COM (2005) 438 final). In dat voorstel werd uitgegaan van een bewaartermijn van één jaar vanaf de datum van de communicatie; voor gegevens gerelateerd aan communicatie via internet zou kunnen worden gekozen voor een minimumperiode van zes maanden. In een Algemeen Overleg, gehouden op 5 oktober 2005, is het onderzoek van de Erasmus Universiteit aan de orde gekomen, mede in het licht van de stand van zaken in de onderhandelingen in Brussel (Kamerstukken II 2005/06, 23 490, nr. 398). In de geannoteerde agenda voor de JBZ-Raad van 12 oktober 2005 heeft de regering aangegeven het voorstel, de bewaring van verkeersgegevens te regelen in een richtlijn onder de eerste pijler, te steunen (Kamerstukken II 2005/06, 23 490, nr. 392). Tijdens de JBZ-Raad van 12 oktober 2005 heeft mijn ambtsvoorganger aangegeven dat de Tweede Kamer bezwaren had tegen zowel de inhoud als de vorm van het ontwerp-kaderbesluit en dat Nederland slechts met een richtlijn zou kunnen instemmen.
De Raad concludeerde dat een meerderheid van de delegaties open stond voor de optie van een richtlijn en dat de contacten hierover met het Europees Parlement zouden worden voortgezet (Kamerstukken II 2005/06, 23 490, nr. 395). Daartoe is door het Voorzitterschap een aantal hoofdlijnen geïdentificeerd die uitgangspunt zouden kunnen vormen voor nader overleg met de Commissie en het Europees Parlement (Kamerstukken II 2005/06, 23 490, AZ en nr. 396). Onderdeel daarvan vormde een flexibele bewaartermijn van minimaal zes en maximaal vierentwintig maanden. In de geannoteerde agenda voor de JBZ-Raad van 1 en 2 december 2005 zijn deze hoofdlijnen aan Uw Kamer voorgelegd en is aangegeven dat op basis van het door Coreper aan het Voorzitterschap verleende mandaat de besprekingen met het Europees Parlement zouden worden voortgezet (Kamerstukken II 2005/06, 23 490, nr. 399). In het Algemeen Overleg ter voorbereiding van die Raad is hierover uitgebreid gesproken (Kamerstukken II 2005/06, 23 490, nr. 402). Tijdens de JBZ-Raad van 1 en 2 december 2005 is een pakket van wijzigingen van het voorstel van de Commissie goedgekeurd, dat als een compromis zou kunnen worden voorgelegd aan de Commissie en het Europees Parlement. Onderdeel van dit pakket vormde een bewaartermijn van zes tot vierentwintig maanden. Het verslag van de bijeenkomst is aan Uw Kamer gezonden (Kamerstukken II 2005/06, 23 490, nr. 400). Reeds op 14 december 2005 heeft het Europees Parlement in eerste lezing ingestemd met het door het Voorzitterschap voorgestelde compromis (Kamerstukken II 2005/06, 23 490, nrs. BD405). Met de aanvullende geannoteerde agenda is de tekst van de ontwerp-richtlijn op 13 februari 2006 aan Uw Kamer voorgelegd, met de mededeling dat de regering kon instemmen met de ontwerp-richtlijn zoals die toen voorlag (Kamerstukken II 2005/06, 23 490, nr. 405). Op initiatief van de leden Dittrich, Albayrak, Weekers en De Wit heeft Uw Kamer in een motie, voorgesteld op 16 februari 2006, als haar mening uitgesproken dat de voorliggende richtlijn onvoldoende tegemoet kwam aan de wensen van het parlement en de regering verzocht bij de JBZ-Raad van 21 februari

2006 niet met deze richtlijn in te stemmen (Kamerstukken II 2005/06, 23 490, nr. 407). In de JBZ-Raad van 21 februari 2006 heeft Nederland ingestemd met de ontwerp-richtlijn, op basis van het pakket waarover overeenstemming was bereikt tussen de Raad, de Commissie en het Europees Parlement. Bij brief van 28 februari 2006 heeft mijn ambtsvoorganger Uw Kamer geïnformeerd over het instemmen van de Nederlandse regering met de richtlijn en aangegeven dat de door de heer Dittrich ingebrachte bezwaren betrekking hadden op het akkoord met het Europees Parlement en de Commissie over een richtlijn alsmede een aantal essentiële onderdelen van die richtlijn, zoals de te bewaren gegevens en de bewaartermijnen, waaraan de Raad gebonden was. Er bestond daarna geen ruimte meer om de discussie over de inhoud van die voorwaarden weer aan te zwengelen (Kamerstukken II 23 490, 2005/06, nr. 408).
Met het bovenstaande is ingegaan op de totstandkoming en behandeling van de Richtlijn dataretentie en op de wijze waarop in de diverse stadia rekening is gehouden met de bezwaren van de Tweede Kamer, alsmede op de wijzigingen die in de onderscheiden stadia zijn doorgevoerd. Naar ik hoop zijn de hierop betrekking hebbende vragen van de leden van de SP-fractie hiermee naar tevredenheid beantwoord.
Inzake de lengte van de bewaartermijn heeft mijn ambtsvoorganger zich in een Algemeen Overleg op 5 oktober 2005, naar aanleiding van de aanbieding van het rapport van de Erasmus Universiteit Rotterdam aan Uw Kamer, uitgelaten over de bewaartermijn voor de opslag van de gegevens. Hierover zijn ook schriftelijke vragen gesteld door het lid Vos (350, Tweede Kamer, vergaderjaar 2005–2006, Aanhangsel). In het vorenbedoeld Algemeen Overleg heeft mijn ambtsvoorganger aangegeven dat de in het ontwerp-kaderbesluit voorgestelde bewaartermijnen, gelet op de uitkomsten van het onderzoek van de Erasmus Universiteit Rotterdam, voldoende ruimte boden voor de afwegingen op nationaal niveau. Hierbij moet in aanmerking worden genomen dat deze uitlatingen zijn gedaan terwijl er in de Raad nog discussie werd gevoerd over de categorieën van de te bewaren gegevens en er nog geen definitief uitsluitsel bestond over de te bewaren internetgegevens. Dit vormde voor de Nederlandse regering bijvoorbeeld reden te pleiten voor de mogelijkheid van verschillende minimumniveaus voor de bewaartermijnen voor de verschillende categorieën van gegevens. Pas nadat bekend was dat de lijst van de te bewaren gegevens was beperkt tot telefonie, e-mail en internettoegang, werd een daadwerkelijke afweging van alle in het geding zijnde belangen mogelijk. Zoals hieronder aan de orde zal komen, acht ik, gelet op alle in het geding zijnde belangen, een bewaartermijn van achttien maanden niet disproportioneel. Op de bewaartermijn zal hieronder in paragraaf 2.3, naar aanleiding van vragen van de leden van de fracties van het CDA, de ChristenUnie, de PvdA, D66 en de SP, nader worden ingegaan.

2. Hoofdlijnen van het wetsvoorstel

De leden van de CDA-fractie merkten op dat een delegatiebepaling het mogelijk maakt om bij AMvB nadere invulling te geven aan de verplichtingen voor de aanbieders en hebben gewezen op bezwaren vanuit het bedrijfsleven dat aanpassingen van hun verplichtingen kunnen worden doorgevoerd zonder dat het parlement geraadpleegd wordt. Zij vroegen toe te lichten waarom niet is gekozen voor bijvoorbeeld een AMvB met een voorhangprocedure.
Hierop kan ik antwoorden dat, mede naar aanleiding van de adviezen uit het bedrijfsleven, het wetsvoorstel zodanig is aangepast dat de onderdelen van de bewaarplicht die voor de bedrijfsvoering van de aanbieders het meest van belang zijn niet bij algemene maatregel van bestuur maar in het wetsvoorstel zelf worden geregeld. Dit betreft in het bijzonder de categorieën van de te bewaren gegevens en de bewaartermijn. De Tweede

Kamer is hiermee volledig in de gelegenheid op deze onderdelen te reageren. Ingeval in een later stadium aanpassing van de te bewaren gegevens zou worden overwogen, vereist dat aanpassing van de bijlage van de wet. Inmiddels is het ontwerp voor een Besluit dataretentie, waarin nadere regels worden gesteld over de bescherming, de beveiliging en de vernietiging van de te bewaren gegevens, in consultatie gegeven. Na verwerking van de ingekomen adviezen zal dit ontwerpbesluit voor advies worden voorgelegd aan de Raad van State. In dit ontwerpbesluit wordt voor de regels over de bescherming en de beveiliging van de bewaarde gegevens nauw aangesloten bij die van het huidige Besluit beveiliging gegevens aftappen telecommunicatie. Nu de regels die in het ontwerpbesluit zijn uitgewerkt technisch van aard zijn, lijkt er onvoldoende aanleiding te bestaan de Staten-Generaal bij de uitwerking daarvan te betrekken. Teneinde de Kamer evenwel inzicht te verschaffen in de strekking van het bedoelde ontwerpbesluit, is dit ontwerpbesluit ter informatie bij deze nota gevoegd[1] in de versie, zoals die in consultatie is gegeven.

De leden van de CDA-fractie misten een overgangsperiode in het wetsvoorstel en zouden graag vernemen hoeveel tijd wordt uitgetrokken voor de overgangsperiode.
Hierover merk ik op dat de Richtlijn dataretentie de lidstaten verplicht om de nodige wettelijke en bestuurlijke maatregelen te treffen om uiterlijk 15 september 2007 aan deze richtlijn te voldoen. Dit is geregeld in artikel 15 van de richtlijn. Inmiddels is, zoals hieronder aan de orde komt, in een aantal lidstaten wetgeving ter implementatie van de richtlijn van kracht geworden. De Richtlijn dataretentie biedt de lidstaten de mogelijkheid om de toepassing van de richtlijn op de bewaring van telecommunicatiegegevens rond internettoegang, internettelefonie en e-mail uit te stellen voor een periode van achttien maanden, te rekenen vanaf 15 september 2007. Er is echter geen ruimte voor een overgangsperiode voor de telecommunicatiegegevens met betrekking tot de vaste en mobiele telefonie. Voor de telecommunicatiegegevens met betrekking tot internettoegang, internettelefonie en e-mail is die ruimte mede afhankelijk van de voortgang van het wetgevingstraject ter implementatie van de Richtlijn dataretentie. Gedurende dat verdere traject zal ik mij, in overleg met alle betrokken partijen, beraden over een dergelijke overgangsperiode. In ieder geval geldt voor alle aanbieders die onder de wettelijke bewaarplicht vallen dat zij sinds de datum van publicatie van de Richtlijn dataretentie, op 15 maart 2006, op de hoogte kunnen zijn van de belangrijkste onderdelen van de bewaarplicht, zoals de categorieën van de te bewaren gegevens, evenals van de omzettingstermijn in de nationale wetgeving, zodat zij hier rekening mee kunnen houden bij de inrichting van hun bedrijfsprocessen en tijdig de nodige voorbereidingen kunnen treffen.

2.1 De reikwijdte van de Richtlijn dataretentie

De leden van de CDA-fractie constateerden dat de dataretentierichtlijn de lidstaten de ruimte biedt om nadere invulling te geven aan de regeling waardoor alsnog grote verschillen ontstaan. Het hanteren van verschillende bewaartermijnen door de verschillende lidstaten zou volgens deze leden belemmerend werken voor grensoverschrijdende strafrechtelijke onderzoeken en bovendien problemen opwerpen voor internationale aanbieders van telecommunicatiediensten. De leden van deze fractie vroegen om een toelichting op deze twee punten.
Naar aanleiding van dit verzoek wijs ik erop dat de Richtlijn dataretentie inderdaad tot doel heeft de nationale bepalingen van de lidstaten, waarbij aan de aanbieders verplichtingen worden opgelegd inzake het bewaren van bepaalde telecommunicatiegegevens, zoveel mogelijk te harmoniseren. De harmonisatie heeft onder andere betrekking op de te bewaren gegevens, de bewaartermijn, de toepasselijkheid van de algemene regels

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

op het gebied van de bescherming van de persoonlijke levenssfeer van de richtlijnen 95/46/EG en 2002/58/EG en de uitoefening van het toezicht. Erkend moet evenwel worden dat niet op alle gebieden de doelstelling van harmonisatie in regelgeving is geslaagd. Voor het dragen van de kosten van het bewaren van gegevens en de bewaartermijn zijn geen eenvormige regels vastgesteld. Het hanteren van verschillende bewaartermijnen in de lidstaten kan inderdaad beperkend zijn voor grensoverschrijdende strafrechtelijke onderzoeken. Ingeval vanuit Nederland door middel van een verzoek om rechtshulp verkeersgegevens worden opgevraagd vanuit een land dat een kortere bewaartermijn kent dan Nederland, kan dit er toe leiden dat de betreffende gegevens niet meer voorhanden zijn omdat deze conform de aldaar geldende regels vernietigd zijn. Voor de internationale aanbieders van telecommunicatiediensten, die in meerdere EU-lidstaten actief zijn, kan dit betekenen dat zij in hun bedrijfsvoering rekening moeten gaan houden met verschillende bewaartermijnen. Dat is geen ideale situatie. Dit is echter het gevolg van de procedures van besluitvorming in de Unie.

2.2 De te bewaren gegevens

De leden van de CDA-fractie wezen erop dat gegevens zoals bedrijfsemail en (gratis) e-maildiensten als Hotmail en Yahoo niet worden genoemd in de lijst van de te bewaren gegevens en betreuren het dat de regering hier niet verder over heeft uitgewijd. Zij gaven aan dat, doordat het gebruik van dergelijke e-maildiensten een zeer groot aandeel heeft in het internetverkeer, er een gat valt in de strijd tegen de misdaad en vroegen welke stappen worden ondernomen om deze e-maildiensten alsnog in een parallel voorstel gelijk te schakelen.
In antwoord op deze vraag kan worden opgemerkt dat de Telecommunicatiewet van toepassing is op openbare telecommunicatie diensten en/of -netwerken. Bedrijfsemail en de e-maildiensten, zoals vermeld in de vraagstelling, vallen niet onder de werking van Telecommunicatiewet. Overigens is het criterium hier niet of het een gratis e-mail dienst betreft of niet, maar of het een aanbieder betreft die onder de reikwijdte van de Nederlandse wet valt. Ik erken dat dit nadelig is voor de effectiviteit van de maatregel. Mijns inziens behoeft die vaststelling niet in de weg te staan aan de keuze voor een bewaarplicht als zodanig. Ook als een maatregel niet voor alle gevallen effectief is, blijft zij van belang als zij in vele andere gevallen wel effectief is. De voorgestelde bewaarplicht is een belangrijke maatregel omdat hierdoor waardevolle gegevens beschikbaar blijven die van belang kunnen zijn bij de opsporing van strafbare feiten. Ook in die gevallen waarin gebruik zou worden gemaakt van anonimiseringsdiensten of van versleutelde berichtgeving, leveren verkeersgegevens nuttige inzichten op, omdat gegevens over adressering en tijdstippen in bepaalde gevallen al veel informatie bevatten. Bovendien is volledige onttrekking aan het oog van de opsporing minder eenvoudig dan op het eerste gezicht wellicht lijkt, omdat er altijd wel sporen lopen naar personen in de directe omgeving van de verdachte, zoals slachtoffers of betrokkenen, die geen gebruik maken van dergelijke voorzieningen.

De leden van de CDA-fractie wezen op de verplichting voor de aanbieders om de bewaarde gegevens binnen acht dagen na afloop van de bewaartermijn te vernietigen. Zij vroegen of dit betekent dat de aanbieders *alle* gegevens dienen te vernietigen of dat zij een mogelijkheid hebben informatie te bewaren voor hun eigen bedrijfsvoering.
Naar aanleiding van deze vraag roep ik in herinnering dat de voorgestelde bewaarplicht ertoe strekt dat de aanbieders de telecommunicatiegegevens, die worden gegenereerd of verwerkt in het kader van de aanbieding van telecommunicatiediensten, bewaren ten behoeve van het

onderzoeken, opsporen en vervolgen van ernstige strafbare feiten. Het is echter niet uitgesloten dat deze gegevens ook voor zakelijke doeleinden worden verwerkt, zoals bedoeld in de artikelen 11.5 en 11.5a van de Telecommunicatiewet. Dit zijn doeleinden als facturering en marktonderzoek. Dit volgt ook uit de in het wetsvoorstel voorgestelde wijziging van artikel 11.3, tweede lid, van de Telecommunicatiewet. Ingeval de bewaarde gegevens op grond van de Telecommunicatiewet, na het verstrijken van de voorgestelde bewaartermijn verder kunnen worden verwerkt voor andere doeleinden dan zijn de voor die doeleinden geldende verplichtingen tot anonimisering of vernietiging op de verdere verwerking van die gegevens van toepassing. Dit zou zich bijvoorbeeld kunnen voordoen ingeval van een geschil met een abonnee over een factuur. Hieruit mag echter niet worden afgeleid dat de gegevens die onder de wettelijke bewaarplicht vallen, vrijwel altijd langer kunnen worden verwerkt ten behoeve van zakelijke doeleinden van de aanbieders. In de praktijk zal de duur van de bewaarplicht de termijn, gedurende welke de verdere verwerking van de gegevens ten behoeve van zakelijke doeleinden is toegestaan, voor het merendeel der verwerkingen overstijgen zodat na afloop van de wettelijke bewaartermijn uitsluitend vernietiging van de gegevens aan de orde zal zijn.

De leden van de PvdA-fractie merkten op dat het door de toenemende technologische ontwikkelingen voor criminelen relatief eenvoudig is om informatie te verbergen of moeilijk traceerbaar maken. De leden van deze fractie vroegen of het correct is dat bij het gebruik van bijvoorbeeld proxyservers of versleuteling de daadwerkelijke verkeersgegevens onzichtbaar blijven voor de provider en dat opslag van verkeersgegevens dus in die gevallen helemaal geen informatie oplevert. Ook vroegen zij of de regering al nagedacht heeft hoe ze daarmee om denkt te gaan.
In reactie op de gestelde vragen moet voorop worden gesteld dat de verkeersgegevens voor de aanbieders altijd zichtbaar zijn. Deze gegevens zijn namelijk nodig voor de signalering in de netwerken en de routering van het verkeer. Zonder deze verkeersgegevens is communicatie dus niet mogelijk. Het is voor een gebruiker niet mogelijk om verkeersgegevens te versleutelen, zoals dat wel mogelijk is met de inhoud van berichten. Verkeersgegevens worden namelijk niet door de gebruiker gegenereerd, maar door de dienst en het netwerk dat wordt gebruikt. Door gebruik te maken van bijvoorbeeld proxyservers kan het voor de opsporing wel lastiger zijn om bepaalde verkeersgegevens te relateren aan een bepaalde eindgebruiker. In de gevallen dat van een dergelijke constructie gebruik wordt gemaakt, zal doorgaans nader onderzoek nodig zijn om het gebruik van een bepaalde communicatie te koppelen aan een bepaalde gebruiker. Dat maakt de bewaarde en verkregen verkeersgegevens echter bepaald niet nutteloos. De gegevens bieden immers waardevolle informatie in de totale keten om de herkomst en de bestemming van een bepaalde communicatie vast te stellen, ook al is het dan wellicht maar voor een deel van het traject.

De leden van de SP-fractie vroegen om een reactie op het risico dat stelselmatige kennisneming van verkeers- en locatiegegevens de mogelijkheid biedt een min of meer volledig beeld te krijgen van bepaalde aspecten van iemands leven. Het consequent inzicht krijgen met wie een persoon belt en e-mailt, hoe lang telefoongesprekken duren en vanaf welke locaties dit alles plaatsvindt, kan naar het oordeel van de leden van deze fractie bezwaarlijk anders worden opgevat dan dat er ook een inhoudelijk beeld ontstaat, en dat daarmee wel degelijk fors inbreuk kan worden gemaakt op iemands levenssfeer. De leden vroegen of ik deze interpretatie kan delen.
In antwoord op de gestelde vraag merk ik het volgende op. Met het vorderen van verkeers- en locatiegegevens ten behoeve van de opsporing

van strafbare feiten kan inderdaad een beperking worden gesteld ten aanzien van de persoonlijke levenssfeer van de betrokkene, omdat, in geval van vergaande vormen van gebruik daarvan, aan de hand van dergelijke gegevens een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van diens leven. Daarmee wordt echter voorbij gegaan aan de eisen die voor het gebruik van toepassing zijn. Op mijn afwegingen zal hieronder in paragraaf 2.3, naar aanleiding van vragen van de fracties van PvdA en D66, nader worden ingegaan. Op deze plaats wil ik er nog op wijzen dat ook thans telecommunicatiegegevens, die worden verwerkt door de aanbieders, ter beschikking kunnen komen ten behoeve van de opsporing van strafbare feiten. De afweging van het belang van de opsporing tegen het belang van de bescherming van de persoonlijke levenssfeer die hierbij aan de orde is, heeft reeds plaatsgevonden bij de totstandkoming van de bestaande bevoegdheden voor het vorderen van verkeersgegevens voor de opsporing. De bewaarplicht brengt daarin geen verandering. Wel wordt de kans, dat de gegevens daadwerkelijk voor dit doel beschikbaar zijn, door de bewaarplicht vergroot.

De leden van de VVD-fractie hadden uit de toelichting op het wetsvoorstel begrepen dat indien gegevens niet worden gegenereerd, die niet bewaard hoeven te worden. De leden van deze fractie zouden op dit punt graag een toelichting met enkele voorbeelden krijgen, bijvoorbeeld of van aanbieders bekend is dat zij bepaalde gegevens niet genereren. Ook vroegen zij of er aanwijzingen zijn dat aanbieders voornemens zijn de bedrijfsvoering aan te passen, door te stoppen met het genereren van bepaalde gegevens, om zich te onderscheiden van andere aanbieders en wellicht aantrekkelijker te worden voor bepaalde consumenten.
Graag reageer ik als volgt op de gestelde vragen. Een voorbeeld van een situatie waarbij aanbieders niet alle gegevens genereren – en dus opslaan – die bij een communicatie horen, is die waarbij de aanbieder van de dienst en de aanbieder van het netwerk niet één en dezelfde entiteit zijn. Met name in de IP wereld komt dit in toenemende mate voor. De netwerkgegegevens zijn dan beschikbaar bij de aanbieder van het netwerk en de gegevens van de specifieke dienst bij de aanbieder van die dienst. Dat kan betekenen dat, om een volledig beeld van het gebruik van de communicatiedienst te verkrijgen, een combinatie gemaakt moet worden van de gegevens die bij de beide aanbieders (dienst- en netwerkaanbieder) worden verwerkt of gegenereerd. Bij bepaalde vormen van VOIP doet zich dit voor (de zogenaamde ontbundelde VOIP diensten). Om voor de opsporingsdiensten de toegang tot de gegevens te faciliteren die betrekking hebben op één communicatie, maar bij verschillende aanbieders beschikbaar zijn, is in feite een systeem nodig waarbij de gegevens bij de aanbieders vanuit één punt bevraagd kunnen worden. Een dergelijke voorziening bestaat niet.
Aanbieders kunnen moeilijk stoppen met het genereren van gegevens door de bedrijfsvoering te wijzigen, omdat de gegevens worden gegenereerd in de systemen en netwerken van de aanbieders bij het gebruik van een bepaalde dienst. Stoppen met het genereren van bepaalde gegevens zou betekenen dat de configuratie van hele systemen en netwerken aangepast zou moeten worden. Gelet op het belang van verkeersgegevens ook voor de netwerken en systemen zelf waarmee de dienst wordt aangeboden, acht ik dit geen reëel scenario. Zonder deze gegevens zijn de netwerken en systemen namelijk niet in staat om de communicatie over te dragen.

De leden van de VVD-fractie konden uit het wetsvoorstel en de toelichting niet goed opmaken wat nu dient te gebeuren met de gegevens die gedurende de bewaarperiode zijn «geraadpleegd dan wel vastgelegd». Zij

vroegen wat er met de gegevens gebeurt als deze niet na de bewaartermijn worden vernietigd.
In antwoord op deze vragen kan worden opgemerkt dat de bewaarde gegevens na afloop van de bewaartermijn worden vernietigd, behoudens de gevallen waarin verdere verwerking van die gegevens ten behoeve van zakelijke doeleinden van de aanbieders is toegestaan. Op dit punt is hierboven, naar aanleiding van een vraag van de leden van de CDA-fractie, reeds nader ingegaan. Ingeval de gegevens worden verstrekt aan de politie ten behoeve van het gebruik van die gegevens in een opsporingsonderzoek, zijn de regels van de Wet politieregisters, die op 1 januari 2008 zal worden vervangen door de Wet politiegegevens, op de verdere verwerking van de gegevens van toepassing. De gegevens kunnen dan worden verwerkt zo lang dat noodzakelijk is voor het doel van het opsporingsonderzoek. Worden de gegevens verstrekt aan de inlichtingen- en veiligheidsdiensten in het kader van hun taakuitvoering als bedoeld in artikel 6, tweede lid, of artikel 7, tweede lid, van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), dan zijn de regels van die wet op de verdere verwerking van toepassing. De gegevens worden dan verwijderd zodra deze, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren (artikel 31, eerste lid, Wiv 2002).

2.3 De bewaartermijn

Er is een aantal vragen gesteld over de voorgestelde bewaartermijn. Omwille van de overzichtelijkheid zal ik de gestelde vragen in een bepaalde volgorde beantwoorden. Daarbij zal ik, naar aanleiding van vragen van de fracties van de PvdA, het CDA, de ChristenUnie en de SP, eerst ingaan op de keuze voor een bewaartermijn van achttien maanden en de verhouding met de richtlijn. Daarna zal ik, naar aanleiding van vragen van de fracties van PvdA en D66, ingaan op de behoefte vanuit de opsporing en vervolging, mede op basis van praktijkvoorbeelden. Vervolgens zal, naar aanleiding van vragen van de fracties van de PvdA en D66, aandacht worden geschonken aan de beperking van de persoonlijke levenssfeer. Tenslotte zal, naar aanleiding van vragen van de fracties van de ChristenUnie en D66, de mogelijkheid van het verrichten van nader onderzoek aan de orde komen.

De leden van de CDA-fractie vroegen waarom gekozen is voor een termijn van achttien maanden, en niet voor vierentwintig maanden zoals bepleit door de Raad van Hoofdcommissarissen. Zij waren van mening dat een langere termijn bevorderlijk is in het kader van grootschalige internationale onderzoeken, en ontvingen graag een toelichting op dit punt. De leden van de PvdA-fractie constateerden dat verschillende instanties in hun reacties op het wetsvoorstel aangaven een solide argumentatie te missen voor het instellen van een bewaartermijn van achttien maanden en hebben een reactie op deze kritiek gevraagd. Zij misten een behoorlijke onderbouwing voor de keuze van achttien maanden en vroegen waarom een keuze voor achttien maanden noodzakelijk is. De leden van de ChristenUnie-fractie vroegen zich af of de argumenten als genoemd in de reactie op het advies van de Raad van State voldoende zijn om de keuze voor een termijn van achttien maanden te dragen. Ook vroegen zij of in kwantitatieve zin inzicht gegeven kan worden in de behoefte aan een bewaartermijn met de voorgestelde lengte. De leden van de SP-fractie waren van mening dat de behoeften van politie en justitie nadrukkelijk een rol hebben gespeeld bij de keuze voor een bewaartermijn van achttien maanden, maar deze behoeften geen argument op zich zijn waarmee de bewaartermijn nauwelijks verder beargumenteerd zou hoeven worden. Zij vroegen of uiteindelijk iedere bewaartermijn niet enigszins willekeurig is, zodat er goede argumenten nodig zijn om een langere termijn dan de bewaartermijn van zes maanden te verdedigen.

In antwoord op de gestelde vragen over de keuze voor een bewaartermijn van achttien maanden merk ik op dat in de memorie van toelichting en ook in het nader rapport hierover het nodige naar voren is gebracht. Graag maak ik van deze gelegenheid gebruik om de overwegingen die ten grondslag liggen aan de keuze voor een bewaartermijn van achttien maanden nader toe te lichten. Er zijn twee argumenten die pleiten voor een dergelijke bewaartermijn.

Het eerste argument betreft het belang van een lange bewaartermijn voor complexere opsporingsonderzoeken op regionaal en nationaal niveau, onderzoeken waarbij internationale samenwerking nodig is en onderzoeken naar *cold cases.* Mede naar aanleiding van de discussie over het toenmalige voorstel voor een kaderbesluit over een bewaarplicht voor verkeersgegevens is door de Erasmus Universiteit Rotterdam onderzoek verricht naar de behoefte aan een wettelijke bewaartermijn. De onderzoekers hebben geconstateerd dat er behoefte is aan een ruime bewaartermijn met het oog op voornoemde typen onderzoeken. Daarbij kwam naar voren dat de behoefte aan verkeersgegevens bij de opsporingsdiensten niet altijd manifest is direct nadat de communicatie heeft plaatsgevonden. Het kan voorkomen dat pas later in een onderzoek de behoefte aan telecommunicatieverkeergegevens blijkt, bijvoorbeeld in het geval waarin het lijk van een vermiste persoon pas (veel) later wordt aangetroffen, waardoor het opsporingsonderzoek naar de mogelijkheid van een misdrijf reeds vanaf de aanvang op achterstand staat. Het kan ook voorkomen dat het onderzoek reeds langer loopt maar dat tijdens dat onderzoek, op basis van nadere inzichten omtrent de relaties tussen personen, inzicht ontstaat in de mogelijke aard en samenstelling van een netwerk. Bijvoorbeeld omdat de inzet van bijzondere opsporingsbevoegdheden leidt tot het in beeld komen van medeverdachten of omdat getuigen zich bij de politie melden die nieuwe informatie verschaffen over de toedracht van een ernstig misdrijf. Dit kan zich voordoen bij grootschalige onderzoeken naar terroristische groeperingen en criminele organisaties, maar ook bij ernstige feiten die meer op zichzelf staan, zoals het bovengenoemde geval van vermissing. Tevens hebben de onderzoekers geconcludeerd dat een langere bewaartermijn kan leiden tot een meer afgewogen, beperktere bevraging van de verkeersgegevens omdat minder gegevens zullen worden opgevraagd die achteraf bezien niet relevant – en dus ook niet noodzakelijk – waren voor het onderzoek. Onderbouwing voor het belang van een langere termijn voor meer complexe onderzoeken naar ernstiger vormen van criminaliteit kwam ook naar voren in de *Interpol High Tech Crime Working Group,* die heeft aangegeven dat een minimum periode van een jaar noodzakelijk is. In de «extended impact assessment» van 21 september 2005, die als bijlage bij het voorstel voor de richtlijn is bijgevoegd, vormt de bewaartermijn een punt van uitvoerige aandacht. Daaruit blijkt dat een langere bewaartermijn met name ten goede komt aan de bestrijding van ernstige vormen van criminaliteit.

Het tweede argument dat pleit voor een langere bewaartermijn betreft de behoefte aan verkeersgegevens die zich doet gevoelen tijdens het onderzoek ter terechtzitting. Er kan dan twijfel ontstaan aan de aard of inhoud van de bewijsmiddelen, hetgeen nader onderzoek noodzakelijk kan maken. Het onderzoek ter terechtzitting zal in een later stadium een aanvang nemen, mede omdat in de meer grootschalige opsporingsonderzoeken een langere voorbereidingstijd vrijwel onvermijdelijk zal zijn. Het onderzoek van verkeersgegevens zal ook aan de orde kunnen zijn juist op verzoek van de betrokkene, om zijn onschuld aan de telastegelegde feiten aan te kunnen tonen. De verkeersgegevens kunnen dan dienen ter ontlasting van de verdachte. Dat deze mogelijkheid bepaald niet illusoir is kan blijken uit het overzicht van het gebruik van verkeersgegevens ten behoeve van de opsporing, dat is gevoegd bij de brief van 14 februari 2005 aan Uw Kamer (Kamerstukken II 2004/05, 23 490, nr. 360, Bijlage, LJN: AE9632 en LJN: AR5701). In de zaak AE9632 heeft de verdediging

zich beklaagd over het feit dat verkeersgegevens aangaande telefonie niet meer voorhanden waren. In de zaak AR5701 verzocht de raadsman om locatiegegevens die als ontlastend hebben te gelden indien uit hoofde van andere onderzoeksresultaten de aanwezigheid van verdachte ergens wordt vermoed maar deze registraties zouden kunnen uitwijzen dat hij, althans de gebruiker van die aansluiting, in werkelijkheid elders was.
Gelet op het voorgaande is in het wetsvoorstel voorgesteld om in de bewaartermijn een zekere marge in te bouwen zodat de beschikbaarheid van de gegevens zeker wordt gesteld ten behoeve van de hierboven besproken gevallen. Van groot belang daarbij zijn twee overwegingen.
De eerste overweging is, dat een langere bewaartermijn niet evenredig meer belasting en kosten voor het bedrijfsleven met zich meebrengt. Bij een bewaarplicht van achttien maanden zijn de meerkosten, die door de langere bewaartermijn met zich mee worden gebracht, niet exceptioneel hoger dan bij een bewaarplicht van twaalf maanden. Uit berekeningen van het onderzoeksbureau VKA komt naar voren dat de extra investeringskosten in verband met een verlenging van de bewaartermijn met een half jaar ongeveer zeven miljoen euro bedragen. In paragraaf 7 zal hierop nader worden ingegaan.
De tweede overweging is dat de mate waarin een bewaarplicht een aantasting vormt van de persoonlijke levenssfeer evenmin evenredig is aan de duur van de bewaartermijn. Zoals hieronder nog aan de orde zal komen, wordt een beperking van de persoonlijke levenssfeer niet zozeer veroorzaakt door het bewaren van gegevens als zodanig maar door het ten behoeve van de opsporing van strafbare feiten vorderen dat gegevens verstrekt worden aan de met opsporing belaste autoriteiten.

Gelet op de argumenten die pleiten voor een langere bewaartermijn enerzijds, en de overwegingen met betrekking tot de kosten en de gevolgen voor de persoonlijke levenssfeer anderzijds, kom ik tot de keuze voor een bewaartermijn van achttien maanden.

Ik deel de opvatting van de leden van de CDA-fractie dat een bewaartermijn van vierentwintig maanden, als voorgesteld de Raad van Hoofdcommissarissen nog meer bevorderlijk is in het kader van grootschalige internationale onderzoeken. Hierbij moet worden aangetekend dat het advies van de Raad van Hoofdcommissarissen voor een bewaartermijn van vierentwintig maanden niet alleen is gebaseerd op grootschalige internationale onderzoeken. Ook bij nationaal onderzoek van ernstige misdrijven kan een langere bewaartermijn bevorderlijk zijn voor het welslagen van het opsporingsonderzoek. Daarvan zullen hieronder, naar aanleiding van vragen van de fracties van het CDA, de PvdA en de ChristenUnie, enkele voorbeelden worden gegeven. Alles afwegende meen ik evenwel dat met een bewaartermijn van achttien maanden het meest optimaal rekening wordt gehouden met enerzijds de argumenten die pleiten voor een langere termijn en anderzijds de overwegingen met betrekking tot de kosten en de persoonlijke levenssfeer.
Uit het voorgaande volgt dat ik het met de leden van de SP-fractie eens ben dat niet alleen de behoefte van politie en justitie dient ter onderbouwing van de gekozen bewaartermijn, maar dat ook andere overwegingen daarbij een rol spelen. Eveneens volgt uit het voorgaande dat ik niet de mening van deze leden deel dat uiteindelijk iedere bewaartermijn enigszins willekeurig is. Zoals aan de orde kwam, zijn de belangen van de opsporing en vervolging van strafbare feiten gediend met de termijn van achttien maanden, terwijl de overwegingen met betrekking tot de kosten en de persoonlijke levenssfeer niet nopen tot een kortere termijn.
Bij de totstandkoming van de Richtlijn dataretentie hebben eveneens de belangen van de opsporing, de kosten en de bescherming van de persoonlijke levenssfeer een rol gespeeld bij de vaststelling van de toegestane bewaartermijn. Daarbij is in ogenschouw genomen dat in de situatie

van voor de richtlijn een deel van de lidstaten reeds zeer uiteenlopende bewaartermijnen kenden in een *range* van drie maanden tot vier jaar. Ook in het licht van de maximale bewaartermijn van vierentwintig maanden die in de richtlijn wordt voorzien, acht ik de gekozen bewaartermijn van achttien maanden proportioneel.

Samengevat zijn er twee argumenten voor de gekozen bewaartermijn. In de eerste plaats is er de behoefte aan een ruime bewaartermijn met het oog op complexere opsporingsonderzoeken, rechtshulpverzoeken en *cold cases*. Een langere bewaartermijn verzekert dat de gegevens ook in een later stadium voor het opsporingsonderzoek beschikbaar zijn, nadat de behoefte aan die gegevens manifest is geworden op grond van nieuwe inzichten of ontwikkelingen in dat onderzoek. Daarbij kan een langere bewaartermijn leiden tot meer afgewogen en beperktere bevraging van verkeersgegevens. In de tweede plaats kan de behoefte aan verkeersgegevens aan de orde zijn tijdens het onderzoek ter terechtzitting, waarbij de gegevens mede kunnen dienen om de onschuld van de verdachte aan te tonen. Door een zekere marge in de bewaarperiode in te bouwen wordt de kans vergroot dat de gegevens daadwerkelijk beschikbaar zijn. Zoals hierboven besproken zijn de extra kosten, die aan een langere bewaarplicht zijn verbonden, niet exceptioneel. Ditzelfde geldt voor de gevolgen voor de persoonlijke levenssfeer. Ik beschouw deze argumenten en overwegingen als een dragende onderbouwing van de bewaartermijn van achttien maanden.
Ik voeg daar nog aan toe dat thans geen ervaring bestaat met een bewaarplicht voor verkeersgegevens. De discussie over de precieze bewaartermijn zal dan ook niet eenvoudig aan de hand van wetenschappelijke argumenten kunnen worden gevoerd. Duidelijk is echter wel dat de criminaliteitsbestrijding gediend is met een langere bewaartermijn, terwijl andere belangen daarmee niet evident in strijd zijn.

Hiermee hoop ik op toereikende wijze antwoord te hebben gegeven op de vraag van de PvdA-fractie naar een solide argumentatie voor een bewaartermijn van achttien maanden. Daarbij wil ik er nog op wijzen dat het antwoord op de vraag, in hoeverre de argumentatie voor een dergelijke termijn solide is, sterk zal afhangen van de achtergrond en opvattingen van de betrokken partijen en de belangen waar zij voor staan. Het College bescherming persoonsgegevens geeft, mede vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer, de voorkeur aan een bewaartermijn van zes maanden. De opsporingsdiensten hebben, vanwege het belang van de opsporing van ernstige criminaliteit, aangedrongen op een langere bewaartermijn. De politie heeft geadviseerd in het wetsvoorstel een bewaartermijn van tenminste vierentwintig maanden te vermelden, het College van procureurs-generaal acht een bewaartermijn van achttien maanden, mede met het oog op de behoefte aan deze gegevens tijdens het onderzoek ter terechtzitting, niets te lang. Indien in de afwegingen bij dit wetsvoorstel alleen de adviezen van politie en het Openbaar Ministerie leidend zouden zijn dan zou een bewaartermijn van vierentwintig maanden die in de richtlijn als maximale termijn wordt toegestaan, zeker in de rede hebben gelegen. Ik acht het namelijk van groot belang dat de rechtshandhavinginstanties in staat worden gesteld – binnen de wettelijk gestelde grenzen en voorgeschreven waarborgen – hun werk zo goed mogelijk te doen. Daar waar gegevens beschikbaar kunnen zijn voor het aan de het licht brengen van de waarheid in ernstige strafzaken valt bij voorbaat moeilijk in te zien waarom die gegevens binnen redelijke grenzen niet beschikbaar gehouden zouden worden. Gelet op de andere belangen die dienen te worden meegewogen, waaronder de kosten van bewaring en de argumenten die zijn ingebracht met het oog op de bescherming van de persoonlijke levenssfeer, acht ik de voorgestelde bewaartermijn evenwichtig.

Wat betreft de vraag van de ChristenUnie naar een kwantitatieve onderbouwing van de bewaartermijn van achttien maanden, merk ik op dat de genoemde argumenten voor een langere bewaartermijn niet met cijfers zijn te onderbouwen. Omdat de inzet van de bevoegdheid tot het opvragen van verkeersgegevens niet wordt geregistreerd, is er namelijk geen cijfermatig materiaal voorhanden op grond waarvan een voorstel voor een bewaartermijn empirisch kan worden onderbouwd. Uit algemeen onderzoek als dat van de EUR en uit concrete voorbeelden kan echter wel blijken dat bij de opsporingsdiensten regelmatig, en in het bijzonder bij zwaardere zaken, behoefte bestaat aan verkeersgegevens van oudere datum. Die voorbeelden komen hieronder, naar aanleiding van vragen van de PvdA-fractie, aan de orde. Ontbreekt thans een registratie van het aantal verzoeken om verkeersgegevens, in de toekomst zal dit veranderen. De Richtlijn dataretentie voorziet namelijk in de verplichting om de Commissie jaarlijks statistisch materiaal aan te bieden dat inzicht geeft in het aantal verzoeken om informatie, de periode die verstreken is tussen het moment van opslag en het verzoek en de aantallen verzoeken die niet konden worden gehonoreerd. Dit statistische materiaal zal in de toekomst in kwantitatieve zin een meer diepgaand inzicht kunnen bieden in de behoefte die in de praktijk bestaat aan een bewaartermijn van een bepaalde lengte. Op dit punt wordt hieronder in paragraaf 2.9, naar aanleiding van vragen van de VVD-fractie, nader ingegaan.

De leden van de ChristenUnie-fractie wezen er op dat ondanks een daartoe strekkende vraag van de Raad van State, naar hun mening niet duidelijk wordt gemaakt waarom Nederland met de duur van de bewaartermijn van achttien maanden een stuk verder wil gaan dan andere lidstaten. Zij vroegen of de argumenten die de regering voor deze keuze aandraagt niet of in mindere mate voor andere lidstaten gelden en zouden hierover graag een nadere reactie ontvangen. Ook vroegen zij een reactie op een brief van het Adviescollege toetsing administratieve lasten (Actal) en het CBP van 12 oktober jongstleden.
Op de vraag van de leden van deze fractie naar de keuze voor een bewaartermijn van achttien maanden ben ik hierboven, naar aanleiding van vragen van de fracties van het CDA, de PvdA en de SP, reeds ingegaan. Op de keuze van de bewaartermijnen in de andere lidstaten zal ik in paragraaf 6 ingaan, bij de beantwoording van de vragen van de fracties van het CDA en de PvdA over de bewaartermijnen in het buitenland. Naar die beantwoording moge ik verwijzen. Op de brief van het Actal en het CBP zal verderop in deze paragraaf worden ingegaan.

De leden van de SP-fractie meenden dat de keuze voor een langere bewaartermijn dan het minimum van zes maanden niet kon worden gerechtvaardigd met een beroep op het harmoniseren van regelgeving, nu er in de richtlijn een zekere bandbreedte bestaat voor de in de nationale wetgeving op te nemen bewaartermijn. Ook de fractie van het CDA wierp de vraag op of de regering van mening is dat nog wel kan worden gesproken van harmonisatie binnen de EU als er grote verschillen zijn tussen de lidstaten.
In antwoord op de gestelde vragen merk ik op dat de Richtlijn dataretentie voorziet in bewaarplicht voor bepaalde telecommunicatiegegevens, waarbij is gestreefd naar harmonisatie van de verplichtingen van de lidstaten. Daartoe bevat de richtlijn een gedetailleerde lijst van de te bewaren categorieën van gegevens evenals regels inzake de bescherming en beveiliging van de te bewaren gegevens (artikel 7), het toezicht op de toepassing van die regels (artikel 9) en de periodieke verstrekking van statistische informatie aan de Commissie (artikel 10). De harmonisatie is echter niet volledig. Zo geldt geen eenduidige bewaartermijn. De lidstaten moeten ervoor zorgen dat de gegevens tenminste gedurende zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie

worden bewaard (artikel 6). Met deze «bandbreedte» wordt de lidstaten inderdaad een zekere marge geboden voor het maken van eigen keuzes en afwegingen. Dit hangt nauw samen met het sterk uiteenlopen van de posities van de lidstaten terzake. Aan de keuze voor een bewaartermijn van achttien maanden liggen, anders dan de fractie van de SP kennelijk veronderstelde, geen redenen ten grondslag die samenhangen met het harmoniseren van regelgeving. Hierboven heb ik, naar aanleiding van vragen van de fracties van de PvdA, het CDA, de ChristenUnie en de SP, reeds aangegeven welke overwegingen ten grondslag liggen aan mijn keuze voor een bewaartermijn van achttien maanden. Die keuze vloeit juist voort uit een afweging op nationaal niveau, die binnen de door de richtlijn geboden bandbreedte moet vallen. Het feit dat de richtlijn een dergelijke bandbreedte biedt, impliceert dat op dit punt geen volledige harmonisatie binnen de Unie kan worden verwacht. Een volledig geharmoniseerde bewaartermijn is, vanwege het uiteenlopen van de voorkeuren van de lidstaten, in Brussel niet haalbaar gebleken.

De leden van de PvdA-fractie vroegen toe te lichten in welke mate de huidige regelgeving onvoldoende mogelijkheden biedt ten behoeve van strafrechtelijke opsporing en hoe zich dit verhoudt tot de maatschappelijke opbrengst van dataretentie. Zij vroegen naar voorbeelden van zaken die het afgelopen jaar niet zijn opgelost, die eveneens niet opgelost hadden kunnen worden indien er een bewaarplicht van zes maanden had bestaan, maar die wel opgelost hadden kunnen worden met behulp van een bewaarplicht van achttien maanden. Ook vroegen zij of kan worden aangegeven welke zaken in de toekomst opgelost zouden kunnen worden met dank aan een bewaartermijn van achttien maanden die niet oplosbaar zijn met een bewaartermijn van zes maanden. Tot slot vroegen zij waarom er is afgeweken van het advies vanuit de Erasmus Universiteit voor een bewaartermijn van één jaar.
In antwoord op de gestelde vragen merk ik op dat een eerste verschil tussen de huidige regelgeving en de voorgestelde regelgeving is, dat de huidige regelgeving niet voorziet in een algemene wettelijke verplichting voor de aanbieders van communicatiediensten en -netwerken om telecommunicatiegegevens gedurende een bepaalde termijn te bewaren ten behoeve van de opsporing of vervolging van ernstige misdrijven. Dit betekent dat de wettelijke bewaarplicht in de eerste plaats zeker stelt dat bepaalde gegevens door de aanbieders zullen worden bewaard, zodat deze beschikbaar zijn indien dit voor de opsporing en vervolging van strafbare feiten nodig is. Thans bestaat deze zekerheid niet en komt het voor dat tevergeefs een beroep wordt gedaan op gegevens die kunnen bijdragen aan de opheldering van strafbare feiten. Dit wordt nog van groter belang nu de ontwikkelingen op het gebied van de elektronische communicatie ertoe zullen leiden dat aanbieders in afnemende mate verkeersgegevens zullen opslaan ten behoeve van de «billing». Hierbij kan worden gedacht aan zogenaamde «flat rate»-tarieven, prepaid telefonie en *Voice over IP*. Indien verkeersgegevens niet meer voor zakelijke doeleinden worden bewaard, zullen zij niet meer beschikbaar zijn voor politie en justitie. Daarom is een wettelijke bewaarplicht ten behoeve van opsporing en vervolging noodzakelijk. Een dergelijke bewaarplicht biedt zowel aan de zijde van de aanbieders als aan de zijde van de zogenaamde behoeftestellers duidelijkheid over welke gegevens beschikbaar dienen te worden gehouden. Ten tweede is een verschil met de huidige regelgeving dat de bewaartermijn duidelijkheid biedt over de periode gedurende welke de gegevens beschikbaar zijn ten behoeve van de opsporing of vervolging van ernstige misdrijven. Thans verschilt het per aanbieder over welke periode nog gegevens beschikbaar zijn. Daarbij speelt mee dat de bewaarplicht bevorderlijk is voor de waarheidsvinding, zoals die ook tijdens het onderzoek ter terechtzitting aan de orde kan zijn. De verdachte kan een beroep doen op de bewaarde gegevens om zijn onschuld aan te

tonen. Thans zal het in de fase van het onderzoek ter terechtzitting vaak twijfelachtig zijn of bepaalde gegevens bij de aanbieder nog beschikbaar zijn.
Zoals hierboven, naar aanleiding van vragen van de fracties van de PvdA, het CDA en de ChristenUnie naar voren is gekomen, beschik ik helaas niet over een lijst van voorbeelden van zaken die het afgelopen jaar niet zijn opgelost, die eveneens niet opgelost hadden kunnen worden indien er een bewaarplicht van zes maanden had bestaan maar die wel opgelost hadden kunnen worden met behulp van een bewaarplicht van achttien maanden. Wel is mij vanuit de praktijk door politie en Openbaar Ministerie geadviseerd dat in het licht van concrete ervaringen met het gebruik van telecommunicatiegegevens moet worden vastgesteld dat een langere beschikbaarheid van verkeersgegevens van essentieel belang kan zijn voor het welslagen van de opsporing en vervolging in ernstige zaken, zoals ontvoeringen, overvallen en moord. Juist in dat soort zaken kan er een lange tijd verstrijken tussen het plegen van het delict en het achterhalen van de verdachte, zodat een termijn van twaalf maanden tekort kan schieten. Nu de PvdA-fractie vraagt om voorbeelden, noem ik het geval van vermissing van een kind dat een jaar later dood werd aangetroffen. Van de verdachte die later in beeld is gekomen bleken geen verkeersgegevens meer beschikbaar. Ook is bekend een geval waarin een getuige verklaarde over de betrokkenheid van een verdachte bij een gewapende overval. De getuige verklaarde tevens over de betrokkenheid van de verdachte bij een eerdere mislukte overval. Daarover had de getuige een jaar eerder telefonisch contact gehad met de verdachte. Deze verklaring bleek echter niet te verifiëren omdat de telecommunicatiegegevens niet meer beschikbaar waren. Een drievoudige moord uit 2004 is eveneens een goed voorbeeld. Tijdens dit onderzoek zijn er bij de mobiele aanbieders gegevens bevraagd van tussen achttien maanden en twee jaar oud in verband met een vierde moord die eerder had plaats gevonden met dezelfde daders als verdachten. Deze moord had direct relaties tot de drievoudige moord. Uit de verkeersgegevens, die bij een aanbieder nog beschikbaar waren, werd bewijs gehaald dat verdachten op bepaalde plaatsen waren geweest ten tijde van de verdwijning van de vermoorde man. Nader onderzoek hiernaar heeft geleid tot nieuwe verdenkingen. Een ander voorbeeld betreft een moord in november 2005. In maart 2007 houdt de politie een verdachte aan. Van de verdachte waren zestien maanden later geen telecommunicatiegegevens meer beschikbaar. Was dit wel het geval geweest dan zouden deze gegevens als steunbewijs hebben kunnen dienen dan wel voor de verdachte ontlastend materiaal hebben kunnen opleveren.
Naast deze specifieke voorbeelden geldt voor de onderzoeken die door de FIOD-ECD worden gedaan meer algemeen dat veel onderzoeken gericht zijn op strafbare feiten die enige tijd voor de ontdekking ervan gepleegd zijn. Te denken valt bijvoorbeeld aan faillissementsfraude en belastingfraude. Voordat in dit soort zaken het onderzoek kan worden opgestart is veel vooronderzoek nodig alsmede afstemming tussen de opsporingsinstanties en, ingeval van faillissementsfraude, bijvoorbeeld de curator. Tegen de tijd dat het onderzoek daadwerkelijk kan worden opgestart is niet zelden een jaar of meer verstreken. Voor de rechercheur die dit soort onderzoek verricht is het van wezenlijk belang om over verkeersgegevens te kunnen beschikken van het telefoon- of e-mailverkeer om verklaringen van de betrokken personen te kunnen verifiëren.
Op de vraag waarom er is afgeweken van het advies vanuit de Erasmus Universiteit voor een bewaartermijn van één jaar, ben ik hierboven, naar aanleiding van vragen van de fracties van PvdA, het CDA en de ChristenUnie, reeds ingegaan.

De leden van de SP-fractie hebben hun twijfels geuit bij de conclusie van de onderzoekers dat een langere bewaartermijn kan leiden tot een meer

afgewogen, beperktere bevraging van de verkeersgegevens en vroegen regering dit toe te lichten. De leden van deze fractie vroegen zich af of er dan langer gewacht wordt met het bevragen van gegevens.
In antwoord op de gestelde vraag kan worden opgemerkt dat uit het onderzoek van de Erasmus Universiteit naar voren is gekomen dat bij de opsporingsinstanties een neiging bestaat om, vanwege de onzekerheid over de beschikbaarheid van de gegevens in een later stadium, terstond bij aanvang van het onderzoek zoveel mogelijk gegevens op te vragen. Daarbij is gebleken dat in eerste instantie de verkeersgegevens van alle op het eerste gezicht relevant lijkende telefoonnummers worden opgevraagd terwijl later dikwijls blijkt dat slechts een deel van de gegevens daadwerkelijk van belang was. Een langere bewaartermijn biedt de mogelijkheid op basis van verkregen inzichten meer afgewogen vorderingen tot het verstrekken van de verkeersgegevens te doen. Dat geldt zowel voor het tijdsbestek waarover de gegevens worden opgevraagd als voor bepaalde telefoonnummers met betrekking waartoe gegevens worden gevraagd. Bij een langere bewaartermijn bestaat niet het risico dat kort na aanvang van het onderzoek de gegevens vernietigd zullen worden. Tijdens het onderzoek zal de bevraging van gegevens derhalve gerichter en op het moment van het ontstaan van de behoefte kunnen plaatsvinden.

De leden van de SP-fractie merkten op dat de regering de keuze voor een bewaartermijn van achttien maanden ondermeer verdedigt door te wijzen op een gemiddelde doorlooptijd van zeven en een halve maand, waarbij hoger beroep niet is meegerekend. Zij vroegen of de gegevens ten aanzien waarvan de bewaarplicht komt te gelden meestal niet al in een vroeg stadium van de zaak zijn opgevraagd en of het vaak voorkomt dat gegevens pas in hoger beroep moeten worden opgevraagd.
Dat dit laatste in de praktijk voorkomt kan blijken uit het overzicht van het gebruik van verkeersgegevens ten behoeve van de opsporing in de brief van 14 februari 2005 waarnaar ik hierboven, bij de beantwoording van de vragen van de fracties van PvdA, CDA en SP, heb verwezen. Niet altijd worden aan het begin van een opsporingsonderzoek gegevens veilig gesteld. Gegevens kunnen soms namelijk pas worden veiliggesteld als men een verdachte op het spoor is gekomen. Zoals hierboven aan de orde kwam, is daarvan soms pas na verloop van tijd sprake, en ook het College van procureurs-generaal heeft in zijn advies uitdrukkelijk op dit aspect gewezen. De rechter in eerste aanleg en de rechter in hoger beroep kunnen in de loop van het onderzoek ter zitting, bijvoorbeeld op verzoek van de verdediging, bevelen dat nadere informatie dient te worden opgevraagd. Ik beschik echter niet over cijfermatig materiaal waaruit zou blijken hoe vaak het voorkomt dat gegevens pas in hoger beroep worden opgevraagd.

De leden van de PvdA-fractie vroegen voorts of de regering onderschrijft dat verkeers- en locatiegegevens van telecomgebruik een zeer uitvoerig beeld geven van het dagelijks leven van een burger en derhalve dat het bewaren van dergelijke gegevens en het inzien van dergelijke gegevens een zeer zware inbreuk op de privacy van burgers betreft. Zij vroegen de regering toe te lichten waarom zij ervoor kiest die inbreuk op de privacy drie keer zo zwaar te maken als volgens de richtlijn wordt voorgeschreven (te weten een bewaartermijn van achttien maanden waar slechts zes maanden verplicht is).
In antwoord op de gestelde vragen merk ik op dat de veronderstelling dat verkeers- en locatiegegevens van telecommunicatiegebruik in alle gevallen een zeer uitvoerig beeld geven van het dagelijks leven van een burger, nuancering verdient. De gegevens waar het om gaat worden reeds door de aanbieders in het kader van hun eigen bedrijfsvoering verwerkt. Het gaat niet om de inhoud van gesprekken maar om gegevens die inzicht kunnen geven in de contacten en het belgedrag van personen. De betref-

fende gegevens worden doorgaans verspreid opgeslagen in de systemen van de aanbieders en zijn, zo lang zij niet kan worden gekoppeld aan informatie die elders beschikbaar is, veelal nog niet zo veelzeggend. De veronderstelling dat dergelijke gegevens in alle gevallen een zeer uitvoering beeld geven van het dagelijks leven van de burger acht ik dan ook onjuist. Dit neemt echter niet weg dat het hier gaat om persoonsgegevens en dat degene op wie de gegevens betrekking hebben het recht heeft op een zorgvuldige omgang met zijn gegevens, alsmede het recht op bescherming van zijn persoonlijke levenssfeer. De persoonlijke levenssfeer van de burger wordt mijns inziens evenwel niet zozeer aangetast door het bewaren van gegevens als wel door het eventuele gebruik ervan. Voor de beoordeling van de mate van aantasting van de privacy van burgers acht ik dan ook minder leidend het feit dat bepaalde gegevens worden bewaard als wel de omstandigheden en voorwaarden waaronder toegang kan worden verkregen tot die gegevens. Op dit moment worden verkeersgegevens, die door de aanbieders van telecommunicatiediensten ten behoeve van bedrijfsdoeleinden worden verwerkt, ook reeds door opsporingsinstanties opgevraagd. Deze bevraging is met wettelijke waarborgen omkleed. De thans ter implementatie van de Richtlijn dataretentie voorgestelde wettelijke regeling bevat geen afzonderlijke regels over de toegang tot de bewaarde gegevens en zal er, in vergelijking met de huidige situatie, als zodanig dan ook niet toe leiden dat verdergaande beperkingen worden gesteld ten aanzien van de rechten van burgers. Wel wordt met de bewaarplicht gewaarborgd dat de gegevens daadwerkelijk beschikbaar zijn ten behoeve van de opsporing van strafbare feiten. Op de vraag van de PvdA-fractie, toe te lichten waarom de regering ervoor kiest de inbreuk op de privacy drie keer zo zwaar te maken als volgens de richtlijn wordt voorgeschreven, merk ik dan ook op dat een verlenging van de bewaartermijn niet hetzelfde is als een verzwaring van de inbreuk op de privacy. De Richtlijn dataretentie biedt de lidstaten hiervoor de ruimte omdat deze voorziet in een verplichting om een bewaartermijn vast te stellen van minimaal zes maanden en ten hoogste twee jaar. De richtlijn houdt er dus rekening mee dat niet alleen een termijn van zes maanden maar ook langere termijnen nodig kunnen zijn voor de opsporing van ernstige strafbare feiten. Op mijn overwegingen om te kiezen voor een bewaartermijn van achttien maanden ben ik hierboven, naar aanleiding van de vragen van de fracties van het CDA, de ChristenUnie. de SP en ook PvdA, reeds nader ingegaan. Daarnaar moge ik thans verwijzen.

De leden van de D66-fractie vroegen op het punt van de noodzaak als bedoeld in artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) een nadere reactie ter onderbouwing van de termijn van achttien maanden. Zij constateerden dat met deze bewaartermijn voor historische verkeersgegevens door opsporinginstanties over een lange periode ook inzicht wordt verkregen in de handel en wandel van personen die niet worden verdacht van een strafbaar feit en meenden dat dit een inbreuk vormt het in artikel 8 EVRM verankerde fundamentele recht op eerbiediging van de persoonlijke levenssfeer. Artikel 8 bepaalt dat inmenging van het openbaar gezag in dit fundamentele recht alleen is toegestaan indien dit in een democratische samenleving noodzakelijk is. Blijkens de toelichting wordt de duur van de bewaartermijn gerelateerd aan de periode dat verkeersgegevens een belangrijke rol kunnen spelen in het richting geven aan het opsporingsonderzoek van strafbare feiten en de bewijsvoering hiervan ter zitting. Naar de mening van de leden van de fractie van D66 was met dit (onderzoeks-) belang de noodzaak van bovengenoemde inbreuk op artikel 8 EVRM niet voldoende aangegeven. Ook misten zij informatie over de hoeveelheid zaken waarop in dit verband wordt gedoeld, de omvang van de gevolgen van het ontbreken van gegevens voor de opsporing en vervolging van

deze zaken en de mate waarin alternatieven bestaan voor deze gegevens in het opsporingsonderzoek en bij de bewijsvoering ter zitting.

Graag beantwoord ik deze vragen als volgt. Hierboven kwam, in het antwoord op de vragen van de leden van de PvdA-fractie, reeds aan de orde dat met de bewaring van verkeersgegevens niet per definitie inzicht wordt verkregen in de persoonlijke levenssfeer van burgers. Pas wanneer gegevens in het kader van een opsporingsonderzoek, met inachtneming van de wettelijke vereisten, door de opsporingsinstanties worden gevorderd kunnen deze instanties inzicht krijgen in de persoonlijke levenssfeer van personen. Ook thans worden met toepassing van de daartoe strekkende bevoegdheden telecommunicatieverkeergegevens voor de opsporing van strafbare feiten gebruikt. Wel brengt de bewaarplicht met zich mee dat gegevens vaker daarvoor beschikbaar zullen zijn, zodat vaker sprake zal kunnen zijn van inmenging in de persoonlijke levenssfeer. Ook brengt de bewaarplicht met zich mee dat gegevens door de aanbieders worden verwerkt voor andere doelen, waarmee wordt afgeweken van het beginsel van doelbinding. Met de leden van de D66-fractie onderschrijf ik dan ook dat de bewaarplicht het recht op bescherming van de persoonlijke levenssfeer kan beperken en dat deze daarom moet voldoen aan het noodzakelijkheidsvereiste van artikel 8 EVRM.
In het voorgaande kwam reeds het belang van gegevens, die worden verwerkt met het oog op de levering van telecommunicatiediensten voor de opsporing en vervolging van strafbare feiten, aan de orde evenals de bijdrage die een bewaarplicht van achttien maanden daaraan kan leveren. In het bijzonder met het oog op de goede uitvoering van meer complexe opsporingsonderzoeken, internationale onderzoeken en de behandeling van *cold cases,* alsmede met het oog op de beschikbaarheid van gegevens in de fase van het onderzoek ter terechtzitting, is een bewaartermijn van achttien maanden van belang. Dit kan worden aangemerkt als een zwaarwegend maatschappelijke belang dat zeker begrepen kan worden onder het vereiste van een «pressing social need», zoals opgenomen in artikel 8 EVRM. Ik relateer de noodzaak van de gekozen bewaartermijn dus aan het algemene belang van de opsporing van strafbare feiten, in het bijzonder bij de typen onderzoek als aangeduid, dat zeer gediend is met de beschikbaarheid van deze gegevens. Vanzelfsprekend onderbouw ik de duur van de termijn door aan te geven dat de betreffende gegevens gedurende een bepaalde periode een rol kunnen spelen in het richting geven aan het opsporingsonderzoek van strafbare feiten en in de bewijsvoering hiervan ter terechtzitting. Ook al ontbreken cijfers over het aantal zaken waarin dit het geval is, dat maakt deze onderbouwing niet minder valide en doet niet af aan de zwaarwegendheid van het belang. De gevolgen van het ontbreken van gegevens voor de opsporing in deze typen onderzoek kunnen zijn dat dergelijke onderzoeken niet tot een goed einde gebracht kunnen worden. Ik verwijs hiervoor naar de hierboven, in antwoord op vragen van de leden van de PvdA-fractie, gegeven voorbeelden van een vermissing, een overval en een moord die zich in het verleden hebben voorgedaan. Over de passendheid van de bewaartermijn van achttien maanden binnen de vereisten van artikel 8 EVRM, merk ik tot slot nog op dat de richtlijn zelf voorziet in de mogelijkheid van een maximale bewaartermijn van vierentwintig maanden. De vraag welke bewaartermijn, gelet op de betrokken belangen, de voorkeur verdient is echter niet alleen een juridische maar ook, en misschien wel vooral, een politieke afweging. Het EVRM biedt terzake, gelet op de in de rechtspraak ontwikkelde «margin of appreciation», de aangesloten landen de nodige ruimte voor het maken van afwegingen die passen bij de nationale situatie. Het is in het licht hiervan weinig verrassend dat de voorkeuren van de betrokken adviesorganen – nu politie en justitie hebben gepleit voor een langere termijn terwijl de Raad van State, het College bescherming persoonsgegevens, Actal en de artikel 29-werkgroep hebben gepleit voor een

kortere termijn – onderling afwijken. De regering ziet echter goede gronden voor een bewaartermijn van achttien maanden.

Alternatieven voor het beschikbaar krijgen van gegevens over de communicatie van personen, die van belang zijn in een opsporingsonderzoek, zijn niet aanwezig. Alleen de aanbieders van telecommunicatiediensten beschikken over deze gegevens. Weliswaar is de vergaring van telecommunicatiegegevens niet de enige methode voor de opsporing van strafbare feiten, en zijn er ook andere methoden om informatie te vergaren die daaraan kan bijdragen, maar telecommunicatiegegevens vormen een essentiële bijdrage aan zeer veel opsporingsonderzoeken, die niet eenvoudig door andere informatie is te vervangen, zo mag blijken uit het onderzoek van de EUR alsmede uit de adviezen van de politie en het openbaar ministerie. Juist dit is de achtergrond van de Richtlijn dataretentie. Als alternatief voor de bewaarplicht is wel gepleit te volstaan met de mogelijkheid van bevriezing van verkeersgegevens («data preservation»). De telecommunicatie verkeersgegevens van een gebruiker worden dan door de aanbieder bewaard nadat politie en justitie een daartoe strekkend verzoek aan de aanbieder hebben gericht. Alsdan zal echter niet in de tijd terug kunnen worden gegaan. Indien politie en justitie niet in staat zouden zijn kennis te nemen van gegevens, die zijn gegenereerd voordat het strafbare feit heeft plaatsgevonden, zullen zij ernstig beperkt zijn. Ook in de fysieke wereld zou het voor de opsporingsdiensten een moeilijke situatie opleveren indien het onderzoeksmateriaal, dat voor het tijdstip van het plegen van het strafbare feit aanwezig is, bij voorbaat vernietigd zou zijn. De noodzaak tot het gebruik van verkeersgegevens en de noodzaak te kunnen beschikken over deze gegevens gedurende een langere periode zijn gebaseerd op de bevindingen van het onderzoek van de Erasmus Universiteit en de ervaring uit de praktijk die naar voren is gebracht in de aan mij uitgebrachte adviezen van de politie en het Openbaar Ministerie.
In antwoord op de hierover door de leden van de D66-fractie gestelde vragen merk ik op dat, zoals in het voorgaande al aan de orde kwam, thans geen cijfermatig materiaal voorhanden is over de hoeveelheid zaken waarbij de beschikking van telecommunicatiegegevens van doorslaggevend belang is geweest tijdens de opsporings- en vervolgingsfase. Evenmin is cijfermatig materiaal bekend van het gebruik van telecommunicatiegegevens als bewijsmateriaal ter zitting. Zoals eerder vermeld, voorziet de richtlijn in de verplichting om statische informatie te verzamelen, onder meer over de gevallen waarin overeenkomstig de toepasselijke nationale wetgeving gegevens zijn verstrekt aan de bevoegde autoriteiten. Op dit punt zal hieronder in paragraaf 2.9, naar aanleiding van vragen van de VVD-fractie, nader worden ingegaan.

De leden van de CDA-fractie constateerden dat verschillende telecommunicatieaanbieders hebben opgemerkt dat het hanteren van verschillende bewaartermijnen in de verschillende Europese lidstaten tot gevolg heeft dat internationaal opererende aanbieders onnodig met extra uitvoeringslasten worden geconfronteerd. De leden vroegen mij hierop te reageren. Zoals hierboven in paragraaf 2.1. reeds in antwoord op een vraag van de leden van de CDA-fractie, naar voren kwam kunnen de verschillende bewaartermijnen in de verschillende Europese lidstaten voor de internationale aanbieders van telecommunicatiediensten inderdaad extra lasten met zich meebrengen. Zij zullen in hun bedrijfsvoering rekening moeten gaan houden met verschillende bewaartermijnen. Dit is een euvel dat in de sector telecommunicatie vaker voorkomt, nu Europese richtlijnen niet steeds door alle lidstaten op dezelfde wijze worden geïmplementeerd. Het hanteren van verschillende bewaartermijnen binnen de lidstaten van de Europese Unie is het rechtstreekse gevolg van het ontbreken van volledige harmonisatie van de Europese regels betreffende het bewaren van

verkeers- en locatiegegevens. Dit houdt verband met bestaande verschillen binnen de lidstaten in methoden van opsporing en vervolging van strafbare feiten en de daarbij toegelaten bewijsmiddelen. Zo zijn er landen die thans een bewaarplicht kennen die langer is dan vierentwintig maanden maar er zijn ook landen met een bewaarplicht van zes maanden of zelfs korter. Deze richtlijn harmoniseert de bewaartermijn binnen de range van zes en vierentwintig maanden. De verschillende bewaartermijnen in de lidstaten brengen wel uitvoeringslasten voor de bedrijven met zich mee, maar hebben geen grote invloed op de hoogte van de kosten die het bewaren van gegevens zullen veroorzaken. De bewaartermijn heeft namelijk vooral invloed op de kosten die gemaakt moeten worden voor opslagcapaciteit waarvan de kosten als gevolg van de voortgaande technische ontwikkelingen steeds minder worden. De meeste kosten worden veroorzaakt door de eisen aangaande de beveiliging van opgeslagen gegevens en het ordenen van de gegevens, waaraan voldaan moet worden. De kosten die gepaard gaan met een langere bewaartermijn dan zes maanden zijn dan ook niet substantieel, zoals hieronder in paragraaf 7 ook aan de orde komt.

De leden van de CDA-fractie hebben opgemerkt dat het voorstelbaar is dat een andere lidstaat in Nederland een informatieaanvraag doet binnen de Nederlandse bewaartermijn, terwijl de eigen nationale bewaartermijn reeds is verstreken. Zij hebben gevraagd toe te lichten hoe er met deze discrepantie wordt omgegaan.
In antwoord op deze vraag merk ik op dat een verzoek om telecommunicatiegegevens van een andere lidstaat langs de weg van een rechtshulpverzoek moet worden ingediend en dat daarover door de officier van justitie wordt beslist. Daarbij toetst de officier van justitie of voldaan is aan de voorwaarden die naar Nederlands recht gelden voor het vorderen van verkeersgegevens. Is dat het geval, dan kan aan het verzoek worden voldaan ook al betreft het gegevens die, wanneer zij in de verzoekende lidstaat zouden zijn verwerkt, in die lidstaat niet meer aanwezig zouden zijn omdat aldaar de bewaartermijn is verstreken. Bedacht moet echter worden dat een verzoek aan Nederland vanzelfsprekend alleen gehonoreerd kan worden wanneer het betrekking heeft op telecommunicatiegegevens die onder de Nederlandse bewaarplicht vallen, dat wil zeggen dat het moet gaan om telecommunicatiegegevens die door de aanbieders, die onder de Nederlandse rechtsmacht vallen, worden gegenereerd of verwerkt. In Nederland zijn doorgaans geen gegevens beschikbaar over communicatie die in zijn geheel op het grondgebied van de verzoekende lidstaat heeft plaatsgevonden. Er zal voor de belanghebbende lidstaat een aanleiding moeten bestaan te veronderstellen dat er in Nederland relevante telecommunicatiegegevens beschikbaar zijn. In het geval de eigen nationale bewaartermijn is verstreken zal die aanleiding er niet zo snel zijn omdat men in de verzoekende lidstaat dan geen beschikking heeft over historische verkeersgegevens die aanknopingspunten kunnen hebben met de gegevens die in Nederland onder de bewaarplicht vallen.

De leden van de CDA-fractie wezen op de ruimte die de richtlijn biedt om verschillende bewaartermijnen te kiezen, ook voor de verschillende categorieën van gegevens, en hebben de regering gevraagd hoe die termijnen zich verhouding tot de keuze voor een termijn van achttien maanden in Nederland. Zij hebben gevraagd hoe de Nederlandse keuze voor achttien maanden zich verhoudt tot de gemiddelde bewaartermijn in de EU, of het juist is dat Nederland een aanzienlijke afwijking vertoont ten opzichte van omringende landen en of het juist is dat het Verenigd Koninkrijk, als mede-indiener van dit voorstel, zelf heeft gekozen voor een bewaartermijn van twaalf maanden voor telefonie en van slechts zes maanden voor e-mail en internetgegevens. Ook de leden van de ChristenUnie-fractie

zouden graag een nadere reactie ontvangen op de verhouding tot de bewaartermijnen in de andere lidstaten.
In antwoord op de gestelde vragen merk ik op dat de Engelse Code of practice, behorend bij de Regulation of Investigatory Powers Act 2000, verschillende bewaartermijnen kent voor verschillende categorieën van gegevens. Abonnee- en telefoniegegevens moeten inderdaad voor een periode van twaalf maanden worden bewaard, voor SMS-, EMS-, e-mail- en bepaalde internetgegevens geldt een bewaartermijn van zes maanden. Op de overwegingen, die aanleiding hebben gegeven tot een keuze voor een bewaartermijn van achttien maanden ben ik hierboven in paragraaf 2.3, naar aanleiding van vragen van de fracties van CDA, PvdA, ChristenUnie en SP, reeds nader ingegaan. Nederland maakt geen gebruik van de mogelijkheid voor verschillende gegevens verschillende bewaartermijnen te hanteren. Op de bewaartermijnen in het buitenland zal ik hieronder in paragraaf 6 nader ingaan. Voorzover de Nederlandse keuze voor een termijn van achttien maanden afwijkt van die in omringende landen is dit een gevolg van de marge die de richtlijn op dit punt biedt, en van de verschillende waardering van de in het geding zijnde belangen in de onderscheiden lidstaten.

De leden van de fracties van ChristenUnie en D66 hebben gewezen op een gezamenlijke brief van het Actal en het CBP aan de vaste Kamercommissie voor Justitie waarin de suggestie wordt gedaan om een nieuw onderzoek te laten uitvoeren naar de meest wenselijke bewaartermijn, dit in aanvulling op het eerdere onderzoek door de Erasmus Universiteit Rotterdam naar de kosten van het wetsvoorstel voor het bedrijfsleven. Deze leden vroegen om een reactie op deze brief.
In antwoord op de gestelde vragen merk ik allereerst op dat de brief van Actal en het CBP aan de vaste Kamercommissie mij niet bekend is. Voorzover ik uit de gestelde vragen kan opmaken, wordt in die brief voorgesteld nader onderzoek te verrichten naar de bewaartermijn en de kosten die aan het wetsvoorstel zijn verbonden. Voor een dergelijk onderzoek zie ik echter geen aanleiding omdat dit onderzoek reeds is verricht. Naar aanleiding van de wens van Uw Kamer om de daadwerkelijke behoefte van de opsporingsinstanties ten aanzien van verkeersgegevens onderzocht te willen hebben is de Erasmus Universiteit Rotterdam (EUR) opdracht gegeven deze behoefte in kaart te brengen. De bevindingen van de onderzoekers van de EUR, alsmede de terzake van het conceptwetsvoorstel ingewonnen adviezen van de adviesorganen, liggen ten grondslag aan de in het wetsvoorstel voorgestelde bewaartermijn. Dit is toegelicht in paragraaf 2.3 van de memorie van toelichting. Voor wat betreft de te verwachten lasten voor het bedrijfsleven heeft het onderzoeksbureau VKA onderzoek verricht en een aantal kostenberekeningen opgesteld. Dit is toegelicht in paragraaf 7 van de memorie van toelichting. Het conceptwetsvoorstel met deze toelichting is bovendien om advies gezonden aan het bedrijfsleven. Na deze onderzoeken en na de uitgebreide raadpleging van de aanbieders in deze sector alsmede van opsporingsinstanties en andere betrokkenen acht ik nader onderzoek niet aangewezen. De uiterste datum voor de implementatie van de richtlijn is 15 september 2007, in een aantal lidstaten is de wetgeving ter implementatie van de richtlijn reeds van kracht. Bij deze stand van zaken acht ik het weinig heilzaam om opnieuw onderzoek te gaan verrichten naar de genoemde aspecten.

De leden van de D66-fractie verwezen naar een onderzoek naar het nut en de noodzaak van het bewaren van verkeersgegevens door de Duitse IT en telecom-brancheorganisatie Bitkom. Dit onderzoek zou de wetgeving en het gebruik van historische verkeersgegevens in een aantal Europese lidstaten en de Verenigde Staten hebben vergeleken. Het CBP en Actal hebben erop gewezen dat in dit rapport werd geconcludeerd dat een

langere bewaartermijn dan (gemiddeld) drie maanden niet kon worden gerechtvaardigd.
Naar aanleiding van de vraag van de leden van de D66-fractie om een reactie op bovengenoemd rapport, kan ik melden dat de Duitse IT en telecom-brancheorganisatie Bitkom op eigen initiatief een rechtsvergelijkend onderzoek naar het gebruik van historische verkeersgegevens heeft gedaan. De onderzoekers concludeerden onder andere: «In der Regel werden Daten angefragt, die bis zu 3 Monate zurückliegen. Nur sehr selten werden Daten angefordert, die älter als 6 Monate sind. Verkehrsdaten, die älter als 3–6 Monate sind, werden von den Law Enforcement Agencies (LEAs) kaum angefordert. Daher sind Speicherungen, die über die derzeit praktizierte Dauer für Unternehmenszwecke hinausgehen, kaum zu rechtfertigen.» De eerste kanttekening die ik bij deze uitkomst van dit rapport zou willen maken is dat elk land eigen opsporingsmethodieken en onderzoeksmethoden hanteert voor de opsporing en vervolging van strafbare feiten. Naast de informatie uit dit Duitse rapport staan de hierboven besproken bevindingen van de onderzoekers van de EUR, die in een heel andere richting wijzen. Een tweede kanttekening is dat het onderzoek is uitgevoerd in een tijd dat er in de meeste landen nog geen sprake was van het bewaren van verkeersgegevens voor opsporingsdoeleinden. De bewaargrond was primair gelegen in het gebruik van de betreffende gegevens voor bedrijfsdoeleinden. Mede uit een oogpunt van kostenbeheersing worden gegevens niet langer bewaard dan uit een oogpunt van bedrijfsvoering strikt noodzakelijk is zo concludeert het onderzoek. Een rol kan derhalve spelen dat het wellicht doorgaans geen zin zou hebben gehad oudere gegevens te bevragen omdat deze niet meer voorhanden waren. De totstandkoming van de richtlijn illustreert dat juist om die reden gewerkt is aan Europese regels inzake een bewaarplicht. De Richtlijn dataretentie biedt de lidstaten de mogelijkheid te kiezen voor een bewaartermijn van minimaal zes en ten hoogste vierentwintig maanden. Deze bandbreedte weerspiegelt de uiteenlopende preferenties van de lidstaten op dit gebied. Inmiddels heeft een aantal van de landen die in het onderzoek betrokken waren wetgeving aanvaard waarin wordt voorzien in uitéénlopende bewaartermijnen. Op deze keuzes wordt hieronder in paragraaf 6 nader ingegaan.

2.4 De bewaring van locatiegegevens

De leden van de CDA-fractie merkten op dat in de memorie van toelichting wordt uitgelegd dat het noodzakelijk is om alle locatiegegevens gedurende een communicatie vast te leggen. Dit zou zijn ingevoerd op voordracht van de aanbieders, als alternatief voor een verplichte registratie van de «prepaidbeller». Deze leden constateerden dat invoering van deze extra gegevens nogal wat voeten in aarde heeft en zouden hierover graag een toelichting tegemoet zien. De leden van de VVD-fractie hebben zich afgevraagd op welke momenten de locatiegegevens bewaard moeten worden. Zij vroegen zich af of dit alleen het begin van de verbinding betreft of ook het einde en wellicht ook gedurende de verbinding, en hebben op dit punt om een nadere toelichting gevraagd.
Het punt van de bewaring van locatiegegevens verdient inderdaad enige nadere toelichting. De bewaring van locatiegegevens is thans al geregeld in het Besluit bijzondere vergaring nummergegevens. Ingeval een aanbieder niet kan voldoen aan zijn verplichting om op vordering van een bevoegde autoriteit gegevens over een gebruiker van telecommunicatie te verstrekken, dient hij deze door een analyse van zijn bestanden te achterhalen. Dit doet zich voor wanneer de gegevens over een gebruiker van telecommunicatie bij de aanbieders niet zijn geregistreerd. Dit is het geval bij vooruit betaalde mobiele telefonie (prepaid cards). Gegevens die in het kader van dit Besluit voor een periode van drie maanden bewaard moeten worden, zijn: de tijdstippen waarop telecommunicatie heeft plaatsge-

vonden, de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers en bij welk basisstation elk van deze gegevens zijn binnengekomen. Om een bestandsanalyse te kunnen verrichten zal de aanbieder over meerdere locatiegegevens moeten kunnen beschikken, ten behoeve van de «match» met het tweetal door de bevoegde autoriteiten aan te leveren tijdstippen. De aanbieders hebben destijds zelf deze methode om gebruikersgegevens te achterhalen aangedragen, omdat zij een registratieplicht van gebruikers van prepaid cards wilden voorkomen. Voor de goede orde wordt daarbij opgemerkt dat de bestandsanalyse door de aanbieders zelf wordt uitgevoerd aan de hand van de door hen te bewaren gegevens. Uitgangspunt van de voorgestelde wettelijke regeling is dat voorkomen moet worden dat de groep van gebruikers die gebruik maakt van vooruitbetaalde diensten bij mobiele telecommunicatie buiten de reikwijdte van de richtlijn komt te vallen. Voor deze gegevens wordt nu voorgesteld de bewaarplicht uit te breiden van drie naar achttien maanden. Dit is voorzien in het voorgestelde derde lid van artikel 13.4. van de Telecommunicatiewet. Hiervoor is gekozen om in de bewaartermijn van de gegevens geen verschillen te laten bestaan. Dit wordt in de toelichting bij het wetsvoorstel aangegeven. De voorgestelde verlenging van de bewaartermijn van drie maanden tot achttien maanden zal overigens niet tot buitenproportionele meerkosten leiden. Het gaat daarbij vooral om de investeringskosten van extra geheugen.

2.5 De consequenties van de bewaarplicht voor de feitelijke mogelijkheden voor de bevoegde autoriteiten om gegevens op te vragen

De leden van de SP-fractie constateerden dat de richtlijn er niet aan in de weg staat dat de te bewaren gegevens worden gebruikt voor andere doelen en hebben gevraagd of dit gevolgen heeft voor in Nederland bewaarde gegevens die door een buitenlandse autoriteit worden opgevraagd.
In antwoord hierop kan worden opgemerkt dat de richtlijn er inderdaad niet aan in de weg staat dat de te bewaren gegevens worden gebruikt voor andere doelen. Dit speelt echter geen rol indien in Nederland bewaarde gegevens door een buitenlandse autoriteit worden opgevraagd. Zoals hierboven is vermeld, naar aanleiding van een vraag van de leden van de CDA-fractie, kunnen gegevens in een dergelijk geval uitsluitend worden verstrekt op basis van een rechtshulpverzoek, ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. Alsdan is geen sprake van gebruik voor andere doelen dan waarvoor de bewaarplicht in het leven is geroepen, namelijk de opsporing en vervolging van ernstige strafbare feiten.

2.6 Gegevensbescherming en gegevensbeveiliging

De leden van de VVD-fractie wezen erop dat in de memorie van toelichting in het kader van de gegevensbescherming en gegevensbeveiliging wordt aangegeven dat er bij algemene maatregel van bestuur nadere regels gesteld *kunnen* worden inzake de voorschriften voor de door de aanbieders te treffen passende technische en organisatorische maatregelen. Zij vroegen in hoeverre ik voornemens ben in de nabije toekomst van deze mogelijkheid gebruik te maken en of ik nader inzicht kan geven in de strekking van deze voorschriften.
De beide vragen kan ik bevestigend beantwoorden. In het ontwerpbesluit dataretentie worden nadere regels gesteld over de bescherming en de beveiliging van de te bewaren telecommunicatiegegevens. Daarvoor wordt nauw aangesloten bij de bestaande regels van het Besluit beveiliging gegevens aftappen telecommunicatie, dat gedetailleerde regels bevat voor de beveiliging van gegevens die de aanbieders verwerken in het kader van het verlenen van medewerking aan de uitvoering van een

vordering of een verzoek tot het aftappen of opnemen van telecommunicatie en het verstrekken van informatie aan een bevoegde autoriteit naar aanleiding van een vordering dan wel een verzoek tot het verstrekken van verkeersgegevens. Dit besluit bevat een aantal kernelementen, zoals een specificering van de aspecten waarop de beveiligingsmaatregelen zich moeten richten, de vastlegging van die maatregelen in een beveiligingsplan, de inschakeling van «gescreend» personeel bij de uitvoering van verzoeken om informatie en het betrachten van geheimhouding door de betrokken personeelsleden. Het ontwerpbesluit dataretentie, dat ter informatie bij deze nota is gevoegd, zal binnenkort voor advies kunnen worden voorgelegd aan de Raad van State.

2.7 Het toezicht op de gegevensverwerking

De leden van de VVD-fractie hebben zich afgevraagd in hoeverre de werkzaamheden van verschillende toezichthouders en handhavende autoriteiten in de praktijk zullen overlappen. Zij hebben geïnformeerd of, bij samenloop van toezichtactiviteiten of opsporing en handhaving, één van de betrokkenen voorrang heeft en hoe de verantwoordelijkheidsverdeling van de verschillende diensten daarbij ligt.
Het toezicht op de naleving van verplichtingen op grond van hoofdstuk 13 van de Telecommunicatiewet geschiedt door het Agentschap Telecom. Dit betreft de verplichtingen inzake de aftapbaarheid en het op een veilige wijze bewaren en overleggen van de gegevens aan bevoegde instanties. Het Agentschap Telecom kan ingrijpen indien blijkt dat aanbieders niet aan deze verplichtingen voldoen. Om dubbel toezicht te voorkomen is met het college van de Opta afgesproken dat het Agentschap ook het toezicht op artikel 11.5 en artikel 11.5a van de Telecommunicatiewet zal overnemen van het college van de Opta. Dat artikel biedt de aanbieders de mogelijkheid verkeersgegevens te bewaren voor de duur van hun administratieve processen (zo willen klanten vaak een gespreksoverzicht bij hun rekening). Omdat dit veelal dezelfde gegevens betreft als die welke nu op grond van de Richtlijn dataretentie bewaard moeten worden ligt het voor de hand dat het toezicht daarop bij één instantie plaatsvindt.
Het College bescherming persoonsgegevens heeft op grond van de Wet bescherming persoonsgegevens, ongeacht de rol van andere toezichthouders, de mogelijkheid om nader onderzoek te plegen. Het College doet dit op grond van signalen uit de samenleving en eigen inschatting van risico's. Het College heeft aangegeven mee te willen denken met de toezichtsystematiek van het Agentschap, zodat het vertrouwen kan hebben in de systematiek van regulier toezicht, maar behoudt zich het recht voor om op grond van signalen eigen onderzoek te doen. Daarnaast zullen het Agentschap Telecom en het College afspraken maken over eventueel gezamenlijk toezicht, dan wel over toezichtactiviteiten bij dezelfde partij. Het toezicht op de rechtmatige bevraging van de bewaarde gegevens geschiedt op dezelfde wijze als bij de thans reeds bestaande verplichtingen gebeurt. Hierop is uitgebreid ingegaan bij de beantwoording van vragen naar aanleiding van de Evaluatie van Hoofdstuk 13 van de Telecommunicatiewet (Kamerstukken II 2006/07, 30 517). Naast bestuursrechtelijke handhaving kunnen de bepalingen die bij of krachtens hoofdstuk 13 van de Telecommunicatiewet worden gesteld ook strafrechtelijk worden gehandhaafd. Daartoe zijn strafbepalingen opgenomen in de Wet op de economische delicten. Uitgangspunt bij handhaving is dat het accent vooral ligt op bestuursrechtelijke handhaving. Strafrechtelijke handhaving vindt eerst plaats als de bestuursrechtelijke middelen minder effectief blijken te zijn.

De leden van de CDA-fractie spraken, onder verwijzing naar de definitie in de Van Dale, hun verbazing uit over het feit dat in de memorie van toelichting is aangegeven dat geen eenduidige termijn kan worden vastgesteld voor het begrip «onverwijld». Gezien het belang van een snelle afhandeling van een informatieverzoek hebben de leden van deze fractie verzocht om een toelichting op de concrete termijnen en wat de bestaande afspraken met de aanbieders hierover inhouden. Ook de leden van de fractie van de VVD zouden graag een nadere toelichting willen krijgen over het begrip «onverwijld». Zij vonden de toelichting op het wetsvoorstel weinig concreet op dit punt en hebben gevraagd of ik kan instemmen met een uitleg van onverwijld als «te verstrekken binnen twee dagen».
Met de leden van de CDA-fractie onderschrijf ik het belang van een snelle afhandeling van informatieverzoeken. Het is dan ook mijn streven de uitwisseling van gegevens tussen de aanbieders enerzijds en de opsporings- en inlichtingen- en veiligheidsdiensten (of: de behoeftestellers) anderzijds zoveel mogelijk geautomatiseerd te laten verlopen. Dat bevordert niet alleen de snelheid van de gegevensuitwisseling maar ook de uniformiteit en de kwaliteit van die uitwisseling. De termijnen waarop de gegevens beschikbaar komen voor de opsporing verschillen thans naar de aard van de gegevens en zijn mede afhankelijk van de inrichting van de bedrijfsvoering en de stand van de techniek in het bedrijf van de betreffende aanbieder. Het begrip «onverwijld» in de richtlijn en in het voorgestelde artikel 13.4, eerste lid, van de Telecommunicatiewet wordt thans opgevat als «zo spoedig als de inrichting van de bedrijfsvoering en de stand der techniek van het betreffende bedrijf dat mogelijk maakt». In deze opvatting zie ik geen wezenlijk verschil met de betekenis die Van Dale aan het begrip onverwijld geeft. Immers, het is de aanbieders niet toegestaan de behandeling van een verzoek om informatie uit te stellen tot een door hen nader te bepalen moment. De afspraken over de termijnen van afhandeling van de verzoeken om informatie verschillen op dit moment per aanbieder of groep van aanbieders en zijn mede afhankelijk van het netwerk waarvan gebruik wordt gemaakt en de diensten van de aanbieder. Verkeersgegevens worden thans in beginsel binnen vijf dagen geleverd. In noodgevallen kan de aanbieder worden verzocht verkeersgegevens eerder te leveren. Een algemene verplichting om een verzoek om informatie binnen twee dagen af te handelen is, gelet op de stand der techniek van een aantal aanbieders, thans niet haalbaar.

De leden van de SP-fractie konden enig begrip opbrengen voor de terughoudendheid die de regering betracht bij het vaststellen van een harde termijn voor het aanleveren van de gegevens door de aanbieders, en de keuze die is gemaakt voor het woord «onverwijld». Toch vreesden deze leden dat hier in een enkel geval een meningsverschil over kan ontstaan en achtten het misschien toch raadzaam termijnen bekend te maken waarnaar de aanbieders zich zouden moeten richten. Daarbij hebben zij de vraag opgeworpen hoe om te gaan met eventuele meningsverschillen en wanneer de handhavingsmogelijkheden, zoals een bestuurlijke boete, moeten worden ingezet.
Op de vragen over de termijn voor de levering van de gegevens ben ik hierboven, naar aanleiding van de vragen van de fractie van het CDA, reeds ingegaan. Voor de beantwoording van de vraag van de SP-fractie wil ik daarnaar verwijzen. Naar aanleiding van de gestelde vragen over de handhavingsmogelijkheden kan worden opgemerkt dat de nadere afspraken over de termijnen van aanlevering van de gegevens, waar ook in de memorie van toelichting naar is verwezen, geen wettelijke status hebben. Dit betreffen afspraken tussen de behoeftestellers enerzijds en de aanbieders anderzijds. Ingeval van niet-naleving van deze afspraken door een aanbieder kan er, bij ernstige termijnoverschrijding, in afzonderlijke

gevallen sprake zijn van het niet voldoen aan de verplichting tot levering van verkeersgegevens, als bedoeld in het voorgestelde artikel 13.2b van de Telecommunicatiewet. De Telecommunicatiewet biedt de mogelijkheid tot het opleggen van een bestuurlijke boete (artikel 15.4 Telecommunicatiewet) door de Minister van Economische Zaken, van ten hoogste 450 000 euro. Daarnaast wordt de opzettelijke niet-nakoming van de bewaarplicht strafbaar gesteld op grond van artikel 1, onder 2°, van de Wet op de economische delicten. Dit betreft een misdrijf dat kan worden bestraft met een gevangenisstraf van ten hoogste twee jaren of een geldboete van de vierde categorie (ten hoogste 16 750 euro). Het voorgaande neemt echter niet weg dat, ingeval van meer structurele vormen van termijnoverschrijding door de aanbieders, overwogen zal moeten worden om te komen tot wettelijke vastlegging van de termijnen en afzonderlijke strafbaarstelling van niet-naleving van de termijnen op grond van de Wet op de economische delicten. Daarvoor kan gebruik worden gemaakt van de algemene maatregel van bestuur, bedoeld in artikel 13.4, vierde lid, van het wetsvoorstel. Overtreding van voorschriften, gesteld bij of krachtens artikel artikel 13.4, vierde lid, van de Telecommunicatiewet, vormt een economisch delict en is strafbaar gesteld in artikel 1, onder 4°, van de Wet op de economische delicten. De naleving van de gestelde termijnen als zodanig kan dan onderwerp vormen van het toezicht door de Minister van Economische Zaken, waarbij in de daarvoor aangewezen gevallen tevens kan worden opgetreden op grond van de Wet op de economische delicten.

De leden van de PvdA-fractie hebben aangegeven het essentieel te vinden dat de gegevens door providers zelf worden bewaard en dat justitie verzoeken indient voor inzage in deze gegevens. Dat is, conform de richtlijn, nu geregeld in het wetsvoorstel, tot tevredenheid van deze leden. Deze leden vroegen of de vrees van telecomoperators dan ook ongegrond is dat in een later stadium, middels lagere regelgeving, alsnog kan worden overgegaan tot een centrale opslag. Zij vonden centrale opslag ongewenst omdat decentrale opslag door de providers en operators bijdraagt tot meer veiligheid en zorgvuldigheid en hebben gevraagd of de regering deze opvatting deelt.
De regering kan de opvatting, dat decentrale opslag van de bewaarde gegevens uit de aard der zaak bijdraagt tot meer veiligheid en zorgvuldigheid, vooralsnog niet delen. De veiligheid van de gegevensopslag en de zorgvuldigheid van de raadpleging van die gegevens zal niet persé afhankelijk zijn van de vraag of decentrale of centrale opslag plaatsvindt maar zal in hoge mate afhankelijk zijn van het stelsel van regelgeving, de naleving van die regels door betrokkenen en het toezicht daarop. Het is binnen de voorgestelde regeling niet uitgesloten dat de aanbieders ervoor kiezen de te bewaren gegevens bij een derde partij op te slaan die dan vervolgens als bewerker van die gegevens fungeert, onder verantwoordelijkheid van de aanbieder. Er zou dan de facto een situatie kunnen ontstaan dat de gegevens van verschillende aanbieders op dezelfde plaats worden bewaard. Verder moet worden bedacht dat het mogelijk is te kiezen voor een model van decentrale opslag van de gegevens door de aanbieders, waarbij echter vanaf een centraal punt toegang kan worden verkregen tot de bewaarde gegevens in die gevallen waarin aan de wettelijke voorwaarden is voldaan. Gelet op de implementatietermijn en het feit dat een eventuele keuze voor een andere optie intensieve afstemming en overleg over alle organisatorische en technische aspecten vereist, wordt in het wetsvoorstel uitgegaan van de opslag en beschikbaarstelling van de bewaarde gegevens door de aanbieders zelf. De aanbieders kunnen wel, in overleg met de overheid, zelf besluiten om de gegevens op een centraal punt op te slaan, bijvoorbeeld door middel van opslag bij een derde partij die dan vervolgens als bewerker van die gegevens fungeert, onder verantwoordelijkheid van de betreffende aanbieder. De vrees van de aanbieders dat de overheid in een later stadium – kennelijk zonder hun betrokkenheid

– middels lagere regelgeving alsnog kan overgaan tot het verplicht stellen van een centrale opslag is echter niet gegrond. Dit zou een aanpassing van de wettelijke grondslag vereisen waarin de aanbieders zeker betrokken moeten worden.

De leden van de VVD-fractie wezen erop dat onderzoek is gedaan naar de verschillende organisatorische varianten voor opslag van gegevens en hebben gevraagd naar de concrete bevindingen van dit onderzoek. Tevens vroegen zij of er nader gevolg zal worden gegeven aan de bevindingen van dit onderzoek, bijvoorbeeld door het verrichten van nader onderzoek.
In antwoord op deze vragen merk ik op dat het onderzoek door het bureau VKA primair was gericht op het verzamelen van informatie over de technische en organisatorische aanpassingen bij aanbieders en behoeftestellers die bij toepassing van verschillende implementatieopties van de bewaarplicht en de daarmee samenhangende bevraging noodzakelijk zijn, inclusief de daaraan verbonden kosten. In het onderzoek hebben verschillende implementatieopties centraal gestaan. De opzet van dit onderzoek was om op basis van de resultaten daarvan in overleg met de betrokken departementen en de aanbieders de eventuele alternatieven naar voorkeur te rangschikken. Gelet op de krappe implementatietermijn en de voorkeuren aan de zijde van de aanbieders is er in het wetsvoorstel voor gekozen om uit te gaan van de bestaande situatie, dat wil zeggen dat de te bewaren gegevens door de aanbieders worden opgeslagen en beschikbaar gehouden voor politie en justitie. Dit laat overigens onverlet dat de aanbieders op vrijwillige basis kunnen kiezen voor opslag bij een derde partij, zoals hierboven naar aanleiding van de vraag van de PvdA-fractie uitéén is gezet. Vooralsnog is er geen voornemen voor nader onderzoek waarbij de vraag centraal staat van centrale dan wel decentrale opslag van gegevens. Wel is de overheid thans in goed overleg met de aanbieders over de verdere uitvoering van de Richtlijn dataretentie.
Op de vraag van de leden van de VVD-fractie om een nadere toelichting op het begrip onverwijld ben ik hierboven, mede naar aanleiding van vragen van de CDA-fractie over dit onderwerp, reeds nader ingegaan. Voor de beantwoording van de vraag van de VVD-fractie wil ik daarnaar verwijzen.

2.9 Statistische informatie

De leden van de VVD-fractie vroegen nader inzichtelijk te maken welke gegevens zullen worden geregistreerd om te kunnen voldoen aan de eis van de richtlijn inzake statistische informatie en of hierbij sprake is van een registratieplicht. Voorts vroegen deze leden of de aanbieders ook een verplichting hebben tot registratie van de verzoeken door de bevoegde autoriteiten, en of ik met de hen van mening ben dat deze registratie (wettelijk) verplicht dient te worden. Tenslotte vroegen deze leden in hoeverre de evaluatie naar de effectiviteit ook het inzichtelijk maken van het aantal verzoeken door de verschillende autoriteiten omvat.
In antwoord op deze vragen merk ik op dat de Richtlijn dataretentie aan de lidstaten aan de lidstaten de verplichting oplegt tot het registeren van bepaalde informatie. Deze informatie heeft betrekking op (1) de gevallen waarin gegevens aan de bevoegde autoriteiten zijn verstrekt, (2) de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop door de bevoegde autoriteiten om overdracht ervan is verzocht en (3) de gevallen waarin verzoeken niet konden worden ingewilligd. De evaluatie zal ook het aantal verzoeken om verstrekking van de gegevens aan de bevoegde autoriteiten zal omvatten. Deze gegevens zullen dus moeten worden geregistreerd om aan de richtlijn te voldoen.
Op dit moment kent Nederland geen algemene registratie van gegevens omtrent het gebruik van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Wel wordt door het Centraal

informatiepunt onderzoek telecommunicatie een registratie gevoerd van de actuele gebruikersgegevens, die door tussenkomst van dit orgaan aan de bevoegde autoriteiten worden verstrekt. De richtlijn noopt dus tot aanvullende maatregelen. De leden van de VVD-fractie hebben er terecht op gewezen dat uit de toelichting niet blijkt op welke wijze en termijn dit ook daadwerkelijk plaats zal vinden. De bewaarplicht wordt ingevoerd ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige strafbare feiten. Het ligt dan ook in de rede dat voor de registratie van de statistische gegevens in eerste instantie een beroep wordt gedaan op de desbetreffende behoeftestellende diensten. Zij zullen bij uitstek in staat zijn om inzicht te verschaffen in de gevallen waarin gegevens aan de bevoegde autoriteiten zijn verstrekt en de gevallen waarin verzoeken niet konden worden ingewilligd. Het is thans echter niet zeker dat dit ook geldt voor de gegevens over de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop door de bevoegde autoriteiten om overdracht ervan is verzocht. Niet uitgesloten is dat dergelijke gegevens slechts kunnen worden verkregen door het combineren van gegevens van aanbieders en van behoeftestellers. Alsdan zou voor die gegevens kunnen worden gekomen tot een registratieplicht voor de aanbieders. Uitgangspunt voor nadere regels zal in ieder geval zijn dat de gegevens door de desbetreffende behoeftestellende diensten beschikbaar worden gesteld, maar dat nader zal moeten worden onderzocht op welke wijze het verzamelen en verwerken van de benodigde gegevens kan worden georganiseerd opdat een betrouwbare en efficiënte registratie wordt gerealiseerd die de bedrijfsvoering van de aanbieders zo weinig mogelijk belast.
Naar aanleiding van de vragen over het loggen van de gegevens merk ik op dat ik vooralsnog weinig aanleiding zie voor een wettelijke verplichting voor de aanbieders tot vastlegging van gegevens omtrent de verzoeken van de bevoegde autoriteiten. Aan een dergelijke vastlegging zijn veiligheidsrisico's verbonden, omdat dergelijke gegevens in handen kunnen komen van onbevoegden. Een dergelijke verplichting is ook thans niet voorgeschreven voor de verstrekking van verkeersgegevens op grond van een vordering of verzoek van de bevoegde autoriteiten. Alleen indien niet op andere wijze voldaan kan worden aan de eisen van de richtlijn om statistische informatie te verschaffen zal een dergelijke verplichting voor de aanbieders worden overwogen.

De leden van de VVD-fractie vroegen een nadere toelichting om het advies van de Raad van State, de evaluatie ook betrekking te laten hebben op de mogelijkheden van de inlichtingen- en veiligheidsdiensten om gegevens op te vragen, niet over te nemen. Deze leden hebben ook gevraagd of het opvragen van gegevens door inlichtingen- en veiligheidsdiensten zelf wel wordt geregistreerd en inzichtelijk gemaakt ter evaluatie voor de commissie voor inlichtingen- en veiligheidsdiensten. De leden van de SP-fractie constateerden dat de informatie over de toepassing van de bevoegdheden door de inlichtingen- en veiligheidsdiensten als staatsgeheim wordt beschouwd. Zij begrepen niet goed waarom statistische informatie staatsgeheim zou moeten zijn en vroegen waarom deze informatie niet openbaar is.
In antwoord op deze vragen kan ik melden dat de evaluatie naar de effectiviteit van de bewaarplicht door de Commissie ook het aantal verzoeken om verstrekking van de gegevens aan de bevoegde autoriteiten zal omvatten. Deze evaluatie vloeit voort uit de Richtlijn dataretentie, die bepaalt dat de Commissie uiterlijk op 15 september 2010 aan het Europees Parlement en de Raad een evaluatieverslag uitbrengt over de toepassing van de richtlijn teneinde na te gaan of het nodig is de richtlijn aan te passen, in het bijzonder voor wat betreft de lijst van de te bewaren gegevens en de bewaartermijnen (artikel 14). Daartoe schrijft de Richtlijn dataretentie voor dat de lidstaten jaarlijks aan de Commissie statistische infor-

matie verstrekken over de bewaarplicht, onder meer de gevallen waarin overeenkomstig de toepasselijke wetgeving gegevens zijn verstrekt aan de bevoegde autoriteiten (artikel 10). De richtlijn is van toepassing op de bewaring van gegevens ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige strafbare feiten en heeft geen betrekking op de taakuitvoering van de inlichtingen- en veiligheidsdiensten. De Europese Unie heeft geen competentie met betrekking tot aangelegenheiden betreffende de nationale veiligheid van de lidstaten, zoals recent in het in Lissabon getekende wijzigingsverdrag ook uitdrukkelijk is vastgelegd. Gelet op het toepassingsbereik van de richtlijn valt het gebruik van de bewaarde gegevens ten behoeve van de taakuitvoering door de inlichtingen- en veiligheidsdiensten dan ook buiten de evaluatieverplichting. Bovendien zou daarmee inzicht kunnen worden verkregen in de operationele werkwijze van de diensten. Zo kan aan de hand van de fluctuatie in de cijfers over de inzet van bijzondere bevoegdheden door inlichtingen- en veiligheidsdiensten over de jaren heen inzicht worden verkregen in de aard en omvang van de toepassing van de desbetreffende bijzondere bevoegdheid alsmede in de mate van toepasbaarheid; en daarmee ook in de effectiviteit van de desbetreffende bevoegdheid voor een inlichtingen- en veiligheidsdienst, hetgeen met het oog op de nationale veiligheid en het effectief kunnen opereren van inlichtingen- en veiligheidsdiensten dan ook geheim dient te blijven. Om deze reden kan over de toepassing van de bevoegdheden door de diensten uitsluitend vertrouwelijk verantwoording worden afgelegd aan de commissie van de inlichtingen- en veiligheidsdiensten van de Tweede Kamer. Die procedure geldt onverkort voor het opvragen van verkeersgegevens door de diensten. Of het opvragen van gegevens door inlichtingen- en veiligheidsdiensten wel wordt geregistreerd en inzichtelijk gemaakt ter evaluatie door de commissie voor de inlichtingen- en veiligheidsdiensten betreft vooraleerst de verantwoordelijkheid van de commissie zelf, en staat los van de implementatie van de richtlijn, zodat daarover in dit kader geen uitspraken worden gedaan.

De leden van de VVD-fractie merkten op dat voor een nadere uitwerking inzake registratie wordt verwezen naar een nader op te stellen amvb. Zij meenden dat politie en OM die gegevens moeten registreren, maar uit de toelichting blijkt niet op welke wijze en termijn dit ook daadwerkelijk plaats zal vinden. Zij stelden daarom voor de algemene maatregelen van bestuur te onderwerpen aan een voorhangprocedure zodat de inhoud ook voorgelegd wordt aan de Kamer.
Hierboven heb ik, naar aanleiding van vragen van deze leden, reeds uiteengezet dat het uitgangspunt voor nadere regels zal zijn dat de gegevens door de behoeftestellende diensten beschikbaar worden gesteld maar dat nader zal moeten worden onderzocht op welke wijze het verzamelen en verwerken van de benodigde gegevens kan worden georganiseerd opdat een betrouwbare en efficiënte registratie wordt gerealiseerd die de bedrijfsvoering van de aanbieders zo weinig mogelijk belast.
Naar aanleiding van een vraag van de leden van de CDA-fractie over een mogelijke voorhangprocedure voor het ontwerp voor een besluit dataretentie is dit ontwerp-besluit, in de versie zoals die in consultatie is gegeven, bij deze nota gevoegd. Ingeval er aanleiding zou bestaan tot het stellen van nadere regels bij algemene maatregel van bestuur in verband met de beschikbaarstelling van gegevens door aanbieders ten behoeve van de registratie van statistische gegevens, zal ik deze wijziging van de algemene maatregel van bestuur eveneens ter informatie aan Uw Kamer zenden.

3. De toegang tot de bewaarde gegevens

3.1 De verstrekking van bewaarde gegevens aan bevoegde autoriteiten in Nederland

De leden van de SP-fractie vroegen of er al gebruik is gemaakt van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering, waarmee een geautomatiseerd gegevensbestand kan worden gevorderd indien dit de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft. Ook vroegen zij om een toelichting op het door het College bescherming persoonsgegevens ingebrachte bezwaar dat artikel 126hh mogelijk strijd oplevert met artikel 4 van de richtlijn, nu het bij artikel 126hh gaat om het onderling vergelijken en het in combinatie brengen van gegevens, en er niet kan worden gesproken van «welbepaalde gevallen» zoals vereist door artikel 4 van de richtlijn. Tenslotte vroegen deze leden of artikel 126hh in combinatie met de voorgestelde bewaarplicht opgevat kan worden als «datamining», het creëren van een grote hoeveelheid te bewaren gegevens waarin (preventief) gezocht gaat worden zonder dat er daadwerkelijk aanwijzingen zijn voor een dreigend gevaar. Een vergelijkbare vraag stelden zij over de gevolgen die de bewaarplicht heeft in combinatie met de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Zij vroegen naar concrete voorbeelden van het gebruik van de verkregen gegevens voor data-analyse. Deze leden merkten op dat het ook hier lijkt te gaan om «datamining», waartegen de leden van deze fractie bedenkingen hebben, en vroegen of deze wijze van analyse effectief en doeltreffend is, en niet verdergaand dan strikt noodzakelijk waarbij de persoonlijke levenssfeer zoveel mogelijk wordt beschermd. In antwoord op de gestelde vragen vermeld ik dat thans geen toepassingen van artikel 126hh bekend zijn. Over het door het CBP ingebrachte bezwaar dat artikel 126hh van het Wetboek van Strafvordering mogelijk strijd oplevert met artikel 4 van de richtlijn, merk ik op dat ik meen dat dit niet het geval is. Artikel 4 van de richtlijn dataretentie schrijft voor dat de lidstaten bepalingen aannemen om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen en in overeenstemming met de nationale wetgeving, aan de bevoegde autoriteiten worden verstrekt. Een verkennend onderzoek, in verband met aanwijzingen van het beramen of plegen van terroristische misdrijven, kan naar mijn oordeel worden beschouwd als een welbepaald geval, als bedoeld in de richtlijn. Mijns inziens wordt met de geldende wettelijke vereisten zeker voldaan aan de eisen van de richtlijn. De wettelijke vereisten houden namelijk in dat het moet gaan om een specifiek verkennend onderzoek dat pas gestart kan worden indien uit feiten en omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd en dat tot doel heeft om de opsporing van terroristische misdrijven voor te bereiden. De wettelijke regeling is, mede in het licht van het recht op de bescherming van de persoonlijke levenssfeer zoals dat onder meer is neergelegd in artikel 8 van het EVRM, met de nodige wettelijke waarborgen omgeven. Op grond van artikel 126hh is de officier van justitie bevoegd om na een voorafgaande schriftelijke machtiging van de rechter-commissaris, in het kader van een verkennend onderzoek naar terroristische misdrijven geautomatiseerde gegevensbestanden op te vragen bij derden, teneinde de in die bestanden opgenomen gegevens te bewerken. De gegevensbestanden kunnen worden doorzocht op bepaalde profielen en patronen van handelingen van personen voor de betreffende terroristische misdrijven van belang zijn. De verwerkte gegevens die niet van belang zijn voor het onderzoek dienen te worden vernietigd en mogen niet verder worden verwerkt. De stelling dat artikel 126hh van het Wetboek van Strafvordering in combinatie met de voorgestelde bewaar-

plicht opgevat kan worden als «datamining, in die zin dat een grote hoeveelheid te bewaren gegevens worden gecreëerd waarin (preventief) gezocht gaat worden zonder dat er daadwerkelijk aanwijzingen zijn voor een dreigend gevaar, onderschrijf ik dan ook niet. Anders dan de leden van de SP-fractie veronderstellen, is een dergelijk onderzoek niet mogelijk zonder dat er daadwerkelijk aanwijzingen zijn van het binnen een groep van personen beramen of plegen van terroristische misdrijven. Er is dus geen sprake van het preventief doorzoeken van gegevensbestanden zonder dat er enige aanwijzing bestaat voor het beramen of plegen van terroristische misdrijven; van een dergelijke aanwijzing kan wel degelijk een dreigend gevaar uitgaan. In elk geval wordt hiermee voldaan aan het vereiste van artikel 4 van de richtlijn, dat gegevens alleen in welbepaalde gevallen kunnen worden gebruikt.
Het voorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar terroristische en andere gevaren met betrekking tot de nationale veiligheid (Kamerstukken I 2005/06, 30 553, nr. A) voorziet in de bevoegdheid van de diensten om zich te wenden tot een aanbieder van communicatiediensten met het verzoek tot verstrekking van een gegevensbestand of delen van een geautomatiseerd gegevensbestand (artikel 29b). De uitoefening van deze bevoegdheid is echter aan stringente waarborgen gebonden. Zo dient de voor de dienst verantwoordelijke minister op een daartoe strekkend verzoek van het hoofd van de dienst daarvoor toestemming te verlenen. In dat verzoek dient onder meer aangegeven te worden waarom de uitlevering van de desbetreffende gegevensbestanden aan de dienst noodzakelijk is. De verkregen gegevens kunnen, indien voldaan is aan de daartoe in de Wiv 2002 opgenomen criteria, door de diensten worden gebruikt voor data-analyse, waaronder begrepen het samenbrengen of met elkaar in verband brengen van gegevens, onder meer door middel van het doorzoeken van gegevens aan de hand van profielen of het vergelijken van gegevens met het oog op de vaststelling van patronen. In artikel 12a van genoemd wetsvoorstel is bepaald dat indien deze gegevensbestanden uitsluitend zijn verstrekt ten behoeve van het doorzoeken aan de hand van profielen of met het oog op het opsporen van patronen, de gegevens die na deze verwerking niet meer relevant zijn voor het desbetreffende onderzoek van de dienst dienen te worden vernietigd; daarvan dient ook een verslag te worden opgemaakt. Concrete voorbeelden van een dergelijke werkwijze, zoals door de leden van de SP-fractie gevraagd, kunnen bezwaarlijk worden verstrekt vanwege het risico dat teveel zicht wordt gegeven op de operationele werkwijze van de diensten en hun actuele kennisniveau. De door deze leden gestelde vragen hebben in feite geen betrekking op de bewaarplicht van telecommunicatiegegevens als zodanig, maar op de doeltreffendheid en wenselijkheid van de toedeling van de hierboven beschreven bevoegdheden bij de bestrijding van terrorisme. Naar mijn oordeel dienen die vragen dan ook niet zozeer te worden beantwoord in het kader van het wetsvoorstel over de bewaarplicht van telecommunicatiegegevens maar in het kader van de betreffende wetgeving.

De leden van de VVD-fractie vroegen voor alle duidelijkheid nader inzicht te verschaffen in de autoriteiten die, na inwerkingtreding van voorliggend wetsvoorstel, bevoegd zullen zijn om het verzoek tot verstrekken van gegevens aan de aanbieder te doen.
In reactie op deze vraag wijs ik volledigheidshalve op paragraaf 3.2 van de memorie van toelichting, waarin een overzicht wordt gegeven van de huidige wetgeving op dit punt. Ten behoeve van de door de leden van de fractie van de VVD gewenste duidelijkheid kan de wettelijke regeling als volgt worden samengevat. Op grond van het Wetboek van Strafvordering is de officier van justitie bevoegd een vordering te doen tot verstrekking

van verkeersgegevens. Vereist is een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Naast de officier van justitie is de opsporingsambtenaar zelfstandig bevoegd een vordering te doen tot verstrekking van de zogenaamde gebruikersgegevens; dit betreft de gegevens inzake naam, adres, woonplaats, nummer en soort dienst. Vereist is een verdenking van een misdrijf of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd. Tot slot hebben de officier van justitie en de opsporingsambtenaar specifieke bevoegdheden in verband met de bestrijding van terrorisme. De officier van justitie is, ingeval van aanwijzingen van een terroristisch misdrijf, bevoegd tot het vorderen van verkeersgegevens. Naast de officier van justitie is de opsporingsambtenaar, ingeval van aanwijzingen van een terroristisch misdrijf, zelfstandig bevoegd tot het vorderen van gebruikersgegevens. Indien een verkennend onderzoek de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft, kan de officier van justitie geautomatiseerde gegevensbestanden laten verstrekken teneinde de hierin opgenomen gegevens te doen bewerken (artikel 126hh Sv.). Daarvoor is een schriftelijke machtiging van de rechter-commissaris vereist. Een dergelijke vordering kan ook aan aanbieders van elektronische communicatiediensten worden gericht.
Op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 zijn de Algemene inlichtingen- en veiligheidsdienst en de Militaire inlichtingen en veiligheidsdienst met inachtneming van de gestelde regels terzake bevoegd bij de aanbieders verkeersgegevens en gebruikersgegevens op te vragen. Zoals uit het voorgaande en uit paragraaf 3 van de memorie van toelichting blijkt, kunnen enerzijds ten behoeve van de opsporing van strafbare feiten gegevens worden gevorderd, hetgeen geregeld is in het Wetboek van Strafvordering, en anderzijds door de inlichtingen- en veiligheidsdiensten, hetgeen geregeld is in de Wiv 2002. In beide gevallen stelt de betreffende wetgeving precieze regels over de gevallen waarin en de voorwaarden waaronder dit kan plaatsvinden.

De leden van de VVD-fractie vroegen of er op dit moment al enig inzicht is in de frequentie waarbij gebruik is gemaakt van art. 126hh Wetboek van Strafvordering jegens aanbieders van telecommunicatiediensten of -netwerken en gegevens betreffende telecommunicatieverkeer. Ook vroegen zij aan te geven of, en zo ja op welke wijze, de «gegevens over een gebruiker» eventueel verschillen van «gegevens die bijdragen aan het identificeren van een persoon».
Voor de beantwoording van de vraag over de frequentie van het gebruik van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering verwijs ik naar hetgeen hierboven, naar aanleiding van een vraag van de fractie van de SP, is opgemerkt. Naar aanleiding van de vraag naar het onderscheid tussen identificerende gegevens en gebruikersgegevens geldt het volgende. Onder identificerende gegevens worden verstaan: naam, adres, woonplaats, geboortedatum, geslacht en administratieve kenmerken van een persoon. Bij administratieve kenmerken kan het gaan om een bankrekeningnummer, een klantnummer of een polisnummer. Een algemene regeling van de bevoegdheid tot het vorderen van identificerende gegevens bij derden maakt onderdeel uit van het Wetboek van Strafvordering (Wet bevoegdheden vorderen gegevens). Met behulp van identificerende gegevens kan worden vastgesteld wie de personen zijn waarop het onderzoek zich richt en welke verbanden er zijn tussen personen en tussen situaties en personen. Identificerende gegevens vormen dan ook de basis voor elk strafrechtelijk onderzoek. Wanneer het gaat om gebruikers van telecommunicatie, dient de in het Wetboek van Strafvordering opgenomen specifieke bevoegdheid van het vorderen van gebruikersgegevens te worden toegepast. Het begrip gebruikersgegevens

is specifiek gericht op het vorderen van telecommunicatie gegevens bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Gebruikersgegevens zijn gegevens betreffende naam, adres, woonplaats, nummer en soort dienst. Deze gegevens vertonen naar hun aard een grote gelijkenis met de identificerende gegevens en vervullen dezelfde functie. Het Wetboek van Strafvordering kende reeds bevoegdheden tot het vorderen van gebruikersgegevens voordat de meer algemene bevoegdheden tot het vorderen van identificerende gegeven van derden aan het wetboek werden toegevoegd. Op verzoek van de telecommunicatieaanbieders zijn de bevoegdheden tot het vorderen van gebruikersgegevens gehandhaafd, omdat zij er de voorkeur aan gaven te blijven werken met de hen bekende en specifiek op deze sector toegesneden bevoegdheden.

3.2 De beschikbaarheid van bewaarde gegevens aan bevoegde autoriteiten in het buitenland

De leden van de PvdA-fractie vroegen of op basis van dit wetsvoorstel ook rechtstreeks gegevens kunnen worden opgevraagd door opsporende instanties van andere lidstaten. Daarnaast wilden de leden van deze fractie graag weten in welke gevallen dat kan en of dat ook voor overtredingen van kleine aard kan, zoals bijvoorbeeld een overtreding van het auteursrecht.
In antwoord op de gestelde vragen merk ik vooraleerst op dat het voorliggende wetsvoorstel niet voorziet in de mogelijkheid dat gegevens door opsporingsinstanties van andere lidstaten rechtstreeks worden opgevraagd. Daarvoor is, zoals hierboven in antwoord op de vraag van de CDA-fractie aan de orde is gekomen, een rechtshulpverzoek vereist. De beschikbaarstelling van telecommunicatiegegevens aan opsporingsinstanties in andere landen wordt beheerst door de regels van het Wetboek van Strafvordering. Op grond van die regels kan de officier van justitie, ingeval van een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. Gelet op deze wettelijke eisen is de toegang tot de bewaarde gegevens voor politie en justitie beperkt tot ernstige misdrijven. Een eenvoudige overtreding van kleine aard, zoals een overtreding van het auteursrecht, valt daar niet onder.

3.3 De aansprakelijkheid van de aanbieders voor de beschikbaarstelling van de gegevens

De leden van de VVD-fractie vroegen in hoeverre een beroep op de wettelijke verplichting door de aanbieder in geval van een rechtszaak over de civielrechtelijke aansprakelijkheid inzake wanprestatie of onrechtmatige daad ook kans van slagen zal hebben wanneer achteraf is gebleken dat het verzoek tot verstrekken onrechtmatig was of de verstrekte gegevens teveel dan wel niet de gevraagde bleken te zijn.
In antwoord op de gestelde vragen merk ik op dat de door de VVD-fractie geschetste situatie, dat een aanbieder telecommunicatiegegevens beschikbaar stelt en vervolgens daar in rechte op wordt aangesproken door de betrokkene, niet of nauwelijks voorkomt. Een dergelijke situatie houdt niet zozeer verband met de bewaarplicht als zodanig als wel met de verplichting van de aanbieders om, onder bepaalde wettelijke voorwaarden, telecommunicatiegegevens te verstrekken aan de bevoegde autoriteiten. De regels over die verplichtingen zijn opgenomen in het Wetboek van Strafvordering, en de Wet op de Inlichtingen- en veiligheids-

diensten 2002. Op dit punt levert de bewaarplicht dus geen verandering op ten opzichte van de bestaande situatie. Overigens gelden wettelijke verplichtingen tot het beschikbaar stellen van gegevens aan de bevoegde autoriteiten, niet uitsluitend voor de aanbieders van telecommunicatiediensten, maar kunnen op grond van de artikelen 126nc tot en met 126ni van het Wetboek van Strafvordering ook anderen gehouden zijn gegevens te verstrekken aan de opsporingsambtenaar of de officier van justitie. Indien achteraf blijkt dat de vordering van gegevens onrechtmatig was, maar met de verstrekking van gegevens op correcte wijze is voldaan aan een vordering van de opsporingsambtenaar of de officier van justitie, is degene die de gegevens verstrekte niet aansprakelijk voor schade, wanneer deze zou ontstaan. Anders ligt het, indien niet op correcte wijze aan een vordering is voldaan. Afgezien van die situatie ligt de verantwoordelijkheid voor het vorderen en verstrekken van gegevens en voor de daarbij te maken afwegingen geheel bij de opsporingsambtenaar of de officier van justitie. Indien de opsporingsambtenaar of de officier van justitie – naar achteraf blijkt – gegevens heeft gevorderd over de verkeerde persoon dan wel dat teveel dan wel verkeerde gegevens zijn verstrekt, en deze persoon hierdoor schade zou kunnen lijden, dan ligt dit risico bij de opsporingsambtenaar of de officier van justitie en niet bij de instelling. Overigens is van civielrechtelijke aansprakelijkheid alleen sprake in geval van onrechtmatig handelen en in geval dit handelen de oorzaak is van de schade. In die gevallen waar het beroep op de wettelijke plicht stand houdt zijn, de leden van de VVD-fractie vroegen hiernaar, vervolgzaken tegen de staat te verwachten. De kans dat door een onrechtmatige vordering van gegevens daadwerkelijk schade ontstaat, is echter gering. Als gezegd, komt een dergelijke situatie niet of nauwelijks voor.

4. De verhouding tot het recht op bescherming van de persoonlijke levenssfeer

De leden van de CDA-fractie plaatsten een kanttekening bij de kritiek op de privacyinbreuk die met het bewaren van de telecommunicatiegegevens wordt gemaakt. In de CDA-visie zijn de verschillende vrijheden onlosmakelijk met elkaar verbonden. Wanneer iemand zich bedreigd voelt in zijn veiligheid heeft dit namelijk direct invloed op het privé-leven. Deze leden staan dan ook niet achter de kunstmatige tegenstelling tussen veiligheid en privacy die in verschillende reacties op de richtlijn wordt gepresenteerd. Vaak zijn er in strafrechtelijk kader juist mogelijkheden binnen het privé-leven nodig om de vrijheden te beschermen. De leden van de CDA-fractie vroegen om mijn reactie hierop. Verder waren deze leden van mening dat slechts het opvragen van de gegevens privacygevoelig is en niet het bewaren ervan, temeer daar de gegevens van technische aard zijn en over de inhoud van communicatie niets wordt vastgelegd. Deze leden meenden dat deze minimale inbreuk op de privacy in het belang van de opsporing ruimschoots opweegt tegen het belang van de bescherming van de persoonlijke levenssfeer.
De door de leden van de CDA-fractie naar voren gebrachte noties deel ik volledig. In het openbare debat worden de begrippen veiligheid en de persoonlijke levenssfeer vaak als uitersten gezien, alsof het een keuze betreft tussen het één of het ander. Dat is wat mij betreft niet het geval. Beiden zijn evenwel essentieel in onze rechtstaat. Bij beiden gaat het om de bescherming van burgers. De burger die telefonisch is bedreigd zal er weinig begrip voor hebben wanneer telecommunicatiegegevens, die inzicht kunnen geven in de identiteit van de beller, zijn vernietigd vanwege het privacybelang van hemzelf. Juist om zich in de maatschappij vrij te kunnen bewegen is het van belang dat de overheid kan optreden ten behoeve van de veiligheid van de burgers. Dat is een belangrijk rechtsstatelijk gegeven. Het voorgaande doet er niet aan af dat veiligheid en privacy aan elkaar kunnen raken. Dan is het van belang om te beoordelen

hoe de beide belangen zich tot elkaar verhouden op het moment dat zich nieuwe omstandigheden voordoen, zoals in dit geval dat de technische ontwikkelingen het voor de aanbieders mogelijk maken om verkeersgegevens van hun klanten te bewaren. Het belang van de veiligheid kan inmenging van de overheid in de persoonlijke levenssfeer rechtvaardigen voor zover bij de wet voorzien en voor zover in een democratische samenleving noodzakelijk in het belang van onder meer de nationale veiligheid en de openbare veiligheid. Daarbij is ook de aard van de te bewaren gegevens van belang. De gegevens die bewaard moeten gaan worden zijn inderdaad technisch van aard en worden doorgaans verspreid opgeslagen in de systemen van de aanbieders. De gegevens zijn, zoals hierboven in paragraaf 2.3 in antwoord op vragen van de leden van de PvdA-fractie aan de orde kwam, nog niet zo veelzeggend zo lang ze niet aan mogelijk strafbare gedragingen van personen kunnen worden gekoppeld. Over de inhoud van de communicatie wordt inderdaad niets vastgelegd. Ik ben dan ook van mening, zoals hierboven ook vermeld, dat de aantasting van de privacy, die door de bewaring van deze gegevens mee wordt gebracht, beperkt is. Die aantasting is vooral aan de orde bij de raadpleging van de gegevens. Daarvoor gelden thans reeds strikte wettelijke vereisten. Hierop ben ik in het voorgaande, naar aanleiding van vragen van de leden van de VVD-fractie, nader ingegaan. Op de afwegingen terzake van de duur van de bewaartermijn ben ik eveneens in het voorgaande ingegaan, bij de beantwoording van de vragen van de fracties van de PvdA, het CDA, de ChristenUnie, de SP en D66. Met de leden van de CDA-fractie meen ik dat het belang van een bewaarplicht van achttien maanden opweegt tegen de hierbij gemaakte afwegingen terzake van de persoonlijke levenssfeer.

De leden van de PvdA-fractie vroegen of de regering met hen van mening is dat de basisregel hoort te zijn dat schending van de privacy van burgers in de mate waarvan sprake is in dit wetsvoorstel pas aan de orde kan zijn als iemand in het kader van onderzoek door inlichtingen- en veiligheidsdiensten of in het kader van een strafrechtelijk onderzoek in beeld komt. In de memorie van toelichting wordt echter gesproken over de mogelijkheden om gegevensbestanden te onderzoeken op bepaalde profielen en patronen van handelingen van personen. Dat houdt in dat de privacy van eenieder in Nederland wordt geschonden om zodoende potentiële verdachten op het spoor te komen. De leden van de PvdA-fractie vroegen tevens of de regering het met hen eens is dat het zeer onwenselijk zou zijn als burgers in beeld komen bij de inlichtingendienst vanwege het simpele feit dat ze «verkeerde» websites bezocht hebben en dat er eerst voldoende aanwijzingen moeten zijn dat een burger betrokken is bij criminele of terroristische activiteiten alvorens wordt overgegaan tot het bestuderen van iemands persoonlijke telecommunicatiegegevens. Voorts informeerden zij of de regering de mening van deze leden deelt dat dit in strijd is met het rechtsbeginsel dat privacy pas in het geding kan komen bij concrete verdenkingen. Tenslotte vroegen deze leden of er sprake is van een toetsing of ook in de Nederlandse situatie de schending van de privacy gerechtvaardigd is indien die wordt afgewogen tegen de aard van de overtreding.
In antwoord op de gestelde vragen merk ik op dat ik de mening van de leden van de PvdA-fractie, dat de basisregel behoort te zijn dat schending van de privacy van burgers door toepassing van overheidsbevoegdheden pas aan de orde kan zijn als iemand in het kader van onderzoek door inlichtingen- en veiligheidsdiensten of in het kader van een strafrechtelijk onderzoek in beeld komt, als zodanig kan delen. Daarbij past echter een belangrijke kanttekening, namelijk dat de mate van betrokkenheid van die burger bij het plegen of beramen van ernstige feiten kan verschillen. Daarbij komt dat de inzet van strafvorderlijke bevoegdheden onder voorwaarden mogelijk is, juist om de personen die betrokken zijn bij het beramen of plegen van deze feiten op het spoor te komen. Ook kent het

Wetboek van Strafvordering bevoegdheden in geval van een vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd en in geval van aanwijzingen van terroristische misdrijven. De mening van deze leden, dat privacy pas in het geding kan komen bij concrete verdenkingen, deel ik dan ook niet. Deze leden kan ik bevestigen dat de beperking van de toegang tot de gegevens inderdaad beoogt te voorzien in een toetsing bij voorbaat of de beperking van de persoonlijke levenssfeer gerechtvaardigd is gelet op de aard van de overtreding. Het is niet wenselijk dat de gegevens in andere gevallen kunnen worden verstrekt ten behoeve van de opsporing en vervolging van strafbare feiten.
De leden van deze fractie verwezen naar de memorie van toelichting, waarin wordt gesproken over de mogelijkheden om gegevensbestanden te onderzoeken op bepaalde profielen of handelingen van personen, en vroegen of het niet zeer onwenselijk zou zijn als burgers in beeld komen bij de inlichtingendienst vanwege het simpele feit dat ze «verkeerde» websites bezocht hebben. Deze opmerking heeft kennelijk betrekking op het voorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar terroristische en andere gevaren met betrekking tot de nationale veiligheid. Dit wetsvoorstel voorziet in de bevoegdheid van de diensten om zich te wenden tot een aanbieder van communicatiediensten met het verzoek tot verstrekking van een gegevensbestand of delen van een geautomatiseerd gegevensbestand. Ik verwijs allereerst kortheidshalve naar hetgeen ik eerder in reactie op vragen van de leden van de VVD-fractie over deze bevoegdheid heb gesteld. Nu de door de fractie van de PvdA gestelde vragen geen betrekking hebben op de bewaarplicht van telecommunicatiegegevens als zodanig, maar op genoemd wetsvoorstel tot uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten bij de bestrijding van terrorisme dienen die vragen naar mijn oordeel dan ook te worden beantwoord in het licht van de behandeling van dat wetsvoorstel.
De leden van de SP-fractie stelden vast dat het in artikel 8 EVRM opgenomen recht op eerbiediging van de persoonlijke levenssfeer een belangrijk grondrecht is, en dat beperkingen hiervan bijzonder goed gemotiveerd moeten zijn. Zij hadden twijfels over de noodzaak van dit wetsvoorstel voor de strafrechtelijke handhaving van de rechtsorde en over de vraag of dit wetsvoorstel de toets van proportionaliteit en subsidiariteit kan doorstaan. Zij vonden de argumentatie voor een bewaartermijn van achttien maanden onvoldoende en vroegen, onder verwijzing naar de mening van onder meer de Raad van State, Actal, het College bescherming persoonsgegevens en de artikel-29 Werkgroep, om een reactie.
De gestelde vragen inzake de voorgestelde bewaartermijn, mede in relatie tot de eisen van artikel 8 EVRM, zijn hierboven in paragraaf 2.3, naar aanleiding van vragen van de verschillende fracties, reeds uitgebreid aan de orde gekomen. Op deze plaats moge ik dan ook volstaan met een verwijzing naar de beantwoording aldaar.

De leden van de SP-fractie betwijfelden de effectiviteit van de bewaarplicht van verkeersgegevens ten aanzien van het doel dat wordt nagestreefd, omdat deze plicht zal leiden tot inventieve methoden om te voorkomen dat gegevens bewaard kunnen worden. Zij vroegen of het bijvoorbeeld mogelijk is de bewaarplicht te omzeilen door gebruik te maken van webmail of door plaatsing van informatie op een publieke website. Ook vroegen zij naar het gebruik van Skype of van een niet beveiligd netwerk van een derde. Dit laatste zou vervelende gevolgen kunnen hebben, zoals een mogelijk verkeerde verdenking.
In reactie op de gestelde vragen moet voorop worden gesteld dat het voorliggende wetsvoorstel zeker beperkingen kent. Het aanbieden van applicaties, zoals Skype, valt als zodanig niet onder het begrip aanbieden

van openbare telecommunicatienetwerken of -diensten, als bedoeld in de Telecommunicatiewet. Indien echter met behulp van Skype een verbinding wordt gelegd met een vaste of mobiele telefoon, of andersom, dan vallen de betreffende verkeers- en locatiegegevens wel onder de bewaarplicht. Dit punt hangt echter niet zozeer samen met de inhoud van de bewaarplicht als wel met de reikwijdte van de Telecommunicatiewet en van de verplichtingen van de Richtlijn dataretentie, die zich beperken tot aanbieders van openbare elektronische communicatiediensten. Bij de beantwoording van eerdere vragen van de fracties van het CDA en de VVD, in paragraaf 2.2, heb ik reeds aangegeven dat de bewaarplicht niet in alle gevallen effectief zal zijn. Niettemin blijkt uit bijvoorbeeld het onderzoek van de Erasmus Universiteit en de impactstudie van de Commissie dat verkeers- en locatiegegevens van groot belang zijn in opsporingsonderzoeken. Het feit dat het wetsvoorstel niet aan 100% van de behoefte voldoet of kan voldoen, laat onverlet dat de informatie die wel verkregen wordt van groot belang is voor het onderzoeken, opsporen en vervolgen van ernstige misdrijven.

5. Rechtsbescherming

De leden van de PvdA-fractie vroegen of het wettelijk inzagerecht uit de Wet bescherming persoonsgegevens, wat inhoudt dat aanbieders op verzoek aan klanten overzichten moeten verstrekken met de opgeslagen en bewaarde gegevens, ook van toepassing is op de gegevens die in het kader van dit wetsvoorstel bewaard gaan worden. Ook hebben zij gevraagd of klanten straks het recht hebben de over hen opgeslagen gegevens bij hun aanbieder op te vragen. De leden van de fractie van de VVD vroegen of ik kan aangeven in hoeverre er wellicht misbruik door burgers zal worden gemaakt van het inzagerecht, in die zin dat er vaak een «volledig overzicht» verzocht zal worden en dit voor de aanbieders enorme (financiële) gevolgen heeft voor de bedrijfsvoering.
In antwoord op de gestelde vragen bevestig ik dat het wettelijk recht op inzage in de gegevens die over de betrokkene worden verwerkt, ingevolge de Wet bescherming persoonsgegevens onverkort geldt voor de gegevens die op grond van de voorgestelde bewaarplicht worden bewaard. Dit houdt in – zoals de leden van de PvdA-fractie opmerkten – dat aanbieders op verzoek van een klant overzichten moeten verstrekken van de bewaarde gegevens die op deze klant betrekking hebben. Hierbij kan worden opgemerkt dat de aanbieder van een universele dienst als vaste telefonie reeds gehouden is de abonnee of gebruiker een gespecificeerde factuur te leveren. Doorgaans zullen ook de andere aanbieders met een gespecificeerde rekening werken. Deze factuur zal de betrokkene reeds inzicht kunnen bieden in de relevante gegevens omtrent zijn belgedrag. In hoeverre er kans bestaat dat burgers misbruik zouden maken van het recht op inzage in de over hen verwerkte gegevens laat zich thans niet goed voorzien. Indien een verzoek om kennisneming echter disproportionele lasten met zich meebrengt zou de aanbieder dit verzoek kunnen weigeren in het belang van een goede bedrijfsvoering. Een dergelijke weigeringsgrond zal eerder kunnen worden ingeroepen indien de betrokkene door middel van een gespecificeerde factuur op de hoogte is of kan zijn van de verwerking van de betreffende gegevens of indien er steekhoudende aanwijzingen zijn dat het verzoek is gedaan zonder redelijk belang, bijvoorbeeld indien een verzoek periodiek wordt herhaald zonder dat blijkt van enig redelijk belang van hernieuwde kennisneming van de bewaarde gegevens.

De leden van de VVD-fractie vroegen of ik kan aangeven of, en zo ja door wie, op welke termijn en onder welke voorwaarden, het opvragen van gegevens over een persoon op enig moment ook aan betrokkene gemeld wordt.

Dat is inderdaad het geval. Op grond van artikel 126bb van het Wetboek van Strafvordering is de officier van justitie gehouden aan betrokkene schriftelijk mededeling te doen van de uitoefening van de bevoegdheid tot het vorderen van verkeersgegevens, zodra het belang van het onderzoek dat toelaat. De mededeling blijft achterwege indien uitreiking van de mededeling redelijkerwijs niet mogelijk is. Als betrokkene wordt aangemerkt de gebruiker van telecommunicatie waarmee de telecommunicatie plaatsvindt. Indien de betrokkene de verdachte is kan de mededeling achterwege blijven indien hij door middel van voeging in de processtukken of van melding van het gebruik van de bevoegdheid in de processtukken, van de bevoegdheidstoepassing op de hoogte raakt.

6. De situatie in andere EU-lidstaten

De leden van de SP-fractie gaven aan het niet eens te zijn met de regering dat de voorgestelde termijn van achttien maanden zich goed zou verhouden met de bewaartermijnen in andere lidstaten en vroegen of in de andere lidstaten ook onderzoek is verricht naar de effectiviteit van de bewaartermijn. De leden van deze fractie vroegen voorts op basis waarvan de afweging in de andere lidstaten kennelijk anders is uitgevallen en en wat de rechtvaardiging is voor een langere bewaartermijn in Nederland.
In antwoord op de gestelde vragen merk ik op dat de lengte van de bewaartermijn in de omringende landen verschilt. Gelet op de bandbreedte van de richtlijn, die een bewaartermijn voorschrijft van ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie, zal dit overigens geen verbazing behoeven te wekken. Het is thans echter niet eenvoudig om hiervan een betrouwbaar overzicht te krijgen, mede vanwege de uitéénlopende stand van zaken rond de implementatie van de richtlijn in de lidstaten. Op de situatie in het Verenigd Koninkrijk ben ik hierboven in paragraaf 2.3, bij de beantwoording van de vraag van de CDA-fractie, reeds nader ingegaan. Italië kent sinds 2003 een bewaarplicht voor telefoniedata van vierentwintig maanden, met een verlengingsmogelijkheid van vierentwintig maanden en voor internetdata een bewaarplicht van zes maanden, met een verlengingsmogelijkheid van zes maanden. In Duitsland is onlangs een wet van kracht geworden die voorziet in een bewaartermijn van zes maanden. Frankrijk kent, zoals in de memorie van toelichting reeds is gemeld, inmiddels een bewaartermijn van twaalf maanden. Spanje en Hongarije hebben onlangs eveneens een wettelijke bewaartermijn van twaalf maanden ingevoerd. Ierland kent thans een bewaartermijn van drie jaar voor telefoniegegevens; op grond van de richtlijn is Ierland dus verplicht tot verlaging van de bewaartermijn tot ten hoogste twee jaar. De Deense uitvoeringsregeling waar in de memorie van toelichting naar is verwezen, die voorziet in een bewaartermijn van een jaar, is met ingang van 15 september 2007 van kracht geworden. Letland heeft inmiddels een bewaartermijn van achttien maanden ingevoerd. In Finland is een wetsvoorstel in voorbereiding dat voorziet in een bewaartermijn van twaalf maanden. In België is bij wet geregeld dat de duur van de bewaring niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn. De vaststelling van de bewaartermijnen geschiedt bij Koninklijk Besluit, dat kan worden vastgesteld zodra een nieuwe regering is aangesteld. In Portugal, Roemenië, Litouwen zijn eveneens wetsvoorstellen in voorbereiding die voorzien in een bewaartermijn van twaalf maanden. In Slowakije is een wetsvoorstel in voorbereiding dat voorziet in een bewaartermijn van vierentwintig maanden voor telefoniegegevens en van zes maanden voor internetgegevens.
In vergelijking met landen als Duitsland, het Verenigd Koninkrijk en Frankrijk kent het Nederlandse voorstel een langere bewaartermijn. In vergelijking met Italië en Ierland kent het Nederlandse voorstel een kortere

bewaartermijn. Alles overziend meen ik dat Nederland met betrekking tot de lengte van de bewaartermijn niet uit de pas loopt met de omringende landen. Of in andere landen onderzoek is verricht naar de effectiviteit van de bewaartermijn is mij niet bekend. De keuze in de omringende landen voor een bepaalde bewaartermijn is naar ik aanneem, bepaald door de omstandigheden die voor deze landen gelden. Daarbij komt de bewaartermijn soms lager uit dan in Nederland en soms komt deze hoger uit dan in Nederland. De rechtvaardiging voor de bewaartermijn in Nederland is besproken in paragraaf 2.3.

7. Bedrijfseffecten

De leden van de CDA-fractie verzochten om een nadere motivering van de toelichting ten aanzien van de kosten van de bewaarverplichting. De leden van deze fractie zouden graag nadere uitleg ontvangen over wat concreet de extra kosten zijn voor het bedrijfsleven en in hoeverre de aanvraagvergoeding door de overheid hieraan tegemoet komt, bijvoorbeeld in percentages. Tenslotte vroegen zij naar concrete cijfers over het aantal aanvragen dat naar verwachting bij de aanbieders zal worden ingediend. Ook de leden van de PvdA-fractie vroegen wat de opslag van alle gegevens totaal gaat kosten en of de providers deze kosten moeten dragen. De leden van deze fractie vroegen voorts of daarmee geen sprake is van een aanzienlijke verzwaring van de administratieve lasten. Tenslotte vroegen zij hoeveel het zou kosten als de bewaarplicht slechts voor zes maanden gaat gelden en of de regering kan aangeven waarom zij de meerkosten voor een bewaarplicht van achttien maanden gerechtvaardigd vindt.
Wat concreet de extra kosten zijn voor het bedrijfsleven en in hoeverre de aanvraagvergoeding door de overheid hieraan tegemoet komt is, zoals in de memorie van toelichting ook is vermeld, slechts bij benadering aan te duiden. Aan het bureau Verdonck, Klooster & Associates BV (hierna ook te noemen: het bureau VKA) is gevraagd te berekenen wat de opslag van gegevens kost. De berekeningen van de lasten voor het bedrijfsleven in verband met het wetsvoorstel zijn gebaseerd op de bevindingen van het onderzoek door dit bureau. Volgens de methode voor het berekenen van de nalevingskosten zouden de kosten, die de aanbieders thans al maken voor het bewaren van gegevens voor eigen bedrijfsdoeleinden, van de door het bureau VKA gepresenteerde kosten dienen te worden afgetrokken. Over de hoogte van deze kosten is door de aanbieders echter geen informatie verschaft. Voor de berekeningen is dan ook uit gegaan van een zogenaamde «green field» situatie, dat wil zeggen dat de te bewaren gegevens door de aanbieders thans niet ten behoeve van de eigen bedrijfsdoeleinden worden opgeslagen. De werkelijke meerkosten zullen daarom aanzienlijk lager uitvallen.
Volgens de berekeningen van het bureau VKA bedragen de investeringskosten voor het bedrijfsleven bij de voorgestelde decentrale opslag, en bij een bewaartermijn van achttien maanden, in totaal 82 miljoen euro. De operationele kosten bedragen aanvankelijk 12 miljoen euro per jaar, maar zullen door een verwachte toename in het bevragingsvolume uiteindelijk uitkomen op 20 miljoen euro per jaar. In dit verband hebben de leden van de CDA-fractie ook gevraagd in hoeverre de aanvraagvergoeding van de overheid tegemoet komt, bijvoorbeeld in percentages, aan extra kosten voor het bedrijfsleven. In de memorie van toelichting is aangegeven dat in de berekeningen van het bureau VKA geen rekening is gehouden met de financiële vergoeding die op grond van de in artikel 13.6 van de Telecommunicatiewet bedoelde ministeriële regeling aan de aanbieder wordt verstrekt in geval van het op vordering van de bevoegde autoriteit verstrekken van gegevens. De werkelijke investeringen en operationele kosten zullen derhalve naar alle waarschijnlijkheid lager uitvallen dan in de «green field» berekeningen van het bureau VKA. Door het ontbreken van inzicht in de kosten die gemoeid zijn met het upgraden van de

bestaande infrastructuur en de personele bezetting bij de providers naar het niveau dat nodig is om aan de verplichtingen van het wetsvoorstel te voldoen, kan niet bepaald worden in hoeverre de aanvraagvergoeding door de overheid hieraan tegemoet komt. De overheid beschikt niet over gegevens waaruit dit kan worden afgeleid.
Op de vraag van de leden van de PvdA-fractie over de mogelijke verzwaring van de administratieve lasten van de aanbieders en de meerkosten van een bewaarplicht van achttien maanden zal hieronder, bij de beantwoording van de vragen van de fracties van D66 en de SP, nader worden ingegaan.

De leden van de SP-fractie waren bezorgd over de bedrijfseffecten die de kosten van het bewaren van gegevens kunnen veroorzaken en beschouwden de kostenverdeling tussen aanbieders en overheid als onvoldoende. Zij hebben gevraagd of de regering voldoende draagvlak verwacht in de sector, dat door de leden van deze fractie als noodzakelijk wordt beschouwd om het wetsvoorstel te doen slagen. Voorts vroegen zij in hoeverre de verwachting reëel is dat aanbieders hun aanzienlijk toegenomen bedrijfskosten zullen afwentelen op de gebruiker van telecommunicatie. De leden van de D66-fractie constateerden dat de aanbieders zelf de investeringskosten dienen te dragen die nodig zijn om te kunnen voldoen aan deze verzoeken van politie en justitie en dat de aanbieders van telecommunicatienetwerken en -diensten ten aanzien van de financiële consequenties van het wetsvoorstel spreken van een zware en onaanvaardbare last op de telecomsector.
In antwoord op de vragen van deze fracties naar de bedrijfseffecten die zijn verbonden aan de invoering van dit wetsvoorstel, merk ik op dat mijns inziens geen sprake is van een aanzienlijke verzwaring van de administratieve lasten van de aanbieders. In de eerste plaats dient in ogenschouw genomen te worden dat ook thans reeds verkeersgegevens worden bewaard door de aanbieders van telecommunicatiediensten ten behoeve van hun eigen bedrijfsdoeleinden. Volgens de methode voor het berekenen van de nalevingskosten zouden de kosten, die de aanbieders thans al maken voor het bewaren van de gegevens voor eigen bedrijfsdoeleinden, van de door het bureau VKA berekende kosten moeten worden afgetrokken. De aanbieders hebben echter geen informatie verschaft over de hoogte van deze kosten. De verplichting tot het bewaren van de gegevens is het directe gevolg van Europese regelgeving. Die verplichting brengt kosten voor het bedrijfsleven met zich mee. De vergoeding van die kosten door de overheid loopt in de verschillende lidstaten sterk uiteen. Er zijn lidstaten die in het geheel geen vergoeding kennen en er zijn lidstaten die alle kosten vergoeden. Nederland neemt een tussenpositie in. Daarbij is aangesloten bij het bestaande stelsel van vergoedingen in hoofdstuk 13 van de Telecommunicatiewet. De hoofdregel is dat de kosten van investeringen en onderhoud niet worden vergoed en de kosten van bevraging wel. Over de hoogte van de vergoeding bestaat discussie tussen overheid en aanbieders. Er vindt overleg plaats over de meest efficiënte en effectieve manier waarop de overheid en bedrijfsleven kunnen samenwerken rond de processen van de uitvoering van de bevoegdheden tot aftappen en tot vordering van verkeersgegevens. Dit overleg zal mede bepalend zijn voor het draagvlak bij het bedrijfsleven. De bedrijven zullen wellicht proberen hun kosten te verdisconteren in de tarieven die zij aan de consument in rekening brengen, voorzover daar geen aparte inkomsten (vergoeding door de overheid) tegenover staan. Het hangt van de marktsituatie af of dit mogelijk is. Niet altijd zullen alle kosten doorberekend kunnen worden omdat de telecommunicatiemarkt een uiterst competitieve markt is waarop aanbieders het zich niet kunnen veroorloven hun tarieven te zeer te laten stijgen. Ze zouden dan onmiddellijk marktaandeel kunnen gaan verliezen. Daarom zijn bedrijven meer geïnteresseerd in kostenbesparing en de

meest efficiënte wijze om aan de verplichtingen te kunnen voldoen. Naar verwachting zal de voorgestelde regelgeving nauwelijks merkbare effecten op de tarieven van de aanbieders hebben.

De leden van de SP-fractie vroegen nader in te gaan op de kostenberekeningen die de regering presenteert. De leden hebben kennis genomen van de opmerking van de regering dat tijdens de onderhandelingen over de richtlijn meegewogen heeft dat het volume van de te bewaren internetgegevens, en de aan de opslag verbonden kosten, beheersbaar zouden moeten zijn en in evenwicht met het doel van de bewaarplicht. Zij vroegen op welke wijze er bij de kostenberekening rekening is gehouden met de toenemende digitalisering van de samenleving, en de verwachting dat steeds meer en ingewikkelder communicatiemiddelen gehanteerd zullen worden en het internetverkeer alleen maar toe zal nemen.
In reactie op de gestelde vragen merk ik op dat de Richtlijn dataretentie een aantal gegevens vermeldt die beschikbaar moeten zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Deze gegevens betreffen verkeers- en locatiegegevens die zijn gegenereerd of verwerkt door aanbieders van openbare telecommunicatiediensten of telecommunicatienetwerken. Deze richtlijn is niet van toepassing op de inhoud van de communicatie. Zou in deze richtlijn sprake zijn geweest van de beschikbaarheid van de inhoud van de communicatie, dan zou inderdaad sprake kunnen zijn geweest van extra kosten om deze opslag te realiseren. Nu slechts sprake is van opslag van verkeers- en locatiegegevens, is het benodigde volume voor beschikbaarheid van gegevens om te voldoen aan het gestelde conform deze richtlijn naar alle waarschijnlijkheid niet dermate groot dat rekening moet worden gehouden met forse investeringen. De technologische ontwikkelingen van de afgelopen jaren laten op het punt van opslag laten zien dat de benodigde investeringen voor opslag of uitbreiding van de opslag als zodanig afgenomen zijn en naar alle waarschijnlijk nog verder zullen gaan afnemen. Op basis van deze ontwikkeling is de verwachting gerechtvaardigd dat de verdere daling van deze kosten een mogelijke stijging van het internetverkeer, zo niet geheel dan in ieder geval voor een belangrijk deel, zal kunnen compenseren.

De leden van de SP-fractie hebben, onder verwijzing naar de redactionele kanttekeningen in het Rechtsgeleerd Magazijn THEMIS (nummer 2007–4), hun twijfels geuit over de beheersbaarheid en het bewaarvolume van de opgeslagen gegevens. In Themis is het voorbeeld verschenen dat bij de huidige verkeersintensiteit reeds een hoeveelheid terabyte wordt gegenereerd die overeenkomt met ongeveer 4 miljoen kilometer gevulde dossierordners. De leden van deze fractie hebben zich afgevraagd of er niet een gigantische onbeheersbare hoeveelheid nutteloze gegevens wordt bewaard, de spreekwoordelijke hooiberg waarin de speld lastig te vinden is, en of ook rekening wordt gehouden met de toenemende hoeveelheid spam. Tenslotte hebben zij gevraagd of het risico, mede met het oog op de onvermijdelijke vervuiling van bestanden, niet groter wordt dat meer onschuldige burgers als verdachte zullen worden bestempeld.
In antwoord op deze vragen merk ik op dat de gegevens uit Themis zijn ontleend aan het betoog van prof. mr. H. Franken, lid van de fractie van het CDA in de Eerste Kamer, tijdens een bijzondere commissie voor de JBZ Raad op 28 juni 2005. Ik heb op het betoog van prof. Franken schriftelijk gereageerd (Kamerstukken I 2005/06, 23 490, BA). Dit is ook aan de orde gekomen in het Algemeen Overleg dat is gehouden op 5 oktober 2005 (Kamerstukken II 2005/06, 23 490, nr. 398). In deze brief ben ik tot de conclusie gekomen dat de door prof. Franken genoemde hoeveelheid data (20 000 tot 40 000 terabyte) geen reële inschatting is. Prof. Franken is vermoedelijk uitgegaan van een aanzienlijk uitgebreidere set van gege-

vens en een aanzienlijk langere bewaartermijn dan waartoe de uiteindelijke richtlijn en het daarop gebaseerde wetsvoorstel verplicht. Gelet op de uitkomsten waren de berekeningen vermoedelijk gebaseerd op de oorspronkelijke gedachte om ook de routeringsgegevens van de communicatie en de gegevens over bezoeken aan websites voor de door het ontwerp-kaderbesluit voorziene maximum bewaartermijn van drie jaar op te slaan. Uit de berekening van het bureau VKA, gebaseerd op de lijst van gegevens uit de bijlage van het wetsvoorstel, blijkt dat het gaat om in totaal zo'n 365 terabyte aan gegevens. Dat is een uit oogpunt van opslag en doorzoekbaarheid alleszins beheersbaar volume. Daarbij wijs ik er nog op dat ook op het internet, dat dus een aanzienlijk groter volume aan data kent dan het volume dat thans bij de bewaarplicht aan de orde is, inmiddels zoeksystemen kunnen worden gebruikt die binnen fracties van seconden de juiste gegevens uit een veelheid aan data kunnen selecteren. Wat betreft de vraag of met de opslag van deze gegevens het risico niet groter wordt dat meer onschuldige burgers als verdacht zullen worden beschouwd, merk ik het volgende op. Een verdenking in de zin van artikel 27 van het Wetboek van Strafvordering is eerst mogelijk als uit feiten en omstandigheden een redelijk vermoeden van schuld aan enig strafbaar feit voortvloeit. Het enkele feit dat een persoon in de gevorderde verkeersgegevens voorkomt, is onvoldoende grond om hem of haar als verdachte in de zin van artikel 27 van het Wetboek van Strafvordering aan te merken.

De toelichting op de te verwachten kosten en bedrijfseffecten was de leden van de VVD-fractie nog niet geheel duidelijk. Zij hebben gevraagd om een toelichting op de overweging dat de extra kosten (meerkosten bij de investeringen van 400 000 en bij operationele kosten van 100 000 euro) gedragen zullen worden door een beperkt aantal grote aanbieders in de mobiele telefonie.
Naar aanleiding van deze vraag kan worden opgemerkt dat deze cijfers betrekking hebben op de opslag van locatiegegevens, op basis van berekeningen van het bureau VKA naar de benodigde opslagcapaciteit, indicatief de verhouding kan worden aangegeven tussen de benodigde opslagcapaciteit voor het geheel van de gegevens en die van mobiele telefonie, waarvan onder andere prepaid telefonie deel uitmaakt. Volgens het bureau VKA komt de totale omvang van de benodigde database voor de opslag van verkeersgegevens uit op 365 terabyte. Het aandeel van de mobiele telefonie daarin is 5 terabyte. Gesteld dat prepaid telefonie een aandeel heeft van 40% van de totale mobiele telefonie, dan bedraagt het aandeel voor het bewaren van locatiegegevens ongeveer 0,5% van de totale opslagcapaciteit voor de gehele sector. De meerkosten bij de investeringen komen daarbij op 400 000 euro, en bij de operationele kosten op 100 000 euro. Deze kosten worden gedragen door een beperkt aantal grote aanbieders in de mobiele telefonie.

De leden van de fractie van D66 vroegen een reactie te geven op de stelling van het CBP en Actal dat het wetsvoorstel ertoe bijdraagt dat Nederlandse bedrijven in een negatieve concurrentiepositie komen ten opzichte van andere bedrijven in de EU die worden geconfronteerd met minder hoge kosten dan in Nederland. Tevens is verzocht bij de beantwoording overweging 6 uit de preambule van de richtlijn te betrekken.
In antwoord op deze vragen moet worden opgemerkt dat de kosten die door een wijziging van de bewaartermijn direct beïnvloed worden, samenhangen met de opslag van de gegevens op gegevensdragers en de daarmee samenhangende besturingslogica. Ook de beheerkosten zullen iets wijzigen. Het bureau VKA heeft berekend dat de kosten van twaalf maanden opslag circa 14 miljoen euro bedragen, waarvan 500 000 euro operationele kosten over een periode van vijf jaar. Daarbij moet worden bedacht dat het hier gaat over de kosten voor de gehele bedrijfstak. Bij de gekozen bewaartermijn van achttien maanden bedragen de investerings-

kosten voor geheugen derhalve 21 miljoen euro. Omdat het volume aan te bewaren gegevens samenhangt met het aantal accounts dat de betreffende aanbieder kent, zullen de zwaarste lasten gedragen worden door de grootste aanbieders die ieder miljardenomzetten kennen. Op basis van dezelfde implementatieoptie is in het geval van een bewaartermijn van een zes maanden een verlaging van de kosten van bijna zeven miljoen euro te verwachten, waarvan 400 000 euro operationele kosten over een periode van vijf jaar. Voor de overige implementatieopties is een vergelijkbaar bedrag van toepassing.
Het verschil van 14 miljoen euro bij een bewaartermijn van zes maanden of achttien maanden heeft mijns inziens geen onaanvaardbare consequenties voor de concurrentiepositie van Nederlandse bedrijven. Dit bedrag moet opgebracht worden door alle betrokken bedrijven samen waarbij bedacht moet worden dat het hierbij gaat om een tiental grotere bedrijven, die ruim 90% van de markt uitmaken, en daarnaast nog eens zo'n driehonderd kleinere bedrijven. De verdeling van de kosten over die bedrijven naar rato van het verkeer dat door hen wordt gerealiseerd leidt per bedrijf tot bedragen die nauwelijks significant zijn in het licht van de omzetcijfers van deze bedrijven. Ook is in dit verband van belang dat de kosten die gemaakt moeten worden om aan de verplichtingen te voldoen naar evenredigheid drukken op alle bedrijven die op de Nederlandse markt actief zijn. Aangezien het veelal internationaal opererende bedrijven zijn, zullen de effecten voor de internationale concurrentiepositie van die bedrijven verwaarloosbaar zijn. Bezien vanuit het perspectief van het functioneren van de interne markt verwacht ik niet dat de Nederlandse regelgeving belemmeringen voor de interne markt voor elektronische communicatie te weeg zal brengen. Een volledige harmonisatie zat er, vanwege tegengestelde belangen van de lidstaten, niet in. Het gevolg is dat ook de kosten voor het nakomen van de verplichtingen in de diverse lidstaten uiteen zullen lopen. Overigens verwacht ik dat afspraken met het bedrijfsleven over een voor alle partijen zo efficiënt mogelijke aanpak, zullen leiden tot beperking van de kosten en positief zullen kunnen uitpakken ten opzichte van landen waar dit soort afspraken met aanbieders niet worden gemaakt. In het licht van deze aspecten rechtvaardigt het grote belang van telecommunicatiegegevens voor veel opsporingsonderzoeken de voorgestelde bewaartermijn. Deze termijn kan proportioneel worden geacht in verhouding tot de belangen van de persoonlijke levenssfeer en de lasten voor de aanbieders.

De leden van de D66-fractie hebben gevraagd wat het regeringsstandpunt is ten aanzien van een nader onderzoek naar de kosten van het wetsvoorstel voor het bedrijfsleven. Dit onder verwijzing naar de brief van CBP en Actal van 12 oktober 2007. Deze vragen zijn hierboven in paragraaf 2.3, naar aanleiding van vragen van de fracties van de ChristenUnie en D66, reeds door mij beantwoord. Naar die beantwoording moge ik thans verwijzen.

Naar ik hoop zijn met het voorgaande alle 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