

Vergaderjaar 2006–2007

30 553

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 en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede enkele andere wijzigingen

Nr. 7

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 10 juli 2007

INLEIDING

De regering heeft met belangstelling kennis genomen van de reacties van de leden van de fracties van CDA, PvdA, VVD, SP en ChristenUnie op het onderhavige wetsvoorstel. Uit de reacties van de meeste fracties blijkt dat zij positief staan tegenover het onderhavige wetsvoorstel, maar uitbreiding van de aan het wetsvoorstel ten grondslag liggende onderbouwing op punten wenselijk achten. Zo hebben de leden van de fractie van het CDA met belangstelling kennisgenomen van het wetsvoorstel, maar resten nog enkele vragen bij de concrete voorstellen. Ook de leden van de PvdA-fractie geven aan met belangstelling kennis te hebben genomen van de voorstellen tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), maar zij hebben behoefte aan toelichting ten aanzien van het gestelde dat de Wiv 2002 in een aantal situaties niet voldoet. Het verheugt de regering dat de leden van de fractie van de VVD zich in grote lijnen kunnen vinden in de motivering bij de voorstellen ter uitbreiding van de bevoegdheden en de mogelijkheden van de inlichtingen- en veiligheidsdiensten. Deze leden geven aan dat sommige aspecten van het wetsvoorstel echter nadere toelichting behoeven. De leden van de fracties van de SP en de ChristenUnie hebben kennisgenomen van het wetsvoorstel. Door de leden van de fractie van de SP wordt aangegeven dat zij sceptisch zijn om te komen tot een verdere uitbreiding van de gegevensverwerking door de diensten. De leden van de fractie van de ChristenUnie hebben op dit moment behoefte aan het stellen van enkele vragen.

In het onderstaande zal de regering op de vragen en opmerkingen van de verschillende fracties ingaan en hoopt daarmee bestaande onduidelikheden of aarzelingen weg te nemen. Voorshands acht de regering het wenselijk nog een enkele opmerking te maken. In de vragen van de verschillende fracties wordt regelmatig verzocht om concrete voorbeelden ten aanzien van onderwerpen die spelen in het kader van dit wetsvoorstel. De regering heeft er in deze nota naar aanleiding van het verslag naar gestreefd deze vragen zo ruimhartig mogelijk te beantwoorden. In

bepaalde gevallen, de regering vraagt hiervoor het begrip van de Kamer, is dit echter niet mogelijk omdat voorkomen moet worden dat teveel zicht wordt gegeven op de operationele werkwijze van de diensten en hun actueel kennisniveau. Dit heeft als gevolg dat in dergelijke gevallen antwoorden slechts in algemene termen of met een enkel voorbeeld beantwoord zijn. Deze nota naar aanleiding van het verslag bied ik aan, mede namens de Minister-President, minister van Algemene Zaken, de minister van Defensie en de minister van Justitie. De nota naar aanleiding van het verslag wordt u aangeboden gezamenlijk met een nota van wijziging op het wetsvoorstel. Deze wijzigingen zijn deels technisch en deels inhoudelijk van aard.

INHOUDSOPGAVE

ALGEMEEN DEEL

- 1. Aanleiding tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002**
- 2. Algemene toelichting op de wijzigingsvoorstellen**
- 3. Inhoud van het wetsvoorstel: bespreking van een aantal hoofdonderdelen van het wetsvoorstel**
 - 3.1. Verplichte gegevensverstrekking door bestuursorganen alsmede door personen en instanties die beroeps- of bedrijfsmatig werkzaam zijn in de financiële sector of in de sector vervoer
 - 3.1.1. Algemeen
 - 3.1.3. *Verplichte verstrekking van gegevens door aan te wijzen categorieën van personen en instanties in de sectoren financiële dienstverlening en vervoer*
 - 3.1.4. *De beschikbaarstelling van geautomatiseerde gegevensbestanden (artikel 29b (nieuw)) door bestuursorganen en de op grond van artikel 29a, eerste lid, aangewezen categorieën van personen en instanties*
 - 3.2. Wijziging van de artikelen 28 en 29 in verband met de uitbreiding van de reikwijdte tot aanbieders van communicatiediensten
 - 3.3. Overige bijzondere bevoegdheden van de diensten
 - 3.3.1. Inleiding
 - 3.3.2. De oprichting en inzet van rechtspersonen
 - 3.3.3. Het bevorderen of treffen van maatregelen
- 4. Artikel 8 EVRM en artikel 10 Grondwet**
- 5. Administratieve lasten**

ARTIKELEN

ALGEMEEN DEEL

1. Aanleiding tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002

Door de leden van de VVD-fractie wordt gevraagd of de regering kan ingaan op de wijze waarop informatie die bij de AIVD ter beschikking is, wordt beveiligd. In antwoord hierop melden wij u het volgende. De beveiliging van informatie is binnen de diensten een belangrijk thema. Op de beveiliging van informatie bij de diensten zijn drie voorschriften van toepassing, te weten het Beveiligingsvoorschrift Rijksdienst 2005, het Besluit voorschrift informatiebeveiliging rijksdienst (Vir) en het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi). Naast deze voorschriften kent de Wiv 2002 enkele specifieke wettelijke bepalingen inzake de informatiebeveiliging van de diensten. Het Beveiligings-

voorschrift Rijksdienst 2005 bevat het organisatiemodel voor de integrale beveiliging van de Rijksdienst en heeft betrekking op de beveiliging van een organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten. In het Vir worden regels gesteld ten aanzien van de integriteit, exclusiviteit en beschikbaarheid van informatie bij de rijksdienst. Het Vir is in beginsel ook van toepassing op de beveiliging van staatsgeheimen. Specifieke regels ten aanzien van de beveiliging van bijzondere informatie, waaronder ook staatsgeheimen vallen, zijn neergelegd in het Vir-bi. Het Vir-bi bevat onder meer het need-to-know principe. Dit houdt in dat medewerkers (ook die van de diensten) alleen toegang krijgen tot informatie indien deze informatie noodzakelijk is voor de uitvoering van de opgedragen werkzaamheden. Door de beveiligingsambtenaar worden hierop controles uitgevoerd. Hierbij wordt onder meer gebruik gemaakt van de logging-gegevens van de computersystemen. Verder kent het Vir-bi voorschriften ten aanzien van de rubricering van staatsgeheimen, hun (fysieke) beveiliging, de organisatie omtrent de beveiliging van staatsgeheimen en voorschriften bij compromittering ervan. Gerubriceerde informatie mag alleen onder strenge voorwaarden buiten de gebouwen van de diensten, die een verboden plaats zijn in de zin van de Wet bescherming staatsgeheimen, gebracht worden. Daartoe behoort het hebben van een schriftelijke machtiging, registratie van de stukken, het op zo'n manier verpakken van de stukken dat compromittering direct onderkend wordt en de controle hierop door middel van visitaties bij in- en uitgang van het gebouw. Bij het verlaten van de dienst krijgen medewerkers een exit gesprek. In dit gesprek wordt onder verwijzing naar de wettelijke regeling terzake in de Wiv 2002 nogmaals gewezen op de geheimhoudingsplicht, in het bijzonder op het feit dat deze ook na beëindiging van het dienstverband voortduurt. De medewerker tekent (opnieuw) een geheimhoudingsverklaring.

De Wiv 2002 kent enkele specifieke vereisten ten aanzien van de beveiliging van informatie. Zo is vereist dat de verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze (artikel 12, derde lid, van de Wiv 2002) en dragen de hoofden van de diensten de verantwoordelijkheid voor de geheimhouding van daarvoor in aanmerking komende gegevens en bronnen waaruit gegevens afkomstig zijn (artikel 15, onder a en b, van de Wiv 2002). Tot slot vereist artikel 16, onder b, van de Wiv 2002 dat de hoofden van de diensten zorg dragen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking.

Het geldende beveiligingsbeleid van de AIVD dateert van 2006. Sinds de grote reorganisatie van 1991 zijn zowel de AIVD als zijn omgeving sterk veranderd. Dit betekent dat de eisen die aan de beveiliging worden gesteld ook aan verandering onderhevig zijn. Er zijn dan ook de nodige aanpassingen in het beleid geweest en in 2004 heeft de dienst vastgesteld dat er behoefte was aan een integraal geactualiseerd beveiligingsbeleid binnen de AIVD. Dit beleid wordt thans geïmplementeerd. De kern van dit beleid wordt gevormd door de volgende punten:

- Elke twee jaar zal worden getoetst of het handboek beveiliging bijstelling behoeft. Daarbij worden de lessen van eventueel opgetreden beveiligingsincidenten betrokken. Ook de ontwikkeling in de externe dreiging speelt daarbij een belangrijke rol door middel van zogenoemde kwetsbaarheidanalyses.
- Er zal externe controle van het beveiligingsbeleid gaan plaatsvinden. In dat kader toetst de auditdienst elke twee jaar het beveiligingsbeleid, inclusief de uitvoering daarvan. Ook kan periodiek of indien daartoe

aanleiding bestaat de beveiliging worden beoordeeld door een onafhankelijke externe deskundige.

- Tot slot is de positionering van de beveiligingsambtenaar in de organisatie gewijzigd. De dagelijkse uitvoering van het beveiligingsbeleid maakt onderdeel uit van de verantwoordelijkheden van het lijnmanagement. De beveiligingsambtenaar is niet langer verantwoordelijk voor veiligheidsonderzoeken en de beveiliging van het gebouw zoals vroeger wel het geval was. De beveiligingsambtenaar kan daardoor zijn toezichtstaak beter uitvoeren en beleid en uitvoering zijn gescheiden.

Tot slot willen wij in het kader van het onderwerp van de beveiliging van informatie bij de AIVD nog verwijzen naar de brief van 20 december 2006 die de minister van Binnenlandse Zaken en Koninkrijksrelaties de Tweede Kamer heeft gezonden over het Vir-bi onderzoek dat is uitgevoerd naar aanleiding van de publicaties in de Telegraaf.¹ In de brief worden maatregelen opgesomd om de beveiliging van informatie binnen de AIVD verder te verbeteren en de kans op herhaling van het in de openbaarheid geraken van geheime AIVD stukken te reduceren.

Door de leden van de SP-fractie wordt voorgesteld om eerst een integrale oplossing te zoeken voor de beveiligingsproblemen die door de journalisten aan het licht zijn gebracht, alvorens voort te gaan met het uitbreiden van bevoegdheden. De regering wil in dit verband ten eerste opmerken dat dit wetsvoorstel meer bevat dan een uitbreiding van bevoegdheden, aangezien het (vooral) ook gaat om de explicitering van bevoegdheden van de diensten. Daarnaast wil de regering benadrukken, en hierover is vele malen met het parlement gesproken, dat zij (de dreiging van) terrorisme met kracht wil bestrijden. Kortom, het zou de regering te verwijten zijn als de diensten niet worden uitgerust met de middelen die daarvoor noodzakelijk zijn. De regering acht het daarom wenselijk dat de voorstellen, gedaan in dit wetsvoorstel, gerealiseerd worden. Hierbij is het uiteraard van groot belang dat de beveiliging van informatie van een meer dan adequaat niveau is. Zoals in de memorie van toelichting wordt betoogd en ook in paragraaf 3 van deze nota uiteen wordt gezet, zijn de nieuwe voorstellen inzake gegevensverwerking noodzakelijk voor de goede taakuitvoering van de diensten, in het bijzonder daar waar het betreft de bestrijding van terrorisme en radicalisme. De regering is niet van mening dat verdere uitbreiding van bevoegdheden inzake gegevensverwerking door de diensten inhoudt dat gegevens nog gemakkelijker in de handen van onbevoegden kunnen vallen, zoals door de leden van de fractie van de SP wordt opgemerkt. De uitbreiding van de bevoegdheden wordt namelijk gekoppeld aan strikte beveiligingsvoorschriften. Te denken valt dan aan beveiligingsmaatregelen inzake cryptografie, protocollering van gegevensbevragingen en te hanteren autorisatiesystemen. Verder verwijzen wij naar de hierboven beantwoorde vraag van de leden van de fractie van de VVD waarin wordt ingegaan op het integraal geactualiseerd beveiligingsbeleid van de AIVD. Op de vraag van de leden van de SP-fractie inzake de stand van zaken betreffende de plannen, de voortgang van de uitvoering en de voltooiing van de evaluatie van de beveiliging verwijst de regering naar de reeds eerder genoemde brief van 20 december 2006 aan de Tweede Kamer.

Een tweede punt waaraan de leden van de SP-fractie refereren, is het rapport van de Commissie bestuurlijke evaluatie AIVD. De leden van de SP-fractie willen weten of de waarborgen voor de kwaliteit van de informatie zijn verbeterd en of de kwaliteit van de informatie dienovereenkomstig hoger is. In antwoord hierop kunnen wij u het volgende melden. De verschillende projecten van het ontwikkelprogramma *Prospect 2007* van de AIVD, waarover de Tweede Kamer bij brief is geïnformeerd, verhogen

¹ Kamerstukken II, vergaderjaar 2006–2007, 29 876, nr. 20.

gezamenlijk de kwaliteit van de dienstproducten en houden rekening met een goede borging in de organisatie van deze kwaliteitsverbetering.¹ Het kwaliteitssysteem van de dienst is bovendien opnieuw bezien om zorg te dragen dat de toetsende rol ten aanzien van informatiekwaliteit binnen de organisatie goed belegd is en adequate methoden en technieken worden gehanteerd. Nieuwe samenwerkingsovereenkomsten en een gestructureerd relatiebeheer (door middel van *key account management*) maken het daarnaast mogelijk dat de AIVD beter in staat is om tijdig te reageren op veranderende verwachtingen en percepties bij samenwerkingspartners.

2. Algemene toelichting op de wijzigingsvoorstellen

De leden van de PvdA-fractie vragen aan welke *situaties* moet worden gedacht, waarin is gebleken dat de Wiv 2002 óf onnodig beperkend is óf onvoldoende expliciet bij de toepassing van de in de wet geregelde (bijzondere) bevoegdheden. Het zal deze leden duidelijk zijn dat de regering in antwoord op deze vraag niet met concrete voorbeelden kan komen, aangezien daarmee zicht zou (kunnen) worden gegeven op zowel (concrete) operationele activiteiten van de dienst als de daarbij gehanteerde (concrete) modus operandi. Niettemin kan wel in algemene zin omtrent de situaties waarop deze leden met hun vraagstelling doelen, het volgende worden opgemerkt. Waar het gaat om situaties waarbij sprake is van een *onnodige beperking* terzake van de toepassing van de in de Wiv 2002 geregelde bijzondere bevoegdheid, wordt in het bijzonder gewezen op de bevoegdheid van de inlichtingen- en veiligheidsdiensten om, indien noodzakelijk, zelf handelend op te treden. Deze bijzondere bevoegdheid (het bevorderen of treffen van maatregelen ter bescherming van door de dienst te behartigen belangen; artikel 21, eerste lid, onderdeel b) is thans gekoppeld aan de inzet van een natuurlijke persoon als bedoeld in artikel 21 van de Wiv 2002 (zogenoeten «agent»), die terzake instructies kan ontvangen. Dat kan in de praktijk een beperking opleveren, met name indien – zoals in de memorie van toelichting is uiteengezet – het voor het treffen of bevorderen van maatregelen niet nodig is deze te doen plaatsvinden in het kader van de bijzondere bevoegdheid ex artikel 21 van de Wiv 2002, te weten de inzet van natuurlijke personen, maar ook kan worden volstaan met de inzet van dienstmedewerkers die niet als zodanig zijn ingezet; daarbij moet bijvoorbeeld worden gedacht aan (verstoring) acties in de sfeer van internet.

Met de herformulering van deze bijzondere bevoegdheid en het onderbrengen in een nieuw hoofdstuk 3a (overige bijzondere bevoegdheden van de diensten) wordt tevens beoogd de beperkingen die thans aan de inzet van deze bevoegdheid kleven – in de parlementaire behandeling van de huidige Wiv 2002 werd de toepassing van deze bevoegdheid gekenschetst met de term «ultimum remedium» – weg te nemen. Weliswaar is het verwerken van gegevens door de diensten in het kader van de nationale veiligheid de primaire taak van de diensten, maar erkend moet worden dat actief handelen door de diensten ter bescherming van de door de diensten te behartigen belangen in ruimere mate – uiteraard onder strikte condities zoals de vereisten van proportionaliteit en subsidiariteit – moet kunnen plaatsvinden. Gewezen wordt onder andere op het treffen van maatregelen in de preventieve sfeer die voorwaardenscheppend zijn voor het op een adequate wijze onder controle krijgen en houden van targets, maar ook ter ondersteuning van gegevensverwerving. Het is in dit verband voorts goed om er op te wijzen dat in het kader van het ontwikkelprogramma Prospect 2007 van de AIVD (zie hiervoor ook paragraaf 1), dat mede naar aanleiding van het rapport van de commissie bestuurlijke evaluatie AIVD (commissie Havermans) in gang is gezet, vier vermogens worden onderscheiden, te weten het onderzoekend, duidend,

¹ Kamerstukken II, vergaderjaar 2004–2005, 29 876, nr. 4.

mobiliserend en handelend vermogen. De bevoegdheid tot het bevorderen of treffen van maatregelen als hier bedoeld vormt de grondslag voor het handelend vermogen van de dienst, dat erop gericht is om, als de (inter)nationale veiligheid dat vraagt, zelfstandig dreigingen te reduceren.

Waar het gaat om de situaties waarbij de wet *onvoldoende expliciet* is, wordt – zoals in de memorie van toelichting is aangegeven – met name bedoeld op de situaties waarbij sprake is van door de diensten gehanteerde methodieken van gegevensverwerking, zoals data-analyse, en de mogelijkheden tot het verkrijgen (c.q. verlenen) van rechtstreeks geautomatiseerde toegang tot bepaalde gegevensbestanden, maar waarbij het bestaan van die mogelijkheden nog onvoldoende uit de tekst van de wet kan worden afgeleid. Het gaat – voor de goede orde – in beide gevallen derhalve niet om het creëren van nieuwe bevoegdheden; de in de toelichting geschetste vormen van data-analyse worden immers al geruime tijd in de praktijk toegepast en gelegitimeerd door (de) artikel(en) 12 (en 13) van de Wiv 2002 en voorts hebben de diensten ook al rechtstreeks geautomatiseerde toegang tot verschillende gegevensbestanden. Het gaat er in casu om beter voor een ieder kenbaar en voorzienbaar te doen zijn, ook in het licht van de eisen die nationaalrechtelijk en internationaalrechtelijk aan de verwerking van persoonsgegevens in relatie tot het recht op bescherming van de persoonlijke levenssfeer worden gesteld, dat dergelijke vormen van gegevensverwerking door de diensten (kunnen) worden toegepast. Voorts wordt waar het gaat om het expliciteren in de wet zelf van de mogelijkheid tot rechtstreeks geautomatiseerde toegang tot gegevensbestanden – vergelijk de voorgestelde wijziging van de artikelen 17, 61 en 62 – tegemoet gekomen aan de wens uit de praktijk om de onduidelijkheid die op dit punt (blijkbaar) bestaat, door expliciete vermelding ervan in de wet, weg te nemen. Het voorgaande geldt evenzeer voor de mogelijkheid tot het beschikbaar stellen van (delen van) geautomatiseerde gegevensbestanden aan de diensten.

De leden van de PvdA-fractie vragen, in verwijzing naar de memorie van toelichting, naar het soort gevallen waaraan moet worden gedacht wanneer door de regering wordt aangegeven dat in een aantal gevallen de afhankelijkheid van louter vrijwillige medewerking niet meer wenselijk is. Daarnaast is het de leden van de fractie van de PvdA niet duidelijk welke problemen zich tot nu toe hebben voorgedaan bij de vrijwillige verstrekking. De regering wil hierover graag het volgende opmerken. Zonder hier concrete voorbeelden te noemen, aangezien ook in deze gevallen bronbescherming geldt, kan worden gesteld dat het niet zozeer gaat om weigerachtigheid; de AIVD constateert in de praktijk bij de personen en instanties die worden benaderd met het oog op verstrekking van gegevens een toenemende bereidheid om aan de dienst gegevens (bestanden) te verstrekken c.q. toegang tot gegevens verlenen. Wat echter wel problematisch is, is dat het hier telkens afspraken zijn met *afzonderlijke* instanties en derhalve niet met alle vergelijkbare entiteiten als geheel. Om een voorbeeld te geven: een afspraak met een enkele luchtvaartmaatschappij die op land x vliegt om bepaalde passagiersgegevens te verstrekken, terwijl er nog enkele andere luchtvaartmaatschappijen zijn die ook op land x vliegen, brengt met zich mee dat het doel waarvoor deze gegevens worden gevraagd en noodzakelijk zijn (bijvoorbeeld nagaan of een bepaald «target» die in het kader van de bestrijding van terrorisme in beeld is gekomen, zich naar land x begeeft) slechts ten dele kan worden gerealiseerd en er dus een hiaat bestaat welke tot onaanvaardbare risico's kan leiden (namelijk dat hij onopgemerkt met een andere luchtvaartmaatschappij naar land x vliegt). Het gegeven voorbeeld maakt duidelijk om welke reden het wenselijk is om niet te volstaan met een afspraak met een enkele instantie, maar dat het soms noodzakelijk is om de gehele desbe-

treffende categorie in de gegevensverstrekking te betrekken. Dit zou – zo geven we toe – wellicht ook gerealiseerd kunnen worden door het maken van afspraken met elk van de afzonderlijke partijen – hetgeen veel tijd kan gaan vergen –, maar een sluitend en dekkend systeem (per categorie uiteraard) vereist wel dat dan ook echt met *alle* partijen tot overeenstemming wordt gekomen. Dat is echter nooit op voorhand zeker. Indien echter wordt vastgesteld dat een goede taakuitvoering van de diensten met zich meebrengt dat bepaalde gegevens die bij bepaalde personen en instanties berust van een dusdanig belang zijn dat zij voor de diensten onder bepaalde voorwaarden beschikbaar zouden moeten komen, dan achten we het onder die omstandigheden aangewezen om te komen tot het opleggen van een daartoe strekkende informatieverplichting. Een dergelijke informatieverplichting biedt de desbetreffende personen en instanties rechtszekerheid, ook richting hun klanten. Het moge evident zijn dat indien tot toepassing van de bevoegdheid tot aanwijzing van (categorieën) bestuursorganen, vervoerders en financiële dienstverleners wordt overgegaan, waarin het wetsvoorstel voorziet, daaraan een weloverwogen beslissing ten grondslag dient te liggen die gedragen dient te worden door de noodzaak om voor een goede taakuitvoering over de desbetreffende gegevens te kunnen beschikken. Dit zal in de toelichting bij de algemene maatregel van bestuur waarmee die aanwijzing wordt gerealiseerd, beargumenteerd dienen te worden (uiteraard met inachtneming van het geheimhouden van de operationele werkwijze van de diensten). Uit de praktijk blijkt daarnaast dat personen of instanties die in het bezit zijn van informatie die van belang is in het kader van de nationale veiligheid, deze in sommige gevallen weigeren te verstrekken of slechts verstrekken na langdurige onderhandelingen, omdat de wet dat niet verplicht. Voor de diensten die zich regelmatig in situaties bevinden waarin op korte termijn gehandeld moet worden, is dit een onwenselijke situatie. Ook is het zo dat de informatie die wordt aangeleverd niet altijd volledig is, terwijl dit bijvoorbeeld in het kader van data-analyse wenselijk is. Tot slot kan het ook zo zijn dat de hoogte van de vergoeding die een leverancier van specifieke informatiebestanden vraagt aan de diensten voor het aanbieden van gegevens in de weg staat aan het verkrijgen van bepaalde informatie. De regering acht het bijzonder onwenselijk dat hierdoor de diensten niet beschikken over informatie die in het kader van hun taakuitvoering wel benodigd zou zijn. Voor de verstrekking van informatie door bestuursorganen aan de AIVD en de MIVD is in artikel 17a, vierde lid, van dit wetsvoorstel bepaald dat dit (in beginsel) kosteloos geschiedt. Voor financiële dienstverleners en vervoerders zal gelden dat er vergoeding zal plaatsvinden van de daadwerkelijke kosten¹. Ook om deze redenen acht de regering, gezien de noodzaak die er kan zijn om als dienst te beschikken over bepaalde informatie, het invoeren van een verstrekkingverplichting voor enkele specifieke categorieën wenselijk. Volledigheidshalve wordt in dit verband opgemerkt dat naast de informatieverplichtingen zoals deze volgen uit de artikelen 17a, 29a en 29b voor de diensten altijd de mogelijkheid openstaat om op grond van artikel 17 van de Wiv 2002 zich te wenden tot specifieke personen en instanties met het verzoek op (op vrijwillige basis) gegevens te verstrekken.

De leden van de VVD-fractie vragen – in relatie tot de wens van een dekkend stelsel van verplichte gegevensverstrekking, hetgeen deze leden als zodanig onderschreven – of, en in welke mate, thans sprake is van een belemmering van de goede taakuitvoering van de diensten en of niet volstaan zou kunnen worden met een verzoek tot (vrijwillig) verstrekken van gegevens. Voorts vragen zij of de regering kan aangeven in hoeveel gevallen niet aan een dergelijk verzoek tegemoet wordt gekomen en in hoeverre dit de goede taakuitvoering schaadt. Ook merken zij op dat de regering niet overtuigend heeft aangetoond dat de informatieverplichtingen noodzakelijk en proportioneel zijn voor de goede taakuitvoering

¹ In paragraaf 5 van deze nota wordt nader ingegaan op het begrip «daadwerkelijke kosten».

van de diensten. Deze leden zouden wij allereerst willen verwijzen naar ons antwoord op deels vergelijkbare vragen van de zijde van de leden van de fractie van de PvdA. Zoals aldaar gesteld: het gaat in beginsel niet om weigerachtigheid aan de zijde van de personen en instanties, maar om de noodzaak in voorkomende gevallen te kunnen beschikken over de gegevens die bij de desbetreffende instanties – en daarmee wordt bedoeld *alle* desbetreffende instanties – berusten. Dit laatste dient naar ons oordeel primair het uitgangspunt te zijn bij het opleggen van een informatieverplichting. Indien er geen noodzaak bestaat om een informatieverplichting op te leggen, kan worden volstaan met vrijwillige medewerking, hetgeen – zoals ook in de memorie van toelichting is aangegeven – waar het gaat om de verstrekking van gegevens aan inlichtingen- en veiligheidsdiensten in zijn algemeenheid, uitgangspunt is. Bestaat er wel voldoende reden om tot het opleggen van een informatieverplichting te komen – zoals al sinds jaar en dag het geval is in de telecommunicatiesector – dan brengt de eis van rechtsgelijkheid naar ons oordeel met zich mee dat deze informatieverplichting dan ook voor alle tot een bepaalde categorie behorende instanties geldt; op deze wijze wordt tegelijkertijd verzekerd dat er sprake is van een dekkend stelsel van informatieverplichtingen. De beantwoording van de vraag of het opleggen van een specifieke informatieverplichting aan bepaalde instanties noodzakelijk en proportioneel is, is een vraag die pas in concreto aan de orde komt bij de aanwijzing van (categorieën van) bestuursorganen (artikel 17a), financiële dienstverleners en vervoerders (artikel 29a). Genoemde wetsartikelen creëren immers slechts de bevoegdheid om bij algemene maatregel van bestuur tot aanwijzing van daarbij nader te duiden instanties over te gaan, een en ander onder de gelijktijdige verplichting daarbij bepaalde onderwerpen te regelen (zoals welke gegevens, de termijn van gegevensverstrekking en de wijze van gegevensverstrekking). Is eenmaal tot een dergelijke aanwijzing gekomen, dan verbindt de wet daaraan de plicht voor de desbetreffende instantie om de gegevens desgevraagd te verstrekken. In dit kader wil de regering het volgende opmerken over de *proportionaliteit* van de voorgestelde informatieverplichtingen: een informatieverplichting is naar zijn aard een bevoegdheid die minder ingrijpend is in de persoonlijke levenssfeer van burgers dan het verkrijgen van gegevens door middel van de toepassing van andere bijzondere bevoegdheden zoals de inzet van agenten of het aftappen van gesprekken met een technisch hulpmiddel. Het (wettelijk) uitgangspunt van de werkzaamheden van de diensten dat bij de inzet van bijzondere bevoegdheden dat middel wordt ingezet dat proportioneel en subsidiair is, wordt daarmee door de informatieverplichtingen ondersteund.

Waar het gaat om de *noodzaak* om in de wet de hier bedoelde wettelijke grondslag tot aanwijzing en de daarmee corresponderende informatieplicht te creëren, wordt het volgende opgemerkt. Zowel in de overheids-sfeer als in de niet-overheids-sfeer worden grote hoeveelheden gegevens verwerkt die voor een goede taakuitvoering van de diensten *van substantieel belang* kunnen zijn. In beginsel is elk gegeven dat in beide sferen beschikbaar is en dat – toegespitst op de taak van de AIVD – bij kan dragen aan het realiseren van de taakstelling van de AIVD, waaronder in het bijzonder het tijdig onderkennen van (ongekende) dreigingen van de democratische rechtsorde, de veiligheid en andere gewichtige belangen van de staat, voor de AIVD van belang. Dat het «van belang» is, betekent echter niet automatisch dat het desbetreffende gegeven voor de dienst ook daadwerkelijk beschikbaar komt. Er bestaat op dit moment immers slechts een beperkt aantal informatieverplichtingen; gewezen wordt op de informatieverplichtingen in de artikelen 61 en 62 van de Wiv 2002 alsmede de al sinds jaar en dag bestaande informatieverplichtingen voor de aanbieders van openbare telecommunicatienetwerken en -diensten (artikelen 28 en 29 Wiv 2002 jo. de artikelen 13.2a en 13.4 van de

Telecommunicatiewet). Waar het gaat om de informatie die beschikbaar is bij de genoemde aanbieders van telecommunicatienetwerken en -diensten zal thans niemand het nut en de noodzaak van de desbetreffende gegevens voor een goede taakuitvoering van de diensten alsmede de verplichting om deze te verstrekken betwisten. Daar komt bij – niet onbelangrijk – dat dergelijke gegevens bij afwezigheid van een vrijwillig arrangement waarbij alle aanbieders¹ zouden zijn betrokken dan wel bij afwezigheid van een verplichting tot verstrekking anders niet dan wel slechts met onevenredige inspanningen zoals de inzet van (andere²) bijzondere bevoegdheden beschikbaar zouden kunnen komen. De inzet van dergelijke bijzondere bevoegdheden – zoals het binnendringen in geautomatiseerde werken («hacken») (bijvoorbeeld de computercentrales van dergelijke aanbieders) – is echter om diverse redenen in deze context niet goed uitvoerbaar. De noodzaak om de gegevens als hier bedoeld beschikbaar te krijgen ziet immers op een veelvoud van personen en instanties (duizenden, zo niet tienduizenden per jaar), waarbij de heimelijke inzet van (andere) bijzondere bevoegdheden zoals hiervoor aangeduid als een relatief zwaar middel (met een door de schaal waarop deze ingezet zou moeten worden toegenomen mogelijkheid tot compromittering) moet worden aangemerkt. Overigens is de kans op mogelijke aantasting van de integriteit van een voor het functioneren van de maatschappij vitaal informatiesysteem door de toepassing van de desbetreffende bijzondere bevoegdheid hierbij niet louter theoretisch. Overwegingen als deze in de context van de telecommunicatiesector, zijn evenzeer van toepassing in de context van vervoer en financiële dienstverlening; beide zijn ook vitale sectoren voor het functioneren van onze maatschappij, waarbij sprake is van de inzet van geavanceerde informatiesystemen. De gegevens die in de sectoren vervoer en financiële dienstverlening worden verwerkt zijn – evenals de gegevens die in de telecommunicatiesector worden verwerkt – echter in almaar toenemende mate van belang voor een effectieve taakuitvoering van de diensten; bovendien gaat het ook daar om grote hoeveelheden van gegevens. Zoals in de memorie van toelichting is uiteengezet, gaat bij de onderzoeken die de diensten in het kader van de nationale veiligheid verrichten naar personen en organisaties de aandacht in het bijzonder uit naar het in kaart brengen van verschillende aspecten van het gedrag van personen en organisaties: identificatie, verplaatsing, communicatie en financiën. Dat gegevens die op dergelijke aspecten betrekking hebben van essentiële betekenis zijn voor een goede taakuitvoering door inlichtingen- en veiligheidsdiensten, wordt in de dagelijkse praktijk van de bestrijding van (internationaal) terrorisme bewezen. Om een aantal voorbeelden te noemen: het onderkennen van financiële transacties welke (mogelijk) strekken ter financiering van terroristische activiteiten, het onderkennen van financiers (onder meer met het oog op het bevriezen van hun tegoeden; nationaal en internationaal), het monitoren van het reisgedrag van (mogelijk) aan terroristische groeperingen gelieerde personen, het communicatiepatroon van dergelijke personen (onder meer nodig voor het in kaart brengen van een netwerk) enzovoort. Wat echter voor de bestrijding van terrorisme geldt, geldt evenzeer voor de andere (onderzoeks)terreinen waarop de inlichtingen- en veiligheidsdiensten actief zijn, zoals de proliferatie van massavernietigingswapens (en hun overbrengingsmiddelen). Gevoegd bij ontwikkelingen als globalisering en toenemende mobiliteit dienen de mogelijkheden voor inlichtingen- en veiligheidsdiensten om hun taakstelling te kunnen blijven realiseren daarop afgestemd te zijn. Met de in het wetsvoorstel voorgestelde regeling wordt dan ook de basis gelegd om op een effectieve en efficiënte (ook voor het bedrijfsleven) wijze te kunnen voorzien in de gegevens betreffende de eerdergenoemde aspecten die voor een goede taakuitvoering van de diensten noodzakelijk zijn. Over specifieke aantallen waarin er sprake is van weigeringen kunnen door de regering vanwege operationele redenen geen uitlatingen worden gedaan.

¹ Dan hebben we het over verzameling van enkele honderden aanbieders, welke door de ontwikkelingen in de markt aan voortdurende wijziging in samenstelling onderhevig is.

² Het opvragen van verkeersgegevens en gegevens betreffende naam, adres, postcode, woonplaats en soort dienst bij aanbieders van openbare telecommunicatienetwerken en -diensten is in de Wiv 2002 eveneens aangemerkt als een bijzondere bevoegdheid, die derhalve aan de wettelijk vastgelegde eisen van noodzakelijkheid, subsidiariteit en proportionaliteit dienen te voldoen (zie paragraaf 3.2.2 van de Wiv 2002).

De leden van de fractie van de ChristenUnie vragen ons om een nadere toelichting omtrent het feit dat hoewel vrijwillige arrangementen elk individueel voldoen, dit niet betekent dat zij als geheel voorzien in de informatie waaraan de diensten behoefte hebben. Deze leden worden allereerst verwezen naar hetgeen in reactie op een vergelijkbare vraag van de leden van de PvdA-fractie is gesteld. In aanvulling daarop wordt opgemerkt dat als wordt gesteld dat vrijwillige arrangementen elk individueel voldoen, dat louter betrekking heeft op de uitvoering van dat specifieke arrangement, maar dat daarmee nog niets gezegd wordt over de mate waarin in de totaal gevoelde informatiebehoefte wordt voorzien. Kort gezegd: indien er 5 luchtvaartmaatschappijen zijn die op land x vliegen en er met één luchtvaartmaatschappij een arrangement is overeengekomen, dan kan dat arrangement volstrekt naar tevredenheid zijn, maar daarmee is nog niet op een goede en toereikende wijze voorzien in de totale informatiebehoefte, namelijk wie vliegt naar land x. Er is aldus geen sprake van een dekkend systeem per categorie waardoor belangrijke informatie wordt gemist en de informatie die wel wordt verkregen slechts ten dele bijdraagt aan de informatiebehoefte. Met de voorgestelde regeling wordt dan ook hiervoor een oplossing geboden: de gehele categorie van personen en instanties waarbij de desbetreffende gegevens beschikbaar zijn, wordt door de informatieverplichting geraakt waardoor er geen hiaten optreden en de informatiebehoefte volledig wordt gedekt. Om in de gevoelde (totale) informatiebehoefte te kunnen voorzien kan, dit in reactie op de vraag van de leden van deze fractie waarom het vrijwillige karakter wordt vervangen door een verplichtende bepaling, uitsluitend worden gegarandeerd indien op voorhand verzekerd is dat een ieder die de desbetreffende informatie beschikt ook daartoe gehouden kan worden deze (desgevraagd) te leveren. Louter aanwijzen van instanties die over informatie beschikken die van essentiële betekenis is voor een goede taakuitvoering door de diensten en die deze vervolgens op grond van een verzoek ex artikel 17 van de Wiv 2002 op vrijwillige basis kunnen verstrekken heeft ten opzichte van de huidige situatie geen toegevoegde waarde; die toegevoegde waarde wordt juist ontleend aan het verplichtende karakter van de gegevensverstrekking.

De leden van de PvdA-fractie vragen of het in een algemene maatregel van bestuur regelen welke bestuursorganen en categorieën van personen en instanties verplicht zouden kunnen worden tot het verstrekken van informatie niet strijdig is met het uitgangspunt van goede wetgeving namelijk dat de reikwijdte van de wet in de wet zelf bepaald moet worden. Wij onderschrijven het uitgangspunt dat de reikwijdte van de wet in de wet zelf moet worden bepaald. Naar ons oordeel voldoet het wetsvoorstel aan dit vereiste. In de voorgestelde artikelen 17a en 29a zijn de buitengrenzen vastgelegd van de voorgenomen informatieverplichtingen voor enerzijds bestuursorganen en anderzijds categorieën personen en instanties werkzaam in de sfeer van financiële dienstverlening en vervoer. De gevallen waarin en de voorwaarden waaronder deze verplichting opgelegd zal kunnen worden, worden vervolgens nader ingevuld in een algemene maatregel van bestuur. Hiermee zal dus niet buiten de kaders zoals deze in dit wetsvoorstel zijn vastgelegd getreden kunnen worden. Er is daarmee een duidelijk onderscheid aangebracht tussen de grondslag van de verplichting, die in de wet zelf is opgenomen, en de uitwerking van deze verplichting die aan de lagere regelgever wordt overgelaten. Het was denkbaar geweest een verplichting in het leven te roepen voor enerzijds alle bestuursorganen en anderzijds alle personen en instanties werkzaam in de sfeer van financiële dienstverlening en vervoer zonder meer. Zo geldt er op basis van de huidige wet (artikel 28 en 29 in samenhang met hoofdstuk 13 van de Telecommunicatiewet) een verplichting voor alle aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. Daarmee zou evenwel de kring van personen

en organisaties waarop een verplichting kan komen te rusten onnodig ruim getrokken worden. Immers lang niet alle bestuursorganen, financiële dienstverleners en vervoerders beschikken over informatie die van zodanig belang geacht kan worden voor de inlichtingen- en veiligheidsdiensten dat een informatie*verplichting* noodzakelijk wordt gevonden. Daarbij merkt de regering op dat het opleggen van informatieverplichtingen beperkt dient te worden tot de gevallen waarin dit met het oog op de goede taakuitvoering van de diensten noodzakelijk wordt geacht; de in de wet neergelegde regeling biedt de mogelijkheid dit effectief te realiseren waarbij tevens op flexibele wijze kan worden gereageerd op tussentijdse ontwikkelingen in de genoemde sectoren.

De leden van de PvdA-fractie vragen om een toelichting bij de lange duur van de studie naar de vraag of de AIVD onderzoek moet doen naar te benoemen ministers en nieuwe leden van het Koninklijk Huis, nu is komen vast te staan dat voor een dergelijke bevoegdheid veel parlementaire steun bestaat. In de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties van 24 januari 2005 (Kamerstukken II 2004/2005, 29 876, nr. 3) wordt aangegeven dat het kabinet de suggestie van de Commissie bestuurlijke evaluatie AIVD om een formele bevoegdheid vorm te geven op basis waarvan een onderzoek naar te benoemen ministers en nieuwe leden van het Koninklijk Huis mogelijk wordt, nader zal onderzoeken. Dit onderzoek is inmiddels afgerond. Over de uitkomsten ervan zal de Kamer separaat geïnformeerd worden.

3. Inhoud van het wetsvoorstel: bespreking van een aantal hoofdonderdelen van het wetsvoorstel

3.1. Verplichte gegevensverstrekking door bestuursorganen alsmede door personen en instanties die beroeps- of bedrijfsmatig werkzaam zijn in de financiële sector of in de sector vervoer

3.1.1. Algemeen

De leden van de PvdA-fractie vragen of het in de memorie van toelichting gegeven voorbeeld dat veiligheidsdiensten «geen of slechts na onderhandeling, toegang (...) kunnen krijgen» tot bepaalde gegevens een voorbeeld is dat zich in de praktijk heeft voorgedaan. In antwoord op deze vraag wordt opgemerkt dat – behoudens het relatief beperkt aantal gevallen waarbij een informatieverplichting bestaat ten opzichte van inlichtingen- en veiligheidsdiensten – de verstrekking van gegevens aan de diensten volledig afhankelijk is van vrijwillige medewerking van de zijde van de personen en instanties die over voor de diensten relevante gegevens beschikken. Dat betekent dat indien de diensten de gegevens die bij deze personen en instanties beschikbaar zijn, willen verkrijgen, aan die personen en instanties een daartoe strekkend verzoek (op grond van artikel 17 van de Wiv 2002) zal worden gericht, waarna – afhankelijk van de aard van de reactie (instemmend, afwijzend, twijfelend e.d.) – een proces op gang komt van overleg, nadere toelichting en onderhandeling (onder welke voorwaarden, technisch, financieel enz.) een verstrekking mogelijk is c.q. kan worden gerealiseerd. Een dergelijk proces vergt over het algemeen gezien – inclusief de implementatie – relatief veel tijd en inspanningen bij beide partijen. Terugkerende vraagstukken daarbij vormen die betreffende de juridische grondslag van de verstrekking, de aansprakelijkheid ten opzichte van hun klanten en – soms – het voorkomen van «imagoschade» indien bekend zou worden dat men gegevens verstrekt aan een inlichtingen- en veiligheidsdienst. Terechte zorgen naar ons oordeel, die echter met een wettelijke informatieverplichting – welke zelfs door sommige instanties wordt geprefereerd vanwege de duidelijkheid die dat schept, ook richting hun klanten – grotendeels worden

weggenomen. In aanvulling op het voorgaande verwijst de regering naar de beantwoording van de vragen inzake de informatieverplichtingen in paragraaf 2 van deze nota, in het bijzonder de antwoorden op vragen van de leden van de fractie van de PvdA.

De leden van de PvdA-fractie vragen in hoeverre er voor bestuursorganen, andere instanties en personen een rechtsmiddel open staat om tegen een verzoek tot verplichte gegevensverstrekking op te komen. De regering antwoordt hierop het volgende. Tegen een verzoek om verstrekking van gegevens als zodanig staat geen rechtsmiddel open. Artikel 91 van de Wiv 2002 bepaalt dat de Algemene wet bestuursrecht niet van toepassing is op de voorbereiding, totstandkoming en tenuitvoerlegging van besluiten op grond van (onder meer) hoofdstuk 3 van de Wiv 2002, het hoofdstuk waarin de voorgestelde informatieverplichtingen zijn opgenomen. Een weigering om te voldoen aan een verzoek om verplichte gegevensverstrekking zal ingevolge artikel 89, eerste lid, van Wiv 2002 strafbaar zijn. Indien een bestuursorgaan, instantie of persoon in verband hiermee vervolgd wordt, zal hiertegen op de gebruikelijke wijze verweer gevoerd kunnen worden.

De leden van de PvdA-fractie vragen voorts hoe de verplichting om gegevens te verstrekken zich verhoudt tot de Europese richtlijn met betrekking tot dataretentie. Allereerst wordt opgemerkt dat de dataretentierichtlijn (richtlijn 2006/24/EG, PB 2006, L105/54) ertoe strekt om de nationale bepalingen van de lidstaten, waarbij aan de aanbieders verplichtingen worden opgelegd inzake het bewaren van bepaalde telecommunicatiegegevens, 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. De richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke personen en rechtspersonen; dus niet op de inhoud van de communicatie. De in deze richtlijn geregelde bewaarplicht strekt ter facilitering van de opsporing en vervolging van ernstige strafbare feiten. Zoals in overweging 25 van de richtlijn is aangegeven, laat de richtlijn evenwel «het recht van de lidstaten onverlet om wetgevingsmaatregelen vast te stellen betreffende het recht op toegang tot en het gebruik door de nationale instanties die zij hebben aangewezen». Aspecten van toegang tot gegevens die door de nationale instanties worden bewaard ingevolge deze richtlijn voor doeleinden, zoals bedoeld in het eerste streepje van artikel 3, lid 2, van Richtlijn 95/46/EG¹, vallen niet onder de communautaire wetgeving. Dat betekent dat nationale instanties, zoals de AIVD en de MIVD, welke belast zijn met taken in het kader van de nationale veiligheid (staatsveiligheid), toegang kunnen hebben tot de gegevens die – als uitvloeisel van de implementatie van de dataretentierichtlijn in de nationale wetgeving – dienen te worden bewaard. Artikel 28 van de Wiv 2002 geeft de AIVD en de MIVD reeds de bijzondere bevoegdheid om bij aanbieders van openbare telecommunicatienetwerken en -diensten zogeheten verkeersgegevens (waaronder ook begrepen locatiegegevens) op te vragen; de aanbieders zijn op grond van artikel 13.2a van de Telecommunicatiewet verplicht aan een dergelijk verzoek te voldoen. De in het wetsvoorstel opgenomen wijziging van artikel 28 van de Wiv 2002 behelst op dit aspect geen wijziging ten opzichte van de huidige situatie. Waar nodig zal het op artikel 28 Wiv 2002 gebaseerde besluit, waarin een opsomming is opgenomen van de verkeersgegevens die door de aanbieders van openbare telecommunicatienetwerken en -diensten dienen te worden verstrekt, worden aangepast aan de in de bijlage bij de dataretentierichtlijn opgenomen lijst van verkeers- en locatiegegevens. Het nieuwe artikel 29b brengt echter wel met zich mee dat bij aanbieders van communicatiediensten (waaronder aanbieders van openbare telecommunicatienetwerken en -diensten zijn begrepen) onder stringente

¹ Het betreft richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (de zog. Algemene privacyrichtlijn). In artikel 3, lid 2, eerste streepje noemt als doeleinden (verwerkingen die betrekking hebben op): openbare veiligheid, defensie, de veiligheid van de Staat (waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van Staatsveiligheid), en de activiteiten van de Staat op strafrechtelijk gebied.

voorwaarden ook (delen van) een geautomatiseerd gegevensbestand zal (zullen) kunnen worden opgevraagd, welke men vervolgens ook verplicht is te verstrekken. Dit kan dus ook zien op (delen van) geautomatiseerde gegevensbestanden met verkeers- en locatiegegevens als bedoeld in de dataretentierichtlijn.

De leden van de fractie van de PvdA vragen, onder verwijzing naar bladzijde 6 van de memorie van toelichting waar staat dat er met diverse instanties convenanten zijn gesloten over het vrijwillig verstrekken van informatie, met welke instanties convenanten zijn gesloten. In antwoord hierop merkt de regering het volgende op. Daar waar in de huidige Wiv 2002 er slechts enkele informatieverplichtingen bestaan, streven de diensten er naar om door middel van convenanten met specifieke instanties ruimere toegang te krijgen tot informatie die noodzakelijk is in het kader van de taakuitvoering van de diensten. Deze convenanten worden met inachtneming van artikel 17 van de Wiv 2002, dus op basis van vrijwilligheid, gesloten. Instanties die informatie verstrekken aan de diensten zijn – ook indien dit geschiedt op basis van artikel 17 – aan te merken als bron van een dienst en hebben om die reden recht op bronbescherming. Uitzondering hierop zijn die afspraken (convenanten) die gepubliceerd zijn in de Staatscourant. Als voorbeeld hiervan kan genoemd worden het convenant dat de AIVD en de IND hebben gesloten inzake de uitwisseling van gegevens.¹

De leden van de fractie van de SP merken op dat de verplichte verstrekking van gegevens aan de inlichtingen- en veiligheidsdiensten een begrijpelijke maatregel is; zij missen echter een toetsingskader om te bezien of de verstrekking wel proportioneel is en verzoeken de regering om een dergelijk kader voor te stellen en bij nota van wijziging in de wet vast te leggen. De regering merkt hierover het volgende op. Het opnemen van een toetsingskader wordt niet noodzakelijk geacht nu een dergelijk kader reeds in de wet is opgenomen. De Wiv 2002 stelt strenge voorschriften aan gegevensverwerking in het kader van de nationale veiligheid. Zo eist in algemene zin artikel 12, tweede lid, dat de verwerking van gegevens slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede taakuitvoering van de Wiv 2002 of de Wet veiligheidsonderzoeken. Daar waar het gaat om de inzet van bijzondere bevoegdheden, en informatieverplichtingen aan commerciële dienstverleners vallen in deze categorie, regelt artikel 31, vierde lid, van de Wiv 2002 bovendien expliciet dat de uitoefening van de bevoegdheid evenredig dient te zijn aan het daarmee beoogde doel (ergo proportioneel). Deze wettelijke eisen worden geconcretiseerd in de interne procedures binnen de diensten en worden telkens toegepast indien de inzet van een bevoegdheid wordt overwogen. Hiernaast geldt dat de commissie van toezicht onderzoek kan doen naar het rechtmatig handelen van de diensten; hieronder vallen ook afwegingen inzake proportionaliteit.

3.1.3. Verplichte verstrekking van gegevens door aan te wijzen categorieën van personen en instanties in de sectoren financiële dienstverlening en vervoer

De leden van de fractie van het CDA vragen de regering waarom niet wordt aangesloten bij het begrip financiële dienstverlener zoals dat recent tot stand is gekomen bij de Wet financiële dienstverlening. Het begrip financiële dienstverlener is ontleend aan het vergelijkbare begrip in de Wet vorderen gegevens financiële sector (deze wet is inmiddels vervangen door de Wet vorderen gegevens). Het begrip dient ruim geïnterpreteerd te worden en ziet op alle instellingen die in de financiële sector werkzaam zijn, met uitzondering van de financiële toezichthouders. Reden om voor deze uitleg van het begrip financiële dienstverlener te

¹ Staatscourant 19 juni 2003, nr. 115, p. 13.

kiezen is dat het wenselijk is dat de Wiv 2002 een ruimere bepaling kent van dit begrip dan in de Wet financiële dienstverlening die immers categorieën van dienstverleners buiten het bereik van de wet plaatst, zoals geldtransactiekantoren.

In de memorie van toelichting (blz. 11) wordt, aldus de leden van de fractie van de PvdA, ingegaan op de te leveren gegevens door vervoerders. Deze leden zouden graag een nadere toelichting ontvangen op het type gegevens dat hier wordt bedoeld. Bij het type gegevens dat in relatie tot vervoerders in beeld komt moet men onder meer denken aan gegevens betreffende personen die worden vervoerd (bijvoorbeeld passagierslijsten van vliegtuigen op bepaalde landen en plaatsen), reisbestemmingen van personen, de wijze waarop het vervoer is betaald en dergelijke. Zoals in de memorie van toelichting is uiteengezet, gaat het in casu echter primair om gegevens die zicht bieden op het verplaatsingsgedrag van personen die in onderzoek zijn bij één van de diensten. Overigens wordt opgemerkt dat in het kader van de voorbereiding van de algemene maatregel van bestuur, waarbij de categorieën van vervoerders zullen worden aangewezen, maar dit geldt evenzeer voor de aan te wijzen bestuursorganen en de aan te wijzen categorieën van financiële dienstverleners, er thans binnen de diensten een precieze inventarisatie plaatsvindt, waarbij tegelijk aandacht moet worden besteed aan de door de leden van de VVD opgeworpen vragen van noodzakelijkheid en proportionaliteit. Deze vragen zullen te zijner tijd hun beantwoording (dienen te) krijgen in de toelichting op de eerder genoemde algemene maatregel van bestuur waarbij de diverse instanties zullen worden aangewezen. Gelet op het voorgaande is het dan ook in dit stadium nog niet mogelijk om deze afwijking per aan te wijzen bestuursorgaan of categorie te verschaffen.

De leden van de VVD-fractie vragen of artikel 29b van het wetsvoorstel zo moet worden uitgelegd dat een dienst banken kan verplichten het gehele klantenbestand, met de door hen verrichte betalingen, te verstrekken om bijvoorbeeld inzicht te krijgen in het betalingsverkeer tussen personen/instellingen uit Nederland met een specifiek derde land. De regering merkt hier in algemene zin het volgende over op. Aangezien een verzoek om informatie ex artikel 29b bestempeld moet worden als de inzet van een bijzondere bevoegdheid, zal een dergelijk verzoek altijd moeten voldoen aan de vereisten van proportionaliteit en subsidiariteit (artikel 31 van de Wiv 2002). Verder mogen gegevens slechts verwerkt worden voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede taakuitvoering van de Wiv 2002 (artikel 12 van de Wiv 2002). Voorts zal het opvragen van een (deel) van het bestand als bedoeld in artikel 29b uitsluitend mogelijk zijn indien de minister naar aanleiding van een daartoe strekkend gemotiveerd verzoek van het hoofd van de dienst persoonlijk daarvoor toestemming heeft gegeven. Voor deze bijzondere bevoegdheid geldt dus dezelfde zware toestemmingseis als bij het aftappen en opnemen van iemands (tele)communicatie. Er zijn derhalve adequate waarborgen aanwezig om te voorkomen dat verzoeken tot verstrekking van geautomatiseerde gegevensbestanden lichtvaardig plaatsvinden. Op de rechtmatige uitoefening van deze bevoegdheid ziet voorts de onafhankelijke commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten toe, die – zoals uit de sinds haar instelling uitgebrachte toezichtsrapporten blijkt – deze taak uitermate consciëntieus pleegt uit te voeren. Onder verwijzing naar de beantwoording van de vragen van de leden van de PvdA hierboven wordt verder opgemerkt dat in het kader van de voorbereiding van de algemene maatregel van bestuur momenteel een precieze inventarisatie plaatsvindt van de aan te wijzen categorieën financiële dienstverleners, wat betekent dat er in de genoemde algemene maatregel van bestuur nadere precisering zal plaatsvinden. Toegespitst op het concrete voorbeeld dat door de leden van de VVD-fractie wordt

genoemd, is – *in het geval dat de in voorbereiding zijnde algemene maatregel van bestuur gaat voorzien in aanwijzing van de desbetreffende categorie van financiële dienstverleners (bankinstellingen) alsmede in de gegevens waaraan in het gegeven voorbeeld wordt gerefereerd* – het inderdaad mogelijk dat, met inachtneming van de hiervoor geschetste waarborgen, de verstrekking van de desbetreffende gegevens kan worden verlangd. Echter pas bij de definitieve vaststelling van de algemene maatregel van bestuur zal duidelijk zijn welke categorieën van personen en instanties worden aangewezen alsmede welke gegevens het betreft.

De leden van de fractie van de VVD vragen of voor de AIVD geldt, net als voor bepaalde politiegegevens, dat in sommige gevallen aan derden, particuliere organisaties zoals beveiligingsbedrijven, gegevens mogen worden verstrekt. De regering merkt hierover het volgende op. Voor een dienst bestaat de mogelijkheid om gegevens te verstrekken aan particuliere instanties wanneer dit noodzakelijk is voor de goede taakuitvoering. Artikel 36, eerste lid, onder c, van de Wiv 2002 biedt hiervoor de rechtsgrondslag. Hierbij kan gedacht worden aan het informeren van een bedrijf of persoon ten opzichte waarvan of van wie door een dienst een dreiging is geconstateerd. Voor het verstrekken van gegevens geldt, net als bij de informatieverplichtingen, dat de wet als hoofdregel stelt dat dit mogelijk is indien het noodzakelijk is voor de goede taakuitvoering van een dienst. Daarnaast biedt de Wiv 2002 tevens de mogelijkheid gegevens aan het openbaar ministerie te verstrekken indien bij de verwerking van gegevens door of ten behoeve van een dienst blijkt van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten (artikel 38) en aan bij AMvB aangewezen personen of instanties die betrokken zijn bij de uitvoering van een publieke taak (artikel 39). Belangrijke uitgangspunten als bronbescherming en geheimhouding van de operationele werkwijze van een dienst behouden hierbij hun volledige gelding.

3.1.4. De beschikbaarstelling van geautomatiseerde gegevensbestanden (artikel 29b (nieuw)) door bestuursorganen en de op grond van artikel 29a, eerste lid, aangewezen categorieën van personen en instanties

De leden van de fractie van de PvdA vragen of met «het doorzoeken aan de hand van profielen of het vergelijken van gegevens met het oog op patronen» datamining en profiling wordt bedoeld. Hierop kan geantwoord worden dat de regering juist uitdrukkelijk heeft vermeden vage verzameltermen als datamining en profiling in dit wetsvoorstel op te nemen om te voorkomen dat er onduidelijkheid bestaat over de reikwijdte van deze bevoegdheden van de diensten. De drie in artikel 12a, tweede lid, neergelegde vormen van bestandsanalyse, te weten het op geautomatiseerde wijze onderling met elkaar vergelijken dan wel in combinatie met elkaar vergelijken, het doorzoeken aan de hand van profielen en het vergelijken met het oog op het opsporen van bepaalde patronen, zijn noodzakelijk voor een adequaat gevulde gereedschapskist van de diensten. Met dergelijke vormen van bestandsanalyse worden immers de mogelijkheden om niet op het eerste gezicht kenbare dreigingen voor de nationale veiligheid en daaraan te relateren personen te ontdekken, vergroot. Opgemerkt dient te worden dat het natuurlijk wel zo is dat de termen datamining en profiling in het spraakgebruik zo gebezigd worden. Gezien de hoeveelheid geautomatiseerde gegevens die de diensten tegenwoordig ontvangen, zijn deze vormen ook om een andere reden noodzakelijk; een «handmatige» analyse van de gegevens is door de grote hoeveelheid informatie eenvoudigweg niet mogelijk en de inzet van de computer is daarom onontbeerlijk. Voor de volledigheid wordt opgemerkt dat de in artikel 12a genoemde vormen van data-analyse reeds een deugdelijke wettelijke grondslag kennen en reeds in de praktijk worden toege-

past, maar dat de regering een expliciete wettelijke normering wenselijk heeft geacht om de redenen zoals uiteengezet in de memorie van toelichting.

De leden van de fractie van de PvdA verzoeken de regering in kaart te brengen welke risico's er verbonden zijn aan geautomatiseerde data-analyse. Hierop kan geantwoord worden dat de vormen van data-analyse zoals deze in artikel 12a, tweede lid, zijn neergelegd geen risico's met zich meebrengen. Het resultaat van een van deze vormen van data-analyse heeft namelijk geen beslissende rol binnen een dienst maar slechts een adviserende en ondersteunende. Op basis van informatie uit data-analyse of in combinatie met dergelijke informatie zal verder onderzoek moeten plaatsvinden waarbij altijd de daadwerkelijke brongegevens gecontroleerd zullen worden en vervolgstappen onderbouwd moeten worden, in het bijzonder daar waar het betreft de proportionaliteit en de subsidiariteit van het handelen van een dienst. Het resultaat van de data-analyse biedt «slechts» de grondslag voor verdere analyse en waardering door een dienst en elk besluit om daaraan enig handelen te koppelen zal gebaseerd zijn op een menselijke afweging.

De leden van de fractie van de PvdA ontvangen tot slot graag toelichting over de beveiliging van gegevens die de diensten kunnen verwerven, evenals op het aspect van de koppeling van diverse gegevensbestanden. De regering verwijst voor de wijze waarop gegevens die bij een dienst berusten, worden beveiligd naar haar uiteenzetting hierover in paragraaf 1. Waar het gaat om de beveiliging van gegevens die op grond van de artikelen 29a of 29b dienen te worden verstrekt, wordt opgemerkt dat – hoewel niet als zodanig wettelijk voorgeschreven – bij de algemene maatregel van bestuur de in acht te nemen beveiligingsbepalingen zullen worden gespecificeerd. Op basis van het huidige artikel 17, derde lid, (het nieuwe artikel 17, vierde lid) jo. artikel 29a, zevende lid en artikel 29b, zesde lid, geldt bovendien dat de verstrekende personen of instanties niet gehouden zijn aan hun protocolleringsverplichtingen. Dit om te voorkomen dat derden – bijvoorbeeld via de weg van inzageverzoeken – op de hoogte kunnen komen van verstrekkingen aan de diensten. Aanvullend kunnen met de verstrekende partners afspraken gemaakt worden over bijvoorbeeld afscherming van logbestanden en encryptie van dataverkeer. In dit kader vindt ook de aanwijzing van vertrouwensfuncties plaats in overleg met de betrokken ministers. Voor wat betreft de beveiliging van de gegevens aan de kant van de verstrekker wordt het volgende opgemerkt: voor die gegevens geldt dat die in vrijwel alle gevallen aan te merken zijn als persoonsgegevens die – voor zover daar geen eigen specifiek aanvullend wettelijk kader voor is getroffen zoals bijvoorbeeld voor de sector telecommunicatie – onder de werking van de Wet bescherming persoonsgegevens vallen. Ingevolge artikel 13 van die wet – en een vergelijkbare plicht komt ook in sectorale wetgeving voor – is de verantwoordelijke voor de gegevensverwerking – naast specifieke wettelijke verplichtingen die een verantwoord omgaan met zogeheten gevoelige gegevens normeren – verplicht om passende technische en organisatorische maatregelen te treffen ter beveiliging van de gegevens tegen verlies of enige vorm van onrechtmatige verwerking. Voor de goede orde wordt opgemerkt dat voor zover het gaat om door de diensten aan de verstrekker van de gegevens verstrekte gegevens (bijvoorbeeld de naam van een persoon met het oog op het opvragen van daarop betrekking hebbende gegevens) ter zake van deze gegevens en de uiteindelijke gegevensverstrekking door de desbetreffende verstrekker de wettelijke geheimhoudingsplicht ex artikel 85 van de Wiv 2002 van toepassing is. Wanneer er sprake is van online koppeling dan zal in ieder geval vereist zijn dat het gaat om een beveiligde verbinding. De regering wil in dit verband nog benadrukken dat de mogelijkheid van bestandslevering aan de diensten, wanneer wordt

gesproken over de beveiliging van informatie, in specifieke gevallen van toegevoegde waarde kan zijn. Immers de bestandsbevragingen, die vaak als staatsgeheim kunnen worden bestempeld, kunnen in een dergelijk geval plaatsvinden binnen de beveiligde omgeving van de systemen van de AIVD en MIVD.

3.2. Wijziging van de artikelen 28 en 29 in verband met de uitbreiding van de reikwijdte tot aanbieders van communicatiediensten

De leden van de fractie van de PvdA vragen om toelichting van het begrip «besloten netwerken en diensten». Besloten netwerken en diensten zijn netwerken en diensten die niet voor eenieder (het algemene publiek) toegankelijk zijn en slechts kunnen worden gebruikt door een beperkte kring van gebruikers. De criteria die een aanbieder stelt, zijn dan zodanig dat het niet aan eenieder vrij staat om van de diensten gebruik te maken. Gedacht kan worden aan bedrijfsnetwerken van een concern en zogenoemde gesloten gebruikersgroepen.

De leden van de VVD-fractie erkennen de toegevoegde waarde van een wettelijke verplichting tot verstrekking van informatie, maar menen dat de helderheid, kenbaarheid en voorzienbaarheid niet gediend zijn met een bepaling die verwijst naar een nader te bepalen algemene maatregel van bestuur. Zij achten een dergelijke carte blanche onwenselijk en dringen aan op een nadere toelichting. De regering acht het wenselijk hierover het volgende op te merken. De voorbereidings- en totstandkomingsprocedure van een algemene maatregel van bestuur is met diverse waarborgen omgeven, waaronder verplichte advisering door de Raad van State. Daar komt bij dat het omtrent een besluit als het onderhavige gebruikelijk is het Overlegorgaan Post en Telecommunicatie te consulteren. Ook is relevant hier op te merken dat de reikwijdte van de in artikel 28, eerste lid, opgelegde verplichting tot verstrekking van (verkeers)gegevens niet verder kan gaan dan waarover de desbetreffende aanbieders in het kader van hun bedrijfsvoering beschikken; uit de in de wet verankerde verplichting en de (niet limitatieve) explicitering van gegevens in het besluit als bedoeld in artikel 28, tweede lid, volgt dus niet dat – indien de gegevens niet voorhanden zijn – men deze dient te vergaren. Er is dan ook naar ons inzicht, anders dan de leden van de VVD-fractie aangeven, geen sprake van een carte blanche. Overigens wijzen wij deze leden erop dat de in artikel 28 (nieuw) voorgestelde systematiek – namelijk dat van een wettelijke vastgelegde informatieverplichting met nadere uitwerking daarvan bij algemene maatregel van bestuur – reeds in het huidige artikel 28 van de Wiv 2002 is neergelegd, zij het dat anders dan in de huidige situatie – om redenen die in de memorie van toelichting zijn uiteengezet (blz. 16) – de algemene maatregel van bestuur niet meer voor alle aanbieders limitatief aangeeft welke gegevens op grond van artikel 28 kunnen worden opgevraagd. De hier bedoelde algemene maatregel van bestuur – het Besluit ex artikel 28 van de Wiv 2002 – bestaat overigens al en zal ingevolge artikel II van het wetsvoorstel op (het nieuwe) artikel 28, tweede lid, komen te berusten. In het bestaande besluit wordt waar het gaat om de aanbieders van vaste en mobiele telefonie alsmede internettoegang (de bestaande categorie van aanbieders van openbare telecommunicatienetwerken en -diensten) wel limitatief omschreven welke gegevens onder de in artikel 28, eerste lid, opgenomen verstrekingsverplichting vallen. Zoals in de memorie van toelichting is aangegeven, zal dit besluit al naar gelang meer duidelijkheid ontstaat met betrekking tot de gegevens die betrekking hebben op de nieuwe vormen van communicatiediensten daarmee worden aangevuld. Overigens zal in het Besluit ex artikel 28 van de Wiv 2002 worden verduidelijkt dat de thans opgenomen opsomming van gegevens betrekking heeft op de aanbieders van openbare telecommunicatienetwerken en -diensten.

Daarnaast vragen de leden van de fractie van de VVD de regering wanneer deze nauwkeurig uitgewerkte en omschreven algemene maatregel van bestuur, waarop dan later eventueel wijzigingen of uitbreidingen kunnen worden aangebracht, te verwachten is. Zoals wij hiervoor reeds hebben aangegeven bestaat deze algemene maatregel van bestuur (het Besluit ex artikel 28 van de Wiv 2002) reeds en zal deze naar gelang de ontwikkelingen in de praktijk worden aangepast.

De leden van de fractie van de VVD vragen of de regering bereid is om de algemene maatregel van bestuur aan een voorhangprocedure voor de Kamer te onderwerpen. Volgens aanwijzing 35 van Aanwijzingen voor de regelgeving wordt in de wet geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving geregeld tenzij daarvoor bijzondere redenen bestaan. Geconstateerd wordt allereerst dat – zoals hiervoor aangegeven – de desbetreffende algemene maatregel van bestuur reeds bestaat. Een eventuele voorhangprocedure zou dus betrekking hebben op mogelijke wijzigingen van deze algemene maatregel. Deze wijzigingen doen niet af aan de in artikel 28, eerste lid, neergelegde informatieverplichting; een wijziging van de algemene maatregel ziet slechts op explicitering van gegevens die – indien voorhanden – in ieder geval dienen te worden verstrekt. Al met al achten we mede gelet hierop geen bijzondere redenen aanwezig om deze algemene maatregel van bestuur aan een voorhangprocedure te onderwerpen.

De leden van de VVD-fractie vragen de regering om opheldering met betrekking tot de soorten gegevens en ten aanzien van de categorie van aanbieders van communicatiediensten, niet zijnde aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. De regering geeft aan dat bij algemene maatregel van bestuur deze gegevens voortaan kunnen worden aangewezen. Betekent dit dat ook gegevens die niet in de maatregel zijn genoemd, verstrekt dienen te worden? Het antwoord hierop is bevestigend. Zoals in artikel 28 is aangegeven, ziet deze verplichting op gegevens omtrent een gebruiker en op gegevens over het communicatieverkeer dat met betrekking tot die gebruiker voor of op het tijdstip van het verzoek heeft plaatsgevonden dan wel na dat tijdstip zal plaatsvinden. Het gaat dus niet om de inhoud van de communicatie. Voorts strekt de verplichting tot verstrekking van de gegevens zich slechts uit tot de gegevens die men reeds in het kader van de eigen bedrijfsvoering voorhanden heeft.

De leden van de ChristenUnie-fractie vragen in navolging van de Raad van State naar het feit dat de inhoud van het besluit ex artikel 28 van de Wiv 2002 nog niet volledig bekend is en naar de eisen van voorzienbaarheid en kenbaarheid. Binnen welke termijn zal de regering duidelijkheid geven over de mogelijke aanpassing van het besluit ex artikel 28 Wiv 2002? Zoals in antwoord op vragen van de leden van de fractie van de VVD reeds is aangegeven, zal ingevolge artikel II van het wetsvoorstel het bestaande Besluit ex artikel 28 na inwerkingtreding van het wetsvoorstel gehandhaafd blijven en komen te berusten op artikel 28, tweede lid. Het verstrekkingstelsel voldoet daarmee in ieder geval wat betreft de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten aan de vereisten van voorzienbaarheid en kenbaarheid. Zoals aangegeven in de memorie van toelichting zal zodra ten aanzien van (nieuwe vormen van) communicatiediensten is uitgekristalliseerd welke gegevens voorhanden zijn en welke daarvan voor een goede taakuitvoering van de inlichtingen- en veiligheidsdiensten noodzakelijk zijn, het Besluit ex artikel 28 Wiv 2002 daarmee worden aangevuld.

3.3. Overige bijzondere bevoegdheden van de diensten (nieuw hoofdstuk 3a)

3.3.1. Inleiding

De leden van de fractie van de PvdA vragen de regering aan te geven waarom het «bij nader inzien wenselijk is geacht om een onderscheid te maken tussen bijzondere bevoegdheden die wel en geen betrekking hebben op het verzamelen van gegevens». Aan het voorstel tot aanpassing van de Wiv 2002 op dit punt liggen wetstechnische redenen ten grondslag. De bijzondere bevoegdheden van de diensten kunnen in twee categorieën worden onderscheiden, te weten bevoegdheden die gericht zijn op het verzamelen van gegevens en bevoegdheden die dat niet zijn. Veruit het grootste deel van de bijzondere bevoegdheden kan slechts worden ingezet ten behoeve van het verzamelen van gegevens. Slechts voor de bevoegdheid tot het oprichten en de inzet van rechtspersonen en de bevoegdheid tot het bevorderen of treffen van maatregelen geldt dit niet. Voorgesteld wordt om de systematiek van de Wiv 2002 dusdanig aan te passen dat dit onderscheid helder wordt gemaakt, waardoor het doel om de bevoegdheid in te zetten direct kenbaar is.

3.3.2. De oprichting en de inzet van rechtspersonen

De leden van de fractie van het CDA vragen of uitgelegd kan worden waarom bij de inzet van rechtspersonen de duur van een onderzoek maatgevend is voor de toestemming, terwijl dit bij de inzet van natuurlijke personen niet het geval is. Hiervoor geldt het volgende. De aard van de bijzondere bevoegdheid tot inzet van een agent leent zich ervoor dat op regelmatige basis wordt overwogen of de inzet van deze bevoegdheid nog steeds voldoet aan alle wettelijke vereisten zoals die van proportionaliteit en subsidiariteit. Gevolg van de uitoefening van deze bevoegdheid kan zijn dat inbreuk wordt gemaakt op de persoonlijke levenssfeer van personen die in onderzoek zijn bij een dienst. Een agent begeeft zich immers veelal in die levenssfeer en op regelmatige basis dient te worden bezien of dit in het licht van de gestelde eisen – zoals hiervoor aangegeven – nog aangewezen is. Dit is anders bij het oprichten en inzetten van rechtspersonen. Het oprichten van een rechtspersoon is een eenmalige (rechts)handeling, waarbij nog geen relatie hoeft te bestaan met concrete operationele activiteiten; zoals in de memorie van toelichting is aangegeven moeten reeds rechtspersonen kunnen worden opgericht ter voorbereiding op operationele activiteiten. De vraag van de leden van de CDA-fractie ziet dan ook meer in het bijzonder op de besluitvorming tot inzet van een rechtspersoon en de voortzetting daarvan in een onderzoek. De inzet van een rechtspersoon strekt primair ter ondersteuning van operationele activiteiten van een dienst. Anders dan bij de inzet van een agent wordt met de toepassing van deze bevoegdheid als zodanig geen inbreuk gemaakt op de persoonlijke levenssfeer van personen. Een periodieke heroverweging en toestemmingsverlening heeft vanuit deze optiek bezien dan ook geen betekenis.

De leden van de SP-fractie vragen of het zo is dat door een dienst opgerichte rechtspersonen als neporganisaties kunnen fungeren om in bepaalde milieus te infiltreren en verzoeken in algemene zin om de reden voor deze bevoegdheid. Rechtspersonen kunnen om meerdere redenen worden opgericht. Zo kan met behulp van een rechtspersoon de noodzakelijke afscherming plaatsvinden van de identiteit van operationele medewerkers van de diensten, de voertuigen en de communicatiemiddelen. Een rechtspersoon kan soms noodzakelijk zijn om de geloofwaardigheid van een aangenomen identiteit te ondersteunen door te kunnen beschikken over bijvoorbeeld een postadres. In een enkel geval dient een

rechtspersoon ertoe om in een staatsgevaarlijke organisatie te kunnen infiltreren. Welke onderzoeksterreinen en welke organisaties het hier betreft kan om operationele redenen, de regering verwijst hierbij terug naar de inleiding, uiteraard niet worden gedeeld. Voor de volledigheid wordt opgemerkt dat het hier om een reeds bestaande bevoegdheid gaat, welke cruciaal is voor een goede taakuitvoering door de diensten.

3.3.3. Het bevorderen of treffen van maatregelen

Naar aanleiding van de voorstellen van de regering inzake het bevorderen of treffen van maatregelen wordt door de leden van de fractie van de PvdA gevraagd naar een toelichting op het soort maatregelen dat getroffen of bevorderd mag worden. Opgemerkt wordt dat het hier niet slechts om een bevoegdheid gaat die ter verstoring van bepaalde activiteiten kan worden ingezet, maar ook om andere redenen. Bij het bevorderen of treffen van maatregelen gaat het er steeds om een bepaalde anti-democratische of staatsgevaarlijke activiteit of een activiteit gericht tegen één van de andere in de Wiv 2002 genoemde belangen te ontmoedigen of in de kiem te smoren met als uiteindelijk doel (preventief) te voorkomen dat de ermee gepaard gaande risico's werkelijkheid worden. De handelingen kunnen verschillende vormen aannemen, zoals het in een bepaalde kring verspreiden van desinformatie of het frustreren van voorgenomen gewelddadige acties. Met de in dit wetsvoorstel opgenomen regeling wordt ook buiten kijf gesteld dat onder het toepassingsgebied van deze bijzondere bevoegdheid tevens wordt begrepen de mogelijkheid om technische hulpmiddelen aan te wenden ten behoeve van het bevorderen of treffen van maatregelen. Hierbij kan gedacht worden aan maatregelen in de sfeer van het internet. Om te voorkomen dat zicht wordt gegeven op de werkwijzen van de diensten acht de regering het niet gewenst dat meer specifieke voorbeelden van maatregelen worden genoemd. In ieder geval geldt dat in artikel 44c, tweede lid, de artikelen 31, derde en vierde lid en 32 van overeenkomstige toepassing worden verklaard. Dit betekent dat de inzet van de bevoegdheid altijd proportioneel en subsidiair moet zijn en niet lichtvaardig zal worden toegepast.

4. Artikel 8 EVRM en artikel 10 Grondwet

De vraag van de leden van de fractie van de PvdA of het College Bescherming Persoonsgegevens (CBP) om advies is gevraagd over het gebruik van persoonsgegevens in dit wetsvoorstel moet negatief worden beantwoord. De Wet bescherming persoonsgegevens (Wbp) is op grond van artikel 2, tweede lid, aanhef en onder b, van die wet niet van toepassing op de verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002. De in artikel 51, tweede lid, van de Wbp opgenomen verplichting om advies te vragen aan het CBP is hierdoor ten aanzien van het onderhavige wetsvoorstel niet van toepassing. Ook de vraag of de regering alsnog bereid is om advies te vragen, zoals de leden van de fracties van de PvdA en de ChristenUnie vragen, moet negatief worden beantwoord. De regering ziet hiertoe geen noodzaak. De gegevensverwerking zoals deze in het onderhavige wetsvoorstel is geregeld, valt immers buiten de kaders van de Wbp en het toezicht van het CBP.

5. Administratieve lasten

De leden van de fractie van het CDA vragen naar het verschil tussen de door de Raad van State voorgestelde garantie voor een volledige kostenvergoeding bij gegevensverstrekking door niet-bestuursorganen en de door de regering in het wetsvoorstel opgenomen daadwerkelijke kosten.

Ook de leden van de fractie van de PvdA vragen op dit punt opheldering. Voorts vragen zij of uitgelegd kan worden wat dat in financiële zin betekent. Onder daadwerkelijke kosten worden verstaan de personeels- en administratiekosten (met inbegrip van de kosten die worden gemaakt om een rekening in te dienen) die een dienstverlener maakt om tegemoet te komen aan een concreet verzoek om informatie. Door te kiezen voor de *daadwerkelijke* kosten wordt aangesloten bij het bestaande systeem van vergoedingen voor de verplichte gegevensverstrekking voor aanbieders van openbare telecommunicatienetwerken en -diensten, waarvoor artikel 13.6, tweede lid, van de Telecommunicatiewet een regeling biedt. Op grond van dat artikel worden eveneens uitsluitend de door de genoemde aanbieders gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan – onder meer – een verzoek om gegevensverstrekking op grond van de Wiv 2002 uit 's-Rijks kas vergoed. Onder *volledige* kosten worden verstaan alle kosten die een organisatie maakt om aan verzoeken om informatie te kunnen voldoen. Hieronder vallen dus niet alleen de administratie- en personeelskosten die voortvloeien uit het voldoen aan een concreet verzoek, maar ook alle overige kosten die worden gemaakt om te kunnen voldoen aan dergelijke verzoeken, zoals de kosten verbonden aan de inrichting van de organisatie, waarbij moet worden gedacht aan aspecten als bereikbaarheid, beveiliging en gekwalificeerd personeel. In financiële zin betekent dit dat volledige kostenvergoeding meer kostenelementen omvat en ook hoger zal uitvallen. Daar komt bij dat ingeval van een systematiek van volledige kostenvergoeding de kosten per organisatie erg uiteen kunnen gaan lopen en een bron voor juridische disputen kan opleveren, met name indien niet precies is omlijnd wat dan wel of niet onder *volledige kosten* dient te worden verstaan.

De regering kan zich volledig vinden in de opmerkingen van de leden van de VVD-fractie dat confidentiële informatie die aan de diensten op rechtstreeks geautomatiseerde wijze wordt verstrekt de uiterste beveiliging behoeft en de grootste voorzorgsmaatregelen dienen te worden getroffen. Voor de wijze waarop deze informatie wordt beveiligd, verwijst de regering naar zijn opmerkingen in paragraaf 1 en paragraaf 3.1.4. In aanvulling daarop en in antwoord op de vraag van de leden van deze fractie of de desbetreffende diensten beschikken over de technische beveiligingsmaatregelen en kennis om dit proces van verstrekking van gegevens op rechtstreekse geautomatiseerde wijze veilig te laten verlopen, reageren wij zonder meer bevestigend.

De leden van de fractie van de VVD vragen de regering of er onderzoek is verricht naar de administratieve lasten die de informatieverplichtingen voor vervoerders en financiële dienstverleners ten gevolge zullen hebben. De artikelen 29a en 29b, waarin de verstrekkingsverplichtingen voor nader bij algemene maatregel van bestuur aan te wijzen categorieën van vervoerders en financiële dienstverleners zijn neergelegd, genereren als zodanig nog geen administratieve lasten. Pas bij de uitvoeringsmaatregelen, die op dit moment worden voorbereid, zal dit het geval zijn. Om de administratieve lasten te kunnen kwantificeren, dient duidelijkheid te bestaan omtrent verschillende parameters, zoals bijvoorbeeld de omvang van de aan te wijzen categorie, de gegevens waarop de verplichting betrekking heeft en de tijd die men kwijt is om aan een informatieverzoek te voldoen. Deze gegevens dienen dan ook bij de voorbereiding van de uitvoeringsmaatregelen in kaart te worden gebracht. De ontwerp algemene maatregel van bestuur alsmede de daaraan verbonden gevolgen voor de administratieve lasten zullen overeenkomstig de geldende regels aan het Adviescollege toetsing administratieve lasten worden voorgelegd. Voor wat betreft de gevraagde toelichting van de leden van de VVD-fractie op het verschil tussen de gemaakte kosten en de volledige vergoeding

van de kosten, verwijzen wij deze leden naar hetgeen eerder in deze paragraaf daaromtrent is gesteld. Voor de vraag van de leden van de fractie van de VVD naar de gevolgen van de extra lasten die bijvoorbeeld de Nederlandse luchtvaartmaatschappijen zullen worden opgelegd voor hun concurrentiepositie binnen de Europese markt verwijst de regering naar het antwoord in deze paragraaf over de administratieve lasten van dit wetsvoorstel.

ARTIKELEN

Artikel 1

B

De leden van de VVD-fractie vragen welke vorm van controle er bestaat op de toestemmingsverlening door het hoofd van een dienst voor het zich bedienen van een aangenomen identiteit of hoedanigheid door een ambtenaar van een dienst met het oog op hun persoonlijke veiligheid. Aan de toestemmingsverlening door het hoofd van een dienst ligt een interne procedure ten grondslag. Centrale vraag daarin is of de persoonlijke veiligheid van de medewerker een maatregel als in artikel 10a is voorzien rechtvaardigt. Van een concrete toestemming van het hoofd van de dienst wordt in beginsel geen afschrift aan de desbetreffende minister – voor de AIVD de minister van Binnenlandse Zaken en Koninkrijksrelaties en voor de MIVD de minister van Defensie – gezonden. Uiteraard zal de verantwoordelijke minister- gevraagd en ongevraagd – omtrent de toepassing van de in artikel 10a opgenomen regeling worden geïnformeerd. Controle op de rechtmatige uitvoering van artikel 10a is ingevolge artikel 64, tweede lid, van de Wiv 2002 belegd bij de onafhankelijke commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten.

C, D en E

Door de leden van de VVD-fractie wordt de vraag gesteld of er een verslag- of protocolplicht bestaat in het geval er vrijwillig data of geautomatiseerde gegevensbestanden worden verstrekt aan een dienst. Voor de kant van de verstrekker van de informatie geldt hierbij dat als gevolg van het huidige artikel 17, derde lid, (het nieuwe artikel 17, vierde lid) de verstreckende personen of instanties niet gehouden zijn aan hun protocoleringsverplichtingen. Dit om te voorkomen dat derden – bijvoorbeeld via de weg van inzageverzoeken – op de hoogte kunnen komen van verstrekkingen aan de diensten. Anders dan bij de verplichte verstrekking van gegevens op grond van de artikelen 28, 29, 29a en 29b geldt bij vrijwillige verstrekking van gegevens aan de kant van de diensten geen wettelijke vastgelegde verslagplicht zoals deze is neergelegd in artikel 33 van de Wiv 2002. Niettemin geldt in dit geval wel dat alle gegevens die door de diensten worden verwerkt, dienen te zijn voorzien van een aanduiding van de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 12, vierde lid, van de Wiv 2002).

F

De leden van de fractie van de VVD vragen wie binnen de diensten toegang heeft tot geautomatiseerde gegevensbestanden die via rechtstreeks geautomatiseerde toegang voor een dienst toegankelijk zijn. Tevens vragen zij of er geen sprake zal zijn van structurele inzage, verwerking en analyse van gegevens. De regering merkt het volgende op. Binnen de diensten wordt gewerkt op basis van het «need to know» principe (dit

beginsel is neergelegd in artikel 35 van de Wiv 2002). Dit houdt in dat een persoon slechts toegang heeft tot bepaalde informatie als dat in het kader van zijn taakuitvoering noodzakelijk is. Dit betekent dat een persoon niet automatisch toegang heeft tot bepaalde informatie, maar dat hij hiervoor moet worden geautoriseerd. Op beperkte schaal worden er permanente geautomatiseerde bewerkingen uitgevoerd op binnenkomende gegevensstromen. Dit heeft te maken met de omvang van de gegevensstromen die de diensten in bepaalde gevallen ontvangen. De in artikel 12 neergelegde – algemene – eisen aan de verwerking van gegevens door de diensten zijn ook bij de hier bedoelde vormen van gegevensverwerking onverkort van toepassing. Dat houdt dus onder meer in dat de gegevensverwerking slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de wet. Voorts dat de verwerking geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze.

De VVD-fractie vraagt in hoeverre de regering meent dat constante data-analyse noodzakelijk is voor een goede taakuitvoering en dit voor de burgers wiens gegevens het betreft het ook duidelijk kenbaar en voorzienbaar is. Zoals de regering ook heeft opgemerkt in paragraaf 3.1.4. is het voor de AIVD en de MIVD heden ten dage absoluut noodzakelijk dat er geautomatiseerde analyse plaatsvindt op ontvangen (delen van) gegevensbestanden. Door middel van het onderling vergelijken dan wel in combinatie met elkaar vergelijken, het doorzoeken aan de hand van profielen en het vergelijken met het oog op het opsporen van bepaalde patronen worden immers de mogelijkheden om niet op het eerste gezicht kenbare dreigingen voor de nationale veiligheid en daaraan te relateren personen te ontdekken, vergroot. De hoeveelheid geautomatiseerde gegevens die de diensten tegenwoordig ontvangen, maken deze vormen van geautomatiseerde analyse ook om een andere reden noodzakelijk; een «handmatige» analyse van de gegevens is door de grote hoeveelheid informatie eenvoudigweg niet mogelijk en de inzet van de computer is daarom onontbeerlijk. Constante vormen van data-analyse zijn, op beperkte schaal weliswaar, noodzakelijk daar waar het gaat om informatie die van grote omvang is.

De leden van de fractie van de VVD vragen in hoeverre de regering heeft geanticipeerd op Europese wetgeving die in voorbereiding is, onder andere met betrekking tot de bescherming van gegevens en het «beschikbaarheidsprincipe». De regering interpreteert deze vraag dusdanig dat de fractie van de VVD refereert aan het kaderbesluit data-protectie dat tot op heden niet is vastgesteld. In het wetsvoorstel is niet geanticipeerd op regelgeving terzake.

Met betrekking tot dit onderwerp vragen de leden van de fractie van de VVD tot slot een toelichting op de wijze van controle op de juiste uitoefening van bevoegdheden en de noodzakelijkheid van maatregelen in het kader van de goede taakuitvoering. Oefent – zo vragen deze leden – de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten toezicht uit door middel van periodieke steekproefcontroles, of oefent zij slechts in geval van aanwijzingen van onregelmatigheden toezicht uit. Wij wijzen erop dat het aan de commissie van toezicht is om te bepalen op welke wijze zij invulling geeft aan haar toezichthoudende taak. Zij kan daarbij kiezen voor één van de methodieken die door de leden van deze fractie worden geopperd, maar ook voor een andere methodiek. Overigens heeft de commissie van toezicht in haar eerste jaarverslag (2003/2004) uiteengezet op welke wijze zij invulling geeft aan haar taak en de wijze waarop zij haar onderzoeksactiviteiten vorm geeft.¹ Hierbij wijzen we erop dat naast de controle die door de commissie van toezicht wordt uitgeoefend, er ook nog andere controlemechanismen –

¹ Zie het jaarverslag van de commissie van toezicht over de periode 2003/2004 en de website van de commissie van toezicht www.ctivd.nl.

intern en extern – bestaan. Waar het gaat om externe controle wordt onder meer gewezen op de controle door het parlement, waaronder begrepen de commissie voor de inlichtingen- en veiligheidsdiensten, de Nationale ombudsman en de rechter. De regering verwijst in dit verband nog graag naar de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties bij het onderzoek naar democratische controlemechanismen op inlichtingen- en veiligheidsdiensten.¹ In het kader van de interne controle wordt volledigheidshalve opgemerkt dat er aan de kant van de diensten wordt bijgehouden dat geautomatiseerde data-analyse plaatsvindt (door middel van een logging systeem).

H, J, K, L en M

De leden van de VVD-fractie menen dat het onwenselijk is dat de AIVD zelf kan bepalen (niet alleen beoordelen of en in hoeverre, maar met gebruikmaking van de instemmingseis) of er interferentie met lopende onderzoeken van de AIVD is door MIVD-onderzoeken. Zij onderkennen dat deze beoordeling in de praktijk al wel altijd door het hoofd van de AIVD namens de minister van Binnenlandse Zaken en Koninkrijksrelaties geschiedt. Toch vragen deze leden de regering op welke wijze de betrokken minister met de interferentie bekend wordt gemaakt en of hij er nog controle (instemmingsvereiste) op uit kan oefenen. Zij geven de voorkeur aan de gebruikmaking van de rechterlijke toets en vragen daarom de regering dit aspect te heroverwegen. Wij antwoorden deze leden als volgt. Allereerst wijzen wij erop dat de hier voorgestelde wijziging geen betrekking heeft op het verlenen van toestemming voor de inzet van bijzondere bevoegdheden. Het gaat hier uitsluitend om een aanpassing, vooral in praktische zin, van de regeling die ten doel heeft te voorkomen dat er een ongewenste interferentie ontstaat tussen de onderzoeken die door de AIVD worden verricht en de onderzoeken die de MIVD wil gaan uitvoeren. Een dergelijke interferentie kan optreden als de MIVD bijzondere bevoegdheden uitoefent buiten plaatsen in gebruik van het ministerie van Defensie (zoals kazerneterreinen) of indien daar geen directe relatie mee bestaat, met andere woorden als de MIVD optreedt in de civiele maatschappij. Zowel de huidige als de voorgestelde regeling heeft ten doel de AIVD in de gelegenheid te stellen te beoordelen of en in hoeverre er interferentie met lopende onderzoeken van de AIVD optreedt. Voorkomen moet immers worden dat de diensten elkaar voor de voeten lopen. In de meest voorkomende situatie blijkt er geen interferentie te bestaan tussen het beoogde onderzoek van de MIVD en de lopende onderzoeken van de AIVD. In dat geval moet thans de minister van Binnenlandse Zaken en Koninkrijksrelaties expliciet instemmen met de door de minister van Defensie verleende toestemming tot het gebruik van de betreffende bijzondere bevoegdheid. De wettekst geeft immers aan dat de toestemming voor de inzet van de betreffende bijzondere bevoegdheid wordt verleend in overeenstemming met de minister van Binnenlandse Zaken en Koninkrijksrelaties. In het wetsvoorstel wordt deze formulering vervangen door de zinsnede: indien de minister van Binnenlandse Zaken en Koninkrijksrelaties of namens deze het hoofd van de AIVD daarmee heeft ingestemd. Dit betekent dat in het geval dat er geen interferentie optreedt de instemming van het hoofd AIVD volstaat en er geen noodzaak is de minister om instemming te vragen. Normaal gesproken zal er in deze gevallen ook geen noodzaak zijn de minister in te lichten over het feit dat er geen interferentie optreedt. In de gevallen dat er wel interferentie optreedt en er geen instemming verleend zal worden, kan er, afhankelijk van de ernst van het geval, uiteraard wel reden zijn de betrokken minister hierover te informeren. In de situatie dat op grond van het mandaatregime de minister van Defensie zelf de goedkeurende instantie is ten opzichte van de inzet van de bijzondere bevoegdheid en er wegens dreigende interferentie tussen de onderzoeken van de beide diensten geen

¹ Kamerstukken II, 2005–2006, 29 876, nr. 8.

instemming wordt verleend, zal er in de praktijk niets veranderen en wordt het besluit geen instemming te verlenen genomen door de Minister van Binnenlandse Zaken en Koninkrijksrelaties zelf, die daar dan ook de volledige controle op heeft. In de gevallen dat er door het hoofd AIVD namens de minister van Binnenlandse Zaken en Koninkrijksrelaties geen instemming wordt verleend, is het, evenals thans, altijd mogelijk de zaak toch naar het ministersniveau te tillen. Voor de door de leden van de VVD-fractie gesuggereerde rechterlijke toets zien wij in dit verband, waar het immers uitsluitend gaat om de onderlinge taakafstemming tussen de beide diensten, geen plaats. Bovendien past, zoals aangegeven in de memorie van toelichting bij de Wiv 2002, het vereiste van rechterlijke toestemming niet goed in het gekozen stelsel van volledige ministeriële verantwoordelijkheid (Kamerstukken II 1997/98, 25 877, nr. 3, blz. 37). Vanwege de geldende tekst van artikel 13 van de Grondwet kent de Wiv 2002 de rechterlijke toets uitsluitend in verband met de bijzondere bevoegdheid tot het openen van brieven en andere geadresseerde zendingen. Voor de uitoefening van alle overige bijzondere bevoegdheden door de diensten wordt de toestemming door of namens de politiek verantwoordelijke bewindspersoon verleend. Deze dient daarvoor immers, mede gelet op het karakter van de activiteiten van de diensten, volledig (politiek) aanspreekbaar te zijn. Wij zien geen aanleiding van dit stelsel af te wijken, noch bij het verlenen van toestemming voor de inzet van bijzondere bevoegdheden, noch bij de beoordeling van mogelijke interferentie tussen de onderzoeken van beide diensten.

L

De leden van de CDA-fractie lijken het wijzigingsvoorstel van de regering op artikel 25 zodanig te interpreteren dat nu de ontwikkelingen in de telecommunicatie zo snel gaan dat met het bestaande instrument van gegevensverstrekking door de telecommunicatieaanbieder in veel gevallen toch geen nummergegevens achterhaald kunnen worden, door ons zou worden voorgesteld gebruik te gaan maken van actieve scanapparatuur. In reactie hierop willen wij opmerken dat actieve scanapparatuur al sinds geruime tijd door de diensten wordt ingezet voor het doel waartoe ook de tekst van het huidige artikel 25, vijfde lid, van de Wiv 2002 dit toelaat, namelijk het verkrijgen van een nummer dat benodigd is om uitvoering te kunnen geven aan een afgegeven taplast. Zoals in de memorie van toelichting is aangegeven, komt de inzet van actieve scanapparatuur met name in beeld ingeval van pre paidbellers waarbij juist geen (identificerende) gegevens bij de aanbieder voorhanden zijn en het alternatief van bestandsanalyse om redenen van spoedeisendheid dan wel door gebrek aan voldoende gegevens om deze analyse uit te kunnen voeren geen reële optie is. De vraag van de leden van de fractie van het CDA of in de toekomst actieve scanapparatuur ook kan worden ingezet als een nummer via de aanbieder van een telecommunicatienetwerk kan worden verkregen, moet door de regering bevestigend worden beantwoord. Daarvoor zijn verschillende redenen aan te geven. Allereerst kan het best zo zijn dat via bestandsanalyse het nummer bij de aanbieder te achterhalen valt, maar zoals in de memorie van toelichting en hiervoor is aangegeven, kunnen zich situaties voordoen dat de voor die analyse benodigde gegevens – te weten gegevens betreffende de locaties waar en tijdstippen waarop de betrokken persoon onder gebruikmaking van zijn mobiele telefoon is gesignaleerd – in onvoldoende mate aanwezig zijn dan wel de spoedeisendheid van de situatie eraan in de weg staan om via observatie – dat enige tijd vergt – voldoende bruikbare gegevens te verkrijgen. Bij dit laatste is men overigens ook afhankelijk van de mate waarin door de betrokkene van een en hetzelfde nummer gebruik wordt gemaakt. Het is een gegeven dat personen die bij een dienst in onderzoek zijn regelmatig van mobiel toestel en nummer wisselen, als gevolg

waarvan uitsluitend door de inzet van actieve scanapparatuur op effectieve wijze de voor de uitvoering van de taplast benodigde nummergegevens kunnen worden verkregen.

M

De leden van de VVD-fractie menen met betrekking tot de voorgestelde verlenging van de in artikel 27, negende lid, opgenomen bewaartermijn dat inderdaad rekening dient te worden gehouden met de knelpunten die vanuit de praktijk kenbaar worden gemaakt. Naar aanleiding van de door deze leden gestelde vraag met betrekking tot de praktische consequenties van de verlenging van de bewaartermijn van één jaar naar drie jaren merken wij het volgende op. De in artikel 27, negende lid, geregelde bewaartermijn ziet op de gegevens die zijn verzameld door de uitoefening van de bevoegdheid, bedoeld in artikel 27, eerste lid (ongerichte interceptie van niet kabelgebonden telecommunicatie), voor zover zij niet zijn geselecteerd. In artikel 27, negende lid, is bepaald dat deze gegevens onder voorwaarden mogen worden bewaard voor een nadere selectie. Het gaat bij de in artikel 27, negende lid, opgenomen bewaartermijn om een bevoegdheid voor de diensten om dergelijke gegevens te bewaren, niet om een bewaarverplichting. Gebleken is echter dat in de praktijk die termijn als te kort wordt ervaren. In het toezichtsrapport inzake het onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen (CTIVD nr. 5a 2005, blz. 12 en 13), constateerde de commissie van toezicht dat de MIVD afwijkt van het voorschrift ex artikel 27, negende lid, Wiv 2002 in de zin dat gegevens ouder dan een jaar momenteel door de MIVD worden bewaard, zij het dat op deze gegevens geen selectie wordt toegepast en dus ook van de inhoud van de communicatie geen kennis wordt genomen. De commissie van toezicht achtte het noodzakelijk dat zo snel mogelijk wordt voorzien in een nadere wettelijke regeling, die het handelen van de MIVD met betrekking tot de vernietigingstermijn ex artikel 27, negende lid, Wiv 2002 zal legaliseren. In het overleg met de Tweede Kamer naar aanleiding van dit toezichtsrapport heeft de minister van Defensie aangekondigd dat de bewaartermijn zal worden verlengd naar drie jaar (Kamerstukken II 2005–2006, 29 876 en 29 924, nr. 14, blz. 8). De onderhavige wijziging betreft derhalve een noodzakelijk geachte voorziening die beter bij de huidige praktijk aansluit en om die reden niet tot majeure praktische consequenties zal leiden.

De leden van de VVD-fractie stelden de vraag of de gegevens «achter een schot» gaan om de privacy beter te beschermen en stelden dat dit wel het geval is met de bij de politie beschikbare gegevens. Als dit zo is, waar blijkt dan de mindere behoefte aan privacy uit bij de AIVD ten opzichte van de politie, zo vroegen de leden van de VVD-fractie. Naar aanleiding van deze vragen merken wij het volgende op. De in artikel 27, negende lid, geregelde bewaartermijn vormt een onderdeel van de in artikel 27 opgenomen regeling van een specifiek bij de diensten behorend werkproces dat uniek is ten opzichte van de politie en welke zich om die reden niet goed leent voor een vergelijking. Dit neemt niet weg dat het volgende kan worden opgemerkt met betrekking tot de privacywaarborgen terzake van de bewaarde gegevens. Ingevolge artikel 27, negende lid, is er een regeling inzake de nadere selectie van de bewaarde gegevens. De gegevens, bedoeld in artikel 27, negende lid, worden inderdaad afzonderlijk bewaard en kunnen worden gebruikt voor een nadere selectie, met dien verstande dat deze ten eerste slechts mag plaatsvinden in het kader van een onderzoek door een dienst op grond van een reden als bedoeld in het vierde lid, onder b, dan wel met betrekking tot een onderwerp als bedoeld in het vijfde lid, onder a, waarvoor op het moment van het ontvangen en opnemen van de desbetreffende gegevens toestemming was verleend, en ten tweede voor de goede uitoefening van het desbetreffende onderzoek dringend wordt gevorderd. Deze regeling zal ook bij de verlenging van de

bewaartermijn van één jaar naar drie jaar van toepassing blijven op de nadere selectie van de te bewaren gegevens.

Voor wat betreft het antwoord op de vraag van de leden van de VVD-fractie of in deze enorme hoeveelheden gegevens nog wel de juiste/benodigde gegevens kunnen worden teruggevonden, verwijzen wij naar de uiteenzetting welke indertijd bij de behandeling van de Wiv 2002 is gegeven in de toelichting op de nota van wijziging (Kamerstukken II 1999–2000, 25 877, nr. 9, blz. 26). Daar is indertijd uitgebreid ingegaan op het proces van (de nadere) selectie van door ongerichte interceptie verkregen gegevens.

De vraag van de leden van de VVD-fractie of de «oudere» gegevens kunnen worden gekoppeld aan de «nieuwe» rechtstreeks toegankelijke geautomatiseerde databestanden voor data-analyse vatten wij op als de vraag of de ingevolge artikel 27, negende lid, bewaarde gegevens onderwerp kunnen worden van de geautomatiseerde data-analyse, bedoeld in het nieuw voorgestelde artikel 12a. De gegevens, bedoeld in artikel 27, negende lid, zijn bulkgegevens welke zijn verkregen door ongerichte interceptie van niet kabelgebonden telecommunicatie (artikel 27, eerste lid) en welke niet zijn geselecteerd. Het selecteren van deze gegevens door de diensten geschiedt met toepassing van de regeling als bedoeld in artikel 27. Wanneer de gegevens op basis van de in artikel 27 geregelde toestemming zijn geselecteerd en het proces van artikel 27 is doorlopen, is het op zich denkbaar dat zij onderwerp zouden kunnen worden van een geautomatiseerde data-analyse als bedoeld in het voorgestelde artikel 12a.

In antwoord op de vraag hoe gegevens uit elkaar worden gehouden (gelet op het verloop van de termijn voor bewaring) als zij in eenzelfde systeem worden bewaard, merken wij op dat berichten bij interceptie worden gelabeld met een interceptiedatum. Op grond van deze interceptiedatum kunnen de berichten worden afgeschermd.

S, T en U

Wijziging artikel 62

De leden van de fractie van de VVD vragen de regering van welke informatie ambtenaren van de IND bij de uitoefening van hun functie kennisnemen die voor de AIVD of de MIVD van belang kan zijn in verband met de goede uitoefening van de aan de diensten opgedragen taken. Hierbij kan aan verschillende soorten informatie worden gedacht. Zo kan in een gehoor van een asielzoeker informatie naar boven komen die van belang is voor de nationale veiligheid en waarvan de diensten op de hoogte moeten zijn. Ook kan het voorkomen dat personen die in onderzoek zijn bij een dienst in afwachting zijn van de uitkomst van een vreemdeling-rechtelijke procedure. Het verloop van een dergelijke procedure is voor de werkzaamheden van een dienst van belang, bijvoorbeeld om te weten waar en hoe lang de betrokkene in Nederland verblijft of gaat verblijven.

W

Door artikel 87, eerste lid van de Wiv 2002 komt de discretionaire bevoegdheid die de rechter op grond van artikel 8:29, derde lid, Awb toekomt, te vervallen, stellen de leden van de VVD-fractie vast. De reden hiervoor is dat de wetgever heeft geoordeeld dat, indien het gaat om inlichtingen of stukken waarbij naar het oordeel van de betrokken minister de veiligheid van de staat in het geding is, een onverkorte toepassing van artikel 8:29, derde lid Awb enkele ongewenste consequenties kan hebben. De leden van de VVD-fractie achten dit echter een onwenselijke situatie en hechten grote waarde aan de rechterlijke toetsing van de gewichtige

redenen van een van de partijen (in bestuursrechtelijke procedures) om niet te voldoen aan een verplichting inlichtingen te geven dan wel stukken te overleggen. Naar wij uit deze vraagstelling begrijpen hebben de leden van de VVD-fractie niet zozeer bezwaar tegen het thans voorliggende voorstel om de regeling van artikel 87, eerste lid, uit te breiden naar situaties waarin de betrokken minister geen partij is maar wordt verplicht tot het geven van inlichtingen op grond van artikel 8:45 van de Algemene wet bestuursrecht (Awb), maar hebben zij bezwaar tegen de bestaande strekking van artikel 87, eerste lid. De regeling van artikel 87, eerste lid, waarbij de discretionaire bevoegdheid die de rechter op grond van artikel 29, derde lid, Awb toekomt, komt te vervallen, maakte deel uit van het oorspronkelijke wetsvoorstel waarop de Wiv 2002 berust en werd in de memorie van toelichting bij dat wetsvoorstel uitvoerig toegelicht (Kamerstukken II, 1997/98, 25 877, nr. 3, blz. 89, waarin het betreffende artikel nog als artikel 83 genummerd was). Wij wijzen er bij deze gelegenheid uitdrukkelijk op dat het hier gaat om informatie die naar het oordeel van de betrokken minister in het belang van de nationale veiligheid niet openbaar mag worden. Daarbij kan gedacht worden aan informatie die zicht geeft op het actueel kennisniveau, de bronnen (waaronder de vaak kwetsbare menselijke bronnen) en de werkwijzen van de inlichtingen- en veiligheidsdiensten. Artikel 87 laat overigens onverlet dat de rechter, zij het onder voorwaarden, weldegelijk van de inhoud kennis kan nemen en deze dus kan beoordelen. Met de regeling van artikel 87 wordt beoogd te voorkomen dat dit soort informatie door de afwijzing door de rechter van het beroep op een gewichtige reden ten onrechte alsnog openbaar kan worden met alle ongewenste gevolgen van dien. Ook zou in het geval dat er meerdere malen een beroep op gewichtige redenen door de rechter zou worden afgewezen, dit als consequentie kunnen hebben dat de kans groter wordt dat de betrokken minister in procedures het verstrekken van inlichtingen dan wel het overleggen van stukken zonder meer zou gaan weigeren. Weliswaar kan in dat geval de rechtbank op grond van artikel 8:31 van de Awb daaruit de gevolgtrekkingen maken die haar geraden voorkomen, maar het moge evident zijn dat dit over het algemeen voor alle partijen een onbevredigende situatie kan opleveren. Door het buiten toepassing verklaren van de discretionaire bevoegdheid van de rechter, wordt bewerkstelligd dat in de gevallen dat door de betrokken minister inlichtingen worden verstrekt c.q. stukken worden overgelegd, ten aanzien waarvan hij van oordeel is dat die ter uitsluitende kennisneming van de rechtbank dienen te blijven, dit ook op voorhand is verzekerd. Tot zover wat betreft de achtergrond van de bestaande regeling van artikel 87. Deze regeling is beperkt tot bestuursrechtelijke procedures inzake de toepassing van de Wiv 2002 en de Wet veiligheidsonderzoeken. Maar ook in andere gevallen kunnen de betrokken ministers op grond van artikel 8:45, eerste lid, van de Awb door de rechtbank worden verzocht tot het geven van schriftelijke inlichtingen of het inzenden van onder hen berustende stukken. Het kan daarbij gaan om bestuursrechtelijke procedures waarbij besluiten van andere bestuursorganen centraal staan, die (mede) gebaseerd zijn op door de diensten op de voet van artikel 36 van de Wiv 2002 verstrekte gegevens (ambtsberichten). Het onderhavige wetsvoorstel beoogt ook in dergelijke procedures de regeling van artikel 87, eerste lid, van overeenkomstige toepassing te laten zijn.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst