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)

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel strekt tot implementatie van Richtlijn nr. 06/24/EG van het Europees Parlement en de Raad van 15 maart 2006, betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn nr. 02/58/EG. Deze richtlijn (hierna ook te noemen: de richtlijn dataretentie) is op 3 mei 2006 in werking getreden (Pb EU, L105/54) en voorziet in een verplichting voor aanbieders van openbare elektronische communicatienetwerken en aanbieders van openbare elektronische communicatiediensten tot het bewaren van een bepaalde lijst van telecommunicatiegegevens gedurende een bepaalde periode. De bewaarplicht beoogt te garanderen dat de te bewaren gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De bewaarplicht is van toepassing op telefoon- of bepaalde internetdiensten en heeft betrekking op verkeers- en locatiegegevens, voorzover deze in het kader van de aanbieding van communicatiediensten door de aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten (hierna ook te noemen: de aanbieders) worden gegenereerd of verwerkt bij het leveren van communicatiediensten. De richtlijn dataretentie bevat verder bepalingen over de te bewaren gegevens, de bewaartermijnen, de bescherming en beveiliging van de bewaarde gegevens evenals het toezicht daarop, de rechtsbescherming en sancties. Mede namens de Staatssecretaris van Economische Zaken licht ik het wetsvoorstel in deze memorie van toelichting toe.

2. De hoofdlijnen van het wetsvoorstel

In het wetsvoorstel worden regels voorgesteld voor de verplichting tot bewaring van gegevens door de aanbieders van openbare telecommunicatienetwerken en aanbieders van openbare telecommunicatiediensten, de te bewaren gegevens, de bewaartermijnen en de bescherming en beveiliging van de bewaarde gegevens. Bij algemene maatregel van bestuur kunnen regels worden gesteld over de maatregelen ter beveiliging en vernietiging van, en de toegang tot, de gegevens. In deze paragraaf wordt de implementatie van de verplichtingen van de richtlijn dataretentie in de Telecommunicatiewet op hoofdlijnen toegelicht.

2.1 De reikwijdte van de richtlijn dataretentie

De richtlijn dataretentie heeft tot doel de nationale bepalingen van de lidstaten, waarbij aan de aanbieders verplichtingen worden opgelegd inzake het bewaren van bepaalde telecommunicatiegegevens, zoveel mogelijk te harmoniseren 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 richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, voorzover deze in het kader van de aanbieding van de communicatiediensten door de aanbieders van openbare elektronische communicatiediensten of openbare elektronische communicatienetwerken worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten (artikelen 1 en 3, eerste lid).

In de richtlijn dataretentie wordt onder het begrip 'gegevens' verstaan verkeers- en locatiegegevens, en de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren (artikel 2, onderdeel a). De begrippen verkeers- en locatiegegevens zijn omschreven in Richtlijn nr. 02/58/EG (Pb EG, L 201, artikel 2, onderdelen b en c).

Het wetsvoorstel voorziet in de verplichting voor de aanbieders om bepaalde gegevens, voor zover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, te bewaren. Wanneer dergelijke gegevens niet worden gegenereerd bij of verwerkt door de aanbieders, is er geen verplichting ze te bewaren.

Met het gebruik van de begrippen openbaar telecommunicatienetwerk en openbare telecommunicatiediensten sluit het wetsvoorstel aan bij de begripsomschrijvingen van artikel 1, onderdeel ee, respectievelijk onderdeel ff, van de Telecommunicatiewet (Kamerstukken II, 28851, nr. 3, blz. 92). Deze terminologie wijkt iets af van de richtlijn dataretentie, waar wordt gesproken van openbare elektronische communicatienetwerken en –diensten. Dit houdt verband met het feit dat het begrip elektronische communicatiedienst, zoals gedefinieerd in artikel 1.1, onderdeel f, van de Telecommunicatiewet, ook de diensten omvat die voor omroep worden gebruikt terwijl het begrip openbaar elektronisch communicatienetwerk, zoals gedefinieerd in artikel 1.1, onderdeel h, van de Telecommunicatiewet, mede het netwerk omvat, bestemd voor het verspreiden van programma's aan het publiek. Om die reden worden in hoofdstuk 13 van de Telecommunicatiewet de begrippen openbare telecommunicatiedienst en openbaar telecommunicatienetwerk gehanteerd. De ONP-richtlijnen (Open Network Provisions) van 2002 gaven geen aanleiding voor de onderwerpen die in hoofdstuk 13 zijn geregeld, de reikwijdte te verbreden tot openbare elektronische communicatienetwerken dan wel –diensten.

Het begrip 'openbaar' is terug te vinden in artikel 1, onderdelen f en g van de Telecommunicatiewet. Het kenmerkende van dit begrip is dat de betreffende telecommunicatiedienst beschikbaar is voor het publiek. Telecommunicatiediensten die uitsluitend beschikbaar zijn voor leden van een besloten gebruikersgroep zijn geen openbare telecommunicatiediensten. Een telecommunicatienetwerk wordt aangemerkt als een openbaar telecommunicatienetwerk als dit daadwerkelijk gebruikt wordt voor de verrichting van openbare telecommunicatiediensten. Daaronder is begrepen het aan het publiek bieden van de mogelijkheid van overdracht van signalen tussen netwerkaansluitpunten. Ook wanneer het telecommunicatienetwerk wordt gebruikt om 'kale' transportcapaciteit openbaar aan te bieden (in de vorm van huurlijnen) is er sprake van een openbaar telecommunicatienetwerk (Kamerstukken II, 1996-1997, 25533, nr. 3, pag. 72).

De begrippen 'verkeers- en locatiegegevens' van Richtlijn nr. 02/58/EG zijn destijds geïmplementeerd in artikel 11.1, onderdelen b en d, van de Telecommunicatiewet. Verkeersgegevens in de zin van de Telecommunicatiewet zijn gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch

communicatienetwerk of voor de facturering ervan. Voorbeelden daarvan zijn gegevens omtrent het oproepende en opgeroepen aansluitnummer, omtrent de datum, het tijdstip en de duur van de communicatie of omtrent de soort telecommunicatiedienst waarvan gebruik is gemaakt. Verkeersgegevens kunnen ook gegevens over namen, adressen en nummers bevatten indien deze informatie wordt omgezet om de transmissie van communicatie tot stand te brengen (Richtlijn nr. 02/58/EG, Overweging 15). Locatiegegevens in de zin van de Telecommunicatiewet zijn gegevens die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparaten van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven. Een voorbeeld daarvan zijn gegevens omtrent de geografische positie van een zendmast bij het gebruik van mobiele telefonie. De met verkeers- en locatiegegevens verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren zijn bijvoorbeeld de naam en het adres van de abonnee of de geregistreerde gebruiker van een communicatie. Deze zijn toegevoegd aan het bereik van de richtlijn omdat deze niet altijd zijn te ontlenen aan de verkeersgegevens terwijl de beschikbaarheid daarvan wel van belang kan zijn voor de criminaliteitsbestrijding.

In het wetsvoorstel wordt voor de interpretatie van het begrip ‘gegevens’ aangesloten bij het bestaande begrippenkader van de Telecommunicatiewet. Dit begrip omvat de verkeers- en locatiegegevens, bedoeld in artikel 11.1, onderdeel b, respectievelijk onderdeel d, van de Telecommunicatiewet. Daarnaast omvat dit begrip de met de verkeers- en locatiegegevens verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren. Hiermee is dit begrip gelijk aan dat van de richtlijn.

2.2 De te bewaren gegevens

De te bewaren gegevens worden in de richtlijn dataretentie gespecificeerd. Daarbij geldt een verdeling in de volgende categorieën van gegevens, die nodig zijn om: de bron van een communicatie te traceren (a), de bestemming van een communicatie te identificeren (b), de datum, het tijdstip en de duur van een communicatie te bepalen (c), het type communicatie te bepalen (d), de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers te identificeren (e) en de locatie van mobiele communicatieapparatuur te bepalen (f). De categorieën van gegevens worden vervolgens in de richtlijn uitgewerkt in een lijst van gegevens (artikel 5).

In de lijst van de te bewaren gegevens wordt onderscheid gemaakt tussen telefonie over een vast of mobiel netwerk enerzijds en internettoegang, e-mail over het internet en internettelefonie anderzijds. Hieruit vloeit voort dat de richtlijn dataretentie uitsluitend betrekking heeft op gegevens die samenhangen met het gebruik van dergelijke telecommunicatiediensten.

De richtlijn dataretentie bevat geen verplichtingen voor de bewaring van telecommunicatiegegevens in verband met niet tot stand gekomen verbindingen. Van een verbinding is sprake indien door middel van een elektronisch communicatienetwerk de mogelijkheid voor het overbrengen van signalen tussen twee of meer netwerkaansluitpunten tot stand wordt gebracht. De richtlijn is wel van toepassing op een oproeppoging zonder resultaat. Dit betreft een communicatie, waarbij een telefoonoproep wel tot een verbinding heeft geleid maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord. Gegevens betreffende oproeppogingen zonder resultaat vallen onder de verplichting tot gegevensbewaring, voorzover deze – wat telefoniegegevens betreft - in verband met de aanbieding van een communicatiedienst worden gegenereerd, verwerkt en opgeslagen of - wat internetgegevens betreft - worden gegenereerd, verwerkt en gelogd (artikel 3, tweede lid).

Het wetsvoorstel bevat de verplichting voor de aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten om bepaalde, in een bijlage bij de wet aangewezen gegevens te bewaren. Daarmee wordt de nodige duidelijkheid geboden over de reikwijdte van de bewaarplicht en de te bewaren gegevens. Dit biedt de aanbieders helderheid over de gegevens die door hen beschikbaar moeten kunnen worden gesteld aan de bevoegde autoriteiten en het biedt deze autoriteiten helderheid over de gegevens, voor de beschikbaarstelling waarvan zij de aanbieders kunnen aanspreken. De lijst van de te bewaren gegevens in de bijlage is gelijk aan de gegevens die op grond van de richtlijn dataretentie dienen te worden bewaard. Ten aanzien van de reeds bestaande beperkte bewaarplicht betreffende locatiegegevens wordt voorgesteld om te voorzien in verlenging van de thans geldende bewaartermijn daarvoor. Dit wordt hierna toegelicht in paragraaf 2.3.

Het wetsvoorstel bevat tevens de verplichting tot het bewaren van gegevens van oproeppogingen zonder resultaat, voor zover deze gegevens door de aanbieders bij het aanbieden van openbare telecommunicatienetwerken of openbare telecommunicatiediensten worden gegenereerd, verwerkt en opgeslagen of gelogd. Op de reikwijdte van deze verplichting zal in het artikelsgewijs deel nader worden in gegaan.

2.3 De bewaartermijn

De richtlijn dataretentie legt aan de lidstaten de verplichting op ervoor te zorgen dat de te bewaren gegevens gedurende ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie worden bewaard (artikel 6). Het wordt aan de lidstaten overgelaten om, binnen de door de richtlijn gestelde kaders, de precieze bewaartermijnen te bepalen. Daarbij wordt ruimte geboden voor het maken van onderscheid tussen gegevens inzake telefonie over een vast netwerk en mobiele telefonie enerzijds en gegevens inzake internettoegang, e-mail over het internet en internettelefonie anderzijds. Tenslotte kunnen lidstaten met specifieke omstandigheden die een in tijd beperkte verlenging van de bewaringsperiode rechtvaardigen, de noodzakelijke maatregelen treffen (artikel 12).

In het voorliggende wetsvoorstel wordt de bewaartermijn op achttien maanden gesteld. Deze termijn geldt voor alle te bewaren gegevens, ongeacht of deze met het gebruik van traditionele (vaste of mobiele) telefonie of met het gebruik van internettoegang, e-mail over het internet dan wel internettelefonie samenhangen. Het wetsvoorstel voorziet niet in de mogelijkheid tot het vaststellen van een langere bewaarperiode in verband met specifieke omstandigheden.

Met de termijn van achttien maanden wordt tegemoet gekomen aan de behoeften van politie en justitie. Onderzoekers van de Erasmus Universiteit Rotterdam hebben over nut en noodzaak van de bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer een rapport uitgebracht (Kamerstukken II, 23 490, nr. 379). In het rapport geven de onderzoekers aan dat een termijn van drie maanden doorgaans voldoende zal zijn voor niet al te complexe opsporingsonderzoeken die op districtsniveau worden verricht, maar dat een dergelijke termijn onvoldoende is voor de langlopende, complexere opsporingsonderzoeken 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, waardoor zelfs in geval van een zeer ruime bewaartermijn altijd de kans bestaat dat gegevens er niet meer zijn op het moment dat een cold case onderzocht wordt. 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 Erasmus Universiteit 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. Wel is de onderzoekers gebleken dat de leeftijd van de historische verkeersgegevens die worden gevorderd over het algemeen hoger wordt naarmate de ernst van het gepleegde delict en de capaciteit die de opsporing inzet teneinde de zaak op te kunnen helderen toeneemt. Uit de interviews die tijdens het onderzoek zijn gehouden is, gebleken dat door de beperkte bewaartermijn vaak 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. Dat geldt zowel voor het tijdsbestek waarover de gegevens worden opgevraagd als voor bepaalde telefoonnummers. De onderzoekers concluderen dat een langere bewaartermijn kan leiden tot een meer afgewogen, beperktere bevraging van de verkeersgegevens. Een langere bewaartermijn zal betekenen dat aanzienlijk minder gegevens zullen worden opgevraagd die achteraf bezien niet relevant - en dus ook niet noodzakelijk - waren voor het onderzoek.

De door de onderzoekers van de Erasmus Universiteit aanbevolen bewaartermijn kan op basis van hun gegevens met het oog op de effectiviteit van de opsporing als een minimum worden beschouwd. In zijn advies naar aanleiding van het wetsvoorstel heeft de Raad van Hoofdcommissarissen gewezen op onderzoeken naar en verband houdend met terrorisme en georganiseerde criminaliteit, die tot een langere bewaartermijn nopen. Voor de zogenaamde ‘cold cases’, die veelal feiten betreffen die de rechtsorde ernstig hebben geschokt, zou zelfs een bewaartermijn van vijf jaar nog gering zijn. In het vorenstaande is hierover reeds opgemerkt dat voor dit soort zaken zelfs een zeer ruime bewaartermijn niet voldoet. Een beperkte bewaartermijn voor de bewaring van telecommunicatiegegevens zal blijkens de advisering door de politie een negatieve invloed kunnen hebben op de opsporing van grootschalige afpersingsonderzoeken, onderzoeken naar meervoudige moord in criminele organisaties en onderzoeken naar terrorisme. Ook van de zijde van het openbaar ministerie is hierop gewezen. In 2005 (WODC) bedroeg de gemiddelde doorlooptijd in maanden vanaf het moment van instroom bij het openbaar ministerie tot het moment van de uitspraak in eerste aanleg bij de meervoudige (straf)kamer, zeven en een halve maand. Dit betreft evenwel een gemiddelde, hoger beroep niet meegerekend. In de veelheid aan strafzaken die jaarlijks aanhangig zijn bij de strafrechter, zijn het de eerdergenoemde categorieën van zaken die vanwege de aard en complexiteit een aanzienlijke doorlooptijd kennen. Dit betreft veelal zaken die de rechtsorde ernstig hebben geschokt en uitgebreid in de publiciteit komen. Bij onderzoeken in verband met de verdwijning of vermissing van personen zal pas in een later stadium van het opsporingsonderzoek, nadat de persoon is teruggevonden of het lijk van betrokkene is gevonden, een verdachte in beeld kunnen komen. De telecommunicatiegegevens met betrekking tot die verdachte zijn dan echter niet meer beschikbaar. Bij onderzoeken naar terroristische groeperingen, criminele organisaties en grootschalige afpersingzaken ontstaat vaak in een later stadium van het onderzoek behoefte aan nadere informatie als gevolg van nieuwe feiten en omstandigheden, bijvoorbeeld doordat er nieuwe verdachten of mededaders in beeld komen. In dergelijke complexe onderzoeken komt doorgaans pas later zicht op de opbouw en structuur van de organisatie. Onderlinge contacten, waar pas na de aanhouding over wordt verklaard, kunnen niet meer worden geverifieerd aan de hand van telecommunicatiegegevens. Ook kan het voorkomen dat bij doorzoekingen tot dan toe onbekende telefoons worden aangetroffen, zodat het opvragen van de bijbehorende verkeersgegevens noodgedwongen later plaatsvindt. Wanneer gedurende het onderzoek, ook in een later stadium, verdachten in beeld komen, kan aan de hand van verkeersgegevens hun betrokkenheid worden vastgesteld dan wel uitgesloten. Deze onderzoeken

overstijgen niet zonder uitzondering de periode van een jaar voordat de zaken gereed zijn voor de zitting. Bovendien moet worden vermeld dat een lange bewaartermijn eveneens van belang is in opsporingsonderzoeken waarin de duurzaamheid van een criminele organisatie moet worden aangetoond, ten behoeve van het bewijs van deelname aan een criminele organisatie als bedoeld in artikel 140 Sr. 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. Ten slotte zij opgemerkt dat tevens tijdens het onderzoek ter terechtzitting behoefte kan bestaan aan onderzoek van telecommunicatiegegevens om de betrokkenheid van personen bij de strafbare feiten aan te tonen of juist uit te sluiten.

Voorgesteld wordt dan ook om in de bewaartermijn een zekere marge in te bouwen zodat de beschikbaarheid van de gegevens zeker wordt gesteld ten behoeve van de meer grootschalige en complexe zaken, de rechtshulpverzoeken en cold cases. Weliswaar geldt in geval van rechtshulpverzoeken dat ook gestreefd kan worden naar verkorting van de procedures, maar niet in alle gevallen en bij alle landen is dit op korte termijn haalbaar. Voor cold cases geldt weliswaar dat ook een termijn van achttien maanden te kort kan zijn, maar een dergelijke bewaartermijn biedt in ieder geval mogelijkheden om in niet op te lossen zaken langer te rechercheren op verkeersgegevens. De voorgestelde termijn van achttien maanden past in de door de richtlijn geboden bandbreedte van zes tot vierentwintig maanden en verhoudt zich goed met de bewaartermijnen zoals deze tot nu toe in de voorstellen van andere lidstaten zijn opgenomen. In paragraaf 6 wordt ingegaan op de termijnen die in andere lidstaten worden gehanteerd. In het voorliggende wetsvoorstel is geen gebruik gemaakt van de mogelijkheid om vanwege specifieke omstandigheden een langere bewaartermijn dan twee jaar vast te stellen. Zolang de behoefte hieraan niet is gebleken zou het opsporingsbelang niet opwegen tegen de kosten die hieraan zijn verbonden en de consequenties voor de persoonlijke levenssfeer.

Zoals gezegd geldt de bewaartermijn voor zowel de traditionele telefonie- als de internetgegevens. Met betrekking tot internetgegevens wordt in het rapport van de Erasmus Universiteit aangegeven dat er op basis van het verrichte dossieronderzoek geen conclusies kunnen worden getrokken ten aanzien van een bepaalde termijn. Hierbij dienen echter een aantal kanttekeningen te worden geplaatst.
Ten eerste dient te worden bedacht dat tot 1 september 2004 een wettelijke bevoegdheid tot het vorderen van gegevens over naam, adres, woonplaats en nummer in het kader van de opsporing ontbrak. Het achterhalen van deze zogenaamde gebruikersgegevens die van belang zijn bij de start van een onderzoek nam daardoor een hoge vlucht. Hierdoor is opsporingsonderzoek met behulp van internetgegevens in feite nog volop in ontwikkeling. In die zin is bovengenoemde constatering dan ook niet verwonderlijk. In lopende onderzoeken valt daarentegen een stijgende lijn te bespeuren wat betreft het gebruik van internetgegevens, waarbij deze niet zelden gegevens betreffen die ouder zijn dan zes maanden.
Voorts is van groot belang dat er van telefonie over het internet verwacht wordt dat het binnen afzienbare tijd de vervanger zal worden van de traditionele telefonie. Dit betekent, zoals door de onderzoekers van de Erasmus Universiteit ook is onderkend, dat de behoefte aan verkeersgegevens van internettelefonie van vergelijkbare omvang zal worden als die van traditionele telefonie, zodat het voor de hand ligt voor beide middelen een gelijksoortige bewaartermijn te hanteren. Deze argumentatie kan worden doorgetrokken naar e-mail over het internet dat eveneens een communicatiemiddel is. Het hanteren van verschillende bewaartermijnen voor verschillende communicatiemiddelen houdt het risico in zich van verplaatsingseffecten waardoor de regeling van de bewaarplicht eenvoudig omzeild zou kunnen worden.
In het verlengde hiervan is verder van belang dat aannemelijk is dat, gelet op de snelle ontwikkeling van nieuwe technologieën, in de nabije toekomst meer nadruk gelegd zal worden op technisch sporenonderzoek en dat deze

sporen een meer prominente rol in het strafrechtelijk onderzoek zullen gaan vervullen. Thans, in onderzoeken waarbij materiaal via internet wordt verspreid, zoals het geval is bij strafbare feiten als de verspreiding van kinderpornografie, extremistische uitingen dan wel terrorismedreigingen, is dergelijk sporenonderzoek al een veelgebruikt middel.
Tengevolge van de ontwikkelingen in het gebruik van internet, zoals de toename van het gebruik van internet onder de Nederlandse bevolking, de omvang van het dataverkeer dat tussen verschillende aansluitpunten plaatsvindt en het aanbod van nieuwe diensten zoals internettelefonie, heeft tijdens de onderhandelingen over de richtlijn aan Nederlandse zijde meegewogen dat het volume van de te bewaren internetgegevens, en de aan de opslag van die gegevens verbonden kosten, beheersbaar zouden moeten zijn en in evenwicht met het doel van de bewaarplicht. Het volume van de op grond van de richtlijn dataretentie te bewaren internetgegevens is echter niet zodanig omvangrijk, of afwijkend van het volume van de inzake de traditionele telefonie te bewaren gegevens, dat dit zou strekken tot vaststelling van een bewaartermijn die afwijkt van die voor de traditionele telefonie.

Gelet op het voorgaande is er in het voorliggende wetsvoorstel voor gekozen om ten aanzien van telefonie- en internetgegevens eenzelfde bewaartermijn te bepalen. Deze keuze is verder gemotiveerd door de uitkomsten van een onderzoek van een onafhankelijk onderzoeksbureau naar de implementatie van de bewaarplicht, met betrekking tot de impact op de kosten van de implementatiemodellen van een wijziging van de bewaartermijn. Dit betreft een onderzoek naar de nationale implementatie van de Europese richtlijn dataretentie door het bureau Verdonck, Klooster & Associates BV (hierna ook te noemen: VKA), waar hieronder (paragraaf 2.8) nader op in zal worden gegaan. Voor de berekening van de kosten van de verschillende modellen zijn de onderzoekers van VKA uitgegaan van een bewaartermijn van één jaar, waarbij ze de additionele kosten van twee jaar opslag hebben berekend, alsook de verlaging daarvan in het geval van een bewaartermijn van een half jaar. In dat laatste geval is, volgens de onderzoekers, een verlaging van de kosten van bijna 7 miljoen euro te verwachten over een periode van vijf jaar. In het geval van een additionele opslag van twee jaar komen er circa 14 miljoen euro bij. Ook hier is voor alle onderzochte opties een vergelijkbaar bedrag te verwachten.

Alle belangen in ogenschouw nemend rechtvaardigt het grote belang van telecommunicatiegegevens voor veel opsporingsonderzoeken de voorgestelde bewaartermijn. Deze termijn kan proportioneel worden geacht in verhouding tot de belangen van de persoonlijke levenssfeer en de lasten voor de aanbieders. Daarbij dient in ogenschouw genomen te worden dat ook thans reeds verkeersgegevens worden bewaard door de aanbieders van telecommunicatiediensten ten behoeve van bedrijfsdoeleinden. Deze gegevens worden ook thans op ruime schaal opgevraagd door opsporingsinstanties. Zowel het bewaren van de gegevens als de bevraging ervan door opsporingsinstanties is met waarborgen omkleed ten behoeve van de bescherming van de persoonlijke levenssfeer van de burger. Dat moet ook zo blijven. In het kader van de consultatie hebben enkele adviesorganen aandacht gevraagd voor de bescherming van de persoonlijke levenssfeer. Het wetsvoorstel voorziet in de nodige waarborgen terzake. Het belang van telecommunicatiegegevens voor de opsporing leidt geenszins tot de conclusie dat een bewaartermijn gekozen zou moeten worden die gelijkstaat aan de kortste termijn die de richtlijn toestaat. Ook met het oog op de economische belangen, zoals de omzet in de telecomsector en de winsten die daarbij worden gemaakt in relatie tot de lasten waarmee het bedrijfsleven wordt geconfronteerd als gevolg van de implementatie van het onderhavige wetsvoorstel, valt niet goed in te zien dat sprake zou zijn van een disproportionele aantasting van de belangen van het bedrijfsleven. De keuze voor een bewaartermijn binnen de marges die door de richtlijn zijn toegestaan zal relatief gezien van minder grote betekenis zijn in verhouding tot de totale lasten voor het bedrijfsleven die samenhangen met de invoering van een bewaarplicht als zodanig. In het licht van de totale kosten die zijn verbonden aan de bewaring van

telecommunicatiegegevens zijn de extra kosten van het langer bewaren van gegevens relatief gezien van minder zwaarwegend belang. De voordelen daarvan zijn onder omstandigheden echter groot. De langere bewaartermijn zal dan ook meer toegevoegde waarde kunnen hebben. Eén en ander in beschouwing genomen is een bewaartermijn van achttien maanden zeker verantwoord te achten.

In paragraaf 7 wordt nader in gegaan op de bedrijfseffecten in verband met dit wetsvoorstel. In het licht van de totale kosten voor het bedrijfsleven bij het door hen voorgestane model van decentrale opslag en beantwoording van de gevraagde gegevens door de aanbieders, zijn de kosten van de opslag van de gegevens niet exceptioneel. De keuze voor een bewaartermijn van achttien maanden zal dan ook niet tot buitenproportionele meerkosten leiden in vergelijking tot de termijn van twaalf maanden die in het rekenmodel van VKA is aangehouden.

2.4 De bewaring van locatiegegevens

Thans kent de Telecommunicatiewet op grond van artikel 13.4, tweede lid, een beperkte bewaarplicht, ten behoeve van het verrichten van de zogenaamde bestandsanalyse. Deze analyse houdt in dat als de aanbieder niet kan voldoen aan zijn verplichting om op vordering van een bevoegde autoriteit gegevens over een gebruiker van telecommunicatie te verstrekken, hij deze door een analyse van zijn bestanden achterhaalt. Dit doet zich voor wanneer de gegevens over een gebruiker van telecommunicatie bij de aanbieders niet zijn geregistreerd, bijvoorbeeld bij vooruit betaalde mobiele telefonie (prepaid cards). In zo'n geval zijn extra handelingen nodig om de gegevens – in het bijzonder het aan de gebruiker verleende nummer - te achterhalen. In het Besluit bijzondere vergaring nummergegevens (Stb. 2002, 31) is deze bestandsanalyse uitgewerkt. De aanbieder is gehouden om de voor de bestandsanalyse benodigde gegevens gedurende een periode van drie maanden te bewaren. Het betreft hier de gegevens betreffende de tijdstippen waarop telecommunicatie heeft plaatsgevonden, de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers en de basisstations waarbij deze gegevens zijn binnengekomen. De basisstations bevatten informatie over de locatie van de gebruiker van telecommunicatie.
De uit de richtlijn dataretentie voortvloeiende bewaarplicht omvat de gegevens die nodig zijn om de bron van een communicatie te traceren en te identificeren. Indien een aanbieder de gegevens omtrent een gebruiker, zoals bedoeld in artikel 13.4, eerste lid, van de Telecommunicatiewet niet direct beschikbaar heeft dan zal de bestandsanalyse moeten kunnen worden verricht. Verlenging van de bewaartermijn van drie naar achttien maanden waarborgt dat gedurende de bewaartermijn kan worden achterhaald welke nummer behoort bij een gebruiker zodat daarmee volledig kan worden voldaan aan de verplichting van de richtlijn tot bewaring van het telefoonnummer en de bijbehorende gegevens, die nodig zijn om de bron van een communicatie te identificeren. Daarnaast kunnen de locatiegegevens van groot belang zijn voor opsporing en vervolging omdat deze gegevens inzicht geeft in de geografische positie van waar uit de communicatie met een mobiele telefoon heeft plaatsgevonden. Aan de hand van deze informatie kunnen verklaringen van personen over hun verblijfplaats ten tijde van die communicatie worden getoetst.

In hun adviezen hebben het CBP, de aanbieders en het Actal aangegeven van mening te zijn dat met de verplichting tot bewaring van locatiegegevens tijdens de communicatie buiten de reikwijdte van de richtlijn wordt getreden. Het CBP acht het bewaren van deze gegevens disproportioneel omdat deze categorie van gegevens met reden is uitgesloten van het toepassingsgebied van de richtlijn, omdat het neerkomt op een te indringende, alomvattende verborgen surveillance van de verplaatsingen van zeer grote aantallen onverdachte burgers. Met deze opvatting wordt echter voorbij gegaan aan de achtergrond van de bestandsanalyse op grond van het Besluit

bijzondere vergaring nummergegevens. De locatiegegevens worden op grond van dat besluit niet bewaard ten behoeve van het opsporingsonderzoek van de politie maar ten behoeve van een bestandsanalyse die wordt verricht door de aanbieder, op basis waarvan de gebruikersgegevens, bedoeld in de artikelen 126na en 126ua van het Wetboek van Strafvordering, kunnen worden achterhaald. Dit betreft gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie. Er is dus geen sprake van verborgen surveillance van de verplaatsingen van burgers, zoals het CBP veronderstelt. De bestandsanalyse is destijds door de aanbieders zelf aangedragen als alternatief voor de door de regering voorgestelde registratie van personen bij de verkoop van prepaid cards (Staatsblad 2002, 31, blz.8). De bestandsanalyse, als alternatief voor een registratieplicht, werd door de regering nodig geacht opdat ook gebruikers van vooruitbetaalde diensten in het belang van opsporingsonderzoeken kunnen worden geïdentificeerd (Kamerstukken 1997/98, 25533, nr. 8, blz. 11). De bestandsanalyse vindt plaats aan de hand van een schriftelijk verzoek van de bevoegde autoriteit, waarin gegevens worden vermeld betreffende twee tijdstippen waarop en locaties waar de gebruiker kennelijk gebruik heeft gemaakt van telecommunicatie (artikel 5, tweede lid, Besluit vergaring bijzondere nummergegevens). Om een bestandsanalyse te kunnen verrichten zal de aanbieder over meerdere locatiegegevens moeten kunnen beschikken, ten behoeve van de 'match' met het tweetal door de bevoegde autoriteiten aan te leveren tijdstippen. Indien deze benadering op overwegende bewaren zou stuiten dan zal voor de geschetste problematiek van pre paidcard-gebruikers naar een alternatieve oplossing moeten worden gezocht. In Denemarken zijn de aanbieders verplicht om voor mobiele telefonie de locatiegegevens te bewaren die betrekking hebben op zowel de aanvang als het einde van de communicatie. In Zweden wordt thans een rapport voorbereid over de implementatie van de richtlijn dataretentie. In het kader daarvan wordt thans overwogen om te komen tot een verplichting tot bewaring van locatiegegevens voor mobiele telefonie die betrekking hebben zowel op de aanvang en het einde van de communicatie als op ieder uur dat de communicatie duurt. In Duitsland geldt voor de aanbieders de verplichting om, indien oproepnummer worden uitgegeven, die nummers vast te leggen evenals de daarbij behorende identificerende gegevens, zoals naam, adres (bij vaste telefonie) en geboortedatum. Niet uitgesloten is dat dan, naar het voorbeeld van Duitsland, gekozen moet worden voor een verplichting voor de aanbieders tot voorafgaande registratie van de identiteit van prepaid card-houders. Voorkomen moet namelijk worden dat de groep van gebruikers die gebruik maakt van vooruitbetaalde diensten bij mobiele telecommunicatie buiten de reikwijdte van de richtlijn zou komen te vallen. Nu in dit wetsvoorstel een bewaartermijn van achttien maanden wordt voorgesteld, impliceert dit de verhoging van de bewaartermijn van het Besluit bewaring nummergegevens tot eveneens achttien maanden. Daarbij moet worden opgemerkt dat het hier gaat om gegevens die de aanbieders ook thans reeds bewaren. De voorgestelde verlenging van de bewaartermijn tot achttien maanden zal niet tot buitenproportionele meerkosten leiden De extra lasten voor de aanbieders, die uit de voorgestelde verlenging voortvloeien, zijn betrokken in de berekening van de bedrijfseffecten. Daarvoor wordt verwezen naar paragraaf 7 (bedrijfseffecten).

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

De richtlijn dataretentie beoogt een harmonisatie tot stand te brengen van de nationale bepalingen van de lidstaten inzake het bewaren van bepaalde telecommunicatiegegevens, teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgeving van de lidstaten. In de richtlijn worden de categorieën van gegevens aangewezen die met het oog op dit doel bewaard moeten worden (artikel 5, eerste lid). De richtlijn staat er niet aan in de weg dat de te bewaren gegevens worden gebruikt voor andere doelen. In de richtlijn wordt bepaald dat de procedure en de te vervullen voorwaarden voor toegang tot de gegevens door elke lidstaat worden vastgesteld in de nationale

wetgeving (artikel 4). Daarbij geldt dat de bewaarde gegevens alleen in welbepaalde gevallen aan de bevoegde nationale autoriteiten worden verstrekt.

Het wetsvoorstel voorziet niet in afzonderlijke bepalingen omtrent de toegang tot de bewaarde gegevens. De Nederlandse wetgeving bevat namelijk reeds de nodige regels over de toegang tot telecommunicatiegegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Deze bevoegdheden worden in paragraaf 3.1. nader beschreven. De toegang tot de gegevens voor de officier van justitie of de opsporingsambtenaar is thans beperkt tot gegevens die bij de aanbieder beschikbaar zijn, De thans, ter implementatie van de richtlijn dataretentie, voorgestelde wettelijke regeling bevat geen afzonderlijke regels over de toegang tot de bewaarde gegevens en zal er, in vergelijking met de huidige situatie, dan ook niet toe leiden dat verdergaande inbreuken worden gemaakt op de rechten van burgers. Wel zullen de gegevens in meer gevallen beschikbaar zijn ten behoeve van de opsporing en vervolging van strafbare feiten. Dat gevolg wordt met de richtlijn en dit wetsvoorstel juist beoogd.

Het voorgaande is tevens van belang voor de taakuitvoering van de inlichtingen- en veiligheidsdiensten 2002. Op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 beschikken de diensten over vergelijkbare bevoegdheden als de politie voor het opvragen van verkeersgegevens en identificerende gegevens. Deze bevoegdheden worden in paragraaf 3.1. eveneens nader beschreven. Ook voor de inlichtingen- en veiligheidsdiensten diensten zal de bewaarplicht met zich meebrengen dat de gegevens in meer gevallen beschikbaar zijn voor de uitoefening van de wettelijke taken van de diensten dan thans het geval is.

Op grond van het voorgaande kan worden geconcludeerd dat de consequenties van de bewaarplicht voor de feitelijke mogelijkheden voor de bevoegde autoriteiten om gegevens op te vragen beperkt zijn omdat de bewaarplicht niet voorziet in uitbreiding van de bevoegdheden voor de bevoegde autoriteiten om gegevens op te vragen bij de aanbieders. Wel zal de bewaarplicht met zich meebrengen dat de gegevens in meer gevallen beschikbaar zullen zijn voor de bevoegde autoriteiten, ten behoeve van de uitvoering van hun wettelijke taken. Daarbij kan nog worden opgemerkt dat thans een wetsvoorstel bij de Kamer in behandeling is dat voorziet in aanpassing van de bestaande bevoegdheden voor de toegang tot telecommunicatiegegevens. In paragraaf 3.1. wordt hier nader op in gegaan.

2.6 Gegevensbescherming en gegevensbeveiliging

De richtlijn dataretentie legt de lidstaten de verplichting op ervoor zorg te dragen dat de aanbieders een aantal beginselen van gegevensbescherming en gegevensbeveiliging respecteren met betrekking tot de gegevens die overeenkomstig deze richtlijn worden bewaard (artikel 7). De bewaarde gegevens dienen dezelfde kwaliteit te hebben en onderworpen te worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk. Passende technische en organisatorische maatregelen zijn vereist ter beveiliging van de gegevens tegen vernietiging, verlies, wijziging of niet-toegelaten of onrechtmatige opslag, verwerking of toegang. De maatregelen dienen te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen. Tenslotte moeten de gegevens aan het einde van de bewaarperiode worden vernietigd, met uitzondering van de geraadpleegde en vastgelegde gegevens.

De verplichtingen van de richtlijn dataretentie vormen een aanvulling op de bestaande regels op het gebied van de gegevensbescherming en gegevensbeveiliging die van toepassing zijn op de gegevensverwerking door de aanbieders. Deze regels houden in de eerste plaats verband met de Wet bescherming persoonsgegevens

(WBP). De WBP is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Ook de gegevensverwerking door de aanbieders in het kader van het aanbieden van openbare telecommunicatienetwerken en openbare telecommunicatiediensten valt onder de reikwijdte van deze wet. De WBP bevat bepalingen omtrent de voorwaarden voor gegevensverwerking, doelbinding en de verdere verwerking van gegevens, de bewaartermijnen, de rechten van de betrokkene, rechtsbescherming en het toezicht. De verantwoordelijke dient de nodige maatregelen te treffen opdat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verder verwerkt, juist en nauwkeurig zijn (artikel 11, tweede lid, WBP). Ook is de verantwoordelijke verplicht passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige gegevensverwerking (artikel 13 WBP).

In aanvulling op de regels van de Wet bescherming persoonsgegevens worden in de Telecommunicatiewet specifieke regels gesteld voor de verwerking van persoonsgegevens door de aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. Dit houdt verband met de implementatie van de eerdergenoemde Richtlijn nr. 02/58/EG van het Europees Parlement en de Raad van de Europese Unie, van 12 juli 2002, betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie). In deze richtlijn worden de beginselen van Richtlijn nr. 95/46/EG (privacyrichtlijn) omgezet in specifieke voorschriften voor de verwerking van persoonsgegevens in de sector elektronische communicatie van de Gemeenschap. Anders dan de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de verwerking van gegevens betreffende natuurlijke personen, strekt de reikwijdte van de bepalingen van de richtlijn betreffende privacy en elektronische communicatie zich in beginsel ook uit tot rechtspersonen. De richtlijn privacy en elektronische communicatie is grotendeels geïmplementeerd in hoofdstuk 11 van de Telecommunicatiewet en de daarop berustende uitvoeringsregelgeving (Kamerstukken II, 2002-2003, 28851, nr. 3). Deze regels hebben onder meer betrekking op de doeleinden met het oog waarop de aanbieders verkeersgegevens kunnen verwerken, de duur van de gegevensverwerking, de veiligheid en de verstrekking van informatie over de gegevensverwerking aan de abonnee of gebruiker. De aanbieders zijn verplicht passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de aangeboden netwerken en diensten (artikel 11.3 TW).

Op grond van de toepasselijke bepalingen van hoofdstuk 11 van de Telecommunicatiewet is het onder voorwaarden mogelijk dat de verwerkte en opgeslagen verkeers- en locatiegegevens, ook indien deze niet meer nodig zijn voor de overbrenging van communicatie, worden verwerkt voor andere doelen, zoals de facturering of het verrichten van marktonderzoek (artikel 11.5 en 11.5a TW). De bepalingen van dit hoofdstuk van de Telecommunicatiewet hebben betrekking op de gegevensverwerking ten behoeve van de zakelijke doeleinden van de aanbieders. Daarom wordt voorgesteld de verplichting tot de bewaring van de gegevens, bedoeld in de richtlijn dataretentie, op te nemen in hoofdstuk 13 van de Telecommunicatiewet. Hiermee wordt onderstreept dat de bewaarplicht geschiedt voor andere doeleinden en dat het gebruik van de bewaarde gegevens in beginsel daartoe beperkt is. Met de voorgestelde wijziging van artikel 11.13 van de Telecommunicatiewet wordt verhelderd dat de gegevens, die op grond van hoofdstuk 13 moeten worden bewaard, uitsluitend worden bewaard ten behoeve van een van hoofdstuk 11 afwijkend doel, namelijk de beschikbaarheid voor de bestrijding van ernstige misdrijven. De op grond van deze verplichting te bewaren gegevens kunnen in beginsel derhalve niet verder worden verwerkt ten behoeve van zakelijke doeleinden van de aanbieders. Dit is slechts anders indien de te

bewaren gegevens dezelfde gegevens zijn als die welke onder de voorwaarden, genoemd in de artikelen 11.5 en 11.5a van de Telecommunicatiewet, kunnen worden verwerkt voor de aldaar genoemde doelen.

In aanvulling op de regels van de Wet bescherming persoonsgegevens en de Telecommunicatiewet schept het voorliggende wetsvoorstel de mogelijkheid tot het stellen van nadere regels terzake van de bescherming en beveiliging van de te bewaren gegevens. Ingevolge de richtlijn dataretentie moeten namelijk regels worden gesteld terzake van de passende technische en organisatorische maatregelen die de aanbieder moet treffen om de gegevens te beveiligen tegen vernietiging, verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking en om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen. Verder moeten regels worden gesteld die de aanbieder verplichten er voor te zorgen dat de bewaarde gegevens dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens van het netwerk en dat de gegevens worden vernietigd na afloop van de bewaarperiode. Daarom zullen, in aanvulling op de Wet bescherming persoonsgegevens en de bepalingen van hoofdstuk 11 van de Telecommunicatiewet, hierover bij algemene maatregel van bestuur nadere regels kunnen worden gesteld. Hiervoor kan aansluiting worden gezocht bij het Besluit beveiliging gegevens aftappen telecommunicatie (Stb. 2003, 472). Dit besluit bevat voorschriften voor de door de aanbieders te treffen beveiligingsmaatregelen rond het aftappen van telecommunicatie.

2.7 Het toezicht op de gegevensverwerking

De richtlijn dataretentie bepaalt dat één of meer overheidsinstanties verantwoordelijk worden gesteld voor de uitoefening van het toezicht op de toepassing van het bepaalde in artikel 7 van de richtlijn met betrekking tot de veiligheid van de bewaarde gegevens. Deze instanties kunnen dezelfde zijn als die welke zijn belast met het toezicht op de naleving van de Wet bescherming persoonsgegevens (artikel 9, eerste lid).

In dit wetsvoorstel wordt voorgesteld het toezicht op de naleving van het bij of krachtens dit wetsvoorstel bepaalde op te dragen aan de Minister van Economische Zaken, met inachtneming van de bevoegdheden van het College bescherming persoonsgegevens terzake.

Het toezicht betreft:

- het naleven van de verplichting tot het bewaren van de gegevens;
- de bij nadere regels te stellen eisen aan de wijze, waarop de gegevens bewaard worden (met name beveiliging);
- de waarborgen tegen misbruik van de bewaarde gegevens, en
- tijdige vernietiging van de gegevens na afloop van de bewaartermijn.

De keuze om het toezicht op te dragen aan de Minister van Economische Zaken is ingegeven door de situatie dat de Minister van Economische Zaken thans reeds toezicht houdt op de naleving van de aftapverplichtingen die voortvloeien uit hoofdstuk 13. Zijn toezichthoudende ambtenaren (het Agentschap Telecom) oefenen actief toezicht uit op de naleving van de verplichtingen die ingevolge hoofdstuk 13 op de aanbieders rusten en bezoeken in dat verband elk jaar meer dan honderd aanbieders. Omdat de verplichting tot het bewaren van gegevens nauw verband houdt met het opsporen en voorkomen van zware criminaliteit evenals het kunnen aftappen van communicatie is het doelmatig en effectief om ook het toezicht op de naleving van de bepalingen inzake de bewaring van telecommunicatiegegevens op te dragen aan de Minister van Economische Zaken. Voorts wordt voorgesteld het toezicht op de naleving van de artikelen 11.5, 11.5a en 11.13 van de wet, waarvan

het toezicht op de naleving thans is opgedragen aan het college van de Opta, voortaan op te dragen aan de Minister van Economische Zaken. Hiertoe wordt voorgesteld artikel 15.1 van de Telecommunicatiewet te wijzigen. De reden van het overbrengen van het toezicht op genoemde artikelen van het college naar de Minister van Economische Zaken houdt verband met de nauwe verwevenheid van de naleving van deze artikelen met de naleving van de nieuwe bepalingen inzake de bewaarplicht. De aanbieders moeten de verkeersgegevens vernietigen wanneer die gegevens niet meer noodzakelijk zijn voor hun bedrijfsvoering (in het bijzonder het kunnen sturen van rekeningen). In de praktijk komt dit doorgaans neer op een bewaarperiode van circa drie maanden. Een actief toezicht op de naleving van de verplichtingen die voortvloeien uit de artikelen 11.5 en 11.5a van de wet is te meer gewenst nu een gedeelte van deze gegevens op grond van de bewaarverplichting langer bewaard zal worden dan nu doorgaans het geval is. Door het toezicht op de naleving van de bepalingen waarin regels worden gegeven ter zake van het bewaren en gebruiken van gegevens in één hand te brengen, wordt de naleving het beste gewaarborgd en kan het toezicht het meest doelmatig worden uitgevoerd met de minste overlast voor de bedrijven. Gelet op het voorgaande hangt de naleving van de voorgestelde regels samen met de naleving van de bepalingen in artikel 11.5, 11.5a en 11.13 van de Telecommunicatiewet, die hiertoe ook bij dit wetsvoorstel worden aangepast. Om die reden is, is in goed overleg met het college (OPTA) besloten ook het toezicht op deze drie artikelen (11.5, 11.5a en 11.13) bij de Minister van Economische Zaken te leggen. Hiertoe wordt artikel 15.1 bij dit wetsvoorstel aangepast. Met deze overheveling van toezichthoudende bevoegdheden kan het college volledig instemmen.

Opgemerkt zij dat het de diverse toezichthouders vrij staat om de door hen benodigde gegevens op te vragen voor hun taken. Met een verwijzing naar het bestaande artikel 18.7 van de Telecommunicatiewet blijft die mogelijkheid voor de periode bedoeld in artikelen 11.5 en 11.5a van de wet (gemiddeld drie maanden) van kracht. Het college van de Opta gebruikt deze gegevens bijvoorbeeld in het kader van het toezicht op de naleving van de spam-regelgeving.

De toezichthoudende taak van de Minister van Economische Zaken ten aanzien van de naleving van de artikelen 11.5, 11.5a en 11.13 en van hoofdstuk 13 van de Telecommunicatiewet doet op geen enkele wijze afbreuk aan de toezichtbevoegdheden die het College bescherming persoonsgegevens heeft met betrekking tot het gebruik van gegevens die zijn aan te merken als persoonsgegevens. In goed overleg met het College bescherming persoonsgegevens zal een aanpak worden uitgewerkt voor de uitvoering van het toezicht. In het kader daarvan zullen naar verwachting daadwerkelijke controles door het Agentschap Telecom worden uitgevoerd. Het vorenstaande laat de bevoegdheid van het CBP, om op ieder gewenst moment ook zelfstandig toezichthoudende activiteiten te ontplooien, evenwel onverlet.

2.8 Vereisten voor de opslag van bewaarde gegevens

De richtlijn dataretentie verplicht de lidstaten om te waarborgen dat de gegevens op zodanige wijze worden bewaard dat deze gegevens, evenals alle andere daarmee verband houdende informatie, onverwijld aan de bevoegde autoriteiten kunnen worden meegedeeld wanneer daarom wordt verzocht (artikel 8). In deze paragraaf zal op de onderscheidene elementen van deze verplichting worden ingegaan.

De verplichtingen van de richtlijn dataretentie, zoals die in het bijzonder zijn neergelegd in artikel 7, onderdelen a en c, houden in dat maatregelen getroffen moeten worden die waarborgen dat de toegang tot de gegevens uitsluitend kan plaatsvinden door de personen die daarvoor gemachtigd zijn en dat de gegevens worden vernietigd na ommekomst van de bewaartermijn. Om daaraan te kunnen voldoen moet de aanbieder de te

bewaren gegevens wellicht gescheiden van de gegevens van het netwerk bewaren. Dit kan anders zijn indien de aanbieder bedoelde maatregelen ook kan treffen zonder een dergelijke scheiding. Indien nodig kunnen de bedoelde maatregelen nader aan de orde komen in de algemene maatregel van bestuur, die op basis van het vierde lid van het voorgestelde artikel 13.5 van de Telecommunicatiewet kan worden opgesteld.

Ten tijde van de onderhandelingen over de richtlijn dataretentie is in de berichtgeving aan de Kamer melding gemaakt van de verschillende modaliteiten voor de opslag van de te bewaren gegevens (Kamerstukken II 2005-2006, 23490, nrs. AM, 355, 360 en 398). Hierbij werd onderscheid gemaakt tussen de opslag van de gegevens bij de aanbieders zelf (decentrale opslag) en de opslag bij een derde partij (centrale opslag). Bij de centrale opslag zouden de bevoegde autoriteiten de bewaarde gegevens op centraal niveau bij een derde partij kunnen vorderen. De kosten, verbonden aan de implementatie van de richtlijn dataretentie, zouden dan lager kunnen zijn dan wanneer de gegevens door de aanbieders zelf zouden worden bewaard. Dit zou ook relevant kunnen zijn voor de verdeling van de kosten omdat de kosten voor de aanbieders dan zouden kunnen worden beperkt tot de kosten die gemoeid zijn met het beschikbaar stellen van de gegevens aan de derde partij en de aanpassingen in hun systemen voor die beschikbaarstelling. Gelet hierop is destijds aangegeven dat het aangewezen was nader onderzoek te verrichten naar de mogelijkheid om de bewaarplicht door middel van een centraal model uit te voeren.

Ten behoeve van de implementatie van de richtlijn dataretentie is in opdracht van de Minister van Justitie een extern onderzoeksbureau belast met het verrichten van onderzoek, teneinde inzicht te verkrijgen in de verschillende organisatorische varianten op basis waarvan uitvoering kan worden gegeven aan de verplichtingen van de richtlijn. Dit onderzoek is verricht door het eerdergenoemde bureau Verdonck, Klooster & Associates BV, in samenwerking met Lucent Technologies (hierna ook te noemen: VKA). Het onderzoek is begeleid door een commissie, bestaande uit vertegenwoordigers van de overheid en van de telecommunicatieaanbieders. Doelstelling van het onderzoek was om informatie te verzamelen over de technische en organisatorische aanpassingen bij aanbieders en behoeftestellers die bij de toepassing van verschillende implementatieopties van de bewaarplicht en de daarmee samenhangende bevraging noodzakelijk zijn, inclusief de daaraan verbonden kosten. Er waren vijftien aanbieders betrokken bij de uitvoering van het onderzoek.

In het rapport van dit onderzoek getiteld ‘Naar de nationale implementatie van de Europese richtlijn datarententie’ (29 september 2006) zijn een aantal modellen of scenario’s uitgewerkt die kunnen worden gebruikt voor de opslag en de bevraging van de te bewaren telecommunicatiegegevens. In het onderzoek hebben verschillende implementatieopties centraal gestaan. Onderzocht zijn onder meer de keuze van de plaats van de opslag van de te bewaren gegevens - namelijk bij de aanbieders zelf (decentraal) of bij een derde partij (centraal) - en de toegang tot de gegevens, te weten beantwoording door de aanbieder of directe toegang door de behoeftestellers.

De bevindingen van VKA bieden onvoldoende houvast om op dit moment reeds te komen tot een definitieve keuze voor één van de opties. Om die reden wordt voorgesteld om voor de implementatie van de richtlijn dataretentie van de bestaande situatie uit te gaan, dat wil zeggen decentrale opslag en bewaring van gegevens. De aanbieder heeft dan de mogelijkheid om de implementatie maximaal te laten aansluiten bij zijn huidige wijze van werken. Hiervoor pleit ook dat de onderzoekers hebben vastgesteld dat alleen de optie van decentrale opslag van de gegevens binnen de in de richtlijn gestelde implementatietermijn kan worden afgerond. Bij alle andere opties is er ontwikkeling van, en veel afstemming en overleg over, technische en organisatorische aspecten nodig hetgeen de haalbaarheid van de implementatie van de opties binnen de door de richtlijn dataretentie gestelde termijn zal bemoeilijken.

Gelet op het voorgaande is het voorliggende wetsvoorstel gebaseerd op de bestaande situatie, namelijk dat de gegevens beschikbaar zijn bij de aanbieders. Dat wil zeggen dat de aanbieders zelf de te bewaren gegevens opslaan en dat deze de gegevens, in het geval van een vordering van een daartoe bevoegde autoriteit die is belast met het onderzoeken, opsporen en vervolgen van strafbare feiten, voor dat doel beschikbaar stelt. Alleen in geval van een vordering van actuele gebruikersgegevens (naam, adres, woonplaats, nummer en soort dienst) verloopt de vordering en beschikbaarstelling door tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie (hierna ook te noemen: CIOT), op de wijze die op grond van artikel 13.4, derde lid, is bepaald in het Besluit verstrekking gegevens telecommunicatie (Stb. 2000,. 71, gewijzigd bij Stb. 2006, 426).

De richtlijn dataretentie verplicht tot waarborgen dat de gegevens onverwijld aan de bevoegde autoriteiten kunnen worden medegedeeld wanneer daarom wordt verzocht (artikel 8). De Telecommunicatiewet voorziet thans niet in een termijn waarbinnen de gegevens door de aanbieders aan de bevoegde autoriteiten moeten worden verstrekt. Evenmin worden er regels gesteld voor de beschikbaarstelling van gegevens in geval van spoed. Wel zijn er afspraken tussen openbaar ministerie, politie en de inlichtingen- en veiligheidsdiensten enerzijds en de aanbieders anderzijds terzake van het verkrijgen van gegevens. De termijnen waarop de gegevens beschikbaar komen voor de opsporing verschillen naar de aard van de gegevens en zijn mede afhankelijk van de inrichting van de bedrijfsvoering en de staat van de techniek in het bedrijf van de betreffende aanbieder. Omdat de huidige praktijk, op basis van de bestaande afspraken, een uitéénlopend beeld geeft en aan het stellen van eenduidige termijnen aanzienlijke lasten voor de aanbieders kunnen zijn verbonden, dient de nodige terughoudendheid te worden betracht ten aanzien van het stellen van termijnen voor het aanleveren van de gegevens door de aanbieders. Het begrip onverwijld in de richtlijn en in het voorgestelde artikel 13.4, eerste lid, van de Telecommunicatiewet wordt in dit verband dan ook opgevat als ‘zo spoedig als de inrichting van de bedrijfsvoering en de stand der techniek van het betreffende bedrijf dat mogelijk maakt’. In de eventuele nadere regeling bij algemene maatregel van bestuur zal op dit punt worden aangesloten bij de bestaande afspraken met de aanbieders.

2.9 Rechtsbescherming, aansprakelijkheid en sancties in verband met de Richtlijn nr. 95/46/EG

De richtlijn dataretentie verplicht de lidstaten tot het treffen van de noodzakelijke maatregelen om te waarborgen dat de nationale maatregelen ter implementatie van hoofdstuk 3 van de Richtlijn nr. 95/46/EG volledig toepasselijk zijn op de verwerking van gegevens onder de richtlijn dataretentie (artikel 13). Hoofdstuk 3 van de eerdergenoemde richtlijn heeft betrekking op de mogelijkheid van beroep op de rechter voor de betrokkene, de aansprakelijkheid voor schade van de voor de verwerking verantwoordelijke en de vaststelling van sancties bij inbreuk op de ter uitvoering van de richtlijn vastgestelde bepalingen.

Zoals eerder aangegeven (paragraaf 2.5) is de Richtlijn nr. 95/46/EG geïmplementeerd in de Wet bescherming persoonsgegevens (WBP) en de daarop berustende uitvoeringsregelgeving. De WBP bevat in de hoofdstukken 8 en 10 specifieke bepalingen over het beroep op de rechter, de aansprakelijkheid en sancties. Deze bepalingen zijn onverkort van toepassing op de gegevens die op grond van de richtlijn dataretentie worden verwerkt zodat het niet noodzakelijk is in het voorliggende wetsvoorstel hieromtrent aanvullend regels op te nemen. Op de rechtsbescherming voor de betrokkene in verband met de bewaring van telecommunicatie verkeersgegevens zal hieronder in een afzonderlijke paragraaf nader worden in gegaan (paragraaf 5).

2.10 Straffen

De richtlijn dataretentie verplicht de lidstaten om de noodzakelijke maatregelen te nemen om te waarborgen dat de opzettelijke toegang of overdracht van gegevens, die in overeenstemming met de richtlijn worden bewaard en die niet is toegestaan in de nationale wetgeving die tengevolge van deze richtlijn is aangenomen, strafbaar wordt gesteld met effectieve, proportionele en ontmoedigende straffen, inclusief administratieve en strafrechtelijke straffen. In Overweging 18 van de richtlijn wordt verwezen naar kaderbesluit 2005/222/JBZ van de Raad, van 24 februari 2005, over aanvallen op informatiesystemen, dat bepaalt dat de opzettelijke onrechtmatige toegang tot informatiesystemen, met inbegrip van de gegevens die daarin worden bewaard, strafbaar wordt gesteld als een strafrechtelijke inbreuk.

In geval er sprake is van het onrechtmatig verschaffen van toegang tot gegevens, die geautomatiseerd worden verwerkt, is een dergelijke handelwijze strafbaar op grond van het Wetboek van Strafrecht. Het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of een deel daarvan is als computervredebreuk strafbaar gesteld (artikel 138a Sr). Met de inwerkingtreding van de Wet computercriminaliteit II, op 1 september 2006, is de strafbaarstelling van handelingen die aanleiding kunnen geven tot het 'binnendringen' in de zin van deze strafbepaling, verruimd. Ingeval er sprake is van het overnemen van de opgeslagen gegevens of indien de computervredebreuk wordt gepleegd door tussenkomst van een openbaar telecommunicatienetwerk dan is, mits onder bepaalde omstandigheden gepleegd, een hoger strafmaximum van toepassing. In geval er sprake is van het vernielen van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, dan is een dergelijke handelwijze eveneens strafbaar. Het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens is als een vorm van vernieling of beschadiging strafbaar gesteld (artikel 350a Sr). Ingeval de vernieling wordt gepleegd na door tussenkomst van een openbaar telecommunicatienetwerk in een geautomatiseerd werk te zijn binnengedrongen, is een hoger strafmaximum van toepassing.

De aanbieder, die niet voldoet aan de verplichtingen op het gebied van de bescherming en beveiliging van de bewaarde gegevens, als neergelegd in het voorgestelde artikel 13.5 van de Telecommunicatiewet, pleegt een overtreding van de Wet op de economische delicten (artikel 1, onder 2º, WED). Aanvullend zijn de mogelijkheden tot handhaving, neergelegd in hoofdstuk 15 van de Telecommunicatiewet, van toepassing. Daartoe behoort de mogelijkheid om aan de aanbieder een bestuurlijke boete op te leggen in geval van overtreding van de voorschriften van de hoofdstukken 11 of 13 van de Telecommunicatiewet (artikel 15.4 Telecommunicatiewet). Tenslotte kent de WBP een afzonderlijke strafbepaling in geval de verantwoordelijke gegevens zou verstrekken aan een land buiten de Europese Unie, in de gevallen waarin geen waarborgen voor een passend beschermingsniveau wordt geboden (artikel 75 WBP). Gelet op het voorgaande is het dan ook niet noodzakelijk in het voorliggende wetsvoorstel hieromtrent aanvullend regels op te nemen.

2.11 Statistische informatie

De richtlijn dataretentie legt aan de lidstaten de verplichting op ervoor te zorgen dat jaarlijks aan de Commissie statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van diensten. Die informatie heeft betrekking op de gevallen waarin gegevens aan de bevoegde autoriteiten zijn verstrekt, de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop door de bevoegde autoriteiten om overdracht ervan is verzocht en de gevallen waarin verzoeken niet konden worden ingewilligd. De statistische informatie bevat geen persoonsgegevens (artikel 10).

Thans vindt geen algemene registratie plaats van gegevens over de toepassing van de bevoegdheden tot het vorderen van telecommunicatiegegevens door de daarvoor bevoegde autoriteiten. Dit met uitzondering van de verstrekking van gegevens door tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie. Dit betreft het vorderen van actuele gebruikersgegevens. Aan elke vordering tot verstrekking wordt een kenmerk toegekend, aan de hand waarvan kan worden herleid door welke aanbieder, aan welke bevoegde autoriteit en op welke rechtsgrondslag informatie is verstrekt.

Van de verstrekking van telecommunicatiegegevens, die niet via het CIOT plaatsvindt, zal bij het openbaar ministerie een registratie kunnen worden bijgehouden. Aan de hand van de door de autoriteiten, die bevoegd zijn tot het vorderen van verkeers- en locatiegegevens, aan te leveren informatie zal dan achteraf kunnen worden nagegaan in welke gevallen gegevens zijn verstrekt aan de bevoegde autoriteiten, de tijd is die is verstreken tussen de datum van bewaring en de datum van het verzoek om overdracht door de bevoegde autoriteiten en de gevallen waarin verzoeken niet konden worden ingewilligd. Een dergelijke registratie is nodig om te kunnen voldoen aan de eis van de richtlijn. Daarnaast biedt de registratie de mogelijkheid om inzicht te verkrijgen in het functioneren van de bewaarplicht in de praktijk, in het bijzonder wat betreft de effectiviteit van de bewaarplicht, mede in het licht van de gekozen bewaartermijn. Dit is van belang voor de evaluatie van de voorgestelde wettelijke regeling op nationaal niveau (artikel 13.9). Op dit moment voorzien de informatiesystemen van de politie en van het openbaar ministerie niet in dergelijke informatie. Nader zal moeten worden onderzocht welke informatie in de toekomst nodig is en op welke wijze het verzamelen en verwerken van de benodigde gegevens kan worden georganiseerd, inclusief de daaraan verbonden kosten. Het kan niet bij voorbaat geheel worden uitgesloten dat de aan de Commissie te verstrekken informatie – bijvoorbeeld de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten – dan wel gegevens die anderszins nodig zijn ten behoeve van bijvoorbeeld de evaluatie op nationaal niveau, slechts kunnen worden verkregen door het combineren van gegevens van aanbieders en behoeftestellers. Een regeling bij algemene maatregel van bestuur biedt de mogelijkheid om te komen tot een afgewogen en werkbaar geheel. Uitgangspunt voor die regeling zal echter zijn dat de gegevens door de behoeftestellende diensten beschikbaar worden gesteld.

Voor wat betreft de gegevens die worden opgevraagd door de inlichtingen- en veiligheidsdiensten, geldt dat de informatie over de toepassing van deze bevoegdheden door de diensten staatsgeheim is. Over de toepassing van de bevoegdheden kan vertrouwelijk verantwoording worden afgelegd aan de commissie voor de inlichtingen- en veiligheidsdiensten van de Tweede Kamer. Statistische informatie met betrekking tot de verstrekking van gegevens aan deze diensten – indien voorhanden – zal dan ook nimmer beschikbaar kunnen komen voor de Commissie.

3. De toegang tot de bewaarde gegevens

3.1 De verstrekking van bewaarde gegevens aan bevoegde autoriteiten in Nederland

De richtlijn dataretentie bepaalt dat de lidstaten bepalingen aannemen om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde autoriteiten worden verstrekt (artikel 4). De richtlijn laat het recht van de lidstaten onverlet om wetgevingsmaatregelen vast te stellen betreffende het recht van toegang tot en het gebruik van gegevens door nationale instanties die zij hebben aangewezen. Dit valt niet onder de reikwijdte van de

communautaire wetgeving (Overweging no. 25). De Nederlandse wetgeving kent reeds de waarborgen dat verkeersgegevens, die worden verwerkt door de aanbieders, alleen in welbepaalde gevallen en onder wettelijk vastgelegde voorwaarden kunnen worden verstrekt aan de bevoegde autoriteiten. Het wetsvoorstel bevat hierover dan ook geen bepalingen. Wel wordt in deze paragraaf een overzicht gegeven van de huidige wetgeving op dit punt.

De beschikbaarstelling van gegevens door de aanbieders van openbare telecommunicatienetwerken en –diensten ten behoeve van de opsporing en vervolging van strafbare feiten wordt beheerst door de regels van het Wetboek van Strafvordering. Op grond van die regels kan de officier van justitie, in geval van een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker (artikel 126n en 126u Sv). Dit betreft het vorderen van verkeersgegevens. Gelet op de wettelijke eisen is de toegang tot verkeersgegevens voor politie en justitie beperkt tot gevallen waarin sprake is van ernstige misdrijven.
Daarnaast geldt dat de opsporingsambtenaar, ingeval van een verdenking van een misdrijf of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek gegevens kan vorderen die bijdragen aan het identificeren van een persoon. Het gaat om de gegevens betreffende de naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie. Dit betreft het vorderen van gebruikersgegevens, en betreft een veel beperktere categorie gegevens dan die welke op grond van de bevoegdheid tot het vorderen van verkeersgegevens kunnen worden verkregen. De toepassing van deze bevoegdheid is daarom niet beperkt tot de gevallen waarin sprake is van ernstige vormen van criminaliteit.

Mede naar aanleiding van het advies van het CBP kan volledigheidshalve nog melding worden gemaakt van de algemene bevoegdheden tot het vorderen van gegevens die met de Wet vorderen gegevens (Stb. 390) in het Wetboek van Strafvordering zijn opgenomen. Deze bevoegdheden zijn niet van belang voor de gegevens waarop de bewaarplicht ziet omdat voor de vordering van die gegevens de specifieke bevoegdheden tot het vorderen van telecommunicatiegegevens dienen te worden toegepast. Gegevens die op grond van deze specifieke bevoegdheden gevorderd kunnen worden, kunnen niet door toepassing van de algemene bevoegdheden worden gevorderd. Dit is vastgelegd in de artikelen 126ng en 126ug van de Telecommunicatiewet.

De Wet tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot het opsporen en vervolgen van terroristische misdrijven van 20 november 2006 (Stb. 580) voorziet in verruiming van de bevoegdheden in verband met de bestrijding van terrorisme. Het betreft de bevoegdheid van de officier van justitie tot het vorderen van identificerende gegevens ten behoeve van een verkennend onderzoek naar terroristische misdrijven alsmede de bevoegdheid om ten behoeve van een dergelijk onderzoek gegevensbestanden van publieke en particuliere instanties te vorderen teneinde de hierin opgenomen gegevens te doen bewerken (artikel 126hh Sv). De officier van justitie kan gegevensbestanden slechts vorderen na machtiging door de rechter-commissaris. De gegevensbestanden kunnen worden doorzocht op bepaalde profielen en patronen van handelingen van personen die in het kader van de bestrijding van terrorisme van belang zijn. Dit betreft algemene bevoegdheden, waarvan verkeersgegevens niet zijn uitgezonderd. Deze bevoegdheden kunnen daarom ook worden aangewend jegens aanbieders van telecommunicatiediensten of -netwerken. Tot slot worden in deze wet bevoegdheden geregeld tot het vorderen van gegevens betreffende telecommunicatieverkeer. In geval van aanwijzingen van een terroristische misdrijf kan

de officier van justitie in het belang van het onderzoek een vordering doen tot verstrekking van verkeersgegevens (artikel 126zh Sv). In geval van aanwijzingen van een terroristisch misdrijf kan de opsporingsambtenaar in het belang van het onderzoek gebruikersgegevens vorderen (artikel 126zi Sv). In de memorie van toelichting bij het wetsvoorstel zijn de bevoegdheden toegelicht (Kamerstukken II, 2004-2005, 30164).

In zijn advies naar aanleiding van het wetsvoorstel heeft het CBP aangegeven de toepassing van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering op de gegevens die onder de bewaarplicht vallen, in strijd te achten met artikel 4 van de richtlijn. Daarbij wijst het CBP op de uitspraak van het Duitse Bundesverfassungsgericht van 4 april 2006, waarin het Hof volgens het CBP concludeert dat preventieve 'Rasterfahndung', zonder dat er daadwerkelijk aanwijzingen zijn voor een dreigend gevaar, een ontoelaatbare inbreuk met zich meebrengt voor de persoonlijke levenssfeer, terwijl datamining nu eenmaal ongeschikt moet worden geacht voor het afwenden van een dergelijk gevaar, alleen al omdat die methode teveel tijd vergt. Zoals het CBP aangeeft beperkt de richtlijn dataretentie de verstrekking van de bewaarde gegevens aan de bevoegde nationale autoriteiten tot welbepaalde gevallen en in overeenstemming met de nationale wetgeving (artikel 4). 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, en voldoet daarmee aan de eis van de richtlijn. Een verkennend onderzoek kan alleen worden ingesteld in geval van aanwijzingen dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Toepassing van de bevoegdheid van artikel 126hh Sv is alleen mogelijk indien het daarbij gaat om terroristische misdrijven. De door het CBP aangehaalde uitspraak van het Duitse Bundesverfassungsgericht zal vooraleerst in de context van de nationale Duitse wetgeving geplaatst moeten worden en is in elk geval niet van betekenis voor de uitleg van artikel 4 van de richtlijn. Daar komt nog bij dat de toepassing van de bevoegdheid van artikel 126hh Sv in het kader van het verkennend onderzoek is gebonden aan nauwe voorwaarden en is omgeven met strikte waarborgen voor een zorgvuldige omgang met persoonsgegevens. De officier van justitie dient af te wegen of het belang van dit onderzoek vordert dat gegevensbestanden gevorderd worden voor een bewerking van gegevens. Deze belangenafweging wordt door de rechter-commissaris getoetst. De officier van justitie stelt de wijze waarop de bewerking plaatsvindt vast; hij dient er tevens op toe te zien dat van de bewerking een proces-verbaal wordt opgemaakt. De bewerking dient plaats te vinden op een wijze die de bescherming van de persoonlijke levenssfeer van personen zo veel mogelijk waarborgt. Uitsluitend van de resultaten van de bewerking kan kennis worden genomen. Tenslotte geldt voor het verkennend onderzoek een toetsingsprocedure, die is opgenomen in de Aanwijzing opsporingsbevoegdheden van het College van procureurs-generaal.

Uit het voorgaande vloeit voort dat de te bewaren gegevens slechts in afzonderlijke gevallen, indien aan de wettelijke eisen wordt voldaan, beschikbaar kunnen komen voor politie en justitie. De gegevens zijn niet breed toegankelijk voor de opsporing.

De bewaarde gegevens kunnen eveneens van belang zijn voor de uitvoering van de wettelijke taken door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze taken zijn neergelegd in artikel 6, tweede lid, respectievelijk artikel 7, tweede lid, van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Stb. 2002, 148). De diensten zijn bevoegd zich te wenden tot de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten met het verzoek gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker (artikel 28 Wiv 2002). Daarnaast zijn de diensten bevoegd zich te wenden tot de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten met het verzoek gegevens te verstrekken

terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie (artikel 29 Wiv 2002). De uitoefening van deze bijzondere bevoegdheden is slechts geoorloofd indien dat noodzakelijk is voor een goede uitoefening van de taken, bedoeld in artikel 6, tweede lid, onder a en d, en de taken, bedoeld in artikel 7, tweede lid, onder a, c en e van de Wiv 2002. Bij de uitoefening van deze bijzondere bevoegdheden dient voorts te worden voldaan aan eisen van proportionaliteit. Zo is een verzoek aan de aanbieders, tot verstrekking van gegevens, slechts geoorloofd indien de gegevens niet of niet tijdig kunnen worden verkregen door raadpleging van voor ieder toegankelijke informatiebronnen of van informatiebronnen ten aanzien waarvan aan de dienst een recht op kennisneming is verleend (artikel 31 Wiv 2002). Van de uitoefening van deze bevoegdheden wordt een schriftelijk verslag gemaakt (artikel 33 Wiv 2002). Op de taakuitvoering door de diensten wordt toezicht uitgeoefend. In paragraaf 5 (rechtsbescherming) van deze memorie van toelichting wordt hier nader op in gegaan.

Tot slot zij vermeld dat het voorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar terroristische en andere gevaren met betrekking tot de nationale veiligheid (Kamerstukken II, 30 553) voorstellen bevat, voor zover hier van belang, voor de bevoegdheid van de diensten om zich te wenden tot een aanbieder van communicatiediensten met het verzoek tot verstrekking van een gegevensbestand of delen van een geautomatiseerd gegevensbestand (artikel 29b). De aanbieder is verplicht gevolg te geven aan een verzoek op grond van artikel 29b. Een dergelijk verzoek is echter uitsluitend mogelijk indien – voorzover het de AIVD betreft – de minister van Binnenlandse Zaken en Koninkrijksrelaties dan wel – voorzover het de MIVD betreft – de minister van Defensie daarvoor zelf toestemming heeft gegeven. De verkregen gegevens kunnen door de diensten worden gebruikt voor data-analyse, waaronder begrepen het samenbrengen of met elkaar in verband brengen van gegevens, onder meer door middel van het doorzoeken van gegevens aan de hand van profielen of het vergelijken van gegevens met het oog op de vaststelling van patronen. Ook hiervoor geldt dat daarvan schriftelijk verslag wordt gedaan en dat op de taakuitvoering door de diensten toezicht wordt uitgeoefend.

In de Telecommunicatiewet zijn, als spiegelbepalingen van de bevoegdheden die zijn neergelegd in het Wetboek van Strafvordering en de Wet op de Inlichtingen- en Veiligheidsdiensten, verplichtingen neergelegd voor de aanbieders om te voldoen aan een vordering of verzoek van de op grond van deze wetten bevoegde autoriteiten tot verstrekking van gegevens. In artikel 13.2a van de Telecommunicatiewet is de verplichting opgenomen te voldoen aan een vordering dan wel een verzoek tot verstrekking van verkeersgegevens. In artikel 13.2b van de Telecommunicatiewet is de verplichting opgenomen te voldoen aan een vordering dan wel een verzoek tot verstrekking van gegevens, op grond van de artikelen 126nc tot en met 126nh en 126uc tot en met 126uh van het Wetboek van Strafvordering (bevoegdheden vorderen gegevens). In artikel 13.4 van de Telecommunicatiewet is de verplichting opgenomen te voldoen aan een vordering dan wel een verzoek tot verstrekking van gebruikersgegevens. Ook zonder deze spiegelbepalingen zou de verplichting tot het voldoen aan strafvorderlijke bevoegdheden bestaan, maar de spiegelbepalingen bevorderen dat daarover geen misverstand kan bestaan.

In dit wetsvoorstel wordt voorgesteld om de verplichtingen van de aanbieders om te voldoen aan een vordering dan wel een verzoek tot verstrekking van verkeersgegevens, inclusief gebruikersgegevens, in één artikel van de Telecommunicatiewet samen te brengen. Dit komt de overzichtelijkheid ten goede (artikel 13.4 Tw). Tevens wordt voorgesteld om de verplichtingen van de aanbieders om te voldoen aan een vordering tot verstrekking van andere gegevens waarover de aanbieders beschikken, op grond van het Wetboek van Strafvordering, in één bepaling van de Telecommunicatiewet samen te brengen (artikel 13.2b Tw). Aanvullend wordt, naar aanleiding van het advies van het College bescherming persoonsgegevens, voorgesteld om een spiegelbepaling op te

nemen in verband met de bevoegdheden tot het vorderen van identificerende gegevens en het opvragen van gegevensbestanden, op grond van de artikelen 126hh en 126 ii van het Wetboek van Strafvordering.

Gelet op het voorgaande kan worden geconcludeerd dat de Nederlandse wetgeving voorziet in adequate procedures en waarborgen voor de toegang tot de bewaarde gegevens door de bevoegde nationale autoriteiten.

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

De richtlijn dataretentie bevat geen bepalingen over de beschikbaarstelling van de bewaarde gegevens aan de daartoe bevoegde autoriteiten in het buitenland. De vordering tot verstrekking van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker (artikel 126n en 126u Sv) en de vordering tot verstrekking van gebruikersgegevens (artikel 126na en 126ua Sv) kunnen worden uitgeoefend voorzover een voor inwilliging vatbaar rechtshulpverzoek daartoe strekt (artikel 552oa, tweede lid, Sv). Het verzoek wordt, zo het niet tot een officier van justitie is gericht, door de geadresseerde onverwijld doorgezonden aan de officier van justitie in het arrondissement waarin de gevraagde handelingen moeten worden verricht (artikel 552i, eerste lid Sv). De officier van justitie beslist onverwijld over het daaraan te geven gevolg. In gevallen waarin het verzoek niet op een verdrag is gegrond wordt aan het verzoek voldaan, tenzij de inwilliging in strijd is met een wettelijk voorschrift (artikel 552k, tweede lid, Sv). Hieruit vloeit voort dat de officier van justitie toetst of is voldaan aan de voorwaarden die naar Nederlands recht gelden voor de toepassing van de gevraagde opsporingsbevoegdheid. De voorwaarden, die op grond van het Wetboek van Strafvordering van toepassing zijn op de toegang tot de bewaarde gegevens, zijn eveneens van toepassing op de toegang tot de gegevens ten behoeve van de verstrekking aan het buitenland. Deze voorwaarden zijn aan de orde gekomen in paragraaf 3.1.

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

Bij de voorbereiding van dit wetsvoorstel is van de zijde van de aanbieders gewezen op de mogelijkheid dat de aanbieder, die voldoet aan de verplichtingen van de artikelen 13.2a, tweede of derde lid, en 13.4 van dit wetsvoorstel, door de abonnee of gebruiker van de door hen aangeboden diensten zou kunnen worden aangesproken op grond van wanprestatie of onrechtmatige daad. Dit zou aan de orde kunnen zijn in het geval waarin de belanghebbende van mening zou zijn dat er geen aanleiding bestaat tot bewaring van de gegevens over het telecommunicatieverkeer waar hij bij betrokken is geweest, dan wel tot beschikbaarstelling van die gegevens aan de bevoegde autoriteiten op grond van artikel 13.4 van de Telecommunicatiewet.
Dat de aanbieders dan civielrechtelijk aansprakelijk zouden zijn is echter niet waarschijnlijk. In een dergelijk geval zal een aanbieder, die in rechte zou worden aangesproken wegens wanprestatie, zich immers met succes kunnen beroepen op het feit dat hij aan een wettelijke plicht heeft voldaan. De verplichtingen op grond van de Telecommunicatiewet prevaleren boven eventuele contractuele verplichtingen, bijvoorbeeld geheimhoudingsverplichtingen, zodat de aanbieder niet aansprakelijk is voor eventuele schade die het gevolg is van de bewaring of de beschikbaarstelling van de gegevens. Wordt de aanbieder aangesproken op grond van onrechtmatige daad dan geldt de wettelijke verplichting als een rechtvaardigingsgrond in de zin van artikel 162, tweede lid, van boek 6 van het Burgerlijk Wetboek, zodat hij ook dan niet aansprakelijk is voor eventuele schade.

Verder geldt dat van gevallen waarin, evenals de wijze waarop, door de bevoegde autoriteiten gebruik wordt gemaakt van de aan hen in het Wetboek van Strafvordering toegekende bevoegdheden op het gebied van het vorderen van telecommunicatiegegevens, verantwoording wordt afgelegd aan de rechter. Het is aan de rechter om – indien dit aan de orde komt - in een concrete strafzaak de rechtmatigheid van de inzet van een bijzondere

opsporingsbevoegdheid, zoals het gebruik van de bevoegdheden van de artikelen 126n/u of 126na/nu van het Wetboek van Strafvordering, te toetsen. Tevens kan een belanghebbende beklag indienen op grond van artikel 552a van het Wetboek van Strafvordering.

Ook kan de belanghebbende, die bezwaar heeft tegen het feit dat op hem betrekking hebbende gegevens door de aanbieder worden bewaard, daartegen opkomen op grond van de Wet bescherming persoonsgegevens. Hij kan het recht op kennisneming van de over hem verwerkte gegevens geldend maken en zich desgewenst tot de rechtbank wenden. Soortgelijke rechten komen aan de belanghebbende toe ingeval de bewaarde gegevens verder worden verwerkt door de autoriteiten die zijn belast met de opsporing en vervolging van strafbare feiten. Tenslotte wordt door het College bescherming persoonsgegevens toezicht uitgeoefend op de gegevensverwerking door de diensten die zijn belast bij de opsporing en vervolging van strafbare feiten. Dit is hierna toegelicht. Voor de inlichtingen- en veiligheidsdiensten is de Commissie van Toezicht betreffende de inlichtingen- en veiligheidsdiensten daarmee belast.

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

De richtlijn dataretentie strekt tot de bewaring van bepaalde categorieën van telecommunicatiegegevens ten behoeve van het onderzoeken, opsporen of vervolgen van ernstige misdrijven. Dit betreft verkeers- en locatiegegevens alsook de hiermee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Aan de hand van dergelijke gegevens kan inzicht worden verkregen in de gedragingen van personen. Dit kan betrekking hebben op bijvoorbeeld de telecommunicatiediensten die door een bepaalde persoon worden gebruikt, de aansluitnummers waarmee verbinding is geweest en de duur van die verbinding. Deze gegevens raken aan de persoonlijke levenssfeer. Daarom is bij de voorgestelde bewaarplicht van telecommunicatiegegevens het recht op bescherming van de persoonlijke levenssfeer aan de orde. De voorgestelde bewaarplicht brengt met zich mee dat gegevens, die door de aanbieders worden verwerkt ten behoeve van het verrichten van diensten in verband met telecommunicatie, worden bewaard ook indien ze voor dat doel niet meer nodig zijn. Hiermee wordt een inbreuk gemaakt op het beginsel van doelbinding, dat inhoudt dat persoonsgegevens uitsluitend worden verwerkt met het oog op het doel waarvoor ze zijn verkregen en worden verwijderd of vernietigd zodra het doel van de verwerking is vervuld. Dit wetsvoorstel voorziet in een wettelijke grondslag voor de bewaring van de gegevens ten behoeve van de opsporing en vervolging van strafbare feiten.

De bewaarplicht houdt daarnaast in dat de bewaarde gegevens ter beschikking kunnen komen van de bevoegde autoriteiten ten behoeve van de opsporing en vervolging van strafbare feiten. Dit is echter een reeds bestaande situatie. Ook thans kunnen telecommunicatiegegevens die beschikbaar zijn bij de aanbieders, ter beschikking komen van de opsporing. De afweging van het belang van de opsporing tegen het belang van de bescherming van de persoonlijke levenssfeer die hierbij aan de orde is, heeft reeds plaatsgevonden bij de totstandkoming van de bestaande bevoegdheden voor het gebruik van verkeersgegevens voor de opsporing, zoals deze zijn omschreven in paragraaf 3 van deze memorie van toelichting. De bewaarplicht brengt daarin geen verandering. Wel wordt de kans dat de voor de opsporing benodigde gegevens aanwezig zijn, door de bewaarplicht vergroot. Ook om die reden wordt in deze paragraaf in gegaan op de verhouding van de bewaarplicht tot het grondrecht op bescherming van de persoonlijke levenssfeer.

Het grondrecht op bescherming van de persoonlijke levenssfeer vindt zowel in het internationale als in het nationale recht bescherming. Artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950[1] kent een ieder het recht toe op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Dit betreft het recht op eerbiediging van de persoonlijke levenssfeer. Geen inmenging van enig openbaar gezag in de uitoefening van dit recht is toegestaan dan voor zover bij wet (law) is voorzien en in een democratische samenleving noodzakelijk is in het belang van, onder meer, de nationale veiligheid, de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten. Onder het doelcriterium 'het voorkomen van strafbare feiten' is, zo blijkt uit de rechtspraak van het Europese Hof tot bescherming van de rechten van de mens (EHRM), de strafvorderlijke afwikkeling van strafbare feiten, waaronder de opsporing daarvan, begrepen. Uit de jurisprudentie van het Europese Hof vloeit voort dat de inmenging door enig openbaar gezag in de privacyrechten moet voldoen aan vereisten inzake noodzakelijkheid en evenredigheid, en derhalve specifieke, expliciete en legitieme doeleinden moet dienen en moet plaatsvinden op adequate en relevante wijze, en niet buitensporig mag zijn in verhouding tot het doel van de inmenging. Het 'noodzaakcriterium' wordt in de rechtspraak van het Europese Hof in Straatsburg nader ingevuld aan de hand van de beginselen van proportionaliteit, subsidiariteit en van een 'pressing social need' (er moet een dringende maatschappelijke behoefte bestaan om het legitieme doel te vervullen). Artikel 10, eerste lid, van de Grondwet bepaalt dat ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Beperking van dit recht dient een basis te hebben in een wet in formele zin.

De voorgestelde wettelijke regeling van de bewaarplicht voldoet aan de eisen van artikel 8 EVRM en artikel 10 van de Grondwet. De eis dat de inmenging 'bij de wet is voorzien' houdt in dat in het nationale recht is voorzien in een wettelijke regeling van de maatregel en dat die regeling voor de burger voldoende kenbaar en voorzienbaar is. De verplichting tot het bewaren van de gegevens wordt neergelegd in de Telecommunicatiewet. Ook de inhoud van die verplichting wordt voor een belangrijk deel bij wet in formele zin geregeld. De bewaartermijn en de lijst van de te bewaren gegevens worden in de Telecommunicatiewet beschreven. Het begrip 'law' vereist niet dat er sprake is van een uitputtende regeling in een wet in formele zin; ook regulering in lagere regelgeving is toereikend. De eis van de voorzienbaarheid brengt met zich mee dat de regeling voldoende precies moet zijn geformuleerd, zodat de burger vooraf kan weten onder welke voorwaarden de gegevens worden bewaard. De regeling moet bovendien waarborgen bieden tegen willekeurige inmenging van de overheid in het persoonlijk leven van de burger en tegen misbruik van bevoegdheid (Kruslin en Huvig, EHRM 24 april 1990, NJ 1991, nr. 523). De voorgestelde regeling voldoet aan de eisen van voorzienbaarheid en van waarborgen tegen willekeur en misbruik. De verplichting tot het bewaren van bepaalde categorieën van gegevens, de bewaartermijnen en de lijst van de te bewaren gegevens worden in de wet vastgelegd zodat de reikwijdte van de maatregel helder is.

Bij de eis dat de inmenging in het privacyrecht noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid. De eis van noodzakelijkheid houdt in dat bezien moet worden of de voorgestelde maatregel nodig is voor de strafrechtelijke handhaving van de rechtsorde. Daarbij gaat het om een toetsing aan de eisen van proportionaliteit en subsidiariteit.
De voorgestelde bewaarplicht heeft tot doel bij te dragen aan de voorkoming, opsporing en vervolging van strafbare feiten, waaronder terrorisme. Verkeersgegevens zijn van groot belang voor het opsporingsonderzoek naar ernstige vormen van criminaliteit. Om die reden is de te implementeren EU-richtlijn tot stand gekomen. Deze gegevens kunnen een belangrijke rol vervullen in zowel de opbouw en richting van een opsporingsonderzoek als de bewijsvoering jegens verdachten. Daarbij kunnen de gegevens niet alleen van belang zijn voor de

[1] Trb. 1951, 154, laatstelijk gewijzigd 11 mei 1994, Trb. 1994, 165

beantwoording van vragen naar de betrokkenheid van personen bij strafbaar feiten maar ook voor de uitsluiting van die betrokkenheid. Zoals gemeld in paragraaf 2.3 (De bewaartermijn) heeft de Erasmus Universiteit een onderzoek verricht naar de behoefte aan de bewaring van verkeersgegevens bij de opsporingsinstanties. De onderzoekers van de Erasmus Universiteit komen tot de conclusie dat het aanbeveling verdient een eenduidige bewaarplicht te scheppen voor verkeersgegevens met betrekking tot telefonie- en internetverkeer. Een bewaarplicht voor verkeersgegevens verschaft niet alleen duidelijkheid aan de opsporingsinstanties over de vraag welke gegevens aan de aanbieders kunnen worden gevraagd maar biedt tevens een wettelijke grondslag om de aanbieders op de verstrekking van die gegevens aan te spreken. Daarnaast biedt een bewaarplicht helderheid voor de aanbieders inzake de reikwijdte van de verplichtingen jegens politie en justitie. Tenslotte zijn regels over bewaartermijnen van belang om de daadwerkelijke beschikbaarheid van de gegevens voor de opsporingsinstanties te verzekeren. Dit kan leiden tot meer afgewogen vorderingen. Deze bevindingen bevestigen hetgeen aan de richtlijn dataretentie ten grondslag ligt, namelijk dat de bewaarplicht nodig is voor de strafrechtelijke handhaving van de rechtsorde. De richtlijn laat dan ook geen ruimte om al dan niet te kiezen voor een bewaarplicht, wel laat de richtlijn de ruimte te kiezen voor een bepaalde bewaartermijn tussen de minimale termijn van zes maanden en de maximale termijn van twee jaar. Juist daarbij is de toetsing aan de eisen van proportionaliteit en subsidiariteit van belang. Hierboven (paragraaf 2.3) is reeds aangegeven waarom het aanbeveling verdient om te kiezen voor een bewaartermijn van achttien maanden zodat zeker is dat, gelet op de behoefte van de politie voor de aanpak van langlopende, complexere opsporingsonderzoeken op regionaal en nationaal niveau, de afhandeling van rechtshulpverzoeken en de aanpak van cold cases, de gegevens voor de opsporing beschikbaar zijn. Deze bewaarperiode past goed in de door de richtlijn geboden 'bandbreedte' voor de vaststelling van de bewaartermijn. Voor de afweging is het verder van belang dat de inbreuk op de bescherming van de persoonlijke levenssfeer van de burger zoveel mogelijk wordt beperkt. De gegevens worden niet langer opgeslagen dan noodzakelijk voor het doel van de bewaring. In het licht van de betrokken belangen is de voorgestelde termijn dan ook niet als disproportioneel aan te merken. Ook in paragraaf 2.3 is op de proportionaliteit van de bewaartermijn ingegaan.
Voor de beoordeling van de eisen van proportionaliteit en subsidiariteit is ook de omvang van de bewaarplicht van belang. In het eerdergenoemde rapport van de Erasmus Universiteit wordt een standaardset van telefonie- en internetgegevens geïdentificeerd die door de aanbieders bewaard zouden moeten worden. De door de Erasmus Universiteit opgestelde 'standaardset' van de te bewaren gegevens vertoont grote gelijkenis met de op grond van de richtlijn dataretentie en dit wetsvoorstel te bewaren lijst van gegevens.

Tenslotte bevat de wettelijke regeling, in aanvulling op de Telecommunicatiewet en de Wet bescherming persoonsgegevens, de nodige waarborgen tegen misbruik of onzorgvuldig gebruik van de bewaarde gegevens. Deze waarborgen hebben betrekking op de gegevensbescherming en de gegevensveiligheid. De aanbieders zijn verplicht passende technische en organisatorische maatregelen te nemen zodat gewaarborgd wordt dat de bewaarde gegevens zijn beveiligd tegen onjuist gebruik of toegang door onbevoegde personen en dat de gegevens worden vernietigd na afloop van de bewaartermijn. Daarnaast geldt de verplichting om de bewaarde gegevens onverwijld te vernietigen aan het einde van de bewaartermijn. Deze waarborgen kunnen bij algemene maatregel van bestuur verder worden uitgewerkt.

5. Rechtsbescherming

Hierboven is reeds aangegeven (paragraaf 2.5) dat de Wet bescherming persoonsgegevens van toepassing is op de gegevensverwerking door de aanbieders in het kader van het aanbieden van openbare elektronische

communicatienetwerken en openbare elektronische communicatiediensten. Dit geldt eveneens voor de gegevens die naar aanleiding van de voorgestelde bewaarplicht door de aanbieders worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De WBP biedt de nodige mogelijkheden voor de betrokkene om op de hoogte te raken van het feit dat gegevens over hem worden bewaard en desgewenst tegen een dergelijke gegevensverwerking op te komen. In de eerste plaats geldt voor de aanbieder een informatieplicht, dat wil in dit geval zeggen dat de aanbieder gehouden is om de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging van de hem betreffende gegevens heeft geleid (artikel 34, vijfde lid, WBP). In de tweede plaats heeft de betrokkene het recht op kennisneming, dat wil zeggen dat hij zich tot de aanbieder kan wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt (artikel 35 WBP). Dit recht is onverkort van toepassing op gegevens die ingevolgde dit wetsvoorstel door de aanbieders worden bewaard. Indien zodanige gegevens daadwerkelijk worden bewaard, dan moet de mededeling van de aanbieder daaromtrent een volledig overzicht van de bewaarde gegevens in begrijpelijke vorm bevatten naast andere informatie, zoals een omschrijving van het doel of de doeleinden van de bewaring, de categorieën van gegevens waarop de bewaring betrekking heeft, de ontvangers of categorieën van ontvangers en de herkomst van de gegevens. Weliswaar biedt de WBP de aanbieder de mogelijkheid om artikel 35 buiten toepassing te laten voorzover dit noodzakelijk is in het belang van - onder meer - de veiligheid van de staat of de voorkoming en opsporing van strafbare feiten, maar een redelijke wetstoepassing strekt ertoe dat aangenomen moet worden dat een dergelijk belang nog niet aan de orde is zolang de gegevens bij de aanbieder worden bewaard en er geen sprake is van overdracht van de gegevens aan politie of justitie ten behoeve van het daadwerkelijke gebruik in een concreet opsporingsonderzoek of een strafzaak. In de derde plaats heeft de betrokkene het recht op correctie van de bewaarde gegevens; hij kan de aanbieder verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien de gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de bewaring onvolledig of niet terzake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt (artikel 36 WBP).

In het advies naar aanleiding van het wetsvoorstel hebben de aanbieders aangegeven dat een redelijke uitleg van de verplichting van artikel 35 WBP zou moeten zijn dat de aanbieder kan volstaan met de verstrekking aan de klant van een overzicht van de soorten gegevens die door de aanbieder op grond van de bewaarplicht worden opgeslagen en niet een gedetailleerd overzicht hoeft te verstrekken. Een dergelijke uitleg is echter niet goed verenigbaar met de achtergrond en de inhoud van deze bepaling en zou er in feite op neer komen dat de aanbieder aan de betrokkene die informatie verstrekt waarvan deze reeds wetenschap heeft op grond van kennisneming van de voorgestelde wettelijke regeling. Dit laat onverlet dat de betekenis van het inzagerecht voor de burger in de praktijk van minder groot belang zal zijn omdat relevante gegevens over zijn belgedrag doorgaans reeds zijn af te leiden uit de gespecificeerde factuur, die de aanbieder desgevraagd gehouden is te leveren. Het aantal verzoeken om kennisneming zal waarschijnlijk dan ook beperkt zijn. Daar komt bij dat, zoals hierboven reeds is aangegeven, de aanbieder niet onverkort gehouden is aan een verzoek tot kennisneming te voldoen. Een weigering om inzage te verlenen kan geschieden op grond van de redenen, genoemd in artikel 43 WBP. Van belang daarbij zijn niet alleen de belangen van de opsporing van strafbare feiten en de staatsveiligheid maar eveneens de bescherming van de rechten en vrijheden van anderen dan de betrokkene, als genoemd in onderdeel e van voornoemd artikel. Het CBP wijst er in zijn advies naar aanleiding van het wetsvoorstel op dat de abonnee van een aansluiting via het inzagerecht inzicht zou kunnen verkrijgen in het communicatiegedrag of de locatiegegevens van alle gebruikers over een langere periode, daarbij valt te denken aan werknemers of gezinsleden. Dit gaat echter voorbij aan het feit dat de betrokkene door middel van een gespecificeerde factuur doorgaans op de hoogte zal kunnen zijn van dergelijk communicatiegedrag. Niettemin kan het, ter bescherming van de belangen van derden, voor de aanbieder aangewezen zijn om inzage in de gevraagde gegevens te

weigeren. Voorts kan een verzoek om inzage in de bewaarde gegevens worden geweigerd als de lasten daarvan niet opwegen tegen het belang van betrokkenen. Indien een verzoek om inzage bijvoorbeeld disproportionele administratieve lasten met zich mee zou brengen kan de aanbieder dit verzoek weigeren ter bescherming van het belang van een goede bedrijfsvoering. Het enkele feit dat een verzoek om inzage administratieve lasten met zich meebrengt is echter op zichzelf niet voldoende grond om het verzoek te weigeren. Bij de afweging of de aanbieder deze plichten niet kan nakomen dient hij het belang van de betrokkene uitdrukkelijk mee te wegen. Gelet op het feit dat de betrokkene doorgaans door middel van een gespecificeerde factuur op de hoogte is van de verwerking van de betreffende gegevens door de aanbieder, zal dit voor de laatste reden kunnen vormen om inzage te weigeren indien dit voor hem een disproportionele administratieve belasting met zich mee zou brengen. Dit kan echter anders liggen indien de betrokkene door de politie op de hoogte is gesteld van de vordering van de op hem betrekking hebbende verkeersgegevens. Daarbij zullen echter ook de belangen van derden moeten worden meegewogen.

In geval de aanbieder zou weigeren om gevolg te geven aan een verzoek om kennisneming of correctie van gegevens, dan staat aan de betrokkene de mogelijkheid open om zich tot de rechtbank te wenden met het verzoek de verantwoordelijke te bevelen alsnog een dergelijk verzoek toe te wijzen (artikel 46, eerste lid, WBP). Daarnaast bestaat de mogelijkheid van schadevergoeding (artikel 49, derde lid, WBP). Ook kan de betrokkene zich tot het College bescherming persoonsgegevens wenden met het verzoek te bemiddelen of te adviseren in zijn geschil met de aanbieder (artikel 47, eerste lid, WBP).

Het toezicht op de bewaring van de persoonsgegevens door de aanbieders is in handen van de Minister van Economische Zaken en het College bescherming persoonsgegevens (CBP). Dit is in paragraaf 2.7 toegelicht. Voor een adequate handhaving van de naleving van het bepaalde in de artikelen 11.5, 11.5a en 11.13 van hoofdstuk 11 en de bepalingen van hoofdstuk 13 van de Telecommunicatiewet staat de Minister van Economische Zaken een uitgebreid instrumentarium ter beschikking. Hieronder vallen de bevoegdheid tot het toepassen van bestuursdwang (artikel 15.2 Tw) en het opleggen van een bestuurlijke boete (artikel 15.4 Tw). Het College bescherming persoonsgegevens beschikt over verschillende bevoegdheden tot handhaving van de bij of krachtens de WBP gestelde verplichtingen, waaronder de bevoegdheid tot het betreden van een woning zonder toestemming van de bewoner (artikel 61, tweede lid, WBP) en de toepassing van bestuursdwang ter handhaving van de bij of krachtens de WBP gestelde verplichtingen (artikel 66 WBP).

De verwerking van de te bewaren gegevens door de aanbieders zelf dient te worden onderscheiden van de verdere verwerking van de bewaarde gegevens door de instanties, die wettelijk bevoegd zijn om een vordering of een verzoek tot het verstrekken van die gegevens te richten aan de aanbieders. Ingeval de bewaarde gegevens aan die instanties worden verstrekt dan zijn andere wettelijke regimes van toepassing op de verdere verwerking van de gegevens. De Wet politieregisters geeft regels voor de gegevensverwerking door de politie (en de Koninklijke marechaussee) met het oog op de uitvoering van de politietaak. Deze regels hebben onder meer betrekking op de noodzakelijkheid, rechtmatigheid en veiligheid van de gegevensverwerking, de doelbinding, de toegang tot de gegevens, de verstrekking van politiegegevens aan derden en de verwerkingstermijnen. De Wet politieregisters kent aan de belanghebbende het recht toe op kennisneming en verbetering van de gegevens die in een politieregister zijn opgenomen, met het oog op de uitvoering van de politietaak. Wel geldt dat een verzoek om kennisneming kan worden geweigerd voor zover dit noodzakelijk is voor een goede uitvoering van de politietaak dan wel indien gewichtige belangen van derden daartoe noodzaken (artikel 21, eerste lid, Wpolr). Het College bescherming persoonsgegevens oefent toezicht uit op de naleving van het bij of krachtens de wet bepaalde. Het wetsvoorstel politiegegevens, dat thans bij de Eerste Kamer der Staten-Generaal aanhangig is

(Kamerstukken II, 2005-2006, 30327, nr. 2) en dat naar verwachting begin 2008 in werking zal treden, kent een soortgelijke regeling als de Wet politieregisters.
Indien de bewaarde gegevens worden verwerkt door of ten behoeve van de Algemene Inlichtingen- en Veiligheidsdienst als bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002, is de Wet bescherming persoonsgegevens niet van toepassing. In artikel 2 van de Wet bescherming persoonsgegevens zijn dergelijke verwerkingen namelijk van de toepassing van die wet uitgezonderd. Dat heeft een aantal consequenties. Zo zijn bijvoorbeeld de in de WBP toegekende rechten voor de betrokkene – zoals bijvoorbeeld neergelegd in artikel 35 – niet van toepassing, hetgeen onder meer inhoudt dat de aanbieder nimmer mededeling mag doen van het feit of hij gegevens heeft verstrekt aan de AIVD of MIVD en welke gegevens het betreft; zou hij dit wel doen dan overtreedt hij de in artikel 85 van de Wiv 2002 neergelegde geheimhoudingsplicht. Daarnaast is met betrekking tot verwerkingen als hier bedoeld niet het College bescherming persoonsgegevens het competente toezichtorgaan, maar de in de Wiv 2002 geregelde onafhankelijke commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten. Voor de door de diensten verwerkte gegevens, derhalve ook de gegevens die van de aanbieders zijn verkregen, biedt de Wiv 2002 een uitputtende regeling. In de hoofdstukken 3 en 4 van deze wet worden regels gegeven voor de verwerking van gegevens door de diensten en het recht op kennisneming van door of ten behoeve van de diensten verwerkte gegevens. De Wet op de inlichtingen- en veiligheidsdiensten 2002 kent een ieder het recht toe op kennisneming van de hem betreffende persoonsgegevens die door of ten behoeve van een dienst zijn verwerkt (artikel 47 Wiv 2002). Wel kan de kennisneming worden geweigerd, onder meer indien de gegevensverwerking minder dan vijf jaar geleden heeft plaatsgevonden (artikel 53, eerste lid, Wiv 2002). Het recht op kennisneming geldt ook voor andere gegevens dan persoonsgegevens (artikel 51 Wiv 2002). Op een verzoek daartoe zijn afzonderlijke weigeringsgronden van toepassing (artikel 55 Wiv 2002). De Wet op de inlichtingen- en veiligheidsdiensten 2002 voorziet in een wettelijke regeling van het toezicht op de taakuitvoering door de diensten. Er is een onafhankelijke commissie van toezicht die beschikt over uitgebreide wettelijke bevoegdheden ten behoeve van een goede taakuitvoering, zoals het oproepen van getuigen en het betreden van plaatsen zonder toestemming van de rechthebbende, met uitzondering van de woning (artikelen 64, eerste lid, 74, eerste lid en 77 Wiv 2002). De commissie van toezicht oefent tevens het toezicht uit op de gegevensverwerking door de diensten. De commissie brengt ieder een jaar een openbaar verslag uit van zijn werkzaamheden (artikel 80, eerste lid, Wiv 2002). Tenslotte kan een ieder bij de Nationale ombudsman een klacht indienen over het optreden of vermeende optreden van de diensten jegens een natuurlijke of rechtspersoon (artikel 83, eerste lid, Wiv 2002). De Nationale ombudsman deelt zijn oordeel over de klacht mede aan de betrokken Minister, die de ombudsman binnen zes weken op de hoogte stelt van de gevolgen die hij aan het oordeel verbindt. Ook de commissie van toezicht wordt hiervan in kennis gesteld (artikel 84, eerste, derde en vierde lid, Wiv 2002).

Indien de bewaarde gegevens door het openbaar ministerie in een strafzaak worden gebruikt dan is de Wet justitiële en strafvorderlijke gegevens (WJSG) van toepassing op de gegevensverwerking. Ook deze wet kent de nodige waarborgen op het gebied van de rechtsbescherming, waaronder het recht van de betrokkene op kennisneming en verbetering van de hem betreffende strafvorderlijke gegevens (artikel 39i, eerste lid, en 39m, eerste lid, WJSG). Het College bescherming persoonsgegevens is belast met het toezicht (artikel 27, eerste lid, WJSG).

6. De situatie in de andere EU-lidstaten

In paragraaf 6.1. zal een kort overzicht worden gegeven van de wijze waarop in andere EU-lidstaten tot nu toe uitvoering is gegeven aan de richtlijn dataretentie. Dit betreft tot nu toe alleen Duitsland, Frankrijk en Denemarken. De andere lidstaten hebben ofwel wetgeving in voorbereiding naar aanleiding van de richtlijn dataretentie, ofwel hebben op nationaal niveau reeds regels over de bewaarplicht voor telecommunicatiegegevens. Van die laatstgenoemde lidstaten is thans nog niet bekend in hoeverre de richtlijn aanleiding zal geven tot aanpassing van die regels. Van die lidstaten wordt in paragraaf 6.2. kort de thans bestaande situatie geschetst, in afwachting van eventuele nadere maatregelen ter implementatie van de richtlijn dataretentie.

6.1. De lidstaten die inmiddels wettelijke regels hebben opgesteld ter implementatie van de richtlijn dataretentie

In Duitsland is een wetsvoorstel aanhangig dat voorziet in een nieuwe regeling in het Duitse wetboek van Strafvordering ('Strafprozesordnung') voor het aftappen van telecommunicatie en de inzet van andere heimelijke opsporingsmethoden. De implementatie van de richtlijn dataretentie is deels meegenomen in dit wetsvoorstel. Daarnaast wordt de Duitse Telecommunicatiewet ('Telekommunikationsgesetz') gewijzigd. De aanbieders zijn verplicht om de in de richtlijn aangewezen telecommunicatiegegevens te bewaren. Daarbij wordt onderscheid gemaakt tussen verkeersgegevens (artikel 110a, eerste lid, TKG) en abonnee- of gebruikersgegevens (artikel 111, eerste lid, TKG). De te bewaren gegevens zijn in de Duitse Telecommunicatiewet opgesomd, daarbij wordt onderscheid gemaakt tussen diensten op het gebied van telefonie (inclusief mobiele en internettelefonie), e-mail en toegang tot het internet (artikel 110a, tweede, derde en vierde lid, TKG). De bewaartermijn bedraagt zes maanden. De aanbieders zijn verplicht de bewaarde gegevens onverwijld ter beschikking te stellen aan de bevoegde autoriteiten ten behoeve van de vervolging van strafbare feiten (artikel 110b, eerste lid, TKG). De vraag in hoeverre de gegevens voor andere doelen – bijvoorbeeld het voorkomen van gevaar of de veiligheidsdiensten – moet nog worden besproken (voetnoot 1 bij artikel 110b TKG). De toegang tot de bewaarde gegevens is geregeld in het Duitse wetboek van Strafvordering. Ingeval van verdenking dat een persoon een strafbaar feit van aanzienlijke betekenis ('erheblicher bedeutung') heeft gepleegd, heeft gepoogd te begaan of heeft voorbereid door middel van een strafbaar feit of ingeval een persoon een strafbaar feit door middel van telecommunicatie heeft gepleegd kunnen verkeersgegevens worden gevorderd. In dit laatste geval geldt een extra subsidiariteiseis.
Het wetsvoorstel voorziet niet in schadeloossstelling van de aanbieders. Opgemerkt wordt dat de investeringskosten minder omvangrijk zullen zijn dan aanvankelijk, tijdens de onderhandelingen over de richtlijn, te vrezen was. Daarbij wordt er op gewezen dat de concrete investeringsbehoefte niet eenvoudig vast te stellen zal zijn, mede vanwege de dynamiek op de telecommunicatiemarkt. Te verwachten is dat de betreffende ondernemingen de kosten in hun prijsstelling zullen incalculeren en dit aan hun klanten zullen doorberekenen. Voor een grote Duitse telecomaanbieder, met een omzet van 60 miljard euro, zou de bewaarplicht op jaarbasis ongeveer 700.00 euro aan extra kosten met zich mee kunnen brengen, oftewel 0.00116% van de jaaromzet. In afzonderlijke gevallen kan aan de aanbieders een vergoeding worden verstrekt op grond van de zogenaamde Justitievergoedings- en schadeloosstellingswet (JVEG). Thans geldt een vergoeding van 17 euro per uur voor de verstrekking van verkeersgegevens, waarbij er van wordt uitgegaan dat ieder verzoek om verstrekking een uur verwerkingstijd met zich meebrengt. Deze regeling wordt thans herzien, een ontwerp daarvoor zal binnenkort aan het Duitse parlement worden voorgelegd.

In Frankrijk is op 24 maart 2006 een nieuw artikel toegevoegd aan de Code des postes et des communications électroniques. Op grond van dit artikel kunnen de daartoe aangewezen opsporingsambtenaren van de politie en gendarmerie gegevens van aanbieders vragen ten behoeve van de voorkoming van terroristische daden. Met het

decreet van 24 maart 2006 zijn de aanbieders verplicht om bepaalde categorieën van gegevens rond elektronische communicatie te bewaren ten behoeve van het opsporen, ontdekken en vervolgen van strafbare feiten. De bewaartermijn bedraagt één jaar. Het decreet voorziet niet in de vergoeding aan de aanbieders van de gemaakte kosten met betrekking tot de levering van deze gegevens. Dit is vastgesteld in een Besluit van de minister van Economie, Financiën en Industrie en de minister van Justitie, van 22 augustus 2006. Dit besluit is van toepassing op de aanbieders van telefonie, met de aanbieders van internetdiensten wordt nog overleg gevoerd. In dit besluit zal onderscheid worden gemaakt tussen tarieven die van toepassing zijn voor verschillende categorieën van gegevens.

Denemarken heeft een uitvoeringsregeling ('Executive Order') opgesteld over de bewaring van verkeersgegevens door de aanbieders van elektronische communicatienetwerken of -diensten. De uitvoeringsregeling is gebaseerd op de Wet op de rechtsbedeling ('Administration of Justice Act') en zal op 15 september 2007 in werking treden. Op basis van deze regeling zijn de aanbieders van elektronische communicatienetwerken of -diensten verplicht een lijst van verkeersgegevens te bewaren, op zodanige wijze dat deze gegevens kunnen worden gebruikt ten behoeve van onderzoek naar en vervolging van strafbare feiten. De te bewaren gegevens zijn in de artikelen 4 en 5 van de uitvoeringsregeling opgesomd; daarbij wordt onderscheid gemaakt tussen diensten op het gebied van telefonie, toegang tot het internet en e-mail. De bewaartermijn bedraagt één jaar. De Deense wet biedt de aanbieders de mogelijkheid om de bewaring en opslag van de gegevens te laten uitvoeren door een andere aanbieder of een derde partij (artikel 8). De door de aanbieders te maken kosten om aan de bewaarplicht te voldoen, worden niet vergoed. Wel kunnen de aanbieders aanspraak maken op een vergoeding wanneer door de bevoegde autoriteiten wordt gevraagd om verstrekking van de bewaarde gegevens.

6.2. De lidstaten die reeds regelgeving hebben maar waarvan nog niet bekend is in hoeverre uitvoering van de richtlijn dataretentie tot aanpassing daarvan zal leiden.

In de Engelse Code of practice, behorend bij de Regulation of Investigatory Powers Act 2000, wordt aangegeven welke personen en instanties onder welke voorwaarden communicatiegegevens moeten kunnen verkrijgen. De Code kent verschillende bewaartermijnen voor verschillende categorieën van gegevens. Abonnee- en telefoniegegevens moeten voor een periode van twaalf maanden worden bewaard, voor SMS-, EMS-, email-en bepaalde internet gegevens geldt een bewaartermijn van zes maanden. Daarnaast worden, anders dan in de richtlijn dataretentie, voorzien in een verplichting tot bewaring van gegevens over websurfgedrag (vier dagen). Op grond van artikel 106 van de Anti-terrorisme, misdaad en veiligheidswet 2001 ('Anti-terrorism, Crime and Security Act') en artikel 24 van de Regeling voor onderzoeksbevoegdheden 2000 ('Regulation of Investigatory owers Act) geldt een verplichting voor de regering om te voorzien in een passende vergoeding ('appropriate contributions').

In Ierland is in de Criminal Justice (Terrorist Offences) Act 2005 een bepaling (artikel 63) opgenomen dat de bevoegde autoriteit, de zogenaamde Garda Commissioner, een aanbieder kan verzoeken om verkeers- en locatiegegevens met betrekking tot telefonie te bewaren voor een periode van drie jaar, ten behoeve van de veiligheid van de staat of de voorkoming, het onderzoek of vervolgen van strafbare feiten. Tevens is een regeling opgenomen (artikel 64) omtrent de autoriteiten die bevoegd zijn tot toegang tot de bewaarde gegevens en de daarbij geldende voorwaarden.

Italië kent sinds 2003 een bewaarplicht voor telefoniedata van vierentwintig maanden, met een verlengingsmogelijkheid van vierentwintig maanden en voor internetdata een bewaarplicht van zes maanden, met

een verlengingsmogelijkheid van zes maanden. In juli 2005 is het besluit genomen om alle verkeersgegevens, inclusief internetdata, te bewaren tot 31 december 2007. Italië heeft op dit moment een wetsvoorstel in voorbereiding dat voorziet in de verplichting automatisch opgeslagen gegevens te vernietigen. In dit wetsvoorstel wordt het principe gehanteerd dat automatisch verzamelde gegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel waarvoor ze zijn opgeslagen.

7. Bedrijfseffecten

De berekeningen van de lasten voor het bedrijfsleven zijn gebaseerd op de bevindingen uit het onderzoek door VKA. De kostenberekeningen op basis van de rapportage van VKA dienen gezien te worden als aanduidingen in 'orde van grootte'. Volgens de methode voor het berekenen van de nalevingskosten zouden de kosten, die de aanbieders thans al maken voor het bewaren van gegevens voor eigen bedrijfsdoeleinden, van de door VKA gepresenteerde kosten dienen te worden afgetrokken. Over de hoogte van deze kosten is door de aanbieders echter geen informatie verschaft. Voor de berekeningen is dan ook uit gegaan van een zogenaamde 'green field' situatie, dat wil zeggen dat de te bewaren gegevens door de aanbieders thans niet ten behoeve van de eigen bedrijfsdoeleinden worden opgeslagen. De werkelijke meerkosten zullen daarom lager uitvallen.

Het wetsvoorstel is van toepassing op ongeveer driehonderd aanbieders van openbare telecommunicatiediensten en –netwerken. De kosten die deze bedrijven zullen maken om aan de verplichting tot het bewaren en beschikbaar stellen van de specifieke gegevens te kunnen voldoen verschillen sterk naar gelang de wijze waarop hun bedrijfsvoering is ingericht. In het algemeen zullen de kosten voor deze bedrijven gerelateerd zijn aan:

- de opslag van de gegevens;
- de investeringen die benodigd zijn om de gegevens te ontsluiten;
- de kosten van het beheer van de systemen, en;
- het beschikbaar maken en stellen van de gegevens ten behoeve van de behoeftestellers.

Voor de hoogte van de kosten is met name van belang of op onderdelen in het bewaar- en bevragingsproces automatisering zal worden toegepast. In de voorgestelde optie van decentrale opslag en beantwoording door de aanbieder bestaat voor elke aanbieder de mogelijkheid om op basis van bedrijfsmatige overwegingen al dan niet te kiezen voor automatisering. Uit het door VKA gehouden veldonderzoek bij de aanbieders is naar voren gekomen dat in het algemeen de verwachting is dat een aanbieder die meer dan twee vragen om verkeersgegevens per dag krijgt van de behoeftestellers zeer waarschijnlijk het proces van bevraging op de één of andere manier gaat automatiseren. In het rapport van VKA is daarom uitgegaan van automatisering van de bevraging. Desgevraagd heeft VKA alsnog opgave gedaan van de situatie waarbij er geen of minder sprake is van automatisering van de bevraging. In dat geval nemen weliswaar de investeringskosten aanzienlijk af, tot circa 25%, doch als gevolg van arbeidsintensiviteit nemen de personele kosten met ongeveer een factor 3 toe. De totale kosten voor het bedrijfsleven zouden daarmee substantieel hoger uitkomen dan in geval van automatisering. Voor de rekenkundige modellering van de kosten voor de aanbieders op nationaal niveau is een vertaling gemaakt van de markt waarbij een indeling is gemaakt van grote aanbieders met een gemiddeld aantal accounts van 5 miljoen, middelgrote aanbieders met een gemiddeld aantal accounts van 0,5 miljoen en kleine aanbieders met een gemiddeld aantal accounts van duizend. Voor de automatisering van bewaren en bevragen wordt rekening gehouden met de grote en middelgrote aanbieders. De verwachting is dat voor kleine aanbieders de automatisering veel minder interessant zal zijn. Voor deze categorie van aanbieders zullen de kosten voor de

aanschaf van zoekmachines immers mogelijk niet opwegen tegen de kosten van handmatige bevraging. Het rekenmodel is op een totaal van 280 aanbieders geëxtrapoleerd naar kosten op jaarbasis.

Bij de voorgestelde decentrale opslag, en bij een bewaartermijn van 18 maanden, bedragen de investeringskosten voor het bedrijfsleven € 82 mln. Op termijn zullen vervangingsinvesteringen in hard- en software moeten worden gedaan. VKA heeft bij de berekeningen een inschatting gemaakt van de kosten voor de eerste vijf jaar. Indien we eenzelfde afschrijvingstermijn hanteren bedragen de jaarlijkse kosten van investeringen ongeveer € 16 mln. De operationele kosten bedragen aanvankelijk € 12 mln per jaar, maar zullen door een verwachte toename in het bevragingsvolume uiteindelijk uitkomen op 20 miljoen Euro per jaar.

Het onderzoek van VKA geeft ook informatie over de verdeling naar grote en kleine bedrijven in relatie tot de draagkracht. In de berekeningen van VKA is uitgegaan van 5 grote aanbieders (gemiddeld 5.000.000 accounts), 20 middelgrote aanbieders (gemiddeld 500.000 accounts) en 255 kleine aanbieders, met een gemiddeld aantal accounts van 1000. Het kostenaandeel van deze kleine aanbieders bedraagt circa 2% van de totale kosten. Voor de kleine aanbieders betekent dit ongeveer € 1,6 mln aan investeringen. Verdeeld over het totaal van kleine aanbieders betekent dit een financiële last van € 6.500 aan investeringen per kleine aanbieder.
Door VKA is aangegeven dat waarschijnlijk is dat voor de groep van kleine aanbieders investeringen van meer dan € 10.000,-- een probleem vormen. De hiervoor aangegeven financiële last voor de kleine aanbieders van 6500 euro per aanbieder blijft onder die grens. Aangetekend zij dat het hier om gemiddelden gaat. Het valt niet uit te sluiten dat individuele bedrijven een zwaardere last zullen ondervinden indien zij overgaan tot automatisering. Omdat het volume aan bevragingen bij deze categorie van kleine aanbieders aanzienlijk lager zal liggen dan bij de grote en middelgrote aanbieders zal een deel van de kleine aanbieders in de praktijk kiezen voor handmatige bevraging van de gegevens. Voor de grote en middelgrote bedrijven, waarvan de groten een miljardenomzet kennen, zullen de kosten relatief minder zwaar drukken.

Met de gegevens van VKA kan ook berekend worden wat de verschillen in kosten zijn van verschillende bewaartermijnen. De kosten die direct door de bewaartermijn worden beïnvloed hangen samen met de opslag van de gegevens, dus de benodigde disks, en de daarmee samenhangende besturingslogica. Iedere verlenging van de bewaartermijn met zes maanden betekent dat de investeringskosten naar verwachting stijgen met 7 miljoen euro en de operationele kosten met ongeveer € 100.000.-. Bij de voorgestelde bewaartermijn van achttien maanden zijn de investeringskosten € 14 mln. hoger dan bij de minimumvariant van 6 maanden. De operationele kosten vallen € 200.000 per jaar hoger uit.

In het totaal van de kostenberekeningen zitten vervat de kosten die gemoeid zijn met het bewaren van locatiegegevens. Deze gegevens worden bewaard ten behoeve van het kunnen verrichten van de zogenaamde bestandsanalyse zoals beschreven in paragraaf 2.4. Het bewaren van de locatiegegevens volgt niet rechtstreeks uit de richtlijn. De verplichting tot het bewaren van deze gegevens bestaat reeds en is neergelegd in artikel 13.4 tweede lid van de Telecommunicatiewet. De noodzaak tot het verrichten van een bestandsanalyse doet zich voor wanneer de identificerende gegevens over een gebruiker van telecommunicatie bij de aanbieder niet zijn geregistreerd, bijvoorbeeld bij prepaid telefonie. Het betreft hier overigens geen andere gegevens dan die welke bewaard worden bij elke vorm van mobiele telefonie. De kosten voor het langer bewaren van de locatiegegevens van drie, volgens de huidige verplichting, naar achttien maanden zitten vervat in de totale investeringen en operationele kosten. Het precieze aandeel van het bewaren van locatiegegevens in het geheel van de gegevens voor telefonie en internet en e-mail is niet bekend. Op basis van berekeningen van VKA naar de benodigde opslagcapaciteit is wel indicatief de verhouding aan te geven tussen de benodigde opslagcapaciteit voor het

geheel van de gegevens en die van mobiele telefonie waarvan onder andere prepaid telefonie deel uitmaakt. Volgens VKA komt de totale omvang van de benodigde database voor de opslag van verkeersgegevens uit op 365 terabyte. Het aandeel van de mobiele telefonie daarin is 5 terabyte. Gesteld dat prepaid telefonie een aandeel heeft van 40% van de totale mobiele telefonie (bron KPN), dan bedraagt het aandeel voor het bewaren van locatiegegevens ongeveer 0,5% van de totale opslagcapaciteit voor de gehele sector. De meerkosten bij de investeringen komen daarbij op € 400.000, en bij de operationele kosten op € 100.000. Deze kosten worden gedragen door een beperkt aantal grote aanbieders in de mobiele telefonie.

Opgemerkt moet worden dat in de berekening van VKA vanwege de beperkte beschikbaarheid van gegevens geen rekening kon worden gehouden met het feit dat thans NAW- en verkeersgegevens ook worden bewaard, namelijk voor bedrijfsdoeleinden. Ook thans worden deze gegevens bevraagd door opsporingsinstanties. Tevens is in de berekeningen geen rekening gehouden met de financiële vergoeding die op grond van de in artikel 13.6 van de Telecommunicatiewet bedoelde ministeriële regeling aan de aanbieder wordt verstrekt in geval van het op vordering van de bevoegde autoriteit verstrekken van gegevens. De werkelijke investeringen en operationele kosten zullen derhalve naar alle waarschijnlijkheid lager uitvallen dan in de 'green field' berekeningen van VKA.

De investerings-, exploitatie- en onderhoudskosten voor technische voorzieningen die door de aanbieders worden gemaakt teneinde te kunnen voldoen aan de verplichtingen van hoofdstuk 13 van de Telecommunicatiewet moeten als nalevingskosten worden aangemerkt en niet als administratieve lasten. De informatie betreft hier namelijk geen gedragingen van de bedrijven zelf ten aanzien van een maatschappelijk relevante norm, zoals de definitie van administratieve lasten stelt. Dit geldt ook voor de investerings-, exploitatie- en onderhoudskosten die de aanbieders maken om te kunnen voldoen aan de verplichting tot het bewaren en beschikbaar hebben van gegevens als bedoeld in het wetsvoorstel. Hiervoor geldt hetzelfde uitgangspunt als voor het beschikbaar maken en stellen van de gebruikersgegevens als bedoeld in het Besluit verstrekking gegevens telecommunicatie, als gewijzigd bij Besluit van 13 september 2006[2]. De gemaakte kosten moeten gezien worden als overige nalevingskosten.

Op de bewaartermijnen die worden gehanteerd in andere landen wordt ingegaan in paragraaf 6. Daaruit blijkt dat de situatie, voorzover bekend, zeer divers is en wordt ingegeven door aspecten die specifiek zijn voor het betreffende land. Voor Nederland is de gekozen bewaartermijn voornamelijk gerelateerd aan de periode in de rechtsgang waarbinnen verkeersgegevens een belangrijke rol kunnen spelen in het richting geven aan het opsporingsonderzoek en de bewijsvoering ter zitting. Zie hiervoor ook paragraaf 2.3.

[2] Hierbij gaat de regering uit van de volgende definitie van administratieve lasten:
'Administratieve lasten zijn de kosten voor het bedrijfsleven om te voldoen aan informatieverplichtingen voortvloeiend uit wet- en regelgeving van de overheid'.
In deze definitie is sprake van informatieverplichtingen, welk begrip als volgt kan worden omschreven:
'Een informatieverplichting is een verplichting tot het informeren over handelingen en gedragingen ten aanzien van een maatschappelijk waardevol geachte norm'.
Essentieel is de verplichting dat op enig moment de gegevens beschikbaar moeten zijn en dus opgeleverd kunnen worden. Het moet hierbij gaan om handelingen en gedragingen van het bedrijf. In het voorliggende wetsvoorstel gaat het om de verplichting tot het (langer) bewaren van (verkeers)gegevens en het desgevraagd beschikbaar stellen van deze gegevens aan de overheid ten behoeve van de opsporing. Het betreft hier niet gegevens die gerelateerd zijn aan handelingen of gedragingen van het bedrijf, of aan een maatschappelijk waardevol geachte norm. De door het bedrijf te verlenen informatie betreft gegevens over het gebruik dat zijn klanten maken van de diensten van het bedrijf.

Het toezicht op de juiste naleving van de bewaarplicht wordt in lagere regelgeving uitgewerkt. Het is daarom nu slechts mogelijk om zeer indicatief aan te geven wat de toezichtslasten zullen zijn. Naar verwachting zal een aanbieder die zich aan de wet houdt ongeveer eens in de drie jaar een bezoek krijgen van AT van waarschijnlijk ongeveer een halve dag. Ervan uitgaande dat het bedrijf 1 persoon zal inzetten om AT te woord te staan komt dit bij 300 aanbieders neer op 50 mandagen per jaar, oftwel ongeveer een kwart fte. Uitgaande van € 100.000 per fte zouden de jaarlijkse toezichtslasten ongeveer € 25.000, oftewel € 250 per bezocht bedrijf. Indien een bedrijf in gebreke blijft kunnen de toezichtskosten uiteraard hoger uitvallen.

De richtlijn dataretentie bevat geen specifieke regels over de kosten die voortvloeien uit de verplichtingen van de richtlijn en die samenhangen met het bewaren van de gegevens door de aanbieders.

De Telecommunicatiewet kent een regeling voor de vergoeding van de kosten die door de aanbieders worden gemaakt bij het voldoen aan verzoeken van politie en justitie en de inlichtingen- en veiligheidsdiensten[3]. Op grond van artikel 13.6, eerste lid, van de Telecommunicatiewet moeten de aanbieders zelf de investeringskosten dragen die nodig zijn om te kunnen voldoen aan de verplichtingen die voortvloeien uit hoofdstuk 13 evenals de kosten van exploitatie en onderhoud. De personeelskosten en administratiekosten die rechtstreeks voortvloeien uit het voldoen aan een bevoegd gegeven last, worden vergoed uit 's Rijks kas (artikel 13.6, tweede lid, Tw).

Aangezien voorgesteld wordt om het toezicht aan de Minister van Economische Zaken op te dragen zullen de kosten hiervan ook binnen de begroting van de Minister van Economische Zaken worden opgevangen. Zodra op basis van nadere regels meer duidelijkheid bestaat over de vraag welke aspecten voor het toezicht op de naleving van belang zijn, zal een inschatting gemaakt kunnen worden van de hiermee gemoeide kosten. Vooralsnog wordt uitgegaan van twee fte aan extra toezicht.

8. De adviezen over het wetsvoorstel

Het openbaar ministerie, de politie - verenigd in het Nederlands Politie Instituut (NPI) - het College bescherming persoonsgegevens (CBP), de OPTA en de Nederlandse Orde van Advocaten (NOvA) zijn om advies gevraagd over het wetsvoorstel. Het wetsvoorstel is tevens voorgelegd aan het Adviescollege toetsing administratieve lasten (Actal). Daarnaast is het wetsvoorstel gepubliceerd op de website van het Ministerie van Economische Zaken en is een ieder gedurende een termijn van vier weken in de gelegenheid gesteld een reactie in te brengen.

Naar aanleiding van de publieke consultatie op de website hebben een aantal partijen gereageerd. De aanbieders van openbare telecommunicatienetwerken en –diensten hebben een gezamenlijke reactie opgesteld, deze is ondertekend door CAIW Holding B.V., Essent Labelcom B.V., KPN B.V., Multikabel B.V., Orange Nederland N.V., partijen verenigd in ACT (bbned N.V., BT Nederland N.V., COLT Telecom B.V., Orange Nederland Breedband B.V., Priority Telecom Netherlands B.V., Verizon Nederland B.V., Versatel Nederland B.V.), T-Mobile Netherlands B.V., Stichting NBIP, UPC Nederland N.V., Vodafone Libertel N.V., XS4ALL Internet B.V. en Zeelandnet B.V. De Associatie van Actieve Telecomoperators (ACT), waarvan de leden hierboven zijn

[3] Artikel 13.6, tweede lid: Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hebben aanspraak op vergoeding uit 's Rijks kas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een bijzondere last als bedoeld in artikel 13.2, eerste en tweede lid, onderscheidenlijk het verstrekken van informatie als bedoeld in artikel 13.4.

vermeld, heeft aanvullend tevens een eigen schriftelijke reactie ingezonden. Tenslotte heeft de brancheverenigingen van de IT-, Telecom- en Office en Internetbedrijven in Nederland (ICT~Office) een schriftelijke reactie ingezonden.

De gezamenlijke aanbieders hebben hun bezorgdheid uitgesproken over het wetsvoorstel, in het bijzonder ten aanzien van de reikwijdte van de toekomstige verplichtingen van de aanbieders, de verdeling van de met het wetsvoorstel samenhangende lasten en de verhouding tussen het wetsvoorstel en de Wet bescherming persoonsgegevens (WBP). De ACT meent dat een aantal essentiële onderwerpen in het wetsvoorstel niet zijn geregeld, dat de financiële consequenties en de administratieve lasten van het wetsvoorstel een zware en onaanvaardbare last op de telecomsector leggen, dat de duur van de bewaartermijn onvoldoende is onderbouwd en dat de conclusies van het onderzoek, dat de basis vormt voor de gekozen implementatieoptie, door de aanbieders niet worden gedragen. De Nederlandse politie wijst op het belang van een uniforme bewaartermijn voor de maximalisering van het rendement van de te bewaren gegevens en is verheugd dat er nu een wetsvoorstel ligt. Het College van procureurs-generaal heeft met belangstelling kennis genomen van het wetsvoorstel en maakt een aantal opmerkingen. De in de adviezen aan de orde gestelde punten komen hieronder nader aan de orde.

De bewaartermijn

Het CBP, het Actal, de aanbieders, ICT~office en de NOvA plaatsen kritische kanttekeningen bij de voorgestelde bewaartermijn van achttien maanden. Door het openbaar ministerie en de politie wordt de voorgestelde bewaartermijn als mimimaal ervaren. Zowel het CBP, de aanbieders als ICT~Office spreken van een onverwachte verlenging van de verwachte bewaartermijn van twaalf naar achttien maanden. Het CBP acht de onderbouwing van de noodzaak van een bewaartermijn van achttien maanden in de memorie van toelichting niet voldoende. Het CBP meent dat een zelfstandige toetsing van de nationale bewaartermijn aan de vereisten van artikel 8 EVRM leidt tot een geharmoniseerde minimale toepassing van de bepalingen van de richtlijn met een bewaartermijn die zo min mogelijk afwijkt van het oorspronkelijke doel waarvoor de gegevens door de aanbieders worden opgeslagen. Naar het oordeel van het CBP biedt het onderzoek van de Erasmus Universiteit onvoldoende bewijs van de noodzaak van een langere bewaartermijn dan gehanteerd in de huidige praktijk, waarin aanbieders verkeersgegevens voor hun eigen bedrijfsvoering bewaren. Ook met de door de Erasmus Universiteit aanbevolen bewaartermijn van één jaar is nog niet voldaan aan het noodzakelijkheidscriterium van artikel 8 EVRM. Mede gelet op de in andere lidstaten gekozen bewaartermijnen meent het CBP dat Nederland zou moeten volstaan met de minimaal verplichte bewaartermijn van zes maanden. Het Actal, de aanbieders en de NOvA plaatsen kanttekeningen bij de door de onderzoekers van de Erasmus Universiteit aanbevolen termijn van twaalf maanden en geven de voorkeur aan een bewaartermijn niet langer dan zes maanden. Het College van procureurs-generaal wijst er op dat het onderzoek van de Erasmus Universiteit zich voornamelijk richtte op het opsporingsonderzoek. Ook tijdens het onderzoek ter terechtzitting kan het noodzakelijk zijn te beschikken over de bewaarde gegevens. Mede gelet op de mogelijkheid dat de rechter in hoger beroep nader onderzoek kan gelasten is de voorgestelde bewaartermijn naar het oordeel van het college niets te lang. De Raad van Hoofdcommissarissen wijst er op dat de richtlijn ruimte biedt voor een bewaartermijn van vierentwintig maanden. Vooral in het kader van onderzoeken naar terrorisme en zware georganiseerde criminaliteit is een termijn van vijf jaar nodig. Voor de zogenoemde ‘cold cases’ is een termijn van vijf jaar zelfs nog te gering. Vanuit het oogpunt van een veiliger samenleving en een succesvolle opsporing adviseert de politie een bewaartermijn van tenminste vierentwintig maanden vast te stellen.

Deze adviezen geven geen aanleiding tot aanpassing van de in het wetsvoorstel opgenomen bewaartermijn. Wel is paragraaf 2.3 aangevuld met een nadere onderbouwing van de gekozen bewaartermijn. Daarbij is nader ingegaan op de in de adviezen aangedragen argumenten.

De te bewaren gegevens
De aanbieders, de ACT, het CBP en ICT~Office stellen vast dat de lijst van de te bewaren gegevens wordt geregeld bij algemene maatregel van bestuur en bepleiten om de te bewaren gegevens in de wet vast te leggen. Het CBP wijst daarvoor op het voorbeeld van het Duitse wetsvoorstel (paragraaf 6:1). De politie wijst er op dat de overige gegevens rond internet en internettoegang, zoals websurfgedrag, bedrijfse-mail, e-maildiensten als Hotmail en hostingdiensten niet onder de reikwijdte van de richtlijn vallen. Betreurd wordt dat voor de totstandkoming van dit wetsvoorstel geen nader onderzoek is gedaan naar het bewaren van verkeersgegevens betreffende inkomende en uitgaande IP-paketten.

Naar aanleiding van deze adviezen is tegemoet gekomen aan het bezwaar dat een aanzienlijk deel van de verplichtingen voor de aanbieders wordt vastgelegd in lagere regelgeving. Daartoe is de lijst van de te bewaren gegevens opgenomen in een bijlage, behorend bij de Telecommunicatiewet. Daarmee wordt, overeenkomstig de wens van de adviesorganen, bij wet in formele zin de nodige duidelijkheid geboden over de vraag welke gegevens onder de bewaarplicht vallen. Tevens wordt hiermee de helderheid en overzichtelijkheid van de Telecommunicatiewet gehandhaafd. De bewaring van andere gegevens met betrekking tot internetcommunicatie, zoals bepleit door de politie, valt buiten het kader van de richtlijn dataretentie en daarmee buiten dit wetsvoorstel, dat strekt tot implementatie van de richtlijn.

De verplichting tot bewaring van locatiegegevens
Het CBP, de aanbieders en het Actal zijn van mening dat met de verplichting tot bewaring van locatiegegevens tijdens de communicatie buiten de reikwijdte van de richtlijn wordt getreden. Het CBP wijst er op dat het Besluit bijzondere vergaring nummergegevens geen vergaarplicht omvat en geen verplichting schept voor de aanbieders om de locatiegegevens tijdens de communicatie voor een periode van drie maanden te bewaren. Ook de aanbieders menen dat locatiegegevens gedurende de communicatie op grond van het eerdergenoemde besluit niet bewaard hoeven te worden. Tevens geldt dat een aanbieder alleen die gegevens hoeft te bewaren die hij verwerkt. Het Actal stelt vast dat met name de kosten die zijn verbonden aan de verlenging van de bewaartermijn voor de opslag van de locatiegegevens bij mobiel telefoonverkeer – van drie tot achttien maanden - niet apart zijn gekwantificeerd en afgewogen tegen de baten van de uitbreiding, en adviseert hier alsnog zorg voor te dragen.

Naar aanleiding van deze adviezen kan worden opgemerkt dat de richtlijn dataretentie de lidstaten verplicht tot bewaring van bepaalde gegevens over de abonnee of de geregistreerde gebruiker. Dit betreffen namen en adressen. Deze gegevens zijn nodig om de identiteit van personen, die betrokken zijn bij telecommunicatieverkeer, te kunnen achterhalen. De identiteit van de gebruiker van prepaid cards wordt in Nederland echter, anders dan in sommige andere lidstaten van de Unie, niet geregistreerd. Destijds, bij de totstandkoming van het Besluit vergaring bijzondere nummergegevens, is afgezien van een wettelijke verplichting tot registratie van de identiteit van prepaid card-gebruikers en gekozen voor het door de aanbieders zelf voorgestelde systeem van een bestandsanalyse, door middel waarvan de identiteit van een gebruiker van telecommunicatie kan worden achterhaald. Dit systeem kan alleen goed functioneren indien alle locatiegegevens gedurende de communicatie worden bewaard. Daarnaast kunnen de locatiegegevens van groot belang zijn voor de opsporing en vervolging omdat aan de hand van deze gegevens inzicht kan worden verkregen in de geografische positie van mobiele telefoons. Om die reden wordt voorgesteld om deze locatiegegevens even lang

te doen bewaren als de gegevens die onder de richtlijn vallen. Zou dit achterwege blijven dan zou dit tot een leemte in de wetgeving leiden. In paragraaf 2.4 is hier nader op in gegaan.

Decentrale opslag van gegevens

In het wetsvoorstel is gekozen voor decentrale opslag van de te bewaren gegevens, dat wil zeggen dat de aanbieders zelf de te bewaren gegevens opslaan en dat deze de gegevens, naar aanleiding van een vordering van een bevoegde autoriteit, beschikbaar stellen. Het CBP geeft ervan blijk dit te steunen en adviseert een decentrale, logisch gescheiden opslag van de specifiek voor opsporingsdoeleinden te bewaren verkeersgegevens. Centrale opslag brengt risico's met zich mee, zoals thans nog niet voorzien nevengebruik. Decentrale opslag heeft het bijkomende voordeel dat de aanbieders extra controle uitvoeren op de uitvoerbaarheid van een bevel, aldus het CBP. Het Actal constateert daarentegen dat het alternatief van een centrale opslag van verkeersgegevens door een extern onderzoeksbureau is onderzocht en als gunstigste optie voor het bedrijfsleven wordt gepresenteerd en adviseert deze optie nader te onderzoeken. De aanbieders stellen vast dat de memorie van toelichting niet uitsluit dat in de toekomst alsnog voor een andere optie wordt gekozen waardoor de aanbieders geconfronteerd zouden worden met nieuwe investeringsverplichtingen. Het College van procureurs-generaal is een groot voorstander van een centrale opslag van gegevens, gelijk aan het systeem van het CIOT. Daarvoor wordt gewezen op de bevindingen van het VKA-rapport. Het College heeft begrip voor het feit dat op dit moment wordt gekozen voor een decentrale opslag van de gegevens maar dringt er tevens op aan dat tegelijkertijd de benodigde stappen worden gezet om te komen tot een centrale opslag van gegevens. Het CBP meent echter dat de keuze van een CIOT-achtige oplossing (de gegevens worden bewaard bij een derde partij, naar het model van het Centraal Informatiepunt Opsporing Telecommunicatie) een verdubbeling van een bepaalde set van gegevens impliceert, hetgeen in strijd is met de richtlijn dataretentie.

Naar aanleiding van deze adviezen moet worden opgemerkt dat het wetsvoorstel geen onduidelijkheid laat bestaan over het feit dat het de aanbieders zijn die de gegevens, die onder de voorgestelde bewaarplicht vallen, bewaren. Dit volgt uit de tekst van het voorgestelde artikel 13.2a, tweede lid, van dit wetsvoorstel. Het wetsvoorstel sluit anderzijds de mogelijkheid niet uit dat de aanbieders er, in overleg met de bevoegde autoriteiten, zelf voor zouden kiezen om de te bewaren gegevens bij een derde partij op te slaan die dan vervolgens als bewerker van die gegevens fungeert, onder verantwoordelijkheid van de aanbieders. De door het CBP aanbevolen decentrale, logisch gescheiden opslag van de specifiek voor opsporingsdoeleinden te bewaren gegevens, behoeft niet in de weg te staan aan een eventuele keuze door de aanbieders voor een dergelijke opslag van de gegevens bij een derde. Om niettemin tegemoet te komen aan de kennelijk bij het CBP en de aanbieders gevoelde vrees, dat bij algemene maatregel van bestuur aan de aanbieders wordt voorgeschreven te komen tot een dergelijke op een centrale plaats, is de betreffende delegatiebepaling herzien. De voorgestelde tekst van artikel 13.4, vierde lid, van de Telecommunicatiewet is aangepast zodat deze uitsluitend is toegesneden op de beschikbaarstelling van actuele gebruikersgegevens door tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie, zoals dat is voorzien in het huidige artikel 13.4, tweede lid, van de Telecommunicatiewet. Een voorschrift in de toekomst voor de opslag van de te bewaren gegevens bij een derde partij veronderstelt een uitwerking bij algemene maatregel van bestuur. Om in een deugdelijke rechtsgrondslag daarvoor te voorzien is dan een wijziging van de Telecommunicatiewet noodzakelijk, zodat het parlement volledig is betrokken.

De termijn voor de levering van de gegevens

Het CBP acht het van belang dat in de memorie van toelichting wordt vastgelegd dat de huidige afspraken een periode van één tot vijf werkdagen bestrijken, afhankelijk van de bewerkingen die de aanbieder moet verrichten

om de gevraagde gegevens te produceren. Een eventueel op te stellen algemene maatregel van bestuur zou een reflectie moeten zijn van de praktijk bij grote en kleine aanbieders, zonder een eventuele leversnelheid van één specifieke aanbieder dwingend aan alle aanbieders op te leggen. Het College van procureurs-generaal wijst op het belang van nadere invulling van het begrip 'onverwijld' en stelt voor in de memorie van toelichting op te nemen dat het begrip 'onverwijld' betekent dat in normale gevallen een responstermijn van twee dagen kan worden aangehouden. Het Actal adviseert de onduidelijkheid over de snelheid waarmee de data moeten worden opgeleverd op korte termijn te minimaliseren zodat de onzekerheid over de gevolgen van het wetsvoorstel afneemt. Dit dient bij voorkeur in de wetstekst te geschieden en anders in de memorie van toelichting. De ACT merkt op dat veel onduidelijkheid bestaat over de thans geldende afspraken tussen de aanbieders en de behoeftestellende diensten, waarnaar in de memorie van toelichting wordt verwezen, evenals de status daarvan.

Naar aanleiding van deze adviezen moet worden opgemerkt dat de mogelijkheid van een regeling bij algemene maatregel van bestuur niet zozeer is opgenomen om de bestaande termijnen aan te passen als wel om, door middel van vastlegging van de bestaande afspraken met de aanbieders in een algemene maatregel van bestuur, zeker te stellen dat de richtlijn dataretentie volledig wordt geïmplementeerd. Conform de suggestie van het CBP is hieromtrent in paragraaf 2.8 de nodige verheldering opgenomen.

De financiële consequenties en de administratieve lasten
Het heeft de aanbieders bevreemd dat de financiële consequenties van de bewaarplicht, zoals die zijn omschreven in het rapport van het bureau Verdonck, Kloosters en Associates (VKA) in de memorie van toelichting als uitgangspunt zijn genomen, omdat de aanbieders zich hebben gedistantieerd van de conclusies uit dit rapport. De aanbieders zijn van mening dat de verplichtingen van dit wetsvoorstel feitelijk los staan van de bedrijfsvoering van aanbieders en de kosten uitsluitend worden gemaakt ten behoeve van een door de wetgever bepaald belang. Nu wordt een substantieel deel van de opsporingsactiviteiten bij aanbieders belegd en dreigt dit ook voor hun rekening te komen. De vergoeding op basis van artikel 13.6 van de Telecommunicatiewet wordt door de aanbieders geenszins als redelijk of billijk beschouwd. Verwezen wordt naar de lopende procedure tegen de regeling en de uitvoering daarvan (KPN B.V. cs / De Staat der Nederlanden). Zij roepen op tot een constructieve evaluatie van de kostenregeling en een redelijke kostenverdeling en vergoeding van de door de aanbieders te verrichten diensten. De ACT voegt hier aan toe dat de keuze om de financiële consequenties en de administratieve lasten van het wetsvoorstel volledig voor rekening van de telecomsector te doen komen, evenals de onderbouwing van de hoogte van de kosten, onvoldoende wordt onderbouwd. Het Actal wijst er op dat niet is onderzocht in welke mate bedrijven bepaalde gegevens al bewaren voor eigen doeleinden en dat ook veel andere aspecten onduidelijk zijn, zoals de snelheid waarmee de data opgeleverd moeten worden, de mate van automatisering bij kleine bedrijven en de groei van het aantal bevragingen de komende jaren. Geadviseerd wordt deze onduidelijkheden op korte termijn te minimaliseren, zodat de onzekerheid over de gevolgen van het wetsvoorstel afneemt. Verder wordt geconstateerd dat er meer kosten voor de bedrijven kunnen zijn dan uit de memorie van toelichting blijkt (kennisname, opleiding, toezicht) en wordt geadviseerd hier ook aandacht aan te schenken in de memorie van toelichting. Voorts wordt geadviseerd de toekomstige vergoeding van de kosten voor bedrijven niet te beperken tot personeels- en administratiekosten, maar uit te breiden tot alle kosten. Tenslotte bevelen zowel de ACT als het Actal aan de investeringen in ICT niet als nalevingskosten maar als administratieve lasten te behandelen. De ICT~Office wijst er op dat de aanpak en bestrijding van criminaliteit een zaak van publiek belang is. Nu de investeringskosten op grond van artikel 13.6 voor rekening van de aanbieders komen vindt de financiering van het publiek belang plaats met private gelden. Deze situatie is ongewenst en heeft een negatief effect op de winstgevendheid en innovatiekracht van bedrijven.

Naar aanleiding van deze adviezen moet worden opgemerkt dat het alleszins verdedigbaar is dat de lasten voor het bereiken van een maatschappelijk breed gedragen doel als de criminaliteitsbestrijding deels bij het bedrijfsleven wordt gelegd. Naar aanleiding van het evaluatierapport 'Aftapbaarheid van telecommunicatie' heeft het kabinet aangegeven dat uitgangspunt van het beleid is dat de overheid in het algemeen belang verplichtingen kan opleggen aan bedrijven, waarbij deze bedrijven de kosten voor uitvoering van die verplichtingen dragen (Kamerstukken II, 2006-2007, 30517, nr. 2). De aan de bewaarplicht verbonden kosten zullen grotendeels worden doorberekend aan de klanten van de aanbieders. Vergoeding van de uit de bewaarplicht voortvloeiende lasten door de overheid zal in de praktijk niet eenvoudig te realiseren zijn. Nu de te bewaren gegevens deels reeds ten behoeve van zakelijke doeleinden door de aanbieders worden bewaard, bestaat geen goed beeld van de werkelijke lasten die de bewaarplicht met zich meebrengt. Van hun kant hebben de aanbieders tot nu toe weinig bereidheid getoond om daarin inzicht te bieden. Overigens sluit de Nederlandse systematiek voor de vergoeding van de kosten van de aanbieders, waarbij de aanbieders worden gecompenseerd op basis van de vordering van bewaarde gegevens door de behoeftestellers, aan op die van andere EU-lidstaten. Op de financiële consequenties en de administratieve lasten is in paragraaf 7 nader in gegaan.

De toegang tot de bewaarde gegevens

Het CBP meent dat de memorie van toelichting ten onrechte concludeert dat de Nederlandse wetgeving in adequate procedures en waarborgen voorziet voor de toegang tot de bewaarde gegevens door de bevoegde autoriteiten. Het college mist een duidelijke beperking in de doeleinden waarvoor de te bewaren gegevens beschikbaar kunnen komen van de opsporingsinstanties en veiligheidsdiensten. De wet zou een limitatieve opsomming moeten geven van strafvorderlijke toegangsmogelijkheden. De spiegelbepalingen in de Telecommunicatiewet zouden daarbij moeten aansluiten. In het licht van de bewaarplicht ziet het CBP niet in wat nog de toegevoegde waarde is van het bevriezingsbevel. De toepassing van artikel 126hh van het Wetboek van Strafvordering op de bewaarde verkeersgegevens acht het CBP in strijd met het verbod op datamining, als neergelegd in artikel 4 van de richtlijn. Tenslotte wijst het CBP op de mogelijkheid dat bestuursorganen of derden langs civielrechtelijke weg de beschikking krijgen over de bewaarde gegevens. Dit zou door de wetgever expliciet moeten worden uitgesloten. De OPTA heeft aanbevolen om uitdrukkelijk te vermelden dat de gegevens, die thans op grond van hoofdstuk 11 van de Telecommunicatiewet worden opgeslagen, ook toegankelijk blijven voor het toezicht op de naleving van wetgeving, anders dan opsporing van ernstige strafbare feiten.

Naar aanleiding van het advies van het CBP is de memorie van toelichting aangevuld, zodat een nog meer extensief en volledig overzicht wordt geboden van de thans geldende bevoegdheden voor de politie, justitie en de inlichtingen- en veiligheidsdiensten op grond van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002, ten aanzien van de toegang tot de door de aanbieders bewaarde gegevens. Een limitatieve opsomming van de bevoegdheden in de wet is uit de aard der zaak tijdgebonden; eventuele aanpassing van die bevoegdheden in de toekomst zal gevolgen kunnen hebben voor de toegang tot die gegevens. Voorgesteld wordt in artikel 13.2b van de Telecommunicatiewet een spiegelbepaling op te nemen voor de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering, daarmee sluiten de spiegelbepalingen in de Telecommunicatiewet volledig aan bij de bevoegdheden op grond van het Wetboek van Strafvordering. Het bevriezingsbevel, op grond van de artikelen 126ni en 126ui van het Wetboek van Strafvordering, is niet beperkt tot gegevens die worden gehouden door de aanbieders van openbare telecommunicatiediensten maar kan worden gericht tot anderen van wie redelijkerwijs kan worden vermoed dat zij toegang hebben tot bepaalde gegevens. Deze bevoegdheid is dan ook niet beperkt tot de lijst van telecommunicatiegegevens, die op grond van de richtlijn dataretentie door de aanbieders moeten worden bewaard, maar deze kan worden toegepast met betrekking tot bepaalde gegevens die ten tijde van de vordering zijn opgeslagen in een geautomatiseerd werk.

Schrapping van deze bevoegdheid is dan ook niet aan de orde. Anders dan het CBP meent is de toepassing van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering niet in strijd met artikel 4 van de richtlijn. Ook de toepassing van de bevoegdheid van artikel 126hh van het Wetboek van Strafvordering is gebonden aan bepaalde gevallen, zoals hiervoor in paragraaf 3.1 aan de orde kwam. Voor wat betreft de toegang tot de bewaarde gegevens door bestuursorganen en door derden tenslotte valt bij voorbaat niet goed in te zien op grond van welke wettelijke bevoegdheden dan wel rechterlijke beslissingen bestuursorganen of derden toegang zouden kunnen verkrijgen tot de bewaarde gegevens. De doelbinding van artikel 13.2a staat aan een dergelijke toegang in de weg. Om tegemoet te komen aan de door het CBP en de OPTA ingebrachte bezwaren wordt voorgesteld om aan artikel 18.7 een extra lid toe te voegen, waarin uitdrukkelijk wordt bepaald dat de toezichthouder geen bevoegdheid heeft met betrekking tot de gegevens die op grond van artikel 13.2a worden bewaard. Hiermee wordt benadrukt dat andere toezichthoudende organen of derden geen toegang kunnen hebben tot deze gegevens.

Het recht op kennisneming

Voor wat betreft het recht op kennisneming hebben de aanbieders er in hun gezamenlijke reactie op gewezen dat onverkorte toepassing van de verplichting tot mededeling aan betrokkene of hem betreffende persoonsgegevens worden verwerkt, op grond van artikel 35 WBP, een disproportionele impact op de bedrijfsvoering van de aanbieders zal kunnen hebben. Een inzagerecht zou met zich mee kunnen brengen dat iedere aanbieder desgevraagd een overzicht zou moeten verstrekken van alle bewaarde gegevens gedurende de wettelijke bewaartermijn, voorafgaand aan de datum van het verzoek. De aanbieders menen dat een redelijke uitleg van die verplichting zou moeten zijn dat de aanbieder kan volstaan met de verstrekking aan de klant van een overzicht van de soorten gegevens die door de aanbieder op grond van de bewaarplicht moeten worden opgeslagen en niet een gedetailleerd overzicht hoeft te verstrekken.

Naar aanleiding van deze adviezen moet worden opgemerkt dat de voorgestelde wettelijke regeling van de bewaarplicht voor de telecommunicatiegegevens de kenbaarheid van de gegevensverwerking voor de burger vergroot. Dit laat echter onverlet de mogelijkheid voor de betrokkene om op grond van artikel 35 WBP te verzoeken om kennisneming van de gegevens die over hem worden verwerkt. De alsdan te verstrekken gegevens zijn opgesomd in artikel 35, tweede lid, WBP. Deze bepaling laat echter niet de uitleg toe die daaraan door de aanbieders wordt gegeven. Wel kan de vraag worden opgeworpen naar de praktische betekenis van het recht op kennisneming voor de betrokkene omdat toepassing van de mogelijkheid tot correctie van gegevens, als bedoeld in artikel 36, eerste lid, WBP, in de praktijk niet aan de orde zal zijn vanwege het feit dat het gaat om gegevens van meer technische aard die langs geautomatiseerde weg zijn verkregen. Daarnaast zullen weigeringsgronden kunnen worden ingeroepen. Naar aanleiding van het verzoek van de aanbieders om een nadere toelichting op dit punt, is in paragraaf 5 de nodige verheldering opgenomen.

Evaluatie en Statistieken

De aanbieders wijzen erop dat in het wetsvoorstel, anders dan in de richtlijn, een evaluatie geheel ontbreekt. Onafhankelijke begeleiding van de implementatie is noodzakelijk. Ook het CBP meent, gezien het grote maatschappelijke belang van de bewaarplicht, dat de wetgever een eigen evaluatie moet verrichten naast het openbaar evaluatieverslag van de Commissie in 2010. Die evaluatie is gebaat bij openbare statistieken. Een verplichting tot het opstellen daarvan zou in de wet moeten worden opgenomen, deze verplichting zou volgens het CBP op de behoeftestellers moeten rusten en niet op de aanbieders. Daarvoor zou het Duitse model gevolgd kunnen worden. Het CBP refereert tevens aan het publiceren van statistieken over aantallen taps, zoals toegezegd door de regering bij brief van 15 december 2006 (Kamerstukken II 2005/06, 30517). Ook voor de ACT

is onduidelijk waarom dergelijke registratieverplichtingen op de aanbieders zouden moeten rusten, de in de memorie van toelichting genoemde informatie is ook bij de autoriteiten bekend zodat verzameling van deze gegevens door een door de Minister van Justitie aan te wijzen orgaan veel meer voor de hand ligt. Het College van procureurs-generaal constateert dat het openbaar ministerie, gezien de huidige stand van zaken met betrekking tot de automatisering binnen de organisatie, niet in staat zal zijn de gewenste registratie van de statistische gegevens te verzorgen. Daarnaast wijst het college er op dat niet alle informatie ten behoeve van statistisch materiaal binnen de scope van het openbaar ministerie ligt. Zo kan de politie zelfstandig de aanbieders verzoeken NAW-gegevens te verstrekken.

Naar aanleiding van deze adviezen is in het wetsvoorstel een evaluatiebepaling opgenomen. Voor wat betreft de verplichting tot het verzamelen van statistische gegevens wordt, in lijn met de adviezen van de aanbieders en het CBP, onderkend dat het in beginsel een taak van de overheid is om zorg te dragen voor de verzameling en verwerking van statistische gegevens betreffende de vordering van telecommunicatiegegevens in het kader van de opsporing van strafbare feiten. Wel is nader onderzoek nodig van de financiële en organisatorische aspecten die aan een dergelijke registratie verbonden zijn. Op dit punt is de memorie van toelichting aangevuld. Bij de implementatie zal tevens het bijhouden van tapstatistieken voor wat betreft de taps in het belang van de opsporing worden betrokken, zoals door de regering is toegezegd in de eerdergenoemde brief van 15 december 2006.

De notificatieplicht
Het CBP wijst er op dat in het wetsvoorstel niets wordt gezegd over de notificatieplicht bij de bevraging van andere dan identificerende gegevens en ziet een verband met de verplichting tot het bijhouden van statistieken. Ook hier biedt het Duitse implementatievoorstel volgens het CBP een relevant model.

Naar aanleiding van dit advies moet worden opgemerkt dat een vordering van de officier van justitie tot verstrekking van gegevens over telecommunicatieverkeer, op grond van de artikelen 126n en 126u van het Wetboek van Strafvordering, onder de notificatieplicht van artikel 126bb van het Wetboek van Strafvordering valt. Het is dan ook niet nodig om in dit wetsvoorstel regels te geven over de bevraging van andere dan identificerende gegevens, zoals het CBP voorstaat. Die regels zijn er reeds. Op het Duitse implementatievoorstel is hierboven reeds in gegaan. In de evaluatie van de Wet bijzondere opsporingsbevoegdheden is aan de orde gekomen dat de notificatieplicht destijds niet voldoende werd nageleefd. Inmiddels is uit een door het openbaar ministerie bij alle arrondissementsparketten uitgevoerde audit gebleken dat er verbeteringen zijn in de naleving hiervan. De naleving is bij enkele parketten echter nog niet op orde. Om die reden worden ten behoeve van de parketten een instructie en een standaard procesbeschrijving opgesteld voor de uitvoering van de notificatieplicht en wordt toegezien op de implementatie daarvan. In een afzonderlijke brief zal de Tweede Kamer worden geïnformeerd over de resultaten van de audits.

De positie van professioneel verschoningsgerechtigden
Naar aanleiding van het wetsvoorstel spreekt de NOvA nogmaals de zorg uit dat informatie, die een advocaat op grond van zijn geheimhoudingsplicht niet met anderen mag delen, door een vordering gegevensverkeer onbeschermd ter beschikking van politie en justitie komt. De orde concludeert dat de vormgeving van het verschoningsrecht in het huidige tijdsgewricht niet meer voldoet en roept op een bezinning over de wijze waarop het verschoningsrecht in het (tele)communicatietijdperk effectiever kan worden vormgegeven.

Naar aanleiding van dit advies moet worden opgemerkt dat dit wetsvoorstel strekt tot implementatie van de verplichtingen van de richtlijn dataretentie en dat daarin geen bepalingen zijn opgenomen die betrekking hebben op het verschoningsrecht. Het verschoningsrecht houdt geen verband met de thans te bewaren telecommunicatiegegevens, maar uitsluitend met de kennisneming van de inhoud van telecommunicatie die aan de orde is bij de toepassing van de bevoegdheid tot het aftappen van telecommunicatie. Daarop ziet het wetsvoorstel niet. Naar aanleiding van het advies van het CBP over het tappen van geheimhouders is over dit onderwerp in de Tweede Kamer een Algemeen Overleg gevoerd (29800 VI, nr. 134). Naar de uitkomsten van dat overleg wordt thans verwezen.

ARTIKELSGEWIJZE TOELICHTING

Artikel I

Onderdeel A (opschrift hoofdstuk 13)

Hoofdstuk 13 van de Telecommunicatiewet heeft thans als opschrift “Bevoegd aftappen”. Dit houdt verband met de oorspronkelijk in dit hoofdstuk opgenomen verplichting van de aanbieders om medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering of een verzoek op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie. Inmiddels zijn aan dit hoofdstuk ook verplichtingen voor de aanbieders toegevoegd om te voldoen aan een vordering of een verzoek tot het verstrekken van verkeers- of gebruikersgegevens. Dit wetsvoorstel strekt tot toevoeging van een verplichting voor de aanbieders tot het bewaren van bepaalde telecommunicatiegegevens. Voorgesteld wordt het opschrift van hoofdstuk 13 van de wet in overeenstemming te brengen met de ruimere reikwijdte van dit hoofdstuk.

Onderdeel B (wijziging van artikel 11.13)

Artikel 11.13

Tweede lid
Voorgesteld wordt een nieuw tweede lid in te voegen. In het eerste lid wordt de aanbieders de mogelijkheid geboden te voldoen aan de verplichting van de richtlijn tot het bewaren van bepaalde verkeersgegevens. Deze verplichting van de aanbieders kan echter in strijd komen met de verplichtingen die op grond van de artikelen 11.5 en 11.5a van de Telecommunicatiewet op de aanbieders rusten. Deze verplichtingen hebben betrekking op het verwijderen of anonimiseren van de door hen verwerkte en opgeslagen verkeers- en locatiegegevens zodra deze gegevens niet meer nodig zijn voor het overbrengen van communicatie, behoudens de verdere verwerking voor bepaald aangewezen doelen, die verband houden met de bedrijfsvoering van de aanbieders dan wel met toestemming van de desbetreffende abonnee of gebruiker.

In het eerste lid van artikel 11.13 van de Telecommunicatiewet is vastgelegd dat de aanbieders de artikelen 11.5 en 11.5a van die wet buiten toepassing kunnen laten indien dit noodzakelijk is in het belang van de nationale veiligheid en de voorkoming, opsporing en vervolging van strafbare feiten. Hiermee staat buiten twijfel dat de bewaring van de betreffende gegevens door de aanbieders, op grond van de verplichting van artikel 13.2a, tweede lid, van de Telecommunicatiewet, geoorloofd is en dat de verplichtingen op grond van de artikelen 11.5

en 11.5a van de wet daarop niet van toepassing zijn. Met de voorgestelde invoeging van een nieuw tweede lid in artikel 11.13 van de wet wordt verduidelijkt dat de gegevens uitsluitend kunnen worden bewaard ten behoeve van mogelijke beschikbaarstelling aan de daartoe wettelijk bevoegde instanties en niet verder kunnen worden verwerkt ten behoeve van zakelijke doeleinden van de aanbieders, behoudens de verdere verwerking die reeds is voorzien met het oog op de doeleinden van de artikelen 11.5 en 11.5a van de wet.

Onderdeel C (wijziging van artikel 13.2a)

Artikel 13.2a

Eerste lid

In dit lid worden enkele begripsomschrijvingen gegeven.

De omschrijving van het begrip 'gegevens' houdt verband met de verplichting van het tweede lid, tot bewaring van bepaalde gegevens. In de richtlijn dataretentie wordt onder het begrip gegevens verstaan de verkeers- en locatiegegevens, en de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren (artikel 2, onderdeel a). De begrippen verkeers- en locatiegegevens worden reeds omschreven in artikel 11.1 van de wet. Deze begripsomschrijvingen gelden echter niet voor hoofdstuk 13 van de wet. Door dit lid wordt zeker gesteld dat deze begripsomschrijvingen eveneens gelden voor de verplichting van het tweede lid. Aanvullend wordt verhelderd dat naast de verkeers- en locatiegegevens in de zin van hoofdstuk 11 van de Telecommunicatiewet ook gegevens, die nodig zijn om de abonnee of gebruiker te identificeren, onder het begrip 'gegevens' vallen. Deze verruiming houdt verband met het feit dat dergelijke gegevens van belang kunnen zijn voor de criminaliteitsbestrijding.

De omschrijving van het begrip 'oproeppoging zonder resultaat' houdt verband met het vierde lid. Dit wordt aldaar nader toegelicht.

Tweede lid

In dit lid is de verplichting voor de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten neergelegd om ervoor zorg te dragen dat bepaalde gegevens worden bewaard. De te bewaren gegevens worden omschreven in een bijlage, behorende bij de Telecommunicatiewet Daarmee wordt de nodige duidelijkheid geboden over de reikwijdte van de bewaarplicht, zodat het voor de aanbieders kenbaar is welke gegevens zij dienen te bewaren en aan de bevoegde autoriteiten zekerheid wordt geboden over de vraag welke gegevens gevorderd kunnen worden. De richtlijn dataretentie beoogt een harmonisatie tot stand te brengen van de nationale bepalingen van de lidstaten waarbij verplichtingen worden opgelegd aan de aanbieders inzake het bewaren van bepaalde gegevens, 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 gevallen waarin, en voorwaarden waaronder, de gegevens kunnen worden verstrekt ten behoeve van het onderzoeken, opsporen en vervolgen van misdrijven zijn beschreven in paragraaf 3.1 (de beschikbaarstelling van de bewaarde gegevens aan de bevoegde autoriteiten). In de artikelen 13.2b en 13.4 van de wet is de verplichting voor de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten neergelegd om aan voormelde vorderingen te voldoen.

Derde lid

In dit lid is de bewaartermijn vastgelegd. Voor de toelichting op de gekozen bewaartermijn wordt verwezen naar het algemeen deel van deze memorie van toelichting (paragraaf 2.3). De gegevens moeten worden bewaard gedurende een termijn van achttien maanden vanaf de datum van communicatie. Voor de vaststelling van die

datum moet worden uitgegaan van de datum waarop een verbinding tot stand is gekomen door middel waarvan communicatie is overgebracht. Bij het gebruik van internet kan dit met zich meebrengen dat gedurende meerdere dagen een verbinding bestaat door middel waarvan communicatie wordt over gebracht. In dergelijke gevallen dient voor de bewaartermijn te worden uitgegaan van de verschillende dagen, gedurende welke communicatie heeft plaatsgevonden. Indien er bijvoorbeeld gedurende een periode van vijf dagen iedere dag communicatie heeft plaatsgevonden, dan geldt dat de betreffende gegevens worden bewaard gedurende een periode van achttien maanden vanaf de dag waarop de communicatie plaats had. Door middel van geautomatiseerde systemen kunnen de aanbieders uitvoering geven aan de verplichting tot vernietiging van de gegevens na ommekomst van de bewaarperiode; hiervoor wordt verwezen naar de toelichting op artikel 13.5, tweede lid.

Vierde lid

Een oproeppoging zonder resultaat betreft een communicatie waarbij een telefoonoproep wel tot verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord. Gegevens over dergelijke oproeppogingen kunnen voor de opsporingsinstanties van belang zijn voor het verkrijgen van inzicht in de kring personen die bij strafbare feiten betrokken kunnen zijn. Daarnaast kunnen deze gegevens van belang zijn voor de bewijsvoering, omdat verklaringen van de verdachte, bijvoorbeeld dat hij op een bepaald tijdstip op een bepaalde plaats is geweest, kunnen worden getoetst aan de beschikbare gegevens die door de aanbieders zijn bewaard. Daarbij geldt echter als belangrijk aandachtspunt dat het vaste telefonienetwerk vanuit technisch oogpunt niet altijd in voldoende mate is voorbereid op de bewaring van dergelijke gegevens. Dit geldt in het bijzonder voor de transformatoren, die gedurende de jaren zestig van de vorige eeuw in Nederland zijn geïnstalleerd voor de afhandeling van het destijds vaste telefoonverkeer. Een verplichting tot bewaring van de gegevens, als omschreven in de richtlijn dataretentie, zou dan noodzaken tot ingrijpende aanpassing of zelfs volledige vernieuwing van de betreffende transformatoren. Om een dergelijk ingrijpend gevolg van de bewaarplicht vanuit het oogpunt van de effectiviteit voor de opsporing, in relatie tot de kosten van de regeling en de lasten voor de aanbieders, beheersbaar te doen zijn wordt in de richtlijn dataretentie voorgeschreven dat de bewaarplicht de gegevens van oproeppogingen zonder resultaat omvat, voorzover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten worden gegenereerd, verwerkt en opgeslagen (wat telefoniegegevens betreft) of gelogd (wat internetgegevens betreft). Dit betekent dat de bewaring van de gegevens, ook indien gebruik wordt gemaakt van mobiele telefonie, afhankelijk is van de vraag in hoeverre de betrokken gegevens in het kader van de eigen bedrijfsvoering van de betreffende aanbieder worden opgeslagen of gelogd. Voorzover thans bekend, worden dergelijke gegevens door de aanbieders, die in Nederland actief zijn, niet ten behoeve van de eigen bedrijfsvoering bewaard. De verplichting tot het bewaren van de gegevens rond de oproeppogingen zonder resultaat is dan dus niet op deze aanbieders van toepassing. Niettemin strekt de verplichting tot implementatie van de richtlijn dataretentie ertoe dat ook de verplichting tot het bewaren van gegevens met betrekking tot oproeppogingen zonder resultaat in de Telecommunicatiewet wordt opgenomen.

Onderdeel D (wijziging van artikel 13.2b)

Artikel 13.2b

In het algemeen deel van de memorie van toelichting is aan de orde gekomen dat in de Telecommunicatiewet verplichtingen voor de aanbieders zijn opgenomen om te voldoen aan een vordering tot verstrekking van gegevens (‘spiegelbepalingen’). In het huidige artikel 13.2b van de Telecommunicatiewet is de verplichting opgenomen te voldoen aan een vordering dan wel een verzoek tot verstrekking van gegevens op grond van de artikelen 126nc tot en met 126nh en 126uc tot en met 126uh van het Wetboek van Strafvordering. In de Wet van

20 november 2006 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven (Stb. 580) is de bevoegdheid van de officier van justitie opgenomen om, indien een verkennend onderzoek de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft, van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, te vorderen bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon te verstrekken (artikel 126ii Sv). Daarnaast kan de officier van justitie, in geval van een dergelijk onderzoek, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot een geautomatiseerd gegevensbestand schriftelijk vorderen dit bestand, of delen daarvan, te verstrekken teneinde de hierin opgenomen gegevens te doen bewerken (artikel 126hh Sv). Deze bevoegdheden kunnen ook worden gebruikt jegens de aanbieder van een openbare telecommunicatiedienst of een openbaar telecommunicatienetwerk. In het algemeen deel van de memorie van toelichting is aangegeven dat deze bevoegdheden niet kunnen worden gebruikt om gegevens te vorderen die onder de bewaarplicht van het voorgestelde artikel 13.2a van de Telecommunicatiewet vallen. In de eerdergenoemde wet van 20 november 2006 is niet voorzien in een afzonderlijke spiegelbepaling voor de bevoegdheden op grond van de artikelen 126hh en 126ii van het Wetboek van Strafvordering. Om deze omissie te corrigeren wordt voorgesteld om een extra spiegelbepaling op te nemen in verband met deze bevoegdheden. Daarmee wordt geëxpliciteerd dat ook de aanbieders van telecommunicatie gehouden zijn te voldoen aan een vordering tot het verstrekken van gegevens op grond van het Wetboek van Strafvordering.

Onderdeel E (wijziging van artikel 13.4)

Artikel 13.4

Eerste lid

Voorgesteld wordt in artikel 13.4 van de Telecommunicatiewet een nieuw eerste lid in te voegen dat de verplichting bevat voor de aanbieders om te voldoen aan de vordering tot verstrekking van verkeersgegevens. Deze bepaling is thans opgenomen in artikel 13.2a, eerste lid, van de wet. Daarnaast wordt voorgesteld het huidige eerste en tweede lid van artikel 13.4 van de Telecommunicatiewet te vernummeren tot het tweede en derde lid. Dit betreft de verplichtingen van de aanbieders tot het voldoen aan een vordering tot verstrekking van gebruikersgegevens. De verplichtingen van de aanbieders tot verstrekking van verkeersgegevens – inclusief de gebruikersgegevens - ten behoeve van de uitoefening van de bevoegdheden op grond van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002 worden dan in één bepaling samengebracht. Vanuit het oogpunt van wetsystematiek ligt dit in de rede. De verplichting van de aanbieders om te voldoen aan de vordering tot verstrekking van de verkeers- of gebruikersgegevens omvat zowel de gegevens, die op grond van het voorgestelde artikel 13.2a, tweede lid, van de wet dienen te worden bewaard, als de actuele gegevens die bij de aanbieders beschikbaar zijn of worden verwerkt ten behoeve van de eigen bedrijfsvoering.

Derde lid

Op grond van de Telecommunicatiewet zijn de aanbieders verplicht om te voldoen aan een vordering tot verstrekking van gebruikersgegevens. Dit betreffen gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Echter, wanneer de gegevens van een gebruiker van telecommunicatie niet bij de aanbieder geregistreerd zijn dan kan de aanbieder niet door een eenvoudige raadpleging van zijn bestanden de benodigde gegevens opzoeken maar zijn extra handelingen nodig om de gegevens te verkrijgen. Dit kan aan de orde zijn bij vormen van vooruit betaalde mobiele telefonie door middel van prepaid cards. In het Besluit

bijzondere vergaring nummergegevens (Stb. 2002, 31) is een bestandsanalyse uitgewerkt, die inhoudt dat de aanbieder door een analyse van zijn bestanden de benodigde nummergegevens achterhaalt. Daarvoor is nodig dat de aanbieder de volgende gegevens bewaart: de tijdstippen waarop telecommunicatie heeft plaatsgevonden, de met die tijdstippen corresponderende nummers en bij welk basisstation die gegevens zijn binnengekomen (artikel 7 van het Besluit bijzondere vergaring nummergegevens). De aanbieder is verplicht de voor de bestandsanalyse benodigde gegevens te bewaren gedurende een periode van drie maanden.

De uit de richtlijn dataretentie voortvloeiende verplichtingen tot het bewaren en beschikbaar kunnen stellen van verkeersgegevens omvatten de gegevens die nodig zijn om de bron van een communicatie te traceren en te identificeren. Dit betreft gegevens als het oproepende nummer en de naam en het adres van de abonnee of geregistreerde gebruiker en de gebruikte telefoondienst (artikel 5, eerste lid, onderdeel a, punt 1 en punt 2). Deze bewaarplicht omvat de bovenbedoelde gebruikersgegevens. Om zeker te stellen dat de aanbieders deze gegevens beschikbaar kunnen maken door de bovengenoemde bestandsanalyse is de in artikel 13.4, tweede lid, van de Telecommunicatiewet aangepast aan de in artikel 13.2a, tweede lid, van de Telecommunicatiewet voorgestelde bewaartermijn. Zo is verzekerd dat de aanbieder van prepaid card-diensten volledig kan voldoen aan de plicht om de gegevens, die nodig zijn om de bron van een communicatie te achterhalen, te bewaren en beschikbaar te stellen. Dit impliceert dat in de laatste zin van het tweede lid de termijn van drie maanden wordt gewijzigd in achttien maanden. In het algemeen deel van de memorie van toelichting is dit nader uitéén gezet (paragraaf 2.4). Hiermee wordt volledig voldaan aan de verplichtingen van de richtlijn dataretentie.

Vierde lid

De verplaatsing van de verplichting om te voldoen aan de vordering tot verstrekking van verkeersgegevens heeft eveneens consequenties voor het huidige tweede lid van artikel 13.2a van de Telecommunicatiewet. In dit tweede lid wordt de mogelijkheid geboden om bij algemene maatregel van bestuur regels te stellen met betrekking tot de wijze waarop de aanbieders aan de vordering of het verzoek voldoen en de wijze waarop de gegevens beschikbaar worden gehouden. Van deze bevoegdheid is tot op heden geen gebruik gemaakt. Vanwege de voorgestelde verplaatsing van de verplichting van artikel 13.2a, eerste lid, van de Telecommunicatiewet naar artikel 13.4, eerste lid, van de Telecommunicatiewet, wordt thans voorgesteld de mogelijkheid van een algemene maatregel van bestuur in het vierde lid op te nemen.

Anders dan tot nu toe zullen de nadere regels worden gesteld op voordracht van de Minister van Justitie, de Minister van Economische Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie. De Minister van Justitie is eerste ondertekenaar van dit wetsvoorstel. De betrokken ministers zullen de Minister van Justitie kunnen machtigen om de voordracht voor de algemene maatregel van bestuur mede namens hen te doen.

Zoals gezegd verplicht het huidige eerste lid van artikel 13.4 van de Telecommunicatiewet de aanbieders om bepaalde gebruikersgegevens te verstrekken om de bevoegde autoriteiten in staat te stellen om de wettelijke bevoegdheden tot het aftappen of opnemen van telecommunicatie te kunnen uitoefenen. In het eerdergenoemde Besluit verstrekking gegevens telecommunicatie, dat is gebaseerd op het derde lid van dit artikel, wordt deze verplichting uitgewerkt. De aanbieder dient te beschikken over een bestand waarin bepaalde gegevens zijn opgenomen van de personen die gebruik maken van een dienst of netwerk van de aanbieder. Dit betreffen de volgende gegevens: naam, adres, postcode, woonplaats, de telecommunicatiedienst die wordt afgenomen en het aansluitnummer dat aan een gebruiker is verleend (artikel 4 Besluit verstrekking gegevens telecommunicatie). De aanbieder is gehouden om de gegevens in het bestand tenminste iedere vierentwintig uur te actualiseren. De

voor de bevoegde autoriteiten benodigde gegevens worden verstrekt door tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie. Daartoe verleent de aanbieder het informatiepunt langs geautomatiseerde weg gedurende vierentwintig uur per dag rechtstreekse toegang tot het gegevensbestand. De genoemde verplichtingen houden verband met de wijze van uitoefening van de bevoegdheden tot het vorderen van actuele gebruikersgegevens door de daartoe bevoegde autoriteiten, als neergelegd in de artikelen 126na, tweede lid, en 126ua, tweede lid, van het Wetboek van Strafvordering, en staan als zodanig los van de voorgestelde verplichting tot het bewaren van gegevens die op het netwerk worden gegenereerd of gelogd. De bestaande verplichtingen, zoals die zijn uitgewerkt in het Besluit verstrekking gegevens telecommunicatie, worden dan ook niet gewijzigd als gevolg van de implementatie van de richtlijn dataretentie.

Het huidige tweede lid van artikel 13.4 van de Telecommunicatiewet verplicht de aanbieders om een bestandsanalyse te verrichten in die gevallen waarin zij niet beschikken over de vorenbedoelde gegevens. In het Besluit bijzondere vergaring nummergegevens wordt deze verplichting uitgewerkt. Dit is hierboven, bij de artikelsgewijze toelichting bij het derde lid van artikel 13.4 van de Telecommunicatiewet, nader toegelicht. In dat verband is tevens gewezen op de raakvlakken tussen de bestaande verplichting tot het bewaren van bepaalde nummergegevens en de bewaarverplichtingen die uit de richtlijn dataretentie voortvloeien. Behoudens de bewaartermijn van drie maanden worden de bestaande verplichtingen op het terrein van de bestandsanalyse echter niet beïnvloed door de richtlijn. Het Besluit bijzondere vergaring nummergegevens behoeft dan ook niet te worden gewijzigd als gevolg van de implementatie van de richtlijn dataretentie.

In het licht van de verplichting van de richtlijn dataretentie, om de gegevens zodanig te bewaren dat de bewaarde informatie en alle daarmee verband houdende relevante informatie onverwijld aan de bevoegde autoriteiten kan worden meegedeeld wanneer daarom wordt verzocht (artikel 8) is in dit lid tevens de mogelijkheid opgenomen op nadere regels te stellen over de wijze waarop de gegevens worden bewaard en de termijnen waarbinnen de gegevens door de aanbieders beschikbaar worden gesteld. De Telecommunicatiewet voorziet niet in een termijn waarbinnen de gegevens door de aanbieders aan de bevoegde autoriteiten moeten worden geleverd. Evenmin worden er regels gesteld voor een spoedregeling. Wel zijn er inmiddels afspraken gemaakt tussen openbaar ministerie, politie en de inlichtingen- en veiligheidsdiensten enerzijds en de aanbieders anderzijds terzake van het verkrijgen van gegevens en het opnemen van telecommunicatie. Verkeersgegevens worden in beginsel binnen vijf dagen geleverd. In noodgevallen kan de aanbieder worden verzocht verkeersgegevens zo spoedig mogelijk te leveren. Het eerdergenoemde Besluit verstrekking gegevens telecommunicatie geeft regels voor de verstrekking van bepaalde actuele gebruikersgegevens door de aanbieders. Daartoe verleent de aanbieder het Centraal Informatiepunt Onderzoek Telecommunicatie langs geautomatiseerde weg gedurende 24 uur per dag rechtstreeks toegang tot een bestand waarin die gegevens zijn opgenomen. Deze gegevens kunnen worden vergeleken op basis van hit/no hit en komen aldus binnen een zeer korte termijn beschikbaar voor de bevoegde autoriteiten. Bij de in dit lid bedoelde algemene maatregel van bestuur kunnen zonodig nadere regels worden gesteld terzake van de termijnen waarbinnen gegevens beschikbaar kunnen worden gesteld. Zoals in het algemeen deel hieromtrent reeds is opgemerkt, zal hiervoor worden aangesloten bij de thans gelden afspraken die op operationeel niveau tussen de aanbieders en de behoeftestellende diensten zijn overeen gekomen.

Tenslotte is in dit lid een grondslag opgenomen om bij algemene maatregel van bestuur regels te stellen omtrent het registreren van statistische gegevens over de beschikbaarstelling van de bewaarde gegevens aan de bevoegde autoriteiten. Vanwege de verplichtingen van de richtlijn zullen deze gegevens ten minste betrekking moeten hebben op de gevallen waarin gegevens zijn verstrekt, de tijd die is verstreken tussen de datum van bewaring van de gegevens en de datum waarop door de bevoegde autoriteiten is verzocht om overdracht ervan

en de gevallen waarin verzoeken om verstrekking niet konden worden ingewilligd. De registratie van deze gegevens zal kunnen worden gecoördineerd door een door de Minister van Justitie aan te wijzen orgaan. Daarvoor kan worden gedacht aan het Landelijk Parket van het Openbaar Ministerie. In het Besluit verstrekking gegevens telecommunicatie zijn ook regels opgenomen over het vastleggen van informatie over de verstrekking van gegevens (artikel 7).

Onderdeel F (wijziging van artikel 13.5)

Artikel 13.5

Eerste lid
De verwijzing naar het huidige artikel 13.2a van de Telecommunicatiewet kan vervallen omdat in dit wetsvoorstel wordt voorgesteld om de verplichting van de aanbieders te voldoen aan een vordering op grond van de artikelen 126n of 126u van het Wetboek van Strafvordering of op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002, op te nemen in artikel 13.4, eerste lid, van de Telecommunicatiewet. Dit is hierboven, bij de artikelsgewijze toelichting op artikel 13.4 van dit wetsvoorstel, nader toegelicht. Door de voorgestelde vervanging van de woorden ”eerste of tweede lid” door: eerste, tweede of derde lid, wordt gewaarborgd dat de verplichtingen tot beveiliging van gegevens tegen kennisneming door onbevoegden onverkort gelden voor de gegevens rond een vordering of verzoek als bedoeld in het huidige artikel 13.2a van de Telecommunicatiewet.

Tweede lid
In dit lid is de verplichting voor de aanbieders neergelegd om passende technische en organisatorische maatregelen te nemen die nodig zijn om de bewaarde gegevens te beveiligen tegen vernietiging, verlies of wijziging en tegen niet toegelaten opslag, verwerking, toegang of openbaarmaking. Dit is een aanvulling op de bestaande verplichtingen op grond van artikel 11.3 van de Telecommunicatiewet. Daarnaast dienen de aanbieders passende technische en organisatorische maatregelen te nemen om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen en dat de gegevens na het verstrijken van de bewaarperiode worden vernietigd.

In het Besluit beveiliging gegevens aftappen telecommunicatie (Stb. 2003, 472) worden regels gegeven over het treffen van beveiligingsmaatregelen door de aanbieders ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie. In de bijlage bij dit besluit worden de te treffen maatregelen uitgewerkt. Deze maatregelen hebben betrekking op de eisen ten aanzien van het personeel, de fysieke beveiliging, het beheer van communicatie en beheersprocessen, de toegangsbeveiliging van geautomatiseerde systemen en de ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen. De aanbieder moet ervoor zorgen dat de medewerking aan een last tot het aftappen van telecommunicatie uitsluitend wordt verleend door personen die een verklaring omtrent het gedrag (VOG) kunnen overleggen. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens, heeft toegang tot die informatie en die gegevens. Verder geldt dat de toegang tot de ruimte waarin de informatie zich bevindt, evenals de toegang tot het geautomatiseerde informatiesysteem, uitsluitend is voorbehouden aan daartoe geautoriseerd personeel. De autorisaties worden vastgelegd. De fysieke beveiliging en de toegangsbeveiliging moeten zodanig zijn ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt. Alle handelingen met betrekking tot de verwerking van informatie worden persoonsgebonden vastgelegd teneinde onderzoek mogelijk te maken (logging).

Voor een nadere uitwerking van de eisen voor de beveiliging van, en de toegang tot, de bewaarde gegevens bij algemene maatregel van bestuur kan bij de regels van het Besluit beveiliging gegevens aftappen worden aangesloten.

Gelet op de gevoeligheid van de betreffende gegevens, die inzicht kunnen geven in de gedragingen van personen, is het van essentieel belang dat deze na ommekomst van de bewaarperiode daadwerkelijk zijn vernietigd. De verplichting tot vernietiging impliceert dat de bewaarde gegevens dagelijks worden vernietigd zodra achttien maanden zijn verstreken sedert de datum van inwerkingtreding van dit wetsvoorstel. Dit is dus een continu proces, dat een geautomatiseerde werkwijze veronderstelt. De aanbieders dienen passende technische maatregelen te treffen om aan deze verplichting te kunnen voldoen, bijvoorbeeld door het langs geautomatiseerde weg laten vernietigen van de betreffende gegevens of door middel van geautomatiseerde signalering dat de bewaarperiode is verstreken waarna door menselijke tussenkomst de onmiddellijke vernietiging van de gegevens kan volgen. Bij algemene maatregel van bestuur kunnen hierover nadere regels worden gegeven.

Derde lid

In dit lid is de verplichting voor de aanbieders vastgelegd om ervoor te zorgen dat de bewaarde gegevens dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk. Aan het einde van de bewaarperiode, bedoeld in artikel 13.2a, derde lid, van de wet, moeten de bewaarde gegevens onverwijld worden vernietigd. De verplichting van de aanbieders om de bewaarde gegevens na ommekomst van de bewaarperiode onverwijld te vernietigen impliceert niet alleen dat de gegevens niet verder kunnen worden verwerkt voor het doel waarvoor zij zijn bewaard maar strekt er toe dat de betreffende gegevens niet meer in het netwerk van de aanbieders aanwezig zijn of anderszins voor de aanbieders beschikbaar zijn. Het is van groot belang dat er adequaat toezicht wordt uitgeoefend op de naleving van deze verplichting. Daarvoor is het in de eerste plaats van belang dat passende technische en organisatorische maatregelen worden getroffen om aan deze verplichting te kunnen voldoen. Dit is bij het tweede lid toegelicht. Verder kan worden gedacht aan het maken van nadere afspraken tussen de betrokken toezichthoudende autoriteiten – het Agentschap Telecom en het College bescherming persoonsgegevens - over de wijze waarop het toezicht op de naleving van deze verplichting in de praktijk wordt vorm gegeven. Tenslotte zij opgemerkt dat de niet naleving van de verplichting tot onverwijlde vernietiging van de bewaarde gegevens een economisch delict vormt. Indien de bevoegde toezichthoudende autoriteiten kennis zouden verkrijgen van het niet naleven van de vernietigingsplicht door een aanbieder dan zal niet alleen het aan de betreffende toezichthouder ter beschikking staande instrumentarium op het gebied van de handhaving kunnen worden ingezet maar zal tevens aangifte kunnen worden gedaan bij het openbaar ministerie.

In hun advies hebben de aanbieders aangegeven dat uit de artikelen 11.5 en 11.5a van de Telecommunicatiewet slechts voortvloeit dat de gegevens geanonimiseerd moeten worden wanneer ze niet langer voor de limitatief beschreven bedrijfsdoeleinden worden verwerkt. Naar het oordeel van de aanbieders gaat de in dit wetsvoorstel opgenomen verplichting tot vernietiging van de gegevens verder dan de huidige verplichting die de aanbieders als verantwoordelijke hebben. De aanbieders bepleiten om ook op dit punt aansluiting te zoeken bij hoofdstuk 11 van de Telecommunicatiewet en de verplichting van de aanbieders niet verder te laten gaan dan tot het anonimiseren van de gegevens. De door de aanbieders voorgestane benadering is echter strijdig met de uit de richtlijn dataretentie voortvloeiende verplichting tot vernietiging van de bewaarde gegevens en laat bovendien de mogelijkheid bestaan dat de gegevens beschikbaar blijven na ommekomst van de voorgestelde bewaartermijn. Weliswaar biedt artikel 11.5 van de Telecommunicatiewet de aanbieders de keuze tussen anonimisering en

vernietiging van de door hen verwerkte en opgeslagen verkeersgegevens indien deze gegevens niet langer nodig zijn voor de in dat artikel omschreven zakelijke doelen maar dit laat de verplichting tot vernietiging van de gegevens die op grond van hoofdstuk 13 van die wet moeten worden bewaard, onverlet. Hieruit vloeit voort dat de aanbieder is gehouden tot vernietiging van de gegevens die worden bewaard op grond van artikel 13.2a van dit wetsvoorstel. Indien de aanbieder echter kan aantonen dat hij de verkeers- of locatiegegevens heeft verwerkt en opgeslagen ten behoeve van één van de doelen van artikel 11.5 of 11.5a van de Telecommunicatiewet, dan verzet de tekst van de wet zich niet tegen anonimisering van de betreffende gegevens.

De verplichting tot onverwijlde vernietiging geldt niet voor de gegevens die op grond van de artikelen 13.2b en 13.4 van de Telecommunicatiewet zijn bewaard en vervolgens, naar aanleiding van de uitoefening van de bevoegdheden van het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002, aan de bevoegde autoriteiten zijn verstrekt. Op de verdere verwerking van deze gegevens, inclusief de termijnen voor de verwijdering of de vernietiging van de gegevens, zijn de wettelijke regimes van toepassing die gelden voor de gegevensverwerking door de betreffende instantie. Voor de politie is dit thans de Wet politieregisters, voor de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst is dit de Wet op de inlichtingen- en veiligheidsdiensten 2002. Het voorgaande laat de verplichting voor de aanbieder, om de betreffende gegevens na het verstrijken van de bewaarperiode te vernietigen, onverlet.

Vierde lid
In dit artikel worden algemene regels gegeven voor de bescherming, de beveiliging, de toegang tot en de vernietiging van de bewaarde gegevens. Bij algemene maatregel van bestuur kunnen hierover nadere regels worden gesteld. De regels kunnen betrekking hebben op de autorisaties voor de verwerking van, of de toegang tot, de bewaarde gegevens. Daarnaast kunnen de regels betrekking hebben op de bekendmaking van de bewaarde gegevens aan de personen die zijn geautoriseerd tot de verwerking van, of de toegang tot, die gegevens. Tenslotte kunnen de regels betrekking hebben op de vastlegging van bepaalde gegevensverwerkingen (protocollering) - zoals de toekenning van de autorisaties en de verstrekking van bewaarde gegevens aan de bevoegde autoriteiten - en het periodiek (doen) verrichten van privacy-audits.

Anders dan tot nu toe zullen de nadere regels worden gesteld op voordracht van de Minister van Justitie, de Minister van Economische Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie. De Minister van Justitie is eerste ondertekenaar van dit wetsvoorstel. De betrokken ministers zullen de Minister van Justitie kunnen machtigen om de voordracht voor de algemene maatregel van bestuur mede namens hen te doen.

Onderdeel G (wijziging van artikel 13.6)

Artikel 13.6

Eerste en tweede lid
In artikel 13.6 van de Telecommunicatiewet wordt een regeling gegeven voor de kosten en vergoedingen voor de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten om te kunnen voldoen aan de verplichtingen op het terrein van het bevoegd aftappen.
De investeringskosten, alsmede de periodieke onderhouds- en exploitatiekosten, die verband houden met aftappen komen ten laste van de aanbieders. Ook de technische inspanningen die vooraf gedaan moeten worden voor het verstrekken van informatie en voor de beveiliging daarvan komen voor rekening van de aanbieders.

Deze bepaling is ingevoerd als gevolg van de keuze om de kosten voor het aftapbaar maken van systemen niet langer door de overheid te laten vergoeden. Krachtens artikel 13.6, tweede lid, van de Telecommunicatiewet worden de administratiekosten en de personeelskosten die rechtstreeks voortvloeien uit de aftapwerkzaamheden en de gegevensverstrekking, uit de openbare kas vergoed.

In de Regeling kosten aftappen en gegevensverstrekking van de Minister van Economische Zaken (Stcrt. 2005, 62) worden nadere regels gegeven met betrekking tot de vaststelling en vergoeding van de declarabele kosten door de autoriteit die de last, het bevel of het verzoek heeft gedaan. De regeling stelt vast welke personeels- en administratiekosten declarabel zijn.

Voorgesteld wordt de verplichting tot het voldoen aan een vordering op grond van de artikelen 126n of 126u van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 op te nemen in artikel 13.4, eerste lid, van de Telecommunicatiewet. De onderbrenging van deze verplichting in artikel 13.4 van de Telecommunicatiewet heeft tot gevolg dat voor de regeling van de vergoeding van de kosten, die door de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten worden gemaakt om te kunnen voldoen aan de verplichtingen van dit wetsvoorstel, volledig wordt aangesloten bij de bestaande regeling voor de kosten en vergoedingen van dit artikel. Dit kan worden gerealiseerd door middel van aanpassing van het tweede lid van dit artikel. De verwijzing naar artikel 13.4, eerste of tweede lid, van de Telecommunicatiewet wordt vervangen door een verwijzing naar artikel 13.4, eerste, tweede of derde lid, van de Telecommunicatiewet.

De voorgestelde verwijzing in het eerste lid van dit artikel naar artikel 13.5, eerste lid, van de Telecommunicatiewet beoogt te verhelderen dat de regeling voor de kosten en vergoedingen van dit artikel betrekking heeft op de kosten in verband met de te nemen maatregelen in verband met beveiliging, bedoeld in dat artikellid.

Onderdeel H (invoeging van artikel 13.9)

Artikel 13.9

In de richtlijn dataretentie is bepaald dat uiterlijk op 15 september 2010 door de Commissie een evaluatieverslag zal worden uitgebracht aan het Europees Parlement en aan de Raad over de toepassing van deze richtlijn en de weerslag ervan op de marktdeelnemers en de consumenten. Zoals in paragraaf 8 aan de orde kwam wordt, mede naar aanleiding van de adviezen van de aanbieders en het CBP, voorgesteld een evaluatiebepaling op te nemen naar het model van de Aanwijzingen voor de regelgeving (aanwijzing no. 164). Hierbij komen zowel de mate van verwerkelijking van de doelstellingen en de neveneffecten aan de orde als de evenredigheid, subsidiariteit, uitvoerbaarheid, handhaafbaarheid, afstemming op andere regelingen, eenvoud, duidelijkheid en toegankelijkheid, dit alles uiteraard binnen de kaders die door de richtlijn dataretentie worden gesteld. De evaluatie zal zijn beperkt tot de in dit wetsvoorstel voorgestelde wijzigingen van de Telecommunicatiewet in verband met de implementatie van de richtlijn dataretentie.

Onderdeel I (wijziging van artikel 15.1)

Artikel 15.1

Eerste lid
De voorgestelde aanpassing vloeit voort uit de overheveling van het toezicht aangaande de naleving van de artikelen 11.5, 11.5a en 11.13 van de Telecommunicatiewet van het OPTA naar de Minister van Economische Zaken. Voor de toelichting wordt verwezen naar paragraaf 2.7.

Onderdeel J (wijziging van artikel 18.7)

Artikel 18.7

Tweede lid
De toezichthoudende organen zijn op grond van het eerste lid van dit artikel bevoegd alle informatie te vorderen voor zover dat nodig is voor de vervulling van hun taak. Deze bevoegdheid zou kunnen inhouden dat zij verkeersgegevens of locatiegegevens opvragen als bedoeld in artikel 13.2a, welke gegevens door aanbieders worden bewaard ten dienste van het voorkomen, opsporen en vervolgen van strafbare feiten. Het is evenwel niet aannemelijk dat de toezichthouder voor de vervulling van zijn taak deze gegevens nodig zou hebben. Om hierover elke onduidelijkheid weg te nemen en ter bescherming van de persoonlijke levenssfeer van de gebruiker van elektronische communicatiediensten wordt voorgesteld een tweede lid in te voegen, waarin uitdrukkelijk wordt bepaald dat de toezichthouder geen bevoegdheid heeft met betrekking tot deze gegevens. Hierop bestaat één uitzondering. Een deel van de te bewaren gegevens bedoeld in artikel 13.2a mag de aanbieder van een openbaar elektronisch netwerk of een openbare elektronische dienst op grond van de artikelen 11.5 en 11.5a ten dienste van zijn bedrijfsvoering verwerken. Voor zover een aanbieder die gegevens heeft verwerkt is de toezichthouder bevoegd daarover informatie te vorderen bij de aanbieder. Deze bevoegdheid voor de toezichthouder is onder meer van belang bij het toezicht op het versturen van ongewenste elektronische berichten.

Onderdeel K (opneming Bijlage bij de wet)

Artikel 13.10

Voorgesteld wordt een nieuw artikel aan de Telecommunicatiewet toe te voegen, waarin geregeld wordt dat de Bijlage met de lijst van de te bewaren gegevens wordt opgenomen na de ondertekening van de wet (aanwijzing 94 AR).

Artikel II

Overtredingen van een aantal voorschriften, die zijn gesteld bij of krachtens de Telecommunicatiewet, zijn economische delicten als bedoeld in de Wet op de economische delicten (artikel 1, onder 2º en onder 4º, WED). Dit betreft onder meer de verplichtingen van de aanbieders tot het aftapbaar zijn en tot het verlenen van medewerking aan bevoegd gegeven vorderingen tot het aftappen van telecommunicatie of het verstrekken van verkeers- of gebruikersgegevens. Deze verplichtingen zijn opgenomen in hoofdstuk 13 van de Telecommunicatiewet (artikelen 13.1, 13.2, 13.2a, 13.2b en 13.4 Tw).

De verplichtingen van de aanbieders tot het voldoen aan een bevoegd gegeven vordering tot verstrekking van verkeersgegevens zijn thans geregeld in artikel 13.2a van de Telecommunicatiewet. Met het voorliggende wetsvoorstel wordt de inhoud van artikel 13.2a van de Telecommunicatiewet voortaan echter een andere,

namelijk de verplichting tot het bewaren van de bij algemene maatregel van bestuur aan te wijzen gegevens ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Het niet voldoen aan deze verplichting wordt aldus strafbaar gesteld als een economisch delict. Met de voorgestelde verplaatsing van de verplichtingen van artikel 13.2a, eerste lid, van de Telecommunicatiewet naar artikel 13.4, eerste lid, van de Telecommunicatiewet, worden de verplichtingen van de aanbieders om te voldoen aan bevoegd gegeven vorderingen op grond van het Wetboek van Strafvordering dan wel de Wet op de inlichtingen- en veiligheidsdiensten 2002 voortaan in één bepaling samen gebracht. Dit komt het overzicht ten goede. De voorgestelde verplaatsing maakt het echter noodzakelijk om artikel 13.4, eerste lid, van de wet toe te voegen aan artikel 1, van de Wet op de economische delicten.
Overtreding van deze verplichtingen vormt een misdrijf, voorzover opzettelijk begaan (artikel 2, eerste lid, WED). De verplichting van de aanbieders tot het verstrekken van gebruikersgegevens blijft als een overtreding strafbaar op grond van de Wet op de economische delicten (artikel 1, onder 4º, WED).

Artikel III

Vanwege de voorgestelde vernummering of verplaatsing van leden van de artikelen 13.2a, 13.4 en 13.5 van de Telecommunicatiewet kan onduidelijkheid ontstaan over de rechtsgrondslag van de bestaande uitvoeringsregelingen. Om die reden wordt in Artikel III expliciet bepaald op welke artikelleden de betreffende algemene maatregelen van bestuur zijn gebaseerd. Dit betreft:

- het Besluit bijzondere vergaring nummergegevens telecommunicatie, dat thans is gebaseerd op de artikelen 3.10, vierde lid, onderdeel a, en 13.4, tweede lid, van de Telecommunicatiewet. Op grond van de voorgestelde vernummering van het tweede lid tot het derde lid van artikel 13.4, worden dit voortaan de artikelen 3.10, vierde lid, onderdeel a, en 13.4, derde lid, van de Telecommunicatiewet.
- het Besluit verstrekking gegevens telecommunicatie, dat thans is gebaseerd op de artikelen 13.1, tweede lid, 13.2, derde lid, 13.4, derde lid en 20.18 van de Telecommunicatiewet. Op grond van de voorgestelde vernummering van het derde lid tot het vierde lid van artikel 13.4, worden dit voortaan de artikelen 13.1, tweede lid, 13.2, derde lid, 13.4, vierde lid en 20.18 van de Telecommunicatiewet.
- het Besluit beveiliging gegevens aftappen telecommunicatie, dat thans is gebaseerd op de artikelen 13.2, derde lid en 13.5, tweede lid, van de Telecommunicatiewet. Op grond van de voorgestelde verplaatsing van het tweede lid naar het vierde lid van artikel 13.5, worden dit voortaan de artikelen 13.2, derde lid en 13.5, vierde lid, van de Telecommunicatiewet.

Artikel IV

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip. Daarvoor is van belang dat de richtlijn dataretentie uiterlijk op 15 september 2007 moet zijn geïmplementeerd in de nationale wetgeving (artikel 15, eerste lid).

Artikel V

Met de in dit artikel voorgestelde bepaling wordt de mogelijkheid geboden om de toepassing van de richtlijn op de bewaring van telecommunicatiegegevens in verband met internettoegang, internettelefonie en e-mails via het internet uit te stellen voor een periode van achttien maanden. De richtlijn biedt de lidstaten daartoe de mogelijkheid, mits de lidstaat die van deze mogelijkheid gebruik wil maken de Raad of de Commissie daarvan op de hoogte stelt middels een verklaring op het moment van goedkeuring van de richtlijn. Nederland heeft een

dergelijke verklaring afgelegd. In overleg met de betrokken aanbieders zal worden beoordeeld op welk tijdstip de wet in werking zal kunnen treden voor de bewaring van gegevens, die worden gegenereerd of verwerkt in verband met internettoegang, internettelefonie en e-mails via het internet.

De Minister van Justitie,