Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2008–2009

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

C

MEMORIE VAN ANTWOORD

Ontvangen 2 oktober 2008

Inleiding

Graag zeg ik de leden van de fracties dank voor hun uitgebreide inbreng. Het is verheugend te constateren dat dit wetsvoorstel, door middel waarvan de richtlijn van 24 maart 2006 wordt geïmplementeerd, op veel belangstelling van Uw Kamer kan rekenen. Inmiddels heeft de Commissie van de Europese Gemeenschappen de Nederlandse regering, bij brief van 18 september jongstleden, er van in kennis gesteld dat Nederland de verplichtingen van de richtlijn niet tijdig in nationaal recht heeft omgezet en verzocht de nodige maatregelen te treffen zodat deze verplichtingen binnen twee maanden zijn nagekomen. Ik hoop dan ook dat Uw Kamer dit wetsvoorstel voortvarend zal afhandelen, zodat de inbreukprocedure kan worden beëindigd.
De leden van de CDA-fractie hadden met belangstelling, doch ook met enige bevreemding kennis genomen van dit wetsvoorstel. Zij meenden dat met de verschillende factoren, zoals enerzijds de klaarblijkelijke behoefte aan verkeers- en locatiegegevens bij de opsporingsdiensten en justitie in concrete gevallen en anderzijds de weging van de gevolgen van een bewaarplicht voor de persoonlijke levenssfeer van burgers en de praktische en financiële gevolgen voor de telecommunicatieaanbieders en de overheid, serieus rekening gehouden moet worden en dat over deze afweging verantwoording moet worden afgelegd. De CDA-fractie riep in herinnering dat de Eerste Kamer zich bij de behandeling van het ontwerp-kaderbesluit steeds kritisch heeft opgesteld en meende dat deze tenslotte aan dit besluit haar instemming heeft onthouden. Vanzelfsprekend erkenden de leden van deze fractie de verplichting tot implementatie van Richtlijn 2006/24/EG, maar hierbij leek sprake te zijn van een daadwerkelijke schending van het bepaalde in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), zodat principiële vragen naar noodzaak en proportionaliteit van de maatregel aan de orde zijn, aldus de leden van deze fractie.

KST122757
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2008

De leden van de fracties van de PvdA, de VVD, de ChristenUnie en de SGP namen kennis van de parlementaire behandeling van dit wetsvoorstel in de Tweede Kamer. De leden van de VVD-fractie achtten deze discussie voldoende afgerond en kunnen goed leven met de bewaartermijn van twaalf maanden. Volgens hen is een goede balans gevonden tussen het doel van de bewaarplicht, te weten het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, en de inbreuk op de bescherming van de persoonlijke levenssfeer. De leden van de PvdA-fractie hadden met waardering kennis genomen van de gedegen parlementaire behandeling van het wetsvoorstel en wensten twee gerichte vragen aan de regering voor te leggen. De leden van fracties van de ChristenUnie en de SGP waren verheugd dat het amendement Anker was aangenomen, waardoor de door de regering voorgestelde bewaartermijn is teruggebracht naar twaalf maanden, en waren ingenomen met de verkorting van de evaluatietermijn van vijf naar drie jaar. Deze leden hadden slechts enkele vragen.

De leden van de fractie van GroenLinks waren zich bewust van de beperkte toets van onderhavig wetsvoorstel, die zich beperkt tot de wijze van implementatie van de richtlijn door de Nederlandse regering en stelden vast dat de regering met een bewaartermijn van twaalf maanden meer doet dan de door de richtlijn verlangde zes maanden. De leden van de fractie van D66 hadden met zekere gevoelens van aarzeling kennisgenomen van het voorstel. Zij onderschreven de strekking daarvan, voorzover het voorziet in het garanderen en beschikbaarstellen van telecommunicatiegegevens voor een bepaalde tijd ten bate van de bestrijding van ernstige vormen van criminaliteit, maar hadden zorgen over de waarborging van de privacy van burgers en wilden ook op enkele andere punten een vraag stellen. De leden van de fractie van de SP tenslotte, waren buitengewoon bezorgd over het voorliggende implementatievoorstel en vonden de uitbreiding van de bewaartermijn van zes naar twaalf maanden volstrekt onvoldoende gemotiveerd. Zij waren bevreesd dat hier een enorme vracht informatie verzameld en bewaard gaat worden, waarmee artikel 8 van het EVRM geschonden wordt, zonder dat nut, noodzaak en proportionaliteit ervan wordt aangegeven. Ook hadden deze leden zorgen met betrekking tot de kosten die gepaard gaan met deze opslag van gegevens. Zij vroegen of de regering deze zorgen deelt en zo ja, waarom toch gekozen is voor deze, naar hun mening, «overdadige» implementatie van de richtlijn.

Graag beantwoord ik, mede namens de Staatssecretaris van Economische Zaken, de gestelde vragen en reageer ik op de inbreng van de leden van uw commissie. Daarbij merk ik op dat dit wetsvoorstel naar mijn mening een goed voorbeeld vormt van de complexe relatie tussen de voortdurende technische innovatie en de bescherming van de rechtsstaat. Waar de technische ontwikkelingen enerzijds nieuwe mogelijkheden bieden voor het plegen strafbare feiten en het onttrekken van bepaalde handelingen aan het zicht van politie en justitie, bieden diezelfde ontwikkelingen juist ook nieuwe aanknopingspunten voor verdere verbeteringen van de opsporing en vervolging van criminaliteit. Gedurende het afgelopen decennium heeft vooral de telecommunicatie zich sterk ontwikkeld, door middel van de mobiele telefonie en het internet. Dit biedt nieuwe mogelijkheden voor het plegen van strafbare feiten, omdat plegers van strafbare feiten – bijvoorbeeld zedendelinquenten – eenvoudiger in contact kunnen komen met hun slachtoffers. Voor criminele groeperingen is het gemakkelijker om hun activiteiten te organiseren, ook over grotere afstanden. Aldus wordt ook de criminaliteit gekenmerkt door een voortdurende evolutie. Dit uit zich in nieuwe verschijningsvormen van criminaliteit, zoals het aanbieden van kinderpornografisch materiaal via het internet of het bedreigen van personen en het plegen van fraude en

oplichting door middel van e-mail. Dergelijke activiteiten kunnen voor burgers in het bijzonder bedreigend zijn omdat hiermee rechtstreeks in hun huiselijke sfeer wordt binnengedrongen. De bewaarplicht nu biedt de overheid de mogelijkheid om de burgers beter te beschermen als zij het slachtoffer worden van ernstige criminaliteit. Aan de hand van opgeslagen verkeersgegevens kan zicht worden verkregen op de relaties tussen daders en slachtoffers. Daarnaast biedt de bewaarplicht de mogelijkheid om meer zicht te krijgen op de aard en de samenstelling van criminele netwerken en de relaties tussen de deelnemers onderling. Uiteraard zijn hierbij ook rechtsstatelijke overwegingen aan de orde, zoals de mogelijke inmenging in de persoonlijke levenssfeer van burgers, en tevens maatschappelijke en bedrijfseconomische vraagstukken, zoals de vraag in hoeverre van bedrijven kan worden gevraagd om een bijdrage te leveren aan de bestrijding van ernstige criminaliteit. De criminaliteit maakt dankbaar gebruik van de innovatie op het gebied van de telecommunicatie. Om die criminaliteit het hoofd te kunnen bieden moeten politie en justitie adequaat worden toegerust, niet alleen op het gebied van de capaciteit en de expertise, maar juist ook op het gebied van het achterhalen en analyseren van sporenmateriaal. De bewaarplicht is een buitengewoon nuttige maatregel omdat hiermee wordt verzekerd dat verkeersgegevens daadwerkelijk beschikbaar zijn als later, tijdens de fase van de opsporing of vervolging van ernstige misdrijven, aan die gegevens behoefte bestaat om verbanden te kunnen leggen. Uiteraard dient daarbij een goede balans te worden gevonden tussen enerzijds de maatschappelijke behoefte aan de bestrijding van criminaliteit en anderzijds de bescherming van de persoonlijke levenssfeer en beperking van de lasten voor het bedrijfsleven. Daarbij merk ik op dat juist de technische ontwikkelingen de mogelijkheid bieden om deze tegenstelling te overbruggen en de belangen met elkaar in overeenstemming te brengen. De tegenstelling blijkt dan eigenlijk een schijnbare tegenstelling. Daar waar de techniek de overheid in staat stelt in bepaalde omstandigheden en ten behoeve van de bescherming van bepaalde gerechtvaardigde belangen toegang te verkrijgen tot informatie over de gedragingen van burgers, biedt diezelfde techniek tevens de mogelijkheid om de toegang te beperken tot uitsluitend de gegevens die voor het beschermen van die belangen noodzakelijk zijn. Met het voorliggende wetsvoorstel is hierin naar mijn mening een goede balans gevonden. In deze memorie van antwoord hoop ik de vragen van de leden van uw fracties dan ook naar tevredenheid te kunnen beantwoorden en de gevoelens van aarzeling, bevreemding of bezorgdheid aan de zijde van de leden van de fracties van Uw Kamer 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.

Reikwijdte van de richtlijn

De leden van de CDA-fractie stelden een aantal vragen over het doel van de voorgestelde maatregel, namelijk het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Zij vroegen of de regering kan aangeven aan welke misdrijven hier wordt gedacht, of bij de kwalificatie «ernstig» alleen wordt gedacht aan een of meer categorieën van delicten of dat hieronder ook andere soorten van crimineel gedrag vallen, of de in het Wetboek van Strafrecht opgenomen strafbedreiging bepalend is voor de te onderzoeken groep misdrijven en zo ja, waar de grens ligt om van wel of niet ernstige misdrijven te spreken. Tevens vroegen zij hoe andere lidstaten aan dit criterium invulling hebben gegeven en of er sprake is van een catalogus van delicten.
Graag ga ik als volgt op deze vragen in. De richtlijn heeft tot doel een harmonisatie tot stand te brengen van de nationale wetgeving in de

lidstaten waarbij aan de aanbieders verplichtingen worden opgelegd betreffende het bewaren van bepaalde gegevens, die door hen worden gegenereerd of verwerkt, teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, zoals gedefinieerd in de nationale wetgevingen van de lidstaten (artikel 1, eerste lid). De toegang tot de gegevens wordt, binnen de in de richtlijn daaromtrent gegeven voorwaarden, aan de lidstaten zelf overgelaten (artikel 4). Op Europees niveau is er dus geen sprake van een catalogus van delicten.
In Nederland wordt de toegang tot de bewaarde gegevens ten behoeve van de opsporing en vervolging van strafbare feiten, beheerst door de regels van het Wetboek van Strafvordering. Op grond van die regels kan de officier van justitie in het belang van het onderzoek een vordering doen tot verstrekking van verkeersgegevens (art. 126n en 126u Sv.). 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. Dit betreft het vorderen van verkeersgegevens. Daarnaast geldt dat een opsporingsambtenaar in het belang van het onderzoek gegevens kan vorderen die bijdragen aan het identificeren van een persoon (artikel 126na en 126ua Sv.). Vereist is een verdenking van een misdrijf of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Dit betreft het vorderen van gebruikersgegevens (naam, adres, woonplaats, nummer en soort dienst). Daarnaast beschikt de officier van justitie over specifieke bevoegdheden tot bestrijding van terroristische misdrijven. Ingeval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie in het belang van het onderzoek een vordering doen tot verstrekking van verkeersgegevens (art. 126zh Sv.). In een dergelijk geval kan de opsporingsambtenaar gebruikersgegevens vorderen (art. 126zi Sv.). Tenslotte heeft de officier van justitie de bevoegdheid om ten behoeve van een verkennend onderzoek naar terroristische misdrijven gegevensbestanden van publieke en particuliere instanties te vorderen teneinde de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv.). Hiervoor verwijs ik ook naar de memorie van toelichting (Kamerstukken II 2006/07, 31 145, nr. 3, blz. 19–22) en de nota naar aanleiding van het verslag (Kamerstukken II 2007/08, 31 145, nr. 9, blz. 30–33). Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van de misdrijven, genoemd in artikel 67, eerste lid, van het Wetboek van Strafvordering. Aldus wordt bij de kwalificatie «ernstig» gedacht aan één of meer categorieën van delicten, zoals de delicten waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld en de andere, in artikel 67, eerste lid, van het Wetboek van Strafvordering bepaald aangewezen misdrijven. Daaronder zijn terroristische misdrijven begrepen.
Hoe de andere lidstaten aan dit criterium invulling hebben gegeven is mij niet tot in detail bekend. In Duitsland bevat de Telecommunicatiewet de verplichting voor de aanbieders tot verstrekking van de gegevens ten behoeve van onder meer de vervolging van strafbare feiten (§ 113b TKG). Op grond van het Duitse strafprocesrecht is het vorderen van verkeersgegevens thans mogelijk als op grond van bepaalde feiten de verdenking bestaat dat een persoon als dader of deelnemer betrokken is bij het plegen of voorbereiden van een strafbaar feit van aanzienlijke betekenis of een strafbaar feit dat door middel van telecommunicatie is gepleegd (§ 100 StPO). Op de situatie in Duitsland wordt hieronder nader ingegaan, bij de beantwoording van de vragen van de leden van de fractie van het CDA over de uitspraak van het Duitse Bundesverfassungsgericht van 11 maart 2008. In Frankrijk biedt de Wet op de post en de elektronische communicatie de mogelijkheid om verkeersgegevens te bewaren ten behoeve van het onderzoek, de vaststelling en de vervolging van strafbare

feiten, uitsluitend voor het doel om deze gegevens beschikbaar te stellen aan de justitiële autoriteiten (artikel L34-1 Code des postes et des communications electroniques). Daarnaast hebben individueel aangewezen antiterrorisme rechercheurs van politie en gendarmerie de bevoegdheid om deze gegevens van de providers te vorderen – buiten een justitieel onderzoek om – teneinde terroristische daden tegen te gaan (Loi relative a la lutte contre le terrorisme, ook bekend als de wet Sarkozy). In België is de bevoegdheid tot het vorderen van verkeersgegevens, op grond van artikel 88bis van het Wetboek van Strafvordering, voorbehouden aan de onderzoeksrechter. Voorwaarde is dat deze magistraat van oordeel is dat er omstandigheden zijn die het doen opsporen van telefonische mededelingen noodzakelijk maken. Er geldt geen beperking ten aanzien van de ernst of zwaarte van de strafbare feiten, uit het vereiste van de tussenkomst van de onderzoeksrechter vloeit echter voort dat het moet gaan om ernstige strafbare feiten. In het Verenigd Koninkrijk is de bevoegdheid tot het vorderen van de bewaarde gegevens ten behoeve van de voorkoming of bestrijding van misdaad of de voorkoming van wanorde geregeld in The Regulation of Investigatory Powers Act 2000. Toegang is mogelijk voor een persoon die daartoe is geautoriseerd door een persoon die werkzaam is bij de in de wet aangewezen politie-eenheden, ten behoeve van de voorkoming of bestrijding van misdaad of de voorkoming van wanordelijkheden (artikel 22, tweede lid). De autorisatie kan uitsluitend worden verleend als degene die de autorisatie verleent reden aanneemt dat de beschikbaarstelling van de gegevens proportioneel is in verhouding tot hetgeen kan worden bereikt met de verkrijging van de gegevens (artikel 22, vijfde lid). In Denemarken is het vorderen van de bewaarde gegevens afhankelijk van een rechterlijk bevel, uitsluitend ingeval van verdenking van betrokkenheid bij bepaalde ernstige strafbare feiten. In Finland wordt, evenals in Nederland, aangesloten bij de bestaande wetgeving («Coercive Measures Act»). Het vorderen van de bewaarde gegevens is mogelijk bij een delict waarop een maximale gevangenisstraf staat van tenminste vier jaar. In Spanje is de bewaarplicht geregeld in een wet van 18 oktober 2007 (18 243). De beschikbaarstelling van de bewaarde gegevens aan functionarissen van bepaald aangewezen opsporings- en veiligheidsdiensten is afhankelijk van voorafgaande machtiging van een justitiële autoriteit (artikel 6). In de machtiging wordt per geval afzonderlijk gespecificeerd welke gegevens moeten worden overgedragen aan de bevoegde rechtshandhavingsautoriteiten, rekening houdend met de beginselen van noodzakelijkheid en proportionaliteit (artikel 7). In Portugal is de bevoegdheid tot het vorderen van de gegevens op grond van het Portugese Wetboek van Strafvordering gekoppeld aan de delicten ten aanzien waarvan de bevoegdheid tot het aftappen van telecommunicatie kan worden ingezet. Dit betreft misdrijven die kunnen worden bestraft met een maximale gevangenisstraf van meer dan drie jaar en bepaalde categorieën van misdrijven, zoals handel in drugs en wapens, bedreiging of inbreuk op het privé-leven van personen gepleegd met behulp van de telefoon en ontsnapping, wanneer de betrokkene is veroordeeld voor een van de bovengenoemde misdrijven.

Bewaartermijn

De leden van de CDA-fractie stelden vast dat de regering de noodzaak van de bewaarverplichting motiveert met een verwijzing naar de behoeften van politie en justitie en het onderzoek van de Erasmus Universiteit Rotterdam (EUR). Zij merkten daarbij op dat de behoeften van politie en justitie als zodanig, althans zonder nadere onderbouwing, eerder als een wens («nice to have») dan als een noodzaak («must») kunnen worden aangemerkt. Gaarne zagen de leden van deze fractie de onderbouwing als noodzaak tegemoet, zodat de conclusie kan worden getrokken dat het om meer dan een wenselijkheid gaat om de verkeersgegevens langer dan de

in Richtlijn 2002/58/EG genoemde termijn, en zeker langer dan de in Richtlijn 2006/24/EG voorgestelde termijn, te bewaren. Verder meenden de leden van deze fractie dat het rapport van de EUR in het geheel niet als een onderbouwing van een langere dan de minimumtermijn kan worden beschouwd. Gebleken is dat de vraagstelling en de gehanteerde onderzoeksmethode daar niet op zijn geënt. De onderzoekers hadden voor hun onderzoek slechts 65 dossiers ter beschikking waarin verkeersgegevens een belangrijke rol speelden. In die dossiers waren de verkeersgegevens steeds beschikbaar. Daaruit volgt reeds dat een verlenging van de om commerciële redenen aangehouden bewaartermijn, die in overeenstemming is met Richtlijn 2002/58/EG, niet noodzakelijk zou zijn, aldus deze leden. Er waren te weinig dossiers voorhanden waarin verkeersgegevens met betrekking tot internet een rol speelden, zodat voor die categorie op basis van dossieronderzoek met betrekking tot nut en noodzaak van het verruimen van de bewaartermijn geen wetenschappelijk verantwoorde conclusies waren te trekken. Op basis van gesprekken en niet op basis van onderzoek naar het feitelijk gebruik van verkeersgegevens is de conclusie getrokken dat een bewaartermijn van één jaar voor alle gegevens, zowel telefonie als internet, wenselijk is. Onder verwijzing naar de zaak Silver vs United Kingdom meenden deze leden dat met de conclusies van dit onderzoek niet is voldaan aan het noodzakelijkheidscriterium van artikel 8 EVRM. Zij concludeerden dat de door het EVRM vereiste onderbouwing van de proportionaliteit ontbreekt en de noodzaak voor het bewaren van internetgegevens (in ieder geval voor een periode langer dan zes maanden) niet is aangetoond. In dit verband verwezen de leden van de fractie van het CDA naar het manifest van vijftien hoogleraren, dat is gepubliceerd in NRC-Handelsblad van 21 mei 2008, waarin wordt betoogd dat een bewaartermijn van zes maanden niet moet worden overschreden. De leden van de SP-fractie sloten zich bij deze vragen aan.

Ook de leden van de fractie van de PvdA stelden vast dat met dit wetsvoorstel in zoverre sprake is van een «kop» op Europese regelgeving dat hier verder wordt gegaan dan de Europese regelgever voor de bestrijding van terroristische aanslagen en ernstige criminaliteit noodzakelijk acht. Zij vroegen of de regering de vaststelling deelt dat dit betekent dat op de regering een bijzondere verantwoordelijkheid rust om aan te geven waarom de met dit wetsvoorstel teweeggebrachte inbreuk op de persoonlijke levenssfeer noodzakelijk en proportioneel is. Ook vroegen de leden van deze fractie de regering nog eens aan te geven waarom zij de positie is blijven betrekken die zij heeft betrokken en welke doelen haar met een bewaartermijn langer dan zes maanden voor ogen staan. Verder vroegen zij of de regering het aannemelijk acht dat die doelen ook als gevolg van de langere bewaarplicht *in een substantieel aantal gevallen* bereikt zullen worden en daarbij onderscheid kan maken tussen het doel van a) het voorkomen van terroristische aanslagen, b) het opsporen van daders van ernstige criminaliteit en c) het oplossen van gepleegde criminaliteit.

In antwoord op de gestelde vragen naar de noodzaak en de proportionaliteit van een bewaartermijn die langer is dan het Europeesrechtelijk toegestane minimum van zes maanden breng ik – in aansluiting op hetgeen in de memorie van toelichting en de nota naar aanleiding van het verslag reeds aan de orde kwam – graag het volgende naar voren. Ik baseer dit op de ingebrachte adviezen, de door de politie en het Openbaar Ministerie ingebrachte concrete voorbeelden, het rapport van de Erasmus Universiteit Rotterdam en de beschikbare informatie over de doorlooptijden in strafzaken. 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 vergroot de kans 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. Naarmate de gegevens korter bewaard blijven, doet zich vaker de situatie voor dat gegevens niet meer voor het opsporingsonderzoek beschikbaar zijn. Een termijn van twaalf maanden is in dit opzicht in mijn ogen een minimale termijn. Ook in niet al te complexe onderzoeken, kan toch pas na enige tijd blijken dat bepaalde gegevens van belang zijn voor het onderzoek. Dit kan het geval zijn indien het onderzoek reeds langer loopt maar er pas later zicht ontstaat op de relaties tussen personen. Onderlinge contacten, waar pas na aanhouding over wordt verklaard, kunnen bij een korte bewaartermijn dan niet meer worden geverifieerd met behulp van verkeersgegevens. Ook kan het voorkomen dat bij doorzoekingen tot dan toe onbekende telefoons worden aangetroffen zodat het opvragen van de bijbehorende verkeersgegevens noodgedwongen later plaatsvindt. Soms komt het voor dat pas in een later stadium blijkt van een misdrijf, bijvoorbeeld in het geval van vermissing van een persoon. De noodzaak van een ruimere bewaartermijn doet zich het meest gevoelen bij de opsporing van grootschalige afpersingsonderzoeken, onderzoeken naar meervoudige moord in criminele organisaties en onderzoeken naar terrorisme. Hiertoe zijn verschillende voorbeelden aangereikt (Kamerstukken II 2007/08, 31 145, nr. 9) die duidelijk maken dat het belang van telecommunicatiegegevens voor de opsporing geenszins leidt tot de conclusie dat een bewaartermijn gekozen zou moeten worden die gelijkstaat aan de kortste termijn die de richtlijn toestaat. Bovendien vloeit de noodzaak tot een ruime bewaartermijn soms voort uit de specifieke bewijslast in bepaalde strafzaken. Dit is het geval in opsporingsonderzoeken waarin de duurzaamheid van een criminele organisatie als bedoeld in artikel 140 van het Wetboek van Strafrecht moet worden aangetoond. Voor zulke onderzoeken is informatie nodig waaruit blijkt dat de betrokken personen gedurende een langere periode contacten hebben onderhouden. Verkeersgegevens zijn daarvoor van groot belang. In de tweede plaats kan de behoefte aan verkeersgegevens aan de orde zijn tijdens het onderzoek ter terechtzitting. Er kan twijfel ontstaan aan de aard of inhoud van de bewijsmiddelen, waarbij de gegevens mede kunnen dienen om de onschuld van de verdachte aan te tonen. In de bijlage bij de brief aan de Tweede Kamer van 14 februari 2005 zijn hiervan reeds enkele voorbeelden gegeven (Kamerstukken II, 2004/05, 23 490, nr. 360). De gemiddelde doorlooptijd in strafzaken in eerste aanleg bedroeg in 2005 (bron WODC) zeven en een halve maand. Hierbij is hoger beroep niet meegerekend. De meer complexe en ernstiger zaken kennen vaak een langere doorlooptijd in eerste aanleg. Vanuit het gezichtspunt van de opsporing en vervolging van ernstige strafbare feiten geldt dan ook dat een langere bewaartermijn sterk zal kunnen bijdragen aan de opheldering van ernstige strafbare feiten.

Over de proportionaliteit van een langere bewaartermijn en de afweging tegen andere belangen die in het geding zijn, merk ik graag het volgende op.
Een eerste overweging is dat de mate waarin de bewaarplicht een aantasting vormt van de persoonlijke levenssfeer niet evenredig is aan de duur van de bewaartermijn. De aantasting van de persoonlijke levenssfeer wordt namelijk niet zozeer veroorzaakt door het bewaren van de gegevens als zodanig maar door de toegang tot die gegevens ten behoeve van andere doelen dan de afwikkeling van het telecommunicatieverkeer. Hierop zal hieronder, bij de beantwoording van de vragen van de leden van de fracties van het CDA over de verhouding met artikel 8 van het EVRM, nader worden ingegaan.

Een tweede overweging is dat een langere bewaartermijn niet evenredig meer belasting en kosten met zich mee zal brengen voor het bedrijfsleven. Voor het aangeven van de bedrijfseffecten heeft het onderzoek dat is

uitgevoerd door het bureau Verdonck, Klooster & Associates (VKA) de basis gevormd. Met de gegevens van VKA kan worden berekend wat de verschillen in kosten zijn van de verschillende bewaartermijnen. De kosten die direct door de bewaartermijn worden beïnvloed hangen samen met de opslag van de gegevens, dus de benodigde geheugencapaciteit (harddisks) en de daarmee samenhangende besturingslogica. Iedere verlenging van de bewaartermijn met zes maanden betekent een stijging van de investeringskosten met ongeveer 7 miljoen euro en de operationele kosten met ongeveer 100 000 euro. Een dergelijk verschil heeft mijns inziens geen significante invloed op de concurrentiepositie van de aanbieders die in Nederland actief zijn. Daarbij moet ook worden bedacht dat deze kosten naar alle waarschijnlijkheid zullen worden doorberekend aan de consumenten. Inmiddels zijn, tengevolge van de technische ontwikkeling, deze bedragen sterk verminderd zoals hieronder, bij de beantwoording van de vragen van de leden van de fractie van de SP naar de bewaartermijnen, zal worden toegelicht. Indien wordt uitgegaan van het geheel van de kosten zoals die bekend zijn geworden in het kader van de gerechtelijke procedure die door enkele aanbieders zijn gevoerd rond de wettelijke vergoedingsregeling van de kosten voor het aftappen van telecommunicatie en het vorderen van verkeersgegevens, dan zou dit, indien deze kosten geheel worden doorberekend aan de consument, neer komen op 27 à 28 eurocent per eindgebruiker per jaar.

Omdat telefonie via internet de traditionele telefonie zal vervangen ligt het in de rede voor beide gegevenscategorieën eenzelfde bewaartermijn te hanteren. Ook het volume van de te bewaren internetgegevens is niet zodanig omvangrijk dat dit strekt tot een kortere termijn Het kostenaspect is evenmin van zodanige aard dat dit – gelet op het belang van deze gegevens voor de bestrijding van ernstige criminaliteit – tot beperking van de bewaartermijn zou strekken. Ingeval voor de internetgegevens een kortere bewaartermijn wordt gekozen dan zou dit eenvoudig kunnen leiden tot vermijdingsgedrag, waardoor de effectiviteit van de bewaarplicht afneemt, en ook de concurrentiepositie van de aanbieders van telefoniediensten zou kunnen worden geschaad. Ook andere lidstaten hanteren doorgaans eenzelfde bewaartermijn voor zowel telefonie- als internetgegevens.

In antwoord op de hiertoe strekkende vraag van de leden van de PvdA-fractie vermeld ik dat het bij voorbaat niet eenvoudig is om hard te maken waarom een langere bewaartermijn precies nodig is, welke strafbare feiten dan kunnen worden opgelost die op dit moment niet worden opgelost en waarin de bijdrage van de te bewaren gegevens aan de resultaten van de opsporing en de vervolging dan precies zal zijn gelegen. Op dit moment is er geen bewaarplicht, waardoor de politie afhankelijk is van de beschikbaarheid van de gegevens bij de aanbieder. Op grond van de Europese richtlijnen is de aanbieder immers gehouden de gegevens te vernietigen indien deze niet nodig zijn voor bepaalde doeleinden, die verband houden met eigen zakelijke doeleinden van de aanbieder (artikel 6 van Richtlijn 2002/58 EG). De onderzoekers van de Erasmus Universiteit hebben geconstateerd dat het antwoord op de vraag waarom de opsporingsdiensten de historische verkeersgegevens niet aangeleverd krijgen die betrekking hebben op gegevens ouder dan drie maanden, per aanbieder verschillend moet worden beantwoord. Sommige van de aanbieders van telefonie leverden de gegevens tot een jaar terug voor het tijdstip van vordering, andere aanbieders daarentegen hadden slechts beschikking over de gegevens over een periode van drie maanden. De onderzoekers zien hierin een goed argument om over te gaan tot het scheppen van eenduidige regels omtrent de bewaartermijn voor alle aanbieders van telefonie (blz. 10). Het wetsvoorstel is noodzakelijk omdat het ervoor zorgt dat gegevens, die door de aanbieders worden gegene-

reerd of verwerkt, gedurende een termijn van twaalf maanden worden bewaard zodat deze gegevens, indien nodig, kunnen worden opgevraagd ten behoeve van de bestrijding van ernstige criminaliteit. Soms blijkt pas op een later tijdstip dat er een ernstig strafbaar feit is gepleegd of blijkt pas tijdens het opsporingsonderzoek van aanknopingspunten die aanleiding geven tot het bevragen van hun telecommunicatiegegevens. Het is echter niet goed aan te geven na welke periode deze behoefte zich in het geheel niet meer zal voordoen, noch welke categorieën van gegevens dit betreft of wat precies de bijdrage van de bewaarde gegevens aan het opsporingsonderzoek zal zijn. Duidelijk is echter – dit komt ook naar voren in de adviezen van de politie en het Openbaar Ministerie naar aanleiding van het wetsvoorstel – dat hoe eerder de gegevens worden vernietigd, hoe groter het risico is dat ernstige strafzaken onopgelost blijven. Naarmate de termijn korter wordt gesteld, wordt dit risico dus groter. Als ervaring is opgedaan met de bewaartermijn van twaalf maanden kan in het evaluatieonderzoek, dat na drie jaar zal worden verricht, een kwantificering worden gegeven op empirische basis. Ook als het uiteindelijk zou gaan om een beperkt aantal zaken, acht ik het zowel vanuit het algemene belang van de bestrijding van criminaliteit en de veiligheid van de samenleving alsook de belangen van de betrokken slachtoffers niet goed verdedigbaar dat de verkeersgegevens niet meer beschikbaar zouden zijn. Tenslotte merk ik nog op dat er met dit wetsvoorstel geen sprake is van een «kop» op Europese regelgeving. Er wordt namelijk niet verder of minder ver gegaan dan de Europese regelgever voorschrijft. De richtlijn dataretentie laat de lidstaten juist de ruimte om te kiezen voor een bewaartermijn van minimaal zes maanden en maximaal twee jaar.

In antwoord op de vragen van de leden van de CDA-fractie naar het rapport van de Erasmus Universiteit Rotterdam merk ik op dat tijdens de onderhandelingen over het toenmalige ontwerpkaderbesluit tot bewaring van de verkeersgegevens de fracties van de Tweede Kamer hebben aangegeven behoefte te hebben aan een empirische onderbouwing van een bewaarplicht voor telecommunicatiegegevens. Aan de Erasmus Universiteit Rotterdam is toen opdracht gegeven voor een dergelijk onderzoek. Het onderzoek diende binnen een beperkt tijdsbestek te worden uitgevoerd omdat de bevindingen anders niet meer van belang zouden kunnen zijn voor de inbreng van Nederland in de onderhandelingen in Brussel. In het Algemeen Overleg ter voorbereiding van de JBZ-Raad van 2 en 3 juni 2005 is door de Tweede kamer een motie aangenomen waarin de regering werd verzocht in de JBZ-Raad te bewerkstelligen dat overleg over het initiatiefvoorstel inzake de bewaarplicht van verkeersgegevens pas zou worden voortgezet op het moment dat de resultaten van het onderzoek van de Erasmus Universiteit Rotterdam door de Kamer besproken zouden zijn (Kamerstukken II 2004/05, 23 490, nr. 372). Het onderzoek is verricht in de periode van maart 2005 tot en met mei 2005 en het eindrapport is op 20 juni 2005 aangeboden aan de Tweede Kamer (Kamerstukken II 2004/05, 23 490, nr. 379). De opvatting van de leden van de fractie van het CDA, dat het rapport in het geheel niet als een onderbouwing voor een langere dan de minimumtermijn kan worden beschouwd, deel ik niet. De leden van de fractie van het CDA hebben erop gewezen dat de onderzoekers slechts 65 opsporingsdossiers tot hun beschikking kregen. Ten behoeve van het onderzoek is door de opdrachtgever een lijst met afgeronde strafzaken aangeleverd. Uit deze lijst is door de onderzoekers een selectie van zaken gemaakt, zowel naar geografische spreiding als naar zaaksgrootte. Daarnaast zijn de onderzoeksvragen in interviews voorgelegd aan de betrokken opsporingsambtenaren teneinde zo nauwkeurig mogelijk inzicht te verkrijgen in het rendement dat in de praktijk wordt verkregen door toepassing van de bevoegdheid tot het opvragen van verkeersgegevens. In het rapport wordt geconstateerd dat een bewaartermijn van drie maanden voldoende zal zijn voor niet al te

complexe onderzoeken die op districtsniveau worden verricht maar dat een dergelijke termijn onvoldoende is voor langlopende, complexere onderzoeken op regionaal en nationaal niveau. Hierbij valt, aldus de onderzoekers, met name te denken aan onderzoeken naar verdovende middelencriminaliteit, zware milieucriminaliteit, mensenhandel en grootschalige fraudes, maar ook levensdelicten en zware zedendelicten. Ook ten aanzien van rechtshulpverzoeken en onderzoeken naar cold cases constateren de onderzoekers dat er behoefte is aan een ruime bewaartermijn. Uitvoering van rechtshulpverzoeken beslaat veelal een langere periode en ten aanzien van cold cases geldt dat te allen tijde sprake is van misdrijven die (vaak) in een ver verleden zijn gepleegd. De onderzoekers hebben vastgesteld dat de leeftijd van de opgevraagde gegevens in zijn algemeenheid hoger wordt naarmate de ernst van het gepleegde delict en de ingezette opsporingscapaciteit toeneemt. Uit de interviews is gebleken dat als gevolg van de beperkte bewaartermijn de verkeersgegevens van alle op het eerste gezicht relevant lijkende telefoonnummers worden opgevraagd. In een latere fase van het onderzoek blijkt dat slechts een deel van de gegevens daadwerkelijk van belang was. De onderzoekers concluderen dat een langere bewaartermijn kan leiden tot een meer afgewogen, beperktere bevraging van de verkeersgegevens. Hieruit kan worden afgeleid dat een kortere bewaartermijn eerder leidt tot een situatie waarin verkeersgegevens opgevraagd worden op basis van wenselijkheid («nice to have») dan in het geval van een ruimere bewaartermijn. In dit laatste geval leidt een langere bewaartermijn juist tot een meer gerichte bevraging van de gegevens. Deze conclusies komen ook overeen met de conclusies van onderzoeken die in Duitsland zijn verricht. Daarop zal hieronder, naar aanleiding van vragen van de leden van de fracties van GroenLinks en het CDA, nader worden ingegaan.

De conclusie van de leden van de CDA-fractie, dat uit het aantal van «slechts 65 dossiers», waarin verkeersgegevens een belangrijke rol hebben gespeeld, blijkt dat een bewaarplicht niet nodig is omdat de gegevens steeds beschikbaar waren deel ik evenmin. De gegevens waren beschikbaar omdat deze door de aanbieders niet waren vernietigd. Op grond van artikel 6 van de Richtlijn 2002/58/EG (Richtlijn privacy en elektronische communicatie) is de verplichting tot vernietiging in beginsel gekoppeld aan de betaling van de rekening door de klant. In bepaalde gevallen kunnen de gegevens langer worden verwerkt met het oog op bepaalde zakelijke doeleinden. Dit betekent dat die gegevens niet altijd beschikbaar kunnen zijn ten behoeve van het opsporingsonderzoek, dit hangt namelijk af van de bedrijfsvoering van de aanbieder. Dit acht ik geen wenselijke situatie. Dat er «slechts» 65 dossiers beschikbaar waren waarin de gegevens wel een belangrijke rol hebben gespeeld onderstreept juist het belang van een wettelijk vastgelegde bewaartermijn ten behoeve van de opsporing van ernstige strafbare feiten. Immers, deze dossiers betreffen de gevallen waarin de gegevens bij de aanbieders aanwezig waren. In die gevallen waarin de gegevens niet meer aanwezig waren, valt achteraf niet meer vast te stellen of deze gegevens van belang hadden kunnen zijn voor het opsporingsonderzoek en zo ja, welke bijdrage deze gegevens hadden kunnen leveren aan het resultaat van opsporing of vervolging. Een dergelijke vraagstelling zou tot een vrijwel onmogelijke bewijslast voor politie en justitie voeren. Omdat in alle onderzochte zaken de historische verkeersgegevens van belang waren voor het leveren van direct en indirect bewijs in het onderzoek hebben de onderzoekers van de EUR geen antwoord kunnen geven op de vraag in welk percentage van de zaken een verruiming van de bewaarplicht een positieve invloed zou hebben gehad op het verloop van het onderzoek. Zoals hierboven reeds is aangegeven is de onderzoekers wel gebleken van een verband tussen de leeftijd van de historische verkeersgegevens enerzijds en de ernst van het gepleegde feit en de ingezette opsporingscapaciteit

anderzijds. De onderzoekers hebben er eveneens op gewezen dat in een dossier slechts die zaken worden opgeschreven c.q. bijgevoegd die van belang zijn geweest voor de desbetreffende zaak. Het was daardoor onmogelijk voor de onderzoekers om uit de bestudering van slechts de dossiers een beeld te krijgen van die gegevens die men niet heeft gekregen, of die vorderingen die geen resultaat hebben opgeleverd voor het onderzoek. Daarom hebben ook de gesprekken met betrokkenen in de praktijk een belangrijke rol gespeeld binnen dit onderzoek (blz. 6).

De onderzoekers hebben inderdaad geen wetenschappelijk verantwoorde conclusies kunnen trekken over een bewaartermijn voor internetgegevens omdat daarvoor te weinig onderzoeksdossiers voorhanden waren. Hierover heb ik reeds eerder opgemerkt dat tot 1 september 2004 een wettelijke bevoegdheid tot het vorderen van gebruikersgegevens ontbrak. Hierdoor was opsporingsonderzoek met behulp van internetgegevens nog volop in ontwikkeling. Daarbij is ook van belang dat de aanbieders in toenemende mate telefoniediensten via internet aanbieden. Dit betekent, zoals door de EUR-onderzoekers ook is onderkend, dat de behoefte aan verkeersgegevens van internettelefonie van een vergelijkbare omvang zal aannemen als die van traditionele telefonie, zodat het voor de hand ligt voor beide vormen een gelijke bewaartermijn te hanteren. Ook het volume van de op grond van de richtlijn dataretentie te bewaren internetgegevens is niet zodanig omvangrijk ten opzichte van het volume van de op grond van die richtlijn te bewaren gegevens rond traditionele telefonie, dat dit zou strekken tot een afwijkende bewaartermijn. In dit verband merk ik tenslotte nog op dat, met uitzondering van het Verenigd Koninkrijk, ook in de andere lidstaten is gekozen voor één enkele bewaartermijn voor zowel telefonie- als internetgegevens. Niet zelden betreft dit een termijn van twaalf maanden.

De leden van de fractie van het CDA meenden – onder verwijzing naar de zaak Silver vs United Kingdom – dat met de conclusies van het onderzoek van de EUR niet is voldaan aan het noodzakelijkheidscriterium van artikel 8 EVRM. Graag reageer ik hierop als volgt.
De reikwijdte van het recht op bescherming van de persoonlijke levenssfeer zoals dit is neergelegd in artikel 8 van het EVRM vormt de uitkomst van een afweging van belangen. In de zaak Silver vs United Kingdom, van 25 maart 1983, heeft het Europese Hof geoordeeld dat het bijvoeglijk naamwoord «noodzakelijk» niet synoniem is met «onmisbaar», noch de flexibiliteit heeft van uitdrukkingen als «toelaatbaar», «gebruikelijk», «nuttig», «redelijk» of «wenselijk». In overweging no. 97 erkent het Hof echter ook dat aan de verdragspartijen een eigen beoordelingsruimte toekomt bij het opleggen van beperkingen («a certain but not unlimited margin of appreciation») en dat de zin «noodzakelijk in een democratische samenleving» betekent dat de inmenging in overeenstemming moet zijn met een «pressing sociaal need» (er moet een dringende maatschappelijke behoefte bestaan om het legitieme doel te vervullen) en proportioneel moet zijn ten opzichte van het nagestreefde doel.

Naar mijn mening zijn telecommunicatie verkeersgegevens van dermate groot belang voor de opsporing en vervolging van ernstige criminaliteit dat de voorgestelde bewaartermijn aan het noodzakelijkheidscriterium voldoet. De afweging van de Nederlandse regering blijft binnen de «bandbreedte» waarin de richtlijn voorziet. De richtlijn voorziet immers in een bewaarplicht voor een periode van ten minste zes maanden en maximaal twee jaar. Een langere bewaartermijn dan de minimumtermijn van zes maanden is van belang voor de opsporing van ernstige misdrijven in het bijzonder bij uitvoering van meer complexe opsporingsonderzoeken, internationale onderzoeken en de behandeling van cold cases, alsmede de beschikbaarheid van gegevens voor het onderzoek ter terechtzitting. In het

voorgaande is dit – in antwoord op de vragen van de leden van de fracties van het CDA en de PvdA – besproken. Dit kan worden aangemerkt als een zwaarwegend maatschappelijk belang dat zeker begrepen kan worden onder het vereiste van een «pressing social need», zoals opgenomen in artikel 8 EVRM. Naarmate de gegevens korter bewaard blijven, zal zich vaker de situatie voordoen dat gegevens niet meer voor het opsporingsonderzoek beschikbaar zijn. Een termijn van twaalf maanden is in dit opzicht naar mijn mening een minimale termijn.
Het ontbreken van kwantitatieve cijfers over de aantal zaken waarin deze gegevens een rol spelen in het welslagen van de opsporing of de vervolging, of het nemen van beslissingen in dat verband, kan daarvoor niet maatgevend zijn. Ook als de gegevens slechts in enkele gevallen van belang zouden zijn voor het oplossen van een ernstige strafzaak, zou het moeilijk te aanvaarden zijn dat de gegevens niet meer beschikbaar zouden zijn. Dit geldt temeer nu het gaat om het langer bewaren van gegevens die voor een belangrijk deel reeds door de aanbieders ten behoeve van eigen zakelijke doeleinden worden gebruikt. Het betreft gegevens die de burgers doorgaans ook zelf kunnen bevragen ten behoeve van een overzicht van het eigen belgedrag. Het gaat hier niet om de inhoud van gesprekken, het gaat hier ook niet om websurfgedrag. Het gaat om gegevens die inzicht geven in tijdstippen waarop gebruik is gemaakt van communicatieverbindingen en de aansluitnummers die bij die verbinding betrokken waren.

In reactie op het manifest van vijftien hoogleraren, waarnaar de leden van de CDA-fractie verwezen, merk ik op, dat naar mijn mening niet zozeer de bewaring van de gegevens als wel de toegang daartoe, en het verdere gebruik daarvan voor andere doeleinden dan waarvoor de gegevens waren verzameld, maatgevend is voor de aantasting van de persoonlijke levenssfeer. Dit is een essentieel punt, dat ik al eerder naar voren bracht en dat ook door het Duitse Bundesverfassungsgericht wordt erkend in de voorlopige beslissing op het beroep van een groot aantal personen tegen de in dat land vastgestelde wettelijke bewaarplicht. De bevoegdheden tot het vorderen van de gegevens zijn opgenomen in het Wetboek van Strafvordering en de WIV 2002. Voor de strafvordering geldt dat sprake moet zijn van de opsporing van ernstige misdrijven. Omdat slechts een zeer gering percentage van het aantal opgeslagen gegevens zal worden bevraagd, is er geen sprake van een ingrijpende inmenging van de overheid in de persoonlijke levenssfeer van burgers. Uit het onderzoek van de Erasmus Universiteit blijkt dat het overgrote deel van de bevragingen plaatsvindt kort nadat het misdrijf is gepleegd. Eenzelfde bevinding is gedaan door de onderzoekers van het Max Planckinstituut in Freiburg, waarop hierna in reactie op vragen van de fractie van GroenLinks wordt ingegaan. Omdat een latere bevraging van de gegevens naar verwachting minder vaak zal plaatsvinden, zal er ook door de keuze voor een langere bewaartermijn geen sprake zijn van het op grote schaal inmengen in de persoonlijke levenssfeer van burgers door de overheid. In het overgrote deel van de gevallen zullen de opgeslagen gegevens in de beslotenheid van de databases van de aanbieders blijven berusten. Overigens, ook nu kunnen de gegevens, die door de aanbieders ten behoeve van de eigen bedrijfsdoeleinden worden bewaard, door politie en justitie worden bevraagd ten behoeve van de bestrijding van ernstige misdrijven.

Concluderend ben ik, alle belangen afwegend, van oordeel dat een bewaartermijn van twaalf maanden ten minste nodig is. In de eerste plaats is er behoefte aan deze bewaartermijn met het oog op complexere opsporingsonderzoeken en rechtshulpverzoeken, zodat de gegevens daadwerkelijk beschikbaar zijn als daaraan behoefte bestaat. Daarbij kan een langere bewaartermijn leiden tot een 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 tevens kunnen dienen om de onschuld van personen aan te tonen. Voor wat betreft de aantasting van de privacy en de lasten voor het bedrijfsleven heeft een verlenging van de bewaartermijn bepaald geen uitzonderlijke gevolgen.
Met de aanneming van het amendement Anker (Kamerstukken II 2007/08, 31 145, nr. 14), heeft de Tweede Kamer gekozen voor een bewaartermijn van twaalf maanden. In zijn advies heeft ook de Raad van State aangegeven dat, nu de meeste lidstaten bij de implementatie kiezen voor een bewaartermijn van zes of twaalf maanden, het naar het oordeel van de Raad voor de hand ligt om bij deze termijnen aan te sluiten. In dat advies zijn ook de eerbiediging van de persoonlijke levenssfeer en de lasten voor het bedrijfsleven betrokken. Met een bewaartermijn van twaalf maanden sluit Nederland aan bij de keuze in een aantal andere lidstaten, zoals Frankrijk, het Verenigd Koninkrijk, België, Spanje, en Denemarken. Daarbij zijn er goede redenen voor eenzelfde bewaartermijn voor zowel telefonie- als internetgegevens.

De leden van de fracties van ChristenUnie en SGP vroegen zich, naar aanleiding van mijn opmerkingen over de moord op de Hells Angels in Oirsbeek, af of telecombedrijven en internetproviders de gegevens weliswaar twaalf maanden moeten bewaren maar vervolgens niet verplicht zijn deze na afloop van de bewaartermijn te vernietigen.
Deze vraag moet ontkennend worden beantwoord. Ter implementatie van de richtlijn dataretentie (artikel 7) zijn de aanbieders verplicht de bewaarde gegevens na afloop van de bewaarperiode onverwijld te vernietigen. Deze verplichting wordt vastgelegd in de Telecommunicatiewet (artikel 13.5, derde lid, onderdeel b, Tw). In het ontwerpbesluit beveiliging gegevens telecommunicatie is vastgelegd dat de aanbieders ervoor zorg moeten dragen dat de gegevens uiterlijk binnen acht dagen na afloop van de wettelijke bewaartermijn worden vernietigd. Niet uitgesloten is dat de bewaarde gegevens na het verstrijken van de wettelijke bewaartermijn op grond van de Telecommunicatiewet verder kunnen worden verwerkt voor de in de artikelen 11.5 en 11.5a van die wet genoemde doeleinden. Dit betreft de facturering, het verrichten van marktonderzoek en het leveren van diensten met een toegevoegde waarde. Dan zijn de voor die doelen geldende verplichtingen tot anonimisering of vernietiging op de verdere verwerking van toepassing.

De leden van de fractie van GroenLinks vroegen of de regering het met hen eens is dat een ingrijpende inbreuk op de privacy als het bewaren van persoonlijke gegevens gelegitimeerd moet zijn door het aantonen van nut en noodzaak. Zij wezen hierbij op de uitkomsten van het Max Planckinstituut in Freiburg en een onderzoek van het Bundeskriminalamt uit 2005 waaruit zou blijken dat nut en noodzaak van een langere beschikbaarheid dan zes maanden van verkeersgegevens niet zijn aangetoond. Zij vroegen op welke wijze Nederland een bewaartermijn van een jaar rechtvaardigt terwijl andere landen een termijn van zes maanden voldoende achten. Ook de leden van de CDA-fractie refereerden aan het onderzoek van het Max Planckinstituut waarnaar wordt verwezen in een uitspraak van het Bundesverfassungsgericht. Voorts wezen zij op een onderzoek door de brancheorganisatie Bitkom. Zij vernamen graag de visie van de regering op de conclusies van deze onderzoeken.
In antwoord op de gestelde vragen ben ik het met de leden van GroenLinks eens dat een ingrijpende inbreuk op de privacy gelegitimeerd moet zijn door het aantonen van nut en noodzaak van de voorgestelde maatregel. Ik verschil evenwel van mening met de leden van GroenLinks waar de vraagstelling ervan uitgaat dat een ingrijpende inbreuk op de privacy het gevolg is van een bewaartermijn van langer dan zes maanden. Hierboven heb ik, naar aanleiding van vragen van de leden van de fracties van

het CDA, PvdA en SP, aangegeven dat niet zozeer de bewaring van de gegevens een inmenging in de persoonlijke levenssfeer met zich meebrengt als wel de toegang tot die gegevens en het verdere gebruik daarvan voor andere doeleinden dan waarvoor die gegevens oorspronkelijk waren verzameld. Zoals hiervoor beschreven, is die toegang beperkt tot zwaarwegende gevallen. Op de uitspraak van het Duitse Bundesverfassungsgericht wordt hieronder, naar aanleiding van vragen van de leden van de fractie van het CDA naar de gevolgen van aanhangige rechtszaken, nader ingegaan. Met betrekking tot de onderzoeken waaraan door de leden van GroenLinks en de CDA-fractie wordt gerefereerd, merk ik op dat elk land eigen opsporingsmethodieken en onderzoeksmethoden hanteert voor de opsporing en vervolging van strafbare feiten. Dit blijkt ook uit de bevindingen van de onderzoekers van het Max Planckinstituut. Zij melden dat uit schriftelijke bevragingen van regeringen blijkt dat uit enkele Europese landen geen problemen worden gemeld met de toenmalige regelgeving inzake de bewaring van verkeersgegevens, terwijl andere landen wijzen op het probleem van reeds gewiste gegevens waardoor opsporingshandelingen mislukten. Voorts wijst het onderzoek uit dat in Duitsland het aantal bevragingen van (verkeers)gegevens sterk is toegenomen. Vooral de jaren 2004 en 2005 laten een hoge stijging van het aantal aanvragen van verkeersgegevens zien. Deze stijging strookt met het belang dat de opsporing- en vervolgingsautoriteiten hechten aan de beschikbaarheid van verkeersgegevens.
In het onderzoek van het Bundeskriminalamt uit 2005 zijn 381 gevallen onderzocht waarin verkeersgegevens zijn opgevraagd door de politie. Het zwaartepunt lag bij de delicten tegen de seksuele zelfbestemming («Selbstbestimmung»), delicten rond bedrog en misdrijven tegen het eigendom. Van de 381 gevallen hadden er 166 betrekking op internetgegevens (43,6%), 165 op telefoniegegevens (43,3%) en 31 op e-mail via internet (8,1%). Uit het gepresenteerde cijfermateriaal komt naar voren dat bij de bevraging van de gegevens door de opsporingsautoriteiten, de nadruk lag op bevraging tot zes maanden na de bewaring van de gegevens. In 35 zaken kon geen aanwijzing voor een bewaartermijn worden verkregen (z.g. non values).Voor wat betreft de lengte van de bewaartermijn spreken de onderzoekers voor een aantal delicten van een «Idealspeicherzeitraum» tot zes maanden. Uit het beschikbare cijfermateriaal blijkt echter dat het regelmatig voorkomt dat verkeersgegevens ook in een later stadium zijn opgevraagd. Van de 346 resterende zaken kwam in ruim 27% een bewaartermijn van twaalf maanden of meer als ideaal naar voren. Dit betrof 71 gevallen tot twaalf maanden en 23 gevallen langer dan twaalf maanden. Vooral bij de bestrijding van drugsdelicten werd een bewaartermijn van twaalf maanden of meer als ideaal gezien. De onderzoekers stellen vast dat de bewaartermijnen tussen de aanbieders onderling verschillend zijn en tussen de 72 uur en drie tot zes maanden liggen. Volgens de onderzoekers zijn minimumbewaartermijnen voor de opsporing van strafbare feiten dringend gewenst.
In het onderzoek van het Max Planckinstituut uit februari 2008 wordt vastgesteld dat er geen betrouwbare gegevens voorhanden zijn over het gebruik van verkeersgegevens en de gevolgen van de bevraging. De (tot dan toe) beschikbare bevindingen wijzen er op dat het gebruik van de gegevens op korte termijnen is geconcentreerd. Het aantal vorderingen tot de verstrekking van verkeersgegevens is van 2002 tot 2005 sterk toegenomen. Het aantal bevragingen van IMEI-nummers is verviervoudigd. Het totaal aantal vragen om verkeersgegevens is gestegen van onder de 5 000 in 2000 tot ongeveer 40 000 in 2005. De tendens is sterk stijgend. Met de snelle verspreiding van de mobiele communicatie is de bevraging van verkeersgegevens tot een wijdverbreid onderzoeksmiddel geworden. Het onderzoek heeft plaatsgevonden door middel van documentenanalyse in enkele deelstaten, enquêtes binnen het Openbaar Ministerie en interviews met sleutelpersonen. Uit onderzoek van de bevragingen bij twee

aanbieders, over een periode van drie maanden, blijkt dat de maatregel bij telefonie vooral wordt gebruikt voor de opsporing van oplichting en bedrog (30%), roof- en moord (10%) en delicten rond verdovende middelen (8%). Bij internetgegevens spelen kinderpornografie (30%) en inbreuken op het auteursrecht een vermeldenwaardige rol. Opgemerkt wordt dat de bevraging van verkeersgegevens zich aan het ontwikkelen is tot een onderzoeksmiddel voor bijna alle categorieën van strafbare feiten, dat sterk is gericht op de contacten tussen dader en slachtoffer en dat dit als minder belastend wordt beoordeeld. De onderzoekers achten het opvallend dat de rechtspolitieke debatten en de praktijk op dit punt uiteenlopen. Het zwaartepunt van de bevragingen ligt binnen drie maanden, daarbinnen ligt een zwaartepunt binnen één dag. De onderzoekers melden hierover dat de praktijk van de strafvervolging zich kennelijk heeft ingesteld op de opslagpraktijk van het bedrijfsleven («Offensichtlich hat sich die Strafverfolgungspraxis auf die Speicherungspraktiken der Unternehmen eingestelt»). Daarnaast wordt door de vertegenwoordigers van politie en justitie melding gemaakt van verschillende bewaartermijnen bij de aanbieders. De vertegenwoordigers van het Openbaar Ministerie hebben een bewaartermijn van zes tot twaalf maanden bepleit. Uit het documentonderzoek is naar voren gekomen dat problemen met de bewaring in 63 gevallen een rol hebben gespeeld. Bij de aanbevelingen wijzen de onderzoekers er op dat het opvragen van verkeersgegevens ook in gevallen van middelzware criminaliteit wordt ingezet, zoals criminaliteit door middel van eindapparatuur («Endgeräte»), waar de verkeersgegevens het enig bruikbare aanknopingspunt voor het onderzoek bieden. Doordat het wetsvoorstel hiervoor ruimte blijft bieden zal de spanning tussen de behoefte van de opsporing en de bescherming van vrijheidsrechten versterken. Inmiddels is deze kwestie voorgelegd aan het Duitse Bundesverfassungsgericht. Hierop wordt, naar aanleiding van vragen van de leden van de fracties van CDA en GroenLinks, nader ingegaan in de paragraaf over de gevolgen van aanhangige rechtszaken. Verder merken de onderzoekers op dat een bewaartermijn van zes maanden op grond van de uitkomsten van het empirisch onderzoek gegrond is. Op grond van de enquête is het belang van een langere bewaartermijn tot twaalf maanden kenbaar maar op grond van documentonderzoek zou ongeveer 2% van het aantal bevragingen onder de huidige omstandigheden mislukken. Dit betreft de eerdervermelde 63 gevallen.

Hierbij dient echter bedacht te worden dat de onderzoeken zijn 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 in het belang van de bedrijfsvoering strikt noodzakelijk is zo concludeert het onderzoek van Bitkom. Een rol kan derhalve inderdaad spelen dat het wellicht doorgaans geen zin zou hebben gehad oudere gegevens te bevragen omdat deze niet meer voorhanden waren. Dit strookt met de bevindingen van de onderzoekers van de Erasmus Universiteit Rotterdam en het Max Planckinstituut, die dit kwalificeren als anticiperend gedrag. Omdat de verwachting bestaat dat de gegevens niet meer voorhanden zullen zijn worden ze niet meer bevraagd. 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 van Bitkom betrokken waren wetgeving aanvaard waarin

wordt voorzien in uitéénlopende bewaartermijnen. Zo is in Frankrijk een bewaartermijn van twaalf maanden vastgesteld en Italië één van twee jaar.

Dat wetenschappers van diverse disciplines hebben benadrukt dat niet overtuigend is aangetoond dat de bewaarplicht tot het oplossen van veel misdrijven leidt, heb ik niet in het betreffende artikel uit NRC van 2 april 2008 kunnen lezen. Integendeel, deze wetenschappers erkennen dat met een lange bewaarplicht sommige zaken makkelijker opgelost kunnen worden. Zij kwalificeren dit als een belangrijk maar niet afdoende argument. Overigens heb ik ook nooit gesteld of verdedigd dat met een langere bewaartermijn veel misdrijven kunnen worden opgelost. Waar het om gaat is dat een kortere bewaartermijn de kans zal verkleinen dat de gegevens beschikbaar zijn als daaraan behoefte bestaat tijdens het opsporingsonderzoek dan wel in het stadium van de strafvervolging.

Voor de vraag van de leden van de fractie van GroenLinks op welke wijze de Nederlandse situatie een bewaartermijn van een jaar rechtvaardigt, terwijl Duitsland, Finland, Tsjechië en Zweden een termijn van zes maanden voldoende achten, verwijs ik naar de beantwoording van de vragen van de leden van de fracties van het CDA, de PvdA en de SP over de bewaartermijn. In dit verband merk ik nog op dat Zweden nog geen bewaartermijn heeft vastgesteld en dat andere lidstaten juist hebben gekozen voor een langere termijn dan de zes maanden. De richtlijn biedt de lidstaten expliciet de ruimte voor het vaststellen van een langere bewaartermijn. Ierland kende een bewaartermijn van drie jaar. De Ierse regering vindt een maximale bewaartermijn van twee jaar niet voldoende en heeft inmiddels bij het Europese Hof van Justitie beroep ingesteld tegen de rechtsgrondslag van de richtlijn. Italië kende een maximale bewaartermijn van vier jaar voor telefoniegegevens en zal deze termijn naar beneden moeten bijstellen. De keuze voor een specifieke bewaartermijn is afhankelijk van de afweging tussen de betrokken belangen, zoals de behoefte van de opsporing en vervolging, de bescherming van de persoonlijke levenssfeer en de lasten voor de aanbieders. Op dit punt kunnen de lidstaten verschillende accenten plaatsen. In Nederland is het aftappen van telecommunicatie, evenals het vorderen van verkeersgegevens, een belangrijk middel in de opsporing van ernstige strafbare feiten omdat daarmee een goed beeld kan worden verkregen van de kring van personen met wie de betrokken persoon contact onderhoudt. Daardoor kan de inzet van meer ingrijpende bevoegdheden, zoals de infiltratie of het runnen van informanten, worden vermeden. Ook andere landen – zoals het Verenigd Koninkrijk, België, Frankrijk, Italië en Ierland – hebben voor een langere bewaartermijn gekozen.

De bewaring van verkeersgegevens

De leden van de fractie van het CDA wezen op verschillende ontwikkelingen met betrekking tot internet. Dit betrof aspecten als het destilleren van verkeersgegevens uit de databases door de providers van internetdiensten, de enorme hoeveelheid van de te bewaren internetgegevens – ook in relatie tot de explosieve toename van het internetverkeer – en de introductie van het fenomeen van het eenmalige IP-adres. Omdat de netwerken van providers het verkeer van klanten via heel verschillende servers afhandelen, kunnen de complete verkeersgegevens van een klant alleen worden bemachtigd door een volledige tap op een klant te zetten, dat wil zeggen inclusief de inhoud. De leden van deze fractie vroegen deze ontwikkelingen in de beantwoording van de vraag naar nut en noodzaak van de voorgestelde bewaarplicht, dan wel de proportionaliteit daarvan, te betrekken. De leden van de fractie van de SP had de indruk dat de regering niet precies voor ogen heeft tot welke praktische gevolgen het

invoeren van deze ongemotiveerd lange bewaartermijn zal kunnen leiden en zag graag een degelijker onderbouwing van de kant van de regering.

De stelling van de leden van de CDA-fractie, dat de complete verkeersgegevens van een klant alleen kunnen worden bemachtigd door een volledige tap op de klant te zetten (inclusief inhoud) en dat de providers daaruit de verkeersgegevens moeten destilleren, komt mij minder waarschijnlijk voor. Er zijn inmiddels diverse leveranciers van systemen voor dataretentie. Geen van die systemen is gebaseerd op een werkwijze zoals de leden van de CDA-fractie deze beschrijven. Ook de stelling dat het internetverkeer explosief is toegenomen, kan niet zonder meer tot de conclusie leiden dat dit tot een kortere bewaartermijn (dan de voorgestelde twaalf maanden) moet leiden. Immers, de toename van het internetverkeer wordt vooral veroorzaakt door de toename van de bandbreedte die internetgebruikers tot hun beschikking hebben. Dat maakt het namelijk mogelijk om zeer omvangrijke bestanden te downloaden en uit te wisselen. Dit toegenomen internetverkeer leidt echter niet noodzakelijkerwijs tot meer verkeersgegevens, en zeker niet tot meer gegevens die onder de bewaarplicht vallen, nu op grond van dit wetsvoorstel uitsluitend de gegevens voor internettoegang bewaard moeten worden. Ook de toename van het aantal IP-adressen leidt niet per definitie tot een enorme toename van het aantal te bewaren gegevens. Op grond van de richtlijn moeten alleen de gegevens betreffende internettoegang bewaard worden en niet de gegevens over het websurfgedrag. Wanneer eenmaal toegang tot het internet is verkregen, behoeven vervolgens geen gegevens meer bewaard te worden. Bij internettoegang moet onder meer het IP-adres worden vastgelegd. Voor de hoeveelheid te bewaren gegevens maakt dit echter geen verschil omdat van iedere communicatie het IP-adres, dat door de aanbieder aan een communicatie is toegewezen, moet worden bewaard. Dat voor iedere website een ander IP-adres wordt verleend, maakt voor de hoeveelheid te bewaren gegevens dus geen verschil. De richtlijn maakt dan ook geen onderscheid in statische of dynamische IP-adressen (artikel 5, eerste lid, onderdeel c, punt 2, onder i). Daarnaast kan erop gewezen worden dat, mocht al sprake zijn van toename van de te bewaren gegevens, de opslagcapaciteit en de digitale transportcapaciteit door de technologische ontwikkeling elke vierentwintig maanden verdubbelt. Dit betekent dat een toename in de te bewaren gegevens tegelijkertijd wordt gecompenseerd door een toename van de computerkracht en de opslagcapaciteit.

In antwoord op de vraag van de leden van de fractie van de SP merk ik op dat de bewaarplicht geldt voor de gegevens die door de aanbieders worden gegenereerd of verwerkt. Voor een deel worden de gegevens op dit moment door de aanbieders reeds voor eigen bedrijfsdoeleinden bewaard. Volgens de kostenberekening van het onderzoeksbureau VKA zouden de extra kosten die zijn verbonden aan de inzet van extra geheugencapaciteit als gevolg van verlenging van de bewaartermijn met zes maanden ongeveer zeven miljoen euro kosten. Bij de berekeningen ging VKA destijds nog uit van een bedrag van 34 000 euro per terabyte. Inmiddels is de prijs van geheugencapaciteit afgenomen tot 2 200 euro per terabyte. Dit zou betekenen dat een verkorting van een bewaartermijn van een half jaar voor de gehele marktsector thans een kostenreductie zou betekenen van ongeveer 400 000 euro. In de memorie van toelichting is nog uit gegaan van een bedrag van ongeveer 7 miljoen euro per half jaar. De ontwikkelingen in de stand der techniek leiden aldus tot een enorme kostenreductie voor de geheugencapaciteit. Weliswaar is het te verwachten dat de aanbieders deze kosten zullen doorberekenen aan de klanten doch de meerprijs hiervan zal per klant verwaarloosbaar klein zijn. Gelet op de belangen die hierbij aan de orde zijn, en de bedragen die de

Nederlandse burgers op jaarbasis aan hun telefonie- of internetaansluiting besteden, meen ik dan ook dat dit geen onoverbrugbare kostenpost vormt.

De leden van de fractie van D66 stelden de vraag op grond van welke argumenten de keuzes voor nadere regulering in een AMvB zijn gemaakt. Specifiek bedoelden deze leden de nadere regulering van welke gegevens op welke wijze opgeslagen dienen te worden, hoe deze gegevens beschikbaar kunnen worden gemaakt voor de opsporingsdiensten, hoe deze adequaat beschermd kunnen worden en hoe wordt gecontroleerd dat er met deze privacygevoelige gegevens correct wordt omgegaan.
In antwoord op deze vragen merk ik allereerst op dat het ook op dit moment voorkomt dat verkeersgegevens van de aanbieders worden gevorderd ten behoeve van de opsporing van ernstige strafbare feiten. Het Besluit beveiliging gegevens aftappen telecommunicatie is daarop van toepassing. Dit besluit geeft nadere regels voor de beveiliging van de gegevens bij de uitvoering van een vordering tot verstrekking van verkeersgegevens. Het besluit verplicht de aanbieder tot het treffen van maatregelen ter voorkoming van kennisneming door onbevoegden van de informatie welke door de aanbieder aan de bevoegde autoriteit is verstrekt alsmede de gegevens die zijn vervat in het aan deze verstrekking ten grondslag liggende vordering van de bevoegde autoriteit. Ook verplicht het besluit de aanbieders tot het opstellen van een beveiligingsplan, waarin wordt aangegeven op welke wijze uitvoering is gegeven aan de in de bijlage bij die regeling opgenomen maatregelen. Dit betreft beveiligingseisen ten aanzien van het personeel, de fysieke beveiliging van de informatie, het beheer van communicatie- en bedieningsprocessen, de toegangsbeveiliging van geautomatiseerde informatiesystemen en de ontwikkeling en het onderhoud van die systemen. Voor de nadere regulering van de beveiligingsmaatregelen rond de bewaarplicht zal nauw worden aangesloten bij het Besluit beveiliging gegevens aftappen telecommunicatie. Aan die keuze liggen de volgende overwegingen ten grondslag. In de eerste plaats voldoen deze regels ook voor de beveiliging van gegevens in verband met de bewaarplicht. Aansluiting bij dit besluit is goed mogelijk en, bezien vanuit het oogpunt van heldere regelgeving, ook wenselijk. In de tweede plaats zijn de aanbieders goed bekend met deze regels en hebben deze kunnen integreren in hun bedrijfsvoering. De gegevens, die door de aanbieders op grond van de wettelijke bewaarplicht worden verwerkt, worden doorgaans niet in een afzonderlijke database opgeslagen maar vormen onderdeel van een bestand van gegevens die door de aanbieders ook voor zakelijke doeleinden worden verwerkt. De gegevens die onder de bewaarplicht vallen, behoeven dus niet te worden afgezonderd van andere gegevens die door de aanbieders ten behoeve van de eigen bedrijfsvoering worden verwerkt. Dit zou in de praktijk eenvoudig tot dubbele opslag van gegevens kunnen leiden. In de overwegingen bij de richtlijn dataretentie is vastgelegd dat de bewaring van de gegevens op een zodanige manier dient te gebeuren dat voorkomen wordt dat de gegevens twee keer worden bewaard (Overweging no. 13). De beschikbaarstelling van de gegevens door de aanbieders zal zoveel mogelijk geautomatiseerd gaan verlopen. Op dit moment wordt op Europees niveau gewerkt aan de totstandkoming van een gemeenschappelijke standaard voor de verstrekking van de gegevens, de zogenaamde ETSI-standaard. Dit is een gemeenschappelijke standaard voor het door middel van een interface langs elektronische weg verstrekken van de bewaarde telecommunicatiegegevens. Naar verwachting zal van deze standaard in oktober van dit jaar een eerste versie uitgebracht worden. Zodra deze standaard is vastgesteld zal dit aanleiding kunnen zijn tot het stellen van nadere regels in het ontwerpbesluit beveiliging gegevens telecommunicatie, dat thans in voorbereiding is. De Wet bescherming persoonsgegevens en de Telecommunicatiewet geven

regels voor de bescherming van persoonsgegevens die door de aanbieders worden verwerkt. Op grond van de bestaande normen kan reeds een voldoende niveau van bescherming en beveiliging van de gegevens worden geboden. Het is dan ook niet zozeer de bewaring van de gegevens als zodanig die relevant is voor de noodzaak van aanvullende maatregelen ter bescherming en beveiliging, als wel de mogelijkheid tot het leggen van verbanden tussen die gegevens en de opsporing en vervolging van strafbare feiten. Daarom zullen de aanvullende, specifieke verplichtingen voor de aanbieders ten aanzien van de bescherming en de beveiliging van de bewaarde gegevens zich richten op de raadpleging en de verdere verwerking daarvan ten behoeve van opsporing en vervolging. De toegang tot deze gegevens is voorbehouden aan daartoe geautoriseerde personen voorzover dit voor hun functie noodzakelijk is. Het toezicht op de naleving van de regels wordt uitgeoefend door het Agentschap Telecom. Op de taakuitvoering door het AT zal hieronder, naar aanleiding van vragen van de leden van de VVD-fractie over de verhouding tot het recht op bescherming van de persoonlijke levenssfeer, nader worden in gegaan.

Gegevensverwerking en gegevensbeveiliging

De leden van de fractie van het CDA wezen op de kwetsbaarheid van digitale data voor zowel grootschalige als kleinschalige (gerichte) manipulatie op afstand en meenden dat het een fictie is om enkel digitale data richtinggevend te achten voor een effectieve opsporing. Volgens deze leden zou dataretentie een bron zijn van schijnveiligheid omdat verkeersgegevens nooit kunnen aantonen dat een individu verkeer heeft veroorzaakt en omdat criminelen eenvoudig valse sporen kunnen uitzetten als afleiding van hun werkelijke activiteiten. De leden van deze fractie vernamen graag het standpunt van de regering met betrekking tot deze analyse.

In reactie op deze analyse merk ik op dat de leden van de fractie van het CDA terecht stellen dat het een fictie is om enkel digitale data richtinggevend te achten voor een effectieve opsporing. Digitale data moeten worden geïnterpreteerd (is het wel logisch dat deze persoon in dit onderzoek voorkomt), worden vergeleken met andere in het onderzoek beschikbare gegevens en worden geverifieerd (adresgegevens bij de GBA bijvoorbeeld). Maar ook wanneer verkeersgegevens niet de werkelijke bron van communicatie weergeven, zijn het voor de opsporing zeer relevante gegevens op grond waarvan nader onderzoek gedaan kan worden. Immers, juist in zaken van hacken, botnets en andere vormen van computercriminaliteit hebben de betrokkenen dikwijls het een en ander te verbergen en zijn de achtergelaten gegevens juist van belang om het «kwaadwillend gedrag» en de veroorzakers daarvan te achterhalen. Dat daarbij meer nodig is dan het oppervlakkig bestuderen van deze gegevens moge duidelijk zijn.

De leden van de fractie van GroenLinks vroegen of de regering op de hoogte is van de uitkomsten van de expertmeeting die de Eerste Kamer op 20 maart 2008 met betrekking tot gegevensbescherming heeft gehouden en of ik op basis van de in de Senaat breed gedragen criteria die de heer Franken heeft opgesomd een legitimering kan geven van de door de regering voorgestelde implementatiewet.
In antwoord op de gestelde vragen merk ik op dat de regering inderdaad op de hoogte is van de uitkomsten van die expertmeeting. In die bijeenkomst heeft de heer Franken een aantal criteria geformuleerd voor de afweging bij de toekenning van nieuwe bevoegdheden. De door de heer Franken gegeven criteria zijn als volgt:
1. noodzaak, met effectiviteit en hanteerbaarheid daarbij;

2. proportionaliteit;
3. een privacy impact assessment;
4. de mogelijkheid van controle door een onafhankelijk orgaan of door rechtsbescherming;
5. een horizonbepaling, zodat er een review na korte tijd komt[1].

Over de vraag of bepaalde criteria kunnen worden aangelegd voor de toekenning van nieuwe bevoegdheden merk ik op dat ook bij consensus over de aan te leggen criteria, een zeker verschil van inzicht mogelijk zal blijven over de uitkomsten van de afweging. Dat is vrijwel inherent aan het politieke proces. De genoemde criteria zijn voor de legitimering en onderbouwing van het wetsvoorstel van groot belang. Bij eerdere gelegenheden en ook in deze memorie van antwoord, ben ik ingegaan op de noodzaak van het wetsvoorstel, daaronder begrepen de effectiviteit en hanteerbaarheid. Graag verwijs ik naar hetgeen hiervoor aan de orde is gekomen in antwoord op de vragen van de leden van de fracties van het CDA en GroenLinks. Het wetsvoorstel dient ter implementatie van een Europese richtlijn tot bewaring van bepaalde categorieën van telecommunicatiegegevens. De richtlijn dataretentie verplicht tot een bewaartermijn van minimaal zes maanden en maximaal twee jaar. Hiervoor is besproken waarom een bewaartermijn van twaalf maanden naar mijn mening een minimale termijn is. De effectiviteit van de bewaarplicht is daarbij zeer gebaat. Een kortere bewaartermijn zou tot gevolg hebben dat in meer complexere onderzoeken en bij rechtshulpverzoeken alsmede in geval van nader onderzoek ter terechtzitting, verkeersgegevens niet meer beschikbaar zouden zijn.
Een afzonderlijk privacy impact assessment is niet verricht, de implementatietermijn laat daarvoor in dit geval ook geen ruimte. De richtlijn verplicht tot een bewaartermijn van minimaal zes maanden en maximaal twee jaar, zodat een dergelijk assessment zich dan zou moeten beperken tot de vaststelling van de bewaartermijn binnen die bandbreedte. Naar mijn mening zal de waardering van de uitkomsten van een dergelijk onderzoek niet goed kunnen worden losgekoppeld van de afwegingen omtrent nut en noodzaak van de bewaarplicht als zodanig. Het onderzoek van de Erasmus Universiteit Rotterdam beoogt meer inzicht te geven in een aantal concrete onderzoeksvragen die daarbij aan de orde zijn. Daarnaast is in de uitgebrachte adviezen, onder andere het advies van het College bescherming persoonsgegevens, uitgebreid aandacht geschonken aan de verhouding tussen de voorgestelde maatregel en het ook in internationale verdragen vastgelegde recht op eerbiediging van de persoonlijke levenssfeer. Ik ben dan ook van mening dat thans voldoende informatie beschikbaar is voor een afgewogen besluitvorming op politiek niveau.
In de mogelijkheid van controle is voorzien doordat het toezicht op de verwerking van persoonsgegevens wordt uitgeoefend door het Agentschap Telecom van de minister van Economische Zaken. De toezichthoudende taak van de minister van Economische Zaken ten aanzien van de naleving van hoofdstuk 13 van de Telecommunicatiewet doet op geen enkele wijze afbreuk aan de toezichtbevoegdheden die het College bescherming persoonsgegevens (Cbp) heeft met betrekking tot de verwerking van persoonsgegevens. Het Cbp is dan ook bevoegd om op ieder gewenst moment zelfstandig toezichthoudende bevoegdheden te ontplooien. Daarnaast kan de betrokkene zelf met betrekking tot de bewaarde gegevens de rechten uitoefenen die op grond van de Wet bescherming persoonsgegevens (Wbp) aan hem zijn toegekend. De Wbp biedt de nodige mogelijkheden voor betrokkene om op de hoogte te raken van het feit dat over hem gegevens worden verwerkt en desgewenst tegen een dergelijke gegevensverwerking op te komen. Daartoe heeft de betrokkene een recht op kennisneming, dat wil zeggen dat hij zich tot de aanbieder kan richten met het verzoek hem mede te delen of hem betref-

[1] Kamerstukken I 2007/08, 31 200 VI, F, blz. 36.

fende persoonsgegevens worden verwerkt (art. 35 Wbp). Daarnaast heeft de betrokkene het recht op correctie van persoonsgegevens als deze feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn of anderszins in strijd met een wettelijk voorschrift worden verwerkt (art. 36 Wbp). Ingeval de aanbieder zou weigeren aan een dergelijk verzoek gevolg te geven dan kan de betrokkene zich tot de rechtbank wenden voor een bevel aan de aanbieder om aan het verzoek te voldoen (art. 46 Wbp) dan wel tot het College bescherming persoonsgegevens voor advies of bemiddeling (art. 47 Wbp).
Voor wat betreft de horizonbepaling tenslotte, voorzien zowel de richtlijn als het wetsvoorstel in een evaluatiebepaling. Uiterlijk op 15 september 2010 brengt de Commissie aan het Europees parlement en de Raad een evaluatieverslag uit over de toepassing van deze richtlijn en de weerslag ervan op de marktdeelnemers en de consumenten, teneinde na te gaan of het nodig is de bepalingen van deze richtlijn aan te passen, in het bijzonder wat betreft de lijst van gegevens en de vastgestelde bewaringstermijnen. De resultaten van de evaluatie worden openbaar gemaakt (artikel 14, eerste lid). Daarnaast zal, op grond van het amendement Anker, de Wet bewaarplicht telecommunicatiegegevens drie jaar na inwerkingtreding – en vervolgens iedere drie jaar – worden geëvalueerd. Deze evaluatie zal ingaan op de vraag hoeveel vorderingen tot verstrekking van gegevens aan de bevoegde autoriteiten zijn gedaan, alsmede op de vraag hoe oud de gevorderde gegevens waren. Hierdoor zal de noodzaak van de bewaartermijn van twaalf maanden ten opzichte van een bewaartermijn van zes maanden nader beoordeeld kunnen worden.

De verhouding tot het recht op bescherming van de persoonlijke levenssfeer

De leden van de fractie van het CDA vroeg de mening van de regering naar aanleiding van de eerste stelling in het manifest van de hoogleraren, dat is gepubliceerd in NRC Handelsblad van 21 mei 2008, die inhoudt dat onschuldige burgers last zullen krijgen van fouten die onvermijdelijk in de praktijk zullen worden gemaakt. Deze gegevens zullen kunnen leiden tot meer en meer ernstige fouten, bij het nemen van beslissingen over huiszoeking of het treffen van dwangmaatregelen, en kunnen «op straat» komen te liggen. Daarbij komt dat verkeersgegevens niet alleen voor de overheid een interessante bron van informatie vormen. Omdat gericht en ongericht kan worden gezocht vormt de dataset achter dataretentie de heilige graal voor de georganiseerde misdaad, aangezien de toegang tot die data deuren opent voor corruptie op grote schaal, aldus het manifest. In antwoord op deze vraag merk ik op dat, naar ik aanneem, wordt gedoeld op het artikel van vijftien hoogleraren in NRC Handelsblad van 2 april 2008. Over de stelling in dit artikel dat onschuldige burgers last zullen krijgen van fouten die onvermijdelijk gemaakt zullen worden, merk ik op dat deze door de stellers niet wetenschappelijk, bijvoorbeeld aan de hand van cijfermateriaal, wordt onderbouwd. Overigens is het voor mij lastig voor te stellen op welke fouten zij specifiek het oog hebben. In het algemeen dient de politie zorgvuldig om te gaan met ingewonnen informatie. Men moet er altijd rekening mee houden dat informatie verouderd of onjuist kan zijn. Doorgaans zal men informatie trachten te verifiëren voordat men tot handelingen overgaat die ingrijpend voor burgers kunnen zijn. Bij dit wetsvoorstel gaat het om gegevens over aansluitnummers, de tijdstippen van verbinding, de duur van de verbinding en dergelijke. Dit zijn gegevens van technische aard die als zodanig weinig inzicht bieden in de levenssfeer van de betrokkenen. De bewaarde gegevens kunnen onder bepaalde voorwaarden worden opgevraagd ten behoeve van opsporing en vervolging. De bescherming van de persoonlijke levenssfeer van betrokkenen en de afscherming van het opsporingsonderzoek nopen tot een zeer zorgvuldige behandeling van de gegevens-

verstrekking door de aanbieders. Deze gegevens zullen doorgaans niet worden gebruikt voor het nemen van beslissingen omtrent het nemen van dwangmaatregelen, zoals een huiszoeking, maar ten behoeve van het verkrijgen van inzicht in de aard en structuur van de contacten tussen personen die bij die criminele activiteiten zijn betrokken. Vanwege de gevoeligheid van deze verwerking is de toegang tot de gegevens ten behoeve van de opsporing en vervolging, evenals de verstrekking daarvan aan de bevoegde autoriteiten, met strikte waarborgen omgeven. Op grond van het Besluit beveiliging aftappen gegevens telecommunicatie gelden deze waarborgen ook thans reeds voor de afhandeling van verzoeken tot het aftappen van telecommunicatie en de verstrekking van verkeersgegevens. Hierboven is, naar aanleiding van vragen van de leden van de D66-fractie over de bewaring van verkeersgegevens, reeds aangegeven dat voor de nadere regels ter beveiliging van de gegevens die onder de bewaarplicht vallen, zal worden aangesloten bij de regels van dit besluit. Voorzover daarbij toch fouten worden gemaakt dan zullen die doorgaans kunnen worden gecorrigeerd door middel van overleg tussen de aanbieder en de betrokken rechtshandhavingsautoriteit. Overigens voorzien het Wetboek van Strafvordering en de Wet bescherming persoonsgegevens in de nodige voorzieningen voor de betrokkene om eventuele fouten te corrigeren of anderszins te herstellen. Dit alles overziend ben ik van mening dat er onvoldoende aanleiding lijkt te bestaan om in dit verband te spreken van een heilige graal, die aanleiding kan geven tot corruptie op grote schaal.

De leden van de VVD-fractie wezen erop dat de ervaring leert dat veel internetproviders geen prioriteit geven aan de kwaliteit van de te bewaren gegevens en vroegen hoe de regering gaat bevorderen dat de providers maatregelen zullen treffen om de kwaliteit van die gegevens – of ook de juistheid en volledigheid daarvan – te waarborgen. De leden van de PvdA-fractie vroegen of de regering het met hen eens is dat de kans op fouten toenemen naarmate de bewaartermijn langer is. Zij wilden graag weten in hoeverre de bestaande ICT-systemen op deze ingrijpende taakopdracht zijn toegerust, welke mogelijkheden de burger heeft om ingrijpende fouten te (laten) herstellen en aan welke termijn van implementatie de regering in dit verband denkt.
In antwoord op de gestelde vragen merk ik allereerst op dat internetproviders wel degelijk prioriteit geven aan de kwaliteit van de gegevens. Op basis van de verkeersgegevens wordt het betalingsverkeer afgewikkeld. Het betreft overigens gegevens die grotendeels automatisch worden gegenereerd, zodat de kans op fouten klein is. De aanbieder is, op grond van het Besluit beveiliging gegevens telecommunicatie, verplicht een beveiligingsplan op te stellen. In dat plan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de concreet te treffen maatregelen die in de bijlage bij dat besluit zijn opgesomd. Het Agentschap Telecom zal actief toezicht gaan houden op de inhoud en werking van deze beveiligingsplannen. Uit deze plannen moet blijken dat de administratieve organisatie van aanbieders van openbare telecommunicatiediensten en/of openbare telecommunicatienetwerken, zodanig is ingericht dat duidelijk is dat de beveiliging van de bewaarde gegevens van dezelfde kwaliteit zijn als die in het netwerk. Er zal dus toezicht worden gehouden op het proces van gegevensverwerking. Daarbij zal niet alleen de inrichting van dat proces maar ook de uitvoering worden beoordeeld. Een onderdeel hiervan is de wijze waarop de aanbieder geconstateerde fouten in de bewaarde gegevens corrigeert. Dit betreft dan zowel de correctie van gemaakte fouten als de maatregelen ter voorkoming van herhaling. Opslag geschiedt over het algemeen in een geautomatiseerd proces en is onafhankelijk van de lengte van de bewaartermijn. Fouten in de gegevens worden pas een incident als deze vervolgens worden gevorderd en geleverd aan een behoeftesteller.

De leden van de fractie van GroenLinks verzochten de regering in te gaan op de kritiek van het College bescherming persoonsgegevens dat de huidige vage begrenzing van het recht op toegang tot de data in strijd is met artikel 4 van de richtlijn. Ook vroegen zij daarbij in te gaan op de uitspraak van het Bundesverfassungsgericht van 4 april 2006.
In reactie op de gestelde vragen merk ik op dat het College bescherming persoonsgegevens in zijn advies over het wetsvoorstel – van 22 januari 2007 – aangeeft van mening te zijn dat de grenzen voor toegang tot de te bewaren gegevens onvoldoende scherp zijn getrokken. Daarmee is het wetsvoorstel naar het oordeel van het Cbp in strijd met artikel 4 van de richtlijn. De kritiek van het Cbp kan ik niet onderschrijven. Het Cbp heeft geadviseerd om in het wetsvoorstel uit te sluiten dat de bevoegdheid van artikel 126hh Sv kan worden ingezet voor het verkrijgen van het (gedeeltelijke) bestand van bewaarde gegevens (ten behoeve van datamining). Toepassing van deze bevoegdheid achtte het Cbp in strijd met artikel 4 van de richtlijn. Daarbij heeft het Cbp gewezen op de uitspraak van het Duitse Bundesverfassungsgericht (hierna ook te noemen: het Hof) van 4 april 2006. Anders dan het Cbp acht ik deze bevoegdheid niet in strijd met artikel 4 van de richtlijn. Dit artikel beperkt de toegang voor de bevoegde nationale autoriteiten tot welbepaalde gevallen en in overeenstemming met de nationale wetgeving. Toepassing van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering is eveneens beperkt tot een bepaald geval, namelijk een verkennend onderzoek dat tot doel heeft om de opsporing van terroristische misdrijven voor te bereiden. Mede gelet op de strikte wettelijke waarborgen rond het verkennend onderzoek valt daarmee niet goed in te zien waarom toepassing van deze bevoegdheid in strijd zou zijn met de richtlijn. De uitspraak van het Duitse Bundesverfassungsgericht betreft de toepassing van de bevoegdheid van de «Rasterfahndung». Dit betreft een bevoegdheid van de politieautoriteiten om bestanden met persoonsgegevens, die zijn verkregen van publieke of private instanties, aan de hand van bepaalde, tevoren vastgestelde, kenmerken te doorzoeken. Naar aanleiding van de terroristische aanslagen van 11 september 2001 werd een «Rasterfahndung» naar islamitische terroristen aangevangen. Daarbij ging het om de opsporing van zogenaamde «slapers». De inzet van deze bevoegdheid was gebaseerd op § 31 van de Politiewet van Nordrhein-Westfalen, dat een dergelijke bevoegdheid onder bepaalde omstandigheden toelaat. Het Bundesverfassungsgericht merkt op dat de omstandigheden, waaronder kan worden overgegaan tot een dergelijke «Rasterfahndung», tussen de verschillende Duitse deelstaten verschillend zijn. Het Hof stelt vast dat § 31 van de eerdergenoemde Politiewet spreekt van een «gegenwärtige Gefahr». Dan is, naar het oordeel van het Hof, een situatie vereist waarbij in een concreet geval de toereikende waarschijnlijkheid bestaat dat binnen afzienbare termijn een aantasting van waardevolle rechtsgoederen zal plaatsvinden. Een algemene bedreigingsituatie, zoals die zich met betrekking tot de terroristische aanslagen van 11 september 2001 heeft voorgedaan, of buitenlandspolitieke spanning acht het Bundesverfassungsgericht daarvoor niet voldoende.

Naar mijn oordeel dient deze uitspraak vooraleerst in de context van het Duitse rechtssysteem te worden geplaatst. Dit betreft namelijk de toepassing van de criteria die het naar Duits recht mogelijk maken om de bevoegdheid van de «Rasterfahndung» uit te oefenen. Een algemene bevoegdheid tot het doorzoeken van gegevensbestanden aan de hand van bepaalde kenmerken, zoals dat in de Duitse deelstaten kennelijk is toegestaan, kent de Nederlandse wet niet. Wel biedt artikel 126hh van het Wetboek van Strafvordering de officier van justitie de bevoegdheid om gegevensbestanden van particuliere en publieke organisaties te vorderen teneinde de hierin opgenomen gegevens te doorzoeken op bepaalde profielen en patronen van handelingen van personen met het oog op

aanwijzingen dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd. Hiervoor is een machtiging van de rechter-commissaris vereist. De gegevens die niet van belang zijn voor het onderzoek moeten worden vernietigd. Niet goed valt in te zien waarom de uitoefening van deze bevoegdheid inzake telecommunicatiegegevens niet zou voldoen aan de vereisten van artikel 4 van de richtlijn. De toepassing daarvan is immers beperkt tot een bepaald geval, namelijk een verkennend onderzoek dat tot doel heeft om de opsporing van terroristische misdrijven voor te bereiden. Er is geen sprake van het preventief doorzoeken van gegevensbestanden zonder dat er enige aanwijzing bestaat voor het beramen of plegen van terroristische misdrijven. Een dergelijk onderzoek kan alleen worden ingesteld indien uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd. Overigens moge ik de leden van de fractie van GroenLinks verwijzen naar de memorie van toelichting en de nota naar aanleiding van het verslag bij het wetsvoorstel bewaarplicht telecommunicatiegegevens, waar ik reeds uitgebreid ben ingegaan op deze kritiek van het College bescherming persoonsgegevens (Kamerstukken II 31 145, nr. 3, blz. 20/21 en 41/42 en nr. 9, blz. 30/31).

De leden van de fractie van D66 vroegen zich af in hoeverre de na amendering van achttien naar twaalf maanden teruggebrachte bewaartermijn op gespannen voet blijft staan met het fundamentele recht op eerbiediging van de persoonlijke levenssfeer, zoals verankerd in artikel 8 van het EVRM. Onder verwijzing naar de bewaartermijnen in landen als Duitsland, Oostenrijk, Luxemburg, Finland, Zweden en Tsjechië vroegen deze leden hoe nu moet worden aangekeken tegen de situatie dat de Nederlandse bewaartermijn niet synchroon loopt met de ons omringende landen. Zij vroegen hoe de in artikel 8 vervatte proportionaliteitseis moet worden bezien nu er een rechtsongelijkheid wordt gecreëerd tussen de burgers van de verschillende Europese landen en in hoeverre de nu ontstane verschillende regimes aansluiten bij de oproep van de Europese Commissie tot harmonisatie van deze termijnen.
In antwoord op deze vragen moet allereerst worden opgemerkt dat de richtlijn, die destijds is aanvaard door de Commissie, de Raad en het Europees Parlement, de lidstaten de ruimte biedt voor een bewaartermijn van minimaal zes maanden en maximaal twee jaar. Hierboven heb ik, naar aanleiding van vragen van de leden van de fracties van het CDA en de PvdA, reeds aangegeven waarom een termijn van twaalf maanden heel wel verenigbaar is met de vereisten van artikel 8 EVRM. Daarbij merk ik op dat Oostenrijk en Zweden nog geen wettelijke bewaartermijn hebben vastgesteld – daar is dus niet gekozen voor een termijn van zes maanden – en dat landen als Frankrijk, het Verenigd Koninkrijk, Spanje, België, Hongarije, Denemarken hebben gekozen voor een bewaartermijn van twaalf maanden. Andere landen (Italië, Ierland, Estland) geven de voorkeur aan een langere bewaartermijn. In dit geheel bezien loopt Nederland met een bewaartermijn van twaalf maanden bepaald niet uit de pas met de andere – ook de ons omringende – lidstaten. Daarmee is niet gezegd dat ik met de door de richtlijn geboden marge gelukkig ben. Uit het oogpunt van eenheid en samenwerking bij de bestrijding van de criminaliteit was het veel beter geweest dat de hele Europese Unie eenzelfde bewaartermijn zou gelden, zonder keuzemogelijkheden. Een dergelijke termijn zou van een zodanig lengte moeten zijn dat de rechtshandhavingsautoriteiten de mogelijkheid wordt geboden om tijdens het opsporingsonderzoek grensoverschrijdend de nodige gegevens te kunnen opvragen. Voor een dergelijke eenduidige bewaartermijn bleek in Brussel echter geen meerderheid te vinden. Tenslotte merk ik op dat – voor zover mij bekend – de Commissie niet heeft opgeroepen tot harmonisatie van deze termijnen. Wellicht dat dit in de nabije toekomst kan worden gekomen tot

de vaststelling van een enkele bewaartermijn, bijvoorbeeld bij de evaluatie van de richtlijn door de Commissie.

Gevolgen van aanhangige rechtszaken

De leden van de CDA-fractie waren geïnteresseerd in de uitkomst van de opdracht die het Duitse Bundesverfassungsgericht in zijn uitspraak van 11 maart 2008 aan de Duitse regering heeft gegeven over de uitwerking van de bij de implementatiewet vastgestelde bewaarplicht. De leden van de GroenLinks-fractie vroegen hoe de regering deze uitspraak beoordeelt, inclusief een schets van de scenario's die aan de orde kunnen zijn ingeval het Bundesverfassungsgericht ook in de bodemprocedure de toepassing verbiedt, en of het recht op bescherming van de persoonlijke levenssfeer in Duitsland beter is gewaarborgd dan in Nederland.
In antwoord op de gestelde vragen merk ik op dat het Duitse Bundesverfassungsgericht op 11 maart jongstleden uitspraak heeft gedaan in het beroep van een groot aantal personen tegen de sedert december 2007 geldende bewaarplicht van zes maanden, ter implementatie van de richtlijn dataretentie. Volgens de klagers zou deze verplichting in strijd zijn met het Grondwettelijk gewaarborgde recht van «informationelle Selbstbestimmung».

Het Bundesverfassungsgericht heeft overwogen dat de richtlijn dataretentie de lidstaten verplicht tot het bewaren van bepaalde telecommunicatiegegevens ten behoeve van de opsporing en vervolging van *ernstige* strafbare feiten, zoals gedefinieerd in het nationale recht van de lidstaten (art. 1). Ter implementatie van de richtlijn bevat de Duitse Telecommunicatiewet de verplichting voor de aanbieders tot verstrekking van de gegevens ten behoeve van de *vervolging van strafbare feiten*, de afwending van ernstige gevaren voor de openbare veiligheid en de vervulling van opdrachten in verband met de staatsveiligheid (§ 113b TKG). De bevoegdheid tot het vorderen van verkeersgegevens door de verschillende autoriteiten wordt in de afzonderlijke wettelijke regelingen vastgelegd («Fachrecht vorbehalten»). Op grond van het Duitse strafprocesrecht is het vorderen van verkeersgegevens thans mogelijk als op grond van bepaalde feiten de verdenking bestaat dat een persoon als dader of deelnemer betrokken is bij het plegen of voorbereiden van een strafbaar feit van aanzienlijke betekenis («erhebliche Bedeutung») of een strafbaar feit dat door middel van telecommunicatie is gepleegd (§ 100 StPO). Het Hof overweegt dat de bewaarplicht voortvloeit uit de richtlijn dataretentie, die de bewaarplicht tot ernstige strafbare feiten beperkt. Die beperking is echter niet terug te vinden in § 113b TKG, op dat punt gaat de Duitse wet verder dan de richtlijn.

Naar aanleiding van de klacht heeft het Bundesverfassungsgericht geoordeeld dat, in afwachting van een definitieve beslissing, de verplichting van de aanbieders tot het leveren van verkeersgegevens voorlopig wordt beperkt tot de gegevens die nodig zijn voor een opsporingsonderzoek naar de zware strafbare feiten van § 100a, tweede lid, Strafprozessordnung («schwere Straftaten») en met inachtneming van de in dat artikel gestelde voorwaarden. Dit betreft het aftappen van telecommunicatie. Volgens het Hof wordt de opsporing dan niet onnodig belemmerd. In de gevallen waarin een vordering betrekking heeft op andere strafbare feiten, is de aanbieder gehouden de gegevens niet te verstrekken, maar deze beschikbaar te houden totdat het Hof in deze zaak onherroepelijk heeft beslist. Niet uitgesloten is dat de gegevens, die worden bewaard in afwachting van de definitieve uitspraak, dan alsnog verstrekt moeten worden. De Duitse Bondsregering is verzocht de praktische uitwerking van de bewaarplicht en de daarop betrekking hebbende verordening te bezien en het Hof daarover uiterlijk op 1 september 2008 te berichten, zodat het

zich een goed beeld kan vormen van het gebruik van de gegevens (welke doeleinden en welke omvang). Aan de hand daarvan zal het Hof beoordelen of de belangen van de betrokkenen voldoende zijn beschermd. Overigens is de vordering tot vernietiging van de verordening afgewezen.

In antwoord op de vraag, hoe de Nederlandse regering deze uitspraak beoordeelt, merk ik in de eerste plaats op dat het Bundesverfassungsgericht niet tornt aan de wettelijke bewaarplicht voor de verkeersgegevens. Het Hof overweegt dat grote terughoudendheid is geboden bij het beoordelen van maatregelen die voortvloeien uit Europese verplichtingen en laat de bewaarplicht als zodanig, die voortvloeit uit de richtlijn dataretentie, in stand. Het Nederlandse wetsvoorstel bewaarplicht telecommunicatiegegevens strekt eveneens tot implementatie van die richtlijn. De toegang tot de bewaarde gegevens is geen onderdeel van dit wetsvoorstel. Ik zie derhalve niet in dat de uitspraak van het Duitse Bundesverfassungsgericht van invloed kan zijn op de verdere behandeling van het wetsvoorstel. Verder merk ik op dat het Hof overweegt dat de aantasting van de vrijheid en het recht op bescherming van de persoonlijke levenssfeer van de betrokkene die in de bewaring van verkeersgegevens is gelegen, zich pas voordoet bij de vordering van verkeersgegevens die op hem betrekking hebben ten behoeve van de strafvervolging. Daardoor wordt de ernst van de inbreuk ook bepaald door de voorwaarden waaronder de opgeslagen gegevens gevorderd kunnen worden (O. 149). Aan de bewaring als zodanig is geen zwaarwegend nadeel verbonden (O. 150). De vordering van verkeersgegevens ziet het Hof echter als een zwaarwegende inbreuk op het grondrecht van artikel 10 van de Duitse Grondwet. De notie dat de beperking van de persoonlijke levenssfeer niet zozeer gelegen is in de bewaring van de gegevens als zodanig, maar meer in het gebruik van de gegevens voor een ander doel, is ook door mijzelf naar voren gebracht, zowel hierboven – bij de beantwoording van de vragen van de leden van de fracties van het CDA, de PvdA en de SP over de bewaartermijnen- als in de nota naar aanleiding van het verslag (Kamerstukken II 2007/08, 31 145, nr. 9, blz. 17 en 35).

Naar aanleiding van de vraag of het recht op bescherming van de persoonlijke levenssfeer in Duitsland beter is gewaarborgd dan in Nederland merk ik op dat dit in zijn algemeenheid niet gezegd kan worden. Zowel Duitsland als Nederland laten zich bij het waarborgen van het recht op bescherming van de persoonlijke levenssfeer leiden door artikel 8 van het EVRM, het Databeschermingverdrag van 1981 (Trb. 1988, nr. 7) en de EU privacy-richtlijn (Richtlijn 95/46/EG, PbEG L 281). De Nederlandse situatie wijkt op bepaalde punten af van die in Duitsland. In de Duitse Telecommunicatiewet wordt verder gebruik van de bewaarde gegevens voorzien voor de vervolging van strafbare feiten, aanzienlijke schendingen van de openbare veiligheid en de taakuitoefening door de inlichtingendiensten. De bevoegdheden tot het opvragen van de gegevens kunnen door de Duitse overheid nader worden ingevuld binnen de kaders van de Telecommunicatiewet. In de Nederlandse Telecommunicatiewet wordt de bewaarplicht gekoppeld aan het opsporen en vervolgen van ernstige misdrijven. De bevoegdheden tot het vorderen van de gegevens zijn opgenomen in het Wetboek van Strafvordering en de WIV 2002. Voor de strafvordering geldt dat sprake moet zijn van de opsporing van ernstige misdrijven. Het gebruik van de gegevens voor de handhaving van de openbare veiligheid is niet voorzien.

De leden van de fracties van de ChristenUnie en SGP vroegen wat de consequentie zou zijn als de door Ierland aangespannen procedure resulteert in een vaststelling van het Hof van Justitie dat de dataretentierichtlijn tot stand is gekomen op basis van een onjuiste rechtsgrondslag. Deze leden hebben gevraagd of de Wet bewaarplicht telecommunicatie-

gegevens dan ongewijzigd van kracht zou blijven. Ook de leden van de D66-fractie zouden graag een reactie op deze rechtszaak ontvangen.
Naar aanleiding van de gestelde vragen merk ik op dat Ierland beroep heeft ingesteld tegen de richtlijn omdat Ierland zich niet kan verenigen met een maximale bewaartermijn van twee jaar en de voorkeur geeft aan een kaderbesluit onder de derde pijler. Nederland is gehouden een richtlijn te implementeren zodra die volgens de in het EG-Verdrag voorziene procedure is vastgesteld. Dit geldt onverkort indien een andere lidstaat tegen die richtlijn beroep heeft ingesteld bij het Europese Hof van Justitie. Een dergelijk beroep heeft dus geen opschortende werking. Zoals in de Inleiding reeds is opgemerkt, heeft de Commissie inmiddels een inbreukprocedure gestart omdat Nederland niet tijdig heeft voldaan aan de verplichting tot implementatie van de richtlijn (15 september 2007). De Wet bewaarplicht telecommunicatiegegevens kan van kracht worden nadat deze door het Nederlandse parlement is aanvaard. Zodra een wet in Nederland van kracht is, blijft deze gelden, ook indien de door Ierland ingestelde procedure zou resulteren in een vaststelling van het Hof van Justitie dat de dataretentierichtlijn op een onjuiste rechtsgrondslag tot stand is gekomen. Daarbij wijs ik erop dat de Juridische Diensten van de Raad, de Commissie en het Europees Parlement en de Europese Toezichthouder voor gegevensbescherming zich hebben uitgesproken voor de keuze voor een richtlijn.

Situatie in andere lidstaten

De leden van de CDA-fractie vroegen naar de visie van de regering op de onderzoeken die in Duitsland zijn gedaan door respectievelijk de brancheorganisatie Bitkom en door het Max Planck Instituut voor buitenlands en internationaal strafrecht.
Op deze vraag ben ik hierboven, mede naar aanleiding van de vragen van de leden van de fractie van GroenLinks, reeds ingegaan. Graag verwijs ik daarnaar.

Kosten voor gegevensbewaring

De leden van de fractie van het CDA wezen op de kosten die de providers moeten maken om de enorme hoeveelheden gegevens op te slaan en zouden graag een up to date overzicht ontvangen van de geschatte kosten en vergoedingen die daartegenover worden gesteld. Ook de leden van de fractie van de SP wilden graag van de regering vernemen hoe die de kosten, samenhangend met een bewaartermijn van twaalf maanden, inschat.
Met betrekking tot de te maken kosten wordt het volgende opgemerkt. Voor het verkrijgen van inzicht in de bedrijfseffecten heeft het onderzoek dat is uitgevoerd door Verdonck, Klooster & Associates (VKA) de basis gevormd. Uit dit onderzoek is o.a.onder meer gebleken dat bij een bewaartermijn van twaalf maanden en decentrale opslag voor de periode van 5 jaar de investeringskosten ongeveer 75 miljoen euro zullen bedragen en de jaarlijkse exploitatiekosten kunnen groeien tot circa 20 miljoen euro, uitgaande van een verwachte toename in het bevragingsvolume. Deze bedragen moeten opgebracht worden door alle betrokken bedrijven tezamen 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 300 kleinere bedrijven. Volgens berekeningen van VKA bedragen de kosten voor de kleine bedrijven met een gemiddeld aantal van duizend accounts ongeveer 2% van de totale kosten. Ten tijde van het onderzoek heeft VKA gerekend met een aantal van 255 kleine bedrijven. Per bedrijf zouden de investeringskosten dan ongeveer 5900 euro bedragen, gerekend over een periode van vijf jaar. Daarbij dient bedacht te worden dat ICT toepassingen steeds goedkoper worden. Een

mogelijke concurrentie-achterstand voor de kleine(re) internetproviders, waarnaar de leden van de fracties van het CDA, de VVD, de ChristenUnie en de SGP vroegen, wordt door mij dan ook niet gevreesd. Bij de berekeningen voor het benodigd geheugen ging VKA begin 2006 uit van 34 000 euro per terabyte. Inmiddels is de prijs per terabyte opslagcapaciteit drastisch afgenomen met meer dan een factor tien. Volgens dezelfde bron die door VKA is gebruikt kan thans voor 2200 euro per terabyte een geavanceerde en goed beveiligde opslagcapaciteit gekocht worden. Dit betekent dat de investeringskosten voor geheugencapaciteit ook voor de kleine bedrijven aanzienlijk lager zullen uitvallen.
Over de vergoedingen die tegenover de kosten worden gesteld merk ik op dat, op grond van hoofdstuk 13 van de Telecommunicatiewet, de aanbieders van openbare telecommunicatiediensten en/of -netwerken de investeringskosten, de exploitatiekosten en de kosten van onderhoud dragen die uit de verplichtingen van dit hoofdstuk voortvloeien (art. 13.6 Tw). De directe personele en administratieve kosten voor het voldoen van een bevoegd gegeven last worden vergoed door het Rijk. In de Regeling kosten aftappen en gegevensverstrekking is dit nader uitgewerkt. Aangezien het wetsvoorstel bewaarplicht telecommunicatiegegevens de regeling van hoofdstuk 13 van de Telecommunicatiewet ongewijzigd laat, is deze ook van toepassing op het verstrekken van gegevens op basis van een bevoegd gegeven last inzake bewaarde verkeersgegevens. In de richtlijn dataretentie worden geen regels gegeven over de vergoedingen door de nationale overheden aan de telecomsector. Tussen de lidstaten zijn er op dit terrein grote verschillen. Zo geven sommige lidstaten geen enkele vergoeding, zoals Ierland en een aantal nieuwe lidstaten als Hongarije, Polen en Slovenië, terwijl andere lidstaten een ruime vergoeding hanteren, zoals Engeland en Oostenrijk. Nederland neemt, samen met Frankrijk en Duitsland, een tussenpositie in waarbij voor Nederland geldt dat aangesloten is bij het huidige bestaande stelsel van vergoedingen voor het aftappen. Daarom is het belangrijk dat een implementatiewijze wordt gevonden, die voor het bedrijfsleven uitvoerbaar is en die natuurlijk bij voorkeur zo min mogelijk lasten met zich meebrengt. De richtlijn dataretentie vermeldt een aantal gegevens die beschikbaar moeten zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Deze gegevens betreffen verkeers- en locatiegegevens en is dus niet van toepassing op de inhoud van de communicatie. 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 – zoals in voorgaande weergave van de bevindingen op grond van het rapport van VKA naar voren kwam – niet dermate groot dat rekening moet worden gehouden met forse investeringen. Zoals in het voorgaande in antwoord op vragen van de leden van de SP-fractie reeds aan de orde kwam, laten de technologische ontwikkelingen van de afgelopen jaren bovendien op het punt van opslag zien dat de benodigde investeringen voor opslag en/of uitbreiding van de opslag als zodanig afgenomen zijn en naar alle waarschijnlijk nog verder zullen gaan afnemen. De meeste kosten worden veroorzaakt door de eisen waaraan voldaan moet worden aangaande de beveiliging van opgeslagen gegevens en het ordenen van de gegevens, maar ook nu dienen de aanbieders al rekening te houden met lasten ten behoeve van beveiliging van de gegevens. De bedrijven zullen proberen hun kosten te verdisconteren in hun tarieven tenzij daar aparte inkomsten (vergoeding door de overheid) tegenover staan. 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. Het voorliggende wetsvoorstel zal nauwelijks merkbare

effecten op de tarieven van de aanbieders hebben. 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 in Nederland openbare telecommunicatiediensten en/of netwerken aanbieden. Bezien vanuit het perspectief van het functioneren van de interne markt ligt het niet in de lijn der verwachtingen dat de Nederlandse regelgeving belemmeringen voor de interne markt voor elektronische communicatie teweeg zal brengen. Daarnaast wordt verwacht dat de reeds gemaakte afspraken met de aanbieders die goed zijn voor circa 95% van de informatiebevragingen en taplasten over een voor alle partijen zo efficiënt mogelijke aanpak van de afwikkeling daarvan de kosten zullen beperken en dat dit zelfs een concurrentievoordeel kan gaan opleveren ten opzichte van landen die niet dit soort afspraken maken met hun aanbieders.

De leden van de fracties van de SGP, de ChristenUnie, de VVD, de SP en GroenLinks vroegen of de regering kan aangeven op welke wijze de motie-De Wit wordt uitgevoerd. Op 3 september 2007 heeft de staatssecretaris van Economische Zaken een evaluatie van de regeling kosten aftappen en gegevensverstrekking aan de Tweede Kamer gestuurd (Kamerstukken II 2006/07, 30 517, nr. 4). Bij de aanbieding is gemeld dat gesprekken gaande waren met vertegenwoordigers van het bedrijfsleven om te komen tot verbetering van de samenwerking op het terrein van aftappen en gegevensverstrekking. Vanuit de betrokken departementen hebben gesprekken met vertegenwoordigers van de telecomsector plaatsgevonden en is nagegaan of het huidige systeem van het betalen per tap, waaraan de dataretentieverplichting wordt toegevoegd, kan worden vervangen door vaste vergoedingsbedragen voor een bepaalde periode. Daarbij is wel het uitgangspunt dat wordt voldaan aan zowel de huidige verplichtingen als de nieuwe verplichtingen die voortvloeien uit het voorliggende wetsvoorstel. Er zijn afspraken gemaakt tussen overheid en deze aanbieders die nader worden uitgewerkt in een zogenaamde service level agreements (SLA). De basis van de SLA voor deze aanbieders wordt gevormd door de wettelijke verplichtingen. De SLA omvat alle vormen van medewerking van aanbieders aan de overheid ter zake van de strafvordering, hoofdstuk 13 van de Telecommunicatiewet en de Wet op de inlichtingen- en veiligheidsdiensten. Er wordt naar gestreefd om de SLA's in het najaar van 2008 gereed te hebben. Zowel de aanbieders als de overheid verplichten zich om de technische en organisatorische maatregelen te implementeren die het realiseren van de SLA's mogelijk moeten maken. Ten einde budgettaire verrassingen te voorkomen wordt jaarlijks in overleg met de aanbieders overleg gevoerd over de effecten van ontwikkelingen in het werkpakket door wetswijzigingen, mutaties in het dienstenaanbod en te verwachten kostenreducties door de implementatie van de efficiencyverhogende maatregelen. De door de heer De Wit (SP) ingediende motie kan worden gezien als een «steun in de rug» voor de reeds ingezette beleidslijn om te differentiëren naar de omvang van het percentage informatiebevragingen en taplasten waarmee aanbieders van openbare telecommunicatiediensten en/ofnetwerken jaarlijks worden geconfronteerd. Zoals eerder aangegeven is met de aanbieders die goed zijn voor circa 95% van de informatiebevragingen en taplasten per jaar overeenstemming bereikt op hoofdlijnen. Het ligt in der aard der verwachtingen dat ook met de kleine(re) aanbieders overeenstemming kan worden bereikt. Daarbij is het van belang inzicht te verkrijgen in het aantal bevragingen waarmee deze groep aanbieders wordt geconfronteerd ten behoeve van opsporing en vervolging. Wanneer dit inzicht wordt verschaft en niet ter discussie staat, kunnen vervolgens afspraken worden gemaakt over een toe te passen vergoedingssystematiek, waarbij het bereiken van maatwerk leidend zal zijn.

Overig

De leden van de CDA-fractie wezen op verschillende manieren om de bewaarplicht te omzeilen, door middel van het gebruik van speciale software of door middel van het gebruik van bedrijfsmail en diensten als Hotmail, MSN, Skype en Hyves en vroegen zich af waarop de regering nog enig nuttig effect van de voorgestelde regeling baseert. Deze vraag gold voor de maatregel in het algemeen maar zeker ook voorzover deze verder reikt dan de termijn van zes maanden die door de EU wordt opgelegd.
In antwoord op de gestelde vragen merk ik op dat sommige aanbieders van telecommunicatiediensten niet rechtstreeks onder de werkingssfeer van hoofdstuk 13 van de Telecommunicatiewet vallen. Dit betreft diensten die de gebruikers in staat stellen zelfstandig, zonder tussenkomst van een aanbieder, te communiceren. Er kan dan niet gesproken worden van een «openbare telecommunicatiedienst», in de zin van de Telecommunicatiewet, omdat er geen sprake is van het overbrengen van signalen via een electronisch communicatienetwerk door de aanbieder van de betreffende communicatiedienst. Dit betreft diensten als Hyves, MSN en Skype. Bij zulke diensten bestaat de dienstverlening geheel of grotendeels uit het beschikbaar stellen van software met behulp waarvan degene, voor wie een bericht bestemd is, dit zelf bij de een server kan ophalen door verbinding te maken met de betreffende server. Het transport van de gegevens van de afzender naar de server vindt doorgaans plaats door de aanbieder van de verzender die daarmee wel onder de werkingssfeer van artikel 1.1., onderdeel ff, van de Telecommunicatiewet valt. Ditzelfde geldt voor de aanbieder van de geadresseerde die de gegevens van de server ophaalt. Dit betekent dat de verkeersgegevens, die gegenereerd worden met het transport van de berichten, bewaard moeten worden. Er blijft derhalve nog een groot gebied over waarin verkeersgegevens gegenereerd worden die bewaard dienen te worden. Ook bij de behandeling in de Tweede Kamer van het onderhavige wetsvoorstel is gesproken over de werkingssfeer in relatie tot diensten die niet onder de bewaarplicht vallen. Ik heb daarbij opgemerkt dat ondanks het gebruik van deze diensten, het nut van de toepassing van strafvorderlijke bevoegdheden met betrekking tot de nog steeds buitengewoon veel gebruikte telecommunicatie via de mobiele telefoon en de internetvoorzieningen die de traditionele e-mail benutten, waarbij dus gebruik wordt gemaakt van Nederlandse providers, daarmee absoluut niet verminderd is. Dat sommige aanbieders van e-maildiensten zelf niet als aanbieder in de zin van de Nederlandse Telecommunicatiewet kunnen worden aangemerkt, waardoor minder gegevens beschikbaar zijn voor politie en justitie, is een beperking die buiten de sfeer van Europese richtlijn en het onderhavige wetsvoorstel ligt. Ik heb de Kamer toegezegd te onderzoeken hoe dat gat, waar nodig via internationale samenwerking, kan worden gedicht. Hierbij kan ook worden gedacht aan de eerdergenoemde evaluatie van de richtlijn dataretentie, die in 2010 zal plaatsvinden.

De reikwijdte van de evaluatie, op grond van de in artikel 13.9 opgenomen evaluatiebepaling, was de leden van de fractie van D66 niet helemaal helder. Deze leden vroegen in hoeverre nu kan worden gesproken van een duidelijk omschreven kader waarbinnen geëvalueerd dient te worden.
In antwoord op deze vraag merk ik op dat de implementatie van de richtlijn dataretentie strekt tot aanvulling van de Telecommunicatiewet. Dit betreft de artikelen 13.2a, 13.4 en 13.5 van de wet. De evaluatiebepaling is vorm gegeven naar het model van de Aanwijzingen voor de regelgeving (nr. 164). Een dergelijke bepaling wordt dus ook in andere wetten gebruikt. Het kader van de evaluatie betreft de wettelijke regeling ter implementatie van de richtlijn dataretentie. Naar aanleiding van een amendement van het lid van de Tweede Kamer Anker is de evaluatietermijn verkort van vijf

naar drie jaar (Kamerstukken 2007/08, 31 145, nr. 14). In de evaluatie zullen met name betrokken worden het aantal bevragingen en de lengte van de bewaartermijn.

Verder wezen de leden van de fractie van D66 op de specifieke bewaarplicht van artikel 126ni van het Wetboek van Strafvordering, dat is opgenomen naar aanleiding van de Wijzigingswet Computercriminaliteit II (Stb. 2006, 300), en vroegen zij waarom niet meer aansluiting is gezocht bij dit regime. In antwoord op de gestelde vraag merk ik op dat de specifieke bewaarplicht van artikel 126ni van het Wetboek van Strafvordering betrekking heeft op de bevriezing van vluchtige gegevens die zich slechts korte tijd in de systemen van de aanbieders bevinden en die door de houders doorgaans slechts heel kort voor eigen bedrijfsdoeleinden worden bewaard. Naar aanleiding van de artikelen 16 en 17 van het Cybercrime Verdrag is de bewaarperiode gesteld op negentig dagen. De bevoegdheid tot bevriezing van gegevens verschilt op een essentieel punt van de bevoegdheid tot het bewaren van gegevens. Bij de toepassing van de bevoegdheid tot bevriezing is het bij de tot opsporing bevoegde instanties bekend dat vluchtige gegevens aanwezig zijn, die nodig zijn voor het onderzoek. De bevriezingstermijn strekt ertoe te voorkomen dat de degene tot wie de vordering kan worden gericht de betreffende gegevens voortijdig verwijdert of vernietigt. De reden voor de termijn van negentig dagen is dat rekening is gehouden met de lange periode die in een aantal landen is gemoeid met de uitvoering van een rechtshulpverzoek (Kamerstukken II, 2001/02, 28 366, nr. 1, blz. 22). Bij de bewaring van de telecommunicatiegegevens door de aanbieders is de aanwezigheid van de gegevens, en het belang daarvan voor de opsporing van strafbare feiten op het tijdstip van de bewaring doorgaans niet bekend bij de tot opsporing bevoegde instanties. De bewaartermijn heeft juist ten doel om te verzekeren dat de gegevens beschikbaar zijn indien in een later stadium blijkt dat deze van belang kunnen zijn voor opsporingsonderzoek. Doordat de betrokken belangen verschillend zijn, leidt ook de afweging van de duur van de bewaartermijnen tot andere uitkomsten. Op de noodzaak tot een bewaartermijn van twaalf maanden ben ik hierboven, naar aanleiding van vragen van de leden van de fracties van de PvdA, het CDA en de SP, reeds nader ingegaan.

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