Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2007–2008

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

C

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 7 mei 2008

Bij brief van 22 januari 2008 verzoekt de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin van uw Kamer mij om zo spoedig mogelijk aan uw Kamer aan te bieden een kabinetsreactie op het advies van het College bescherming persoonsgegevens (CBP) met betrekking tot het wetsvoorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede enkele andere wijzigingen (Kamerstukken 30 553). Die kabinetsreactie bied ik u hierbij aan, mede namens de minister-president, minister van Algemene Zaken, de minister van Defensie en de minister van Justitie.

Veiligheid en persoonlijke levenssfeer

In deze reactie ga ik in op de opmerkingen die het CBP maakt ten aanzien van het onderhavige wetsvoorstel. Het advies behandelt, met name in de inleiding, ook een aantal algemene ontwikkelingen. Zo is het CBP, in navolging van het rapport Data voor daadkracht, van oordeel dat de precieze omvang en inhoud van eerdere maatregelen op het gebied van veiligheid niet duidelijk is. Het gaat daarbij dan kennelijk niet zozeer om de nationale veiligheid, het werkterrein van de inlichtingen- en veiligheidsdiensten, maar om een algemener begrip veiligheid, en dan met name om de bevoegdheden van politie en justitie. In dat verband zou, zo betoogt het CBP, het risico bestaan dat de gegevensstromen, ook al worden deze met de beste bedoelingen ingericht, door de combinatie van de omvang van de bestanden met de verregaande toepassingsmogelijkheden van ICT leiden tot een disproportioneel volgen en controleren van de burger. Voor wat betreft dit deel van het advies dat niet zozeer gericht is op dit speci-

KST118129
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2008

fieke wetsvoorstel wil ik volstaan met een verwijzing naar mijn reactie, mede namens de minister van Defensie en de minister van Justitie, op het rapport Data voor daadkracht (Kamerstukken II 2006/07, 30 800 VII en 30 800 VI, nr. 65) en naar de daarin vervatte beleidsvoornemens.

Wat betreft de opmerkingen van het CBP die wel direct betrekking hebben op het wetsvoorstel valt mij op dat hierbij de voorgestelde wijzigingen in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV 2002) in geïsoleerd verband worden bezien. Het CBP lijkt zich onvoldoende rekenschap te hebben gegeven van datgene wat de WIV 2002 thans al aan waarborgen voor de burger bevat. Het optreden van de inlichtingen- en veiligheidsdiensten is zorgvuldig wettelijk genormeerd en voldoet aan alle daaraan te stellen eisen. De diensten zelf en de betrokken ministers dragen er zorg voor dat de wettelijke regels en de daarop gebaseerde interne richtlijnen en procedures strikt worden nageleefd. Ten aanzien van bijzondere bevoegdheden van de diensten die het diepst ingrijpen in de persoonlijke levenssfeer, zoals het aftappen van telecommunicatieverkeer en het binnentreden in een woning, is wettelijk gewaarborgd dat de toestemming voor de inzet ervan uitsluitend door de betreffende minister persoonlijk gegeven wordt, zonder mogelijkheid van mandaat. Ten aanzien van de uitoefening van dergelijke bevoegdheden is bovendien voorzien in een notificatieregeling, op grond waarvan de burger tegen wie deze bevoegdheden zijn ingezet daarvan, na verloop van ten minste vijf jaar, op de hoogte wordt gesteld, uiteraard voor zover daarmee geen afbreuk wordt gedaan aan verplichting tot geheimhouding van actueel kennisniveau, bronnen en werkwijzen van de diensten. Dat laatste geldt eveneens bij de kennisnemingsregeling, die hierna nog aan de orde komt en op grond waarvan de burger inzage kan verzoeken in de hem betreffende door een dienst verwerkte gegevens. Tegen besluiten op basis van deze regeling kan de burger bezwaar maken en beroep in stellen. Voorts toetst de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) de rechtmatigheid van het optreden van de diensten, met inbegrip uiteraard van de wijze waarop deze de genoemde notificatie- en kennisnemingsregeling uitvoeren, en beschikt over alle daarvoor benodigde bevoegdheden, waaronder toegang tot alle door de diensten verwerkte gegevens. Het wetsvoorstel versterkt en verduidelijkt het bestaande stelsel van waarborgen op onderdelen en laat dit voor het overige onaangetast. Dit gegeven dient bij de beoordeling van het CBP advies uitdrukkelijk in de beschouwing te worden betrokken. Bij de bespreking van de afzonderlijke kanttekeningen van het CBP zal ik dit nader toelichten.

De toepassing van de Wet bescherming persoonsgegevens (WBP)

Ingevolge het huidige artikel 17, derde lid, WIV 2002, zijn de wettelijke voorschriften voor de verantwoordelijke voor een gegevensverwerking niet van toepassing op een verstrekking gedaan ingevolge een verzoek van de diensten. Naar het oordeel van het CBP zou deze uitsluiting van de WBP en aanpalende wetgeving, zeker nu het wetsvoorstel expliciet voorziet in rechtstreekse verstrekkingen aan de diensten zonder menselijke tussenkomst van de zijde van de verantwoordelijke, tot consequentie hebben dat de transparantie voor burger wordt ondergraven, dat de verantwoordelijke geen afweging kan maken tussen het belang van de burger om de gegevens niet te verstrekken en het algemene belang om deze wel te verstrekken, en dat het CBP geen toezicht kan houden.

Gegevensverwerking door en ten behoeve van de inlichtingen- en veiligheidsdiensten valt onder de werking van de WIV 2002. De WBP is op deze gegevensverwerking niet van toepassing (artikel 2, tweede lid, onder b, WBP). Waarborgen en toezicht liggen dan ook vast in de WIV 2002, niet

in de WBP. Zo valt de rechtmatigheid van deze gegevensverwerking onder het toezicht van de onafhankelijke commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD). Het wetsvoorstel brengt geen wijziging in deze situatie. De transparantie voor de burger is en blijft gebaseerd op de WIV 2002.

Voor het beschermingsregime van de WIV 2002 is aangesloten bij de uitgangspunten van het WBP en dit regime bevat daarom, uiteraard voor zover mogelijk met het oog op de specifieke taakopdracht van de diensten, dezelfde uitgebreide waarborgen. Zo verstrekt de dienst geen persoonsgegevens aan derden, tenzij dit noodzakelijk is voor een goede taakuitvoering. Daarnaast kan een ieder een aanvraag doen tot kennisneming van het feit of, en zo ja, welke, hem betreffende persoonsgegevens de dienst heeft verwerkt. Voorts stelt de WIV 2002 dezelfde algemene rechtmatigheidseisen aan verwerking van (persoons)gegevens als de WBP. Het feit dat sommige rechten voor burgers, die wel in de WBP opgenomen zijn, niet of niet in volle omvang gelden voor gegevensverwerking door de diensten, hangt samen met de taakopdracht van de diensten. Dit geldt voor het recht op mededeling bij eerste opname in een registratie en het recht op informatie aan wie gegevens zijn verstrekt. Een dergelijk recht zou direct zicht geven op het actueel kennisniveau van de diensten en daarmee hun taakuitvoering onmogelijk maken. Wat betreft het inzagerecht, met daarbij specifiek het recht op informatie over de herkomst van gegevens, kan aangegeven worden dat burgers in het kader van de kennisnemingsregeling wel een verzoek kunnen doen tot inzage in hun gegevens, maar dat het recht op informatie over de herkomst van die gegevens afketst op de wettelijke plicht tot bronbescherming. Tot slot kunnen burgers niet onverkort een beroep doen op het zogenoemde correctierecht ten aanzien van diensten. De achtergrond hiervan is gelegen in het feit dat de diensten de bron van gegevens zouden moeten onthullen, indien zij moeten aantonen dat bepaalde gegevens correct zijn. Hier staat tegenover dat burgers wel een verklaring kunnen afgeven over de juistheid van de gegevens. Deze verklaring wordt vervolgens bij de betrokken gegevens gevoegd. Uiteraard dragen de diensten zorg, en hiertoe zijn zij ook verplicht, tot verbetering, dan wel vernietiging, van gegevens die onjuist zijn, dan wel ten onrechte zijn verwerkt.

Uit het systeem van de WIV 2002 blijkt wanneer en onder welke condities door de inlichtingen- en veiligheidsdiensten (AIVD en MIVD) gegevens omtrent burgers mogen worden verwerkt en welke bevoegdheden de diensten in dat kader mogen inzetten. De WIV 2002 voldoet dan ook volledig aan de eisen die daaraan ingevolge artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en de daarop gebaseerde jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) worden gesteld. Zowel bij de parlementaire behandeling van de WIV 2002 als bij de parlementaire behandeling van het onderhavige voorstel tot wijziging van de WIV 2002 in de Tweede Kamer is daar bij stil gestaan. Het specifieke karakter van de aan inlichtingen- en veiligheidsdiensten opgedragen taken maakt geheimhouding van actueel kennisniveau, bronnen en werkwijzen noodzakelijk. Dit beperkt de mate waarin openheid kan worden betracht over de verwerking van gegevens door of ten behoeve van deze diensten, ook richting de burger. Volledige transparantie is dan ook niet mogelijk. Dat is echter waar het gaat om activiteiten van inlichtingen- en veiligheidsdiensten een algemeen aanvaard gegeven; ook in de jurisprudentie van het EHRM. Daarvoor moeten er dan wel compenserende maatregelen zijn, bijvoorbeeld in de vorm van effectief toezicht. Daar is dan ook in voorzien. De CTIVD ziet, als gespecialiseerd toezichtsorgaan, toe op de rechtmatigheid van de taakuitvoering door de diensten, en daarmee ook op de gegevensverstrekking op verzoek van deze diensten. Deze commissie beschikt over

ruime bevoegdheden en brengt omtrent het toezicht openbare rapportages uit.

Wat betreft het verstrekken van gegevens aan inlichtingen- en veiligheidsdiensten geldt dat ook thans degene die met een verzoek om gegevens wordt geconfronteerd, nooit in staat zal zijn, en dat ook niet hoort te zijn, om het belang voor de betreffende dienst van het gevraagde gegeven te beoordelen. Dat geldt zowel in de situatie dat de verstrekking op vrijwillige basis geschiedt als in de situatie dat er een verplichting tot verstrekking bestaat. Wettelijk gezien bestaat er ook geen noodzaak om tot een dergelijke beoordeling te komen. Als een verantwoordelijke voor de gegevensverwerking voldoet aan een verzoek van een inlichtingen- of veiligheidsdienst, om gegevens te verstrekken dan zijn op grond van WIV 2002 (het huidige artikel 17, derde lid) de op de verantwoordelijke van toepassing zijnde wettelijke voorschriften betreffende de verstrekking van zodanige gegevens niet van toepassing op de verstrekking van gegevens aan de desbetreffende dienst. Dat betekent onder meer dat, voor zover er beperkingen gesteld zijn aan de doelen waarvoor gegevens verstrekt mogen worden, deze beperkingen worden doorbroken, dat het recht op kennisneming van de burger omtrent gedane verstrekkingen aan de diensten niet hoeft te worden gehonoreerd – immers dat zou zicht geven op lopende onderzoeken van de dienst – en dat ook het toezicht van het CBP terzake wijkt (Kamerstukken II 1997/98, 25 877, nr. 3, blz. 23–24, waarbij overigens nog sprake is van de Wet persoonsregistraties, de voorganger van de WBP, en van de Registratiekamer, voorganger van het CBP). Met dit laatste valt er echter geen gat in het toezicht, integendeel. De bovengenoemde CTIVD is alsdan immers het competente toezichtsorgaan. Op het hiervoor geschetste stelsel wordt met het thans bij uw Kamer aanhangige wetsvoorstel geen enkele verandering aangebracht.

Tot slot – en dat in reactie op de opmerking van het CBP ter zake – merk ik op dat de voorgestelde maatregelen geen basis bieden om zgn. klassieke geheimhouders, zoals artsen, onder de verplichting tot gegevensverstrekking te brengen.

Noodzaak

Het CBP stelt dat de noodzaak de voorgestelde maatregelen in het belang van de nationale veiligheid in te voeren, onvoldoende onderbouwd is. Het CBP is van oordeel dat niet aannemelijk is gemaakt dat de huidige bevoegdheden onvoldoende mogelijkheden bieden de taken effectief uit te voeren.

Alvorens in te gaan op de concrete kanttekeningen die het CBP plaatst, lijkt het zinvol om meer in het algemeen de taakuitvoering door de diensten te belichten.

De hoofdtaak van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) is het verrichten van onderzoek in binnen- en buitenland, teneinde tijdig dreigingen en risico's te onderkennen voor de nationale veiligheid. Hierdoor behoort de verwerking van gegevens door de diensten tot het zogenoemde primaire bedrijfsproces. Het verkrijgen en behouden van een goede informatiepositie en het verzamelen van gegevens is derhalve, vanzelfsprekend, van het hoogste belang voor een goede taakuitvoering door de diensten. Zoals reeds in de memorie van toelichting uiteengezet hebben de aanslagen in New York, Madrid en Londen, maar ook na enkele voorvallen in Nederland zelf, onmiskenbaar aan het licht gebracht dat de mogelijkheden tot het tijdig onderkennen van terroristische dreigingen en het waar mogelijk voorkomen van op handen zijnde terroristische aanslagen

dienen te worden vergroot. De nu voorgestelde wijzigingen van de WIV 2002 passen binnen het samenhangend geheel van maatregelen en beleid ter verdere intensivering van de terrorismebestrijding dat door het vorige kabinet is ingezet (zie Kamerstukken II 2003/04, 27 925, nr. 123) en behoren tot de noodzakelijk te treffen maatregelen. De voorstellen tot wijziging van de WIV 2002 zijn aangekondigd in de brief van mijn ambtsvoorganger van 15 juli 2004 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II, 2003/04, 29 200 VII, nr. 61). De voorstellen dragen bij aan de mogelijkheden van de diensten tot het handhaven en verbeteren van de eerder genoemde informatiepositie en tot het op efficiëntere en effectievere wijze verwerken van gegevens. Uiteraard slechts met het oog op het hoofddoel van de diensten: het afwenden van dreigingen voor de nationale veiligheid.

Het afwenden van dreigingen vindt zijn startpunt uiteraard in het verrichten van onderzoek naar organisaties en personen welke aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de nationale veiligheid. De diensten richten zich bij dit onderzoek met name op het in kaart brengen van de volgende aspecten van het gedrag van die personen en organisaties: identificatie, verplaatsing, communicatie en financiën. Zonder om begrijpelijke redenen in te kunnen gaan op concrete voorbeelden, kan als illustratie dienen de situatie dat de diensten over informatie beschikken dat een groep personen het idee heeft opgevat om ergens in Nederland om ideologische redenen een aanslag te plegen. In deze situatie is het uiteraard zaak voor de diensten om helderheid te krijgen over de omvang van deze groep, de personen die deel uitmaken van de groep, het potentiële doelwit en de beoogde datum van de aanslag etc. Om hier volledig zicht op te krijgen zullen de diensten de beschikking moeten hebben over gegevens omtrent de identiteit van de leden, hun reisbewegingen, de wijze waarop de leden communiceren en de inhoud van deze communicatie en tot slot de financiële mogelijkheden van de groep. Het behoeft geen verdere uitleg wat in een dergelijke situatie de gevolgen kunnen zijn indien de diensten niet beschikken over de mogelijkheden om de benodigde gegevens voorhanden te krijgen. Het gaat derhalve om gegevens die noodzakelijk zijn voor een goede taakuitvoering door de diensten.

Dit betekent echter geenszins dat de diensten erop gericht zijn ongebreideld gegevensverzamelingen aan te leggen welke niet relevant zijn voor de aan hen opgelegde taken. Hiertoe zijn zij ook niet bevoegd, zo wijzen onder meer de artikelen 12 en 13 van de WIV 2002 uit. In artikel 12 worden de algemene eisen voor de verwerking van gegevens uiteengezet; deze vindt slechts plaats voor een bepaald doel en voorzover dat noodzakelijk is voor een goede uitvoering van de WIV 2002 of de Wet veiligheidsonderzoeken. Voorts geschiedt de verwerking in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. Wat betreft de verwerking van persoonsgegevens stelt artikel 13 nadere eisen aan de groep personen waar deze gegevens betrekking op kunnen hebben. Overigens ziet de CTIVD er permanent op toe dat de gegevensverwerking door de diensten op rechtmatige wijze gebeurt.

Het CBP is van mening dat de onderbouwing van de verplichting tot het voldoen aan een verzoek tot informatieverstrekking van gegevens «feitelijk niet meer inhoudt dan dat thans geen sprake is van een dekkend informatiestelsel». Het CBP lijkt met deze zinsnede te miskennen dat, zoals hierboven reeds uiteengezet, een dekkend informatiestelsel inderdaad onmisbaar is voor een goede taakuitvoering door de diensten. En volledige dekking – toegespitst op die sectoren waarvan is vastgesteld dat daar gegevens beschikbaar zijn die noodzakelijk zijn voor een goede taakuitvoering – wordt, zoals reeds in de memorie van toelichting uiteengezet,

niet bereikt, zolang de diensten uitsluitend afhankelijk zijn van vrijwillige medewerking en wel om de volgende redenen.

Ten eerste gelden de afspraken – op basis van vrijwilligheid – die tot nu toe zijn gemaakt voor de afzonderlijke instanties waarmee die afspraken zijn gemaakt en gelden deze dus niet voor alle vergelijkbare instanties als geheel. Dat levert voor een goede taakuitvoering voor de diensten en daarmee voor een adequate borging van de veiligheid van de burgers onaanvaardbare – maar door een toereikende instrumentatie van de diensten te reduceren – risico's op. Risico's die door de hiervoor reeds vermelde gebeurtenissen die in de afgelopen jaren plaats hebben gevonden nauwelijks nog toelichting behoeven. Ter illustratie de situatie dat één van beide diensten onderzoek doet naar een target dat zich in het buitenland bevindt, maar welke in Nederland een aanslag wil plegen. Indien uitsluitend gegevens beschikbaar zijn van luchtvaartmaatschappij x en y, terwijl dit target vervolgens een vlucht boekt met luchtvaartmaatschappij z, om naar Nederland te reizen, krijgt de dienst geen volledig beeld van zijn reisbewegingen, wat gevolgen heeft voor het «onder controle» houden van het target.

Ten tweede is de informatie die op basis van vrijwilligheid wordt aangeleverd niet altijd volledig. Uiteraard kan vervolgens ten aanzien van de ontbrekende gegevens een nieuw verzoek naar de betrokken instantie uitgaan; dit hoeft echter niet te betekenen dat de gewenste gegevens vervolgens wel compleet aan de diensten worden aangeleverd. Het moge duidelijk zijn dat in het hierboven geschetste voorbeeld de vertraging die hierdoor optreedt in het onderzoeksproces uitermate ongewenst is en zelfs mogelijk gevaarlijke situaties kan opleveren.

De derde reden die genoemd dient te worden voor het niet voldoen van de vrijwillige arrangementen, hoewel deze situatie zich slechts bij uitzondering voordoet, is het feit dat sommige instanties weigeren informatie te verstrekken aan de diensten. Deze terughoudendheid vindt haar oorsprong wellicht in een verstrekkende servicegerichtheid richting de klanten of afnemers van betrokken instantie. Een verplichte informatieverstrekking biedt op dit punt zeker voordeel voor de betreffende bestuursorganen, financiële dienstverleners en vervoerders. Indien het overleggen van informatie niet op vrijwillige basis, maar op grond van een wettelijke verplichting geschiedt, is er geen enkele ruimte voor enige verwijtbaarheid door klanten aan deze organen en instanties. Uit de contacten die de diensten hebben met potentiële informatieleveranciers blijkt keer op keer dat zij juist vragen om een verplichting tot informatieverstrekking. Zij zijn van mening dat een informatieverplichting kenbaarheid en voorzienbaarheid schept met betrekking tot de gegevensverstrekking, waardoor duidelijk aan klanten en afnemers gepresenteerd kan worden op welke gronden verstrekking kan plaatsvinden.

Ten vierde vragen sommige instanties dusdanig hoge bedragen voor verstrekking van gegevens dat dit in de weg staat aan het verkrijgen ervan.

Concluderend kan gesteld worden dat het niet zo kan zijn dat de nationale inlichtingen- en veiligheidsdiensten in de gevallen waarin is vastgesteld dat het gaat om voor de taakuitvoering essentiële informatie slechts afhankelijk zijn van vrijwillige medewerking, terwijl is gebleken dat vrijwilligheid ertoe leidt dat informatie in het geheel niet wordt aangeleverd, dan wel onvolledig, dan wel te laat. Burgers dienen zo goed mogelijk beschermd te worden tegen terroristische aanslagen of andere staatsgevaarlijke activiteiten. Het mag niet zo zijn dat achteraf blijkt dat relevante informatie bij bepaalde instanties voorhanden was geweest, maar door

gebrekkige arrangementen niet tijdig ter beschikking kon komen van de inlichtingen- en veiligheidsdiensten.

Afgezien van bovengenoemde redenen voor het niet voldoen van de vrijwillige verstrekking, kleven hier nog enkele algemene nadelen aan. Zo geldt dat onderhandelingen met partijen vaak moeizaam verlopen en zeer tijdrovend zijn en moeten bovendien voortdurend ad hoc afspraken gemaakt worden.

Daarnaast geeft het CBP aan dat de proportionaliteit van de maatregelen ontbreekt. Het CBP gaat met deze veronderstelling voorbij aan het feit dat juist voor de verplichte informatieverstrekking is gekozen, aangezien een dergelijke handelswijze ter verkrijgen van de benodigde gegevens minder ingrijpend is dan het verzamelen van deze gegevens door de inzet van andere bijzondere bevoegdheden, zoals het aftappen van telecommunicatie of het observeren van bepaalde verdachte subjecten. Bij de afweging welke voorafging aan de voorgestelde maatregelen zijn derhalve de proportionaliteit en subsidiariteit wel degelijk verdisconteerd.

Het CBP geeft voorts aan dat een informatieverplichting er per definitie toe zal leiden dat meer gegevens van meer burgers door de diensten zullen worden verkregen. De hierin besloten stelling van het CBP dat een informatieverplichting zijn eigen vraag creëert, wordt niet door mij onderschreven. Het CBP verliest naar mijn mening uit het oog dat er een onderscheid dient te worden gemaakt tussen het opleggen van een informatieverplichting als zodanig en de toepassing van deze informatieverplichting in de praktijk. In alle gevallen dat door inlichtingen- en veiligheidsdiensten gegevens worden opgevraagd – ongeacht of dit bij een instantie is die op basis van vrijwilligheid dan wel op basis van een verplichting deze gegevens verstrekt – zal voldaan dienen te worden aan de daarvoor in de WIV 2002, in het bijzonder artikel 12 en 13, neergelegde eisen. Dat houdt onder andere in dat het opvragen van de gegevens geschiedt voor een bepaald doel en noodzakelijk moet zijn voor een goede taakuitvoering (lees: het uitvoeren van een concreet onderzoek). Het proportioneel gebruik van de bevoegdheid van de diensten om gegevens op te mogen vragen en daarmee – waar aan de orde – de concrete toepassing van de informatieverplichting, ligt in de van toepassing zijnde eisen inzake gegevensverwerking door de diensten dus besloten. Vanuit het oogpunt van controleerbaarheid en verantwoording – bijvoorbeeld in het kader van een onderzoek door de CTIVD – dienen gegevensbevragingen ook herleidbaar te zijn. In de WIV 2002 is in dit verband onder meer bepaald dat de gegevens die door de diensten worden verwerkt voorzien moeten zijn van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 12, vierde lid, WIV 2002). Deze kwaliteitseis is met name gesteld vanwege de effecten die het gebruik van de door de diensten verwerkte gegevens kunnen hebben voor personen en instanties. Het opleggen van een informatieverplichting aan bepaalde instanties maakt dit allemaal niet anders; het enige wat verandert is dat in bepaalde gevallen nu ook kan worden verzekerd dat de desbetreffende gegevens voor de diensten beschikbaar komen.

Deze opmerking geldt mutatis mutandis ook voor de wijze van verstrekken. Ook nu hebben de diensten rechtstreeks geautomatiseerde toegang tot verschillende gegevensbestanden. De wijze waarop gegevens worden verstrekt of worden verkregen doet niet af aan de daaraan voorafgaande vraag naar de legitimiteit van de verstrekking of verkrijging. Wel is het zo dat dergelijke gegevensverstrekkingen een efficiëntere en effectievere werkwijze oplevert. Dit alles zonder dat er concessies worden gedaan aan een toereikende beveiliging mede met het oog op de bescherming van de

persoonlijke levenssfeer van hen wier gegevens het betreft. In het onderstaande zal ik daar nog nader op ingaan.

Waar het gaat om de in artikel 12a voorgestelde regeling terzake van data-analyse, betreffen het – zoals ook in de memorie van toelichting is toegelicht – geen nieuwe bevoegdheden van de diensten. Het uitvoeren van de verschillende te onderscheiden vormen van data-analyse, vindt reeds in algemene zin zijn grondslag in de artikelen 12 en 13 van de WIV 2002. De verschillende te onderscheiden vormen van geautomatiseerde data-analyse zijn immers, naast de verschillende vormen van handmatige verwerking en analyse van gegevens, allemaal vormen van gegevensverwerking, waartoe de diensten op grond van artikel 12 WIV 2002 in algemene zin bevoegd zijn. Wat betreft de wenselijkheid om een explicitering van de bevoegdheid tot geautomatiseerde data-analyse voor te stellen (zie het voorgestelde artikel 12a), wordt opgemerkt dat deze primair is gelegen in de wens tot vergroting van de kenbaarheid en voorzienbaarheid van deze specifieke vormen van gegevensverwerking. In combinatie met de nieuw voorgestelde bevoegdheid om met het oog op het doorzoeken van gegevensbestanden op profielen en patronen de bij algemene maatregel van bestuur aangewezen bestuursorganen, (categorieën van) financiële dienstverleners en vervoerders, alsmede de in artikel 28, eerste lid, omschreven aanbieders van communicatiediensten tot beschikbaarstelling van deze bestanden te verplichten (zie het voorgestelde artikel 29b jo. artikel 12, tweede lid, onder b of c) wordt het bovendien aangewezen geacht, deze specifieke vormen van geautomatiseerde data-analyse – die zoals ook in de memorie van toelichting is aangegeven, ingrijpend van karakter (kunnen) zijn (bijvoorbeeld omdat ook personen waarop het onderzoek van de diensten zich niet richt in het vizier kunnen komen) – nader wettelijk te normeren zodat ook in aanvullende waarborgen voor de burger kan worden voorzien. Zo is de bevoegdheid om gegevensbestanden van de hier bedoelde derden op te vragen voor het doorzoeken op patronen of profielen aangemerkt als een bijzondere bevoegdheid (zie de daarvoor geldende waarborgen van artikelen 31–34 WIV) waarvoor toestemming van de minister persoonlijk nodig is. Gegevens die na deze specifieke vormen van verwerking niet meer relevant zijn voor het desbetreffende onderzoek van de dienst, dienen namelijk te worden vernietigd en daarvan dient ook een verslag te worden opgemaakt (zie het voorgestelde artikel 12a, derde lid).

Tot slot wil ik opmerken dat niet genoeg benadrukt kan worden dat aan gegevensverwerking bij de diensten *altijd* een gerichte onderzoeksvraag ten grondslag ligt die voortvloeit uit de taakopdracht van de diensten. Fishing expeditions of ongerichte bestandsvergelijking zijn niet geoorloofd en in strijd met artikel 12 van de wet. Bovendien vormt geautomatiseerde data-analyse slechts een onderdeel van het gehele onderzoeksproces bij de diensten en zal de uiteindelijke beslissing tot enig handelen op basis van de uitkomsten altijd gemaakt worden na uitgebreide menselijke deliberatie.

Aanwijzing bij AMvB

Het CBP is van oordeel dat, waar het gaat om de aanwijzing van de (categorieën van) personen en instellingen waaraan een informatieverplichting wordt opgelegd, het principe van de kenbaarheid met het voornemen bij AMvB nadere invulling aan het wetsvoorstel te geven geenszins is gediend. Volgens het CBP betekent dit niet alleen onduidelijkheid voor de sectoren die het betreft, maar ook voor de burger, terwijl de minister aanzienlijke speelruimte heeft bij de invulling van deze categorieën. Ook zou de drempel de categorieën uit te breiden lager liggen dan indien deze zouden zijn neergelegd in het wetsvoorstel zelf.

In dit verband wijs ik allereerst op de in het wetsvoorstel opgenomen voorhangprocedure waardoor de beide kamers der Staten-Generaal in staat zijn om voorafgaand aan de advisering door de Raad van State hun opvatting kenbaar te maken over de wijze waarop bij AMvB de inhoud van het wetsvoorstel nader wordt ingevuld (zie de artikelen 17a, zesde lid, 28, negende lid, 29a, achtste lid en 29b, zevende lid). Deze voorhangprocedure geldt ook als het in een later stadium noodzakelijk wordt geacht de categorieën waarop de informatieverplichting rust uit te breiden. Voorts worden de verplichtingen die de betreffende bepalingen bevatten pas effectief op het moment dat de AMvB's in werking zijn getreden. Op dat moment zullen deze regelingen volledig kenbaar zijn voor de burger, zoals dat ook op grond van het EVRM wordt vereist.

Ik zal nu nader ingaan op de redenen waarom bepaalde regelingen in het wetsvoorstel een nadere uitwerking bij AMvB kennen. Overigens bevat, overeenkomstig de Aanwijzingen voor de regelgeving (aanwijzing 22), in al die gevallen de wettekst de hoofdelementen van de betreffende regeling, terwijl bij AMvB aan die hoofdelementen een nadere invulling wordt gegeven.

De artikelen 17a en 29a bevatten een verplichting om desgevraagd gegevens te verstrekken aan een inlichtingen- en veiligheidsdienst. Het gaat hier niet om een generieke verplichting die komt te rusten op alle bestuursorganen of op alle categorieën van financiële dienstverleners of vervoerders. Een dergelijke verplichting acht ik niet proportioneel, want het is niet noodzakelijk om voor de goede taakuitvoering van de inlichtingen- en veiligheidsdiensten aan alle genoemde instanties een informatieverplichting op te leggen. Met een dergelijke verplichting zou echter wel volledig voldaan zijn aan het principe van de kenbaarheid. De regering heeft gekozen voor een andere weg, door slechts in die gevallen een verplichting te laten gelden als het gaat om instellingen die beschikken over informatie die van wezenlijk belang kan zijn voor de taakuitvoering van de diensten. Zoals in de memorie van toelichting reeds is aangegeven kan hierbij gedacht worden aan banken, creditcardmaatschappijen en luchtvaartmaatschappijen. Bovendien zal aan de aanwijzing van de betreffende bestuursorganen of categorieën van personen en instanties eerst overleg met de betrokken ministers en (koepel)organisaties voorafgaan; in alle gevallen is bepaald dat de aanwijzing geschiedt in overeenstemming met de minister die het aangaat. In dat overleg zullen ook de verdere onderwerpen die ingevolge de betrokken AMvB geregeld moeten worden aan de orde komen. Het gaat dan om zaken als het soort gegevens en de termijn waarbinnen en de wijze waarop die in voorkomende gevallen verstrekt moeten worden. In het geval van de niet tot de overheid behorende organisaties komt ook de kostenvergoeding aan de orde. Naar mijn oordeel gaan we op deze wijze zorgvuldig te werk, maar het betekent wel dat hier nog enige tijd mee gemoeid is.

Artikel 29b regelt de verplichte verstrekking op verzoek van een dienst van gegevens in de vorm van (delen van) geautomatiseerde bestanden. De voorwaarden waaraan een dergelijk verzoek moet voldoen, waaronder toestemming door de betrokken minister persoonlijk (er is geen mandaat mogelijk) op een daartoe strekkend gemotiveerd verzoek van het hoofd van de desbetreffende dienst, liggen vast in de wet. De AMvB op basis van dit artikel regelt de termijn waarbinnen in een voorkomend geval verstrekking dient plaats te vinden en de kostenvergoeding. Ook hier geldt dat aan het totstandkomen van de AMvB overleg met de betrokken partijen vooraf zal gaan. In al deze gevallen is de speelruimte waar het advies op doelt niet zozeer in het uitsluitende belang van de betrokken

minister, maar vooral benodigd om tegemoet te kunnen komen aan gerechtvaardigde verlangens vanuit alle betrokken partijen.

Tot slot enkele opmerkingen over de AMvB op basis van artikel 28 WIV 2002. Op basis van het huidige artikel 28 is er reeds voorzien in een AMvB, te weten het Besluit ex artikel 28 WIV 2002 (Stb. 2005, nr. 289). Ingevolge artikel II van het wetsvoorstel blijft deze AMvB ook gelden na de wijziging van dat artikel die in dit wetsvoorstel wordt voorgesteld. Artikel 28 regelt thans de bevoegdheid van de diensten om aan aanbieders van openbare telecommunicatienetwerken en -diensten te verzoeken gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. Het verzoek kan slechts betrekking hebben op gegevens die in deze AMvB zijn aangewezen. Op grond van hoofdstuk 13 van de Telecommunicatiewet zijn deze aanbieders verplicht aan een dergelijk verzoek gehoor te geven.

De in het wetsvoorstel voorziene wijziging van artikel 28 vervangt het begrip «aanbieder van een openbare telecommunicatiedienst of van een openbaar telecommunicatienetwerk» door: aanbieder van een communicatiedienst. Zoals in de memorie van toelichting (paragraaf 3.2) is aangegeven wordt met de voorgestelde uitbreiding onder meer beoogd onduidelijkheden die bestaan rond de uitleg van het begrip «openbare telecommunicatiedienst» te ondervangen, met name waar het gaat om ontwikkelingen in relatie tot de toepassing en het gebruik van internet, zoals webhosting en internettelefonie. Ook de aanbieders van besloten netwerken en diensten worden op deze manier onder het bereik van dit artikel gebracht. Met betrekking tot de hier bedoelde diensten is het evident dat daar gegevens, waaronder verkeersgegevens, worden verwerkt welke voor een goede taakuitvoering van een dienst noodzakelijk zijn.

Zoals bekend vormt het internet een belangrijk medium waarvan door diverse personen en groeperingen die in de belangstellingssfeer van de diensten actief zijn (radicalisering, terrorisme, links- en rechts extremisme) intensief gebruik wordt gemaakt. Onderzoek op internet vormt dan ook één van de belangrijke middelen om terzake van de genoemde belangstellingsgebieden informatie in te winnen. Met de voorgestelde uitbreiding tot aanbieders van communicatiediensten wordt het mogelijk om personen en instanties die websites hosten waarop dergelijke personen en groeperingen actief zijn te verplichten bepaalde gegevens, onder meer omtrent de gebruikers van die websites (waaronder IP-adressen), te verstrekken. Dat is belangrijke informatie, onder meer bij het in kaart brengen van terroristische netwerken. Het verkrijgen van dit soort informatie is thans slechts mogelijk op basis van vrijwillige medewerking, maar het moge duidelijk zijn dat voor onderzoek als hier bedoeld niet met vrijwillige medewerking kan worden volstaan.

Beveiliging

Wat betreft de kanttekening van het CBP dat de regeling niet voorziet in een regeling omtrent de beveiliging van de verstrekking van de gegevens dient het volgende opgemerkt te worden. Niet valt in te zien waarom het beveiligingsniveau bij de bestuursorganen, financiële dienstverleners en vervoerders anders dient te zijn indien van vrijwillige gegevensverstrekking naar verplichte verstrekking wordt overgegaan. Het CBP lijkt eraan voorbij te gaan dat het wetsvoorstel er slechts toe strekt *de grondslag voor de verstrekking* te wijzigen, niet *de feitelijke verstrekking* als zodanig.
Afgezien daarvan is de constatering van het CBP dat het wetsvoorstel op het gebied van de beveiliging een manco bevat onjuist. Artikel 13 van de

Wet bescherming persoonsgegevens is wel degelijk van toepassing op de verwerking van gegevens door de bestuursorganen, financiële dienstverleners en vervoerders zelf.
Op de verwerking door de diensten van de aan de diensten verstrekte gegevens is echter het informatiebeveiligingsregime van de WIV 2002 van toepassing. Allereerst kan gewezen worden op artikel 12, derde lid, waarin is genormeerd dat de verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. Voorts eist artikel 15 dat de hoofden van de diensten de verantwoordelijkheid dragen voor de geheimhouding van daarvoor in aanmerking komende gegevens en bronnen waaruit gegevens afkomstig zijn. Tot slot dragen de hoofden van de diensten op grond van artikel 16 zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking.

Daarnaast worden meer specifieke eisen gesteld, indien de diensten afspraken maken met personen en instanties omtrent de verstrekking van gegevens langs elektronische weg. Hierbij dienen met name de eisen neergelegd in het Voorschrift informatiebeveiliging – bijzondere informatie (Vir-bi) genoemd te worden; dit voorschrift geldt voor de gehele rijksdienst waar het gaat om de beveiliging van bijzondere informatie (staatsgeheimen en departementaal vertrouwelijke informatie). Voorts zijn het Beveiligingsvoorschrift 2005 en het Besluit voorschrift informatiebeveiliging rijksdienst (Vir) van belang.

Uit het bovenstaande vloeit voort dat de WIV 2002 en de genoemde voorschriften een beveiligingsregime bevatten welke vergelijkbaar is met, zo niet zwaarder is dan, hetgeen artikel 13 WBP voorschrijft. Daar komt nog bij dat ook de algemene maatregel van bestuur ter uitwerking van de voorgestelde artikelen 17a en 29a een regeling zal bevatten omtrent de beveiliging van gegevensverstrekking.

Overigens schept de informatieverplichting ook de mogelijkheid om aanvullende beveiligingsmaatregelen te treffen wat betreft de verstrekking. Momenteel stuit bijvoorbeeld een uniform systeem, welke bij kan dragen aan het hoge beveiligingsniveau voor het transport van de gegevens tussen de verstrekkers en de diensten, af op het feit dat de afspraken met de verschillende verstrekkers onderling verschillen.

Tot slot geeft het CBP aan dat slechts ten aanzien van de aan te wijzen bestuursorganen bij AMvB nadere regels worden gesteld met betrekking tot de ter zake door het bestuursorgaan te treffen technische en organisatorische maatregelen indien de gegevensverstrekking plaats vindt door het verlenen van rechtstreekse geautomatiseerde toegang tot de desbetreffende gegevens. Onverlet het voorgaande ben ik bereid om bij een eerstvolgende wijziging van de WIV 2002 de artikel 29a aan te vullen met een vergelijkbare bepaling als bedoeld in artikel 17a. Dit houdt in dat zal worden geëxpliciteerd dat onder de wijze van verstrekking tevens de mogelijkheid wordt begrepen tot het verlenen van rechtstreekse toegang tot de betreffende gegevens en dat in de AMvB met betrekking tot financiële dienstverleners en vervoerders (aanvullende) technische en organisatorische maatregelen zullen worden voorgeschreven indien van die mogelijkheid gebruik wordt gemaakt.

Data-analyse

Het CBP is van oordeel dat de mogelijkheid die het wetsvoorstel schept om een grote hoeveelheid gegevens te vergaren uit externe databases ten

behoeve van data-analyse leidt tot consequenties die niet of niet voldoende lijken te zijn onderkend.

In de eerste plaats wijst het CBP in dat verband op de steeds grotere hoeveelheid gegevens die de diensten zullen moeten analyseren, hetgeen neerkomt op het zoeken van een naald in een hooiberg. Het CBP acht het niet aannemelijk dat de effectiviteit van het doorzoeken van informatie hiermee gediend is.

Op dit punt lijkt het CBP impliciet uit te gaan van de veronderstelling dat de diensten geen of onvoldoende ervaring hebben met het uitvoeren van data-analyses op grote hoeveelheden gegevens en dat het wetsvoorstel ertoe dient om het mogelijk te maken grotere hoeveelheden gegevens binnen te halen. Geen van deze veronderstellingen is juist. De diensten hebben al geruime tijd ervaring met data-analyses op grote hoeveelheden gegevens die worden verstrekt op basis van de huidige wet. Zoals in de memorie van toelichting vermeld en ook hiervoor gememoreerd beschikken de diensten op grond van de huidige wet over de mogelijkheid data-analyses uit te voeren, maar heeft de regering ervoor gekozen deze mogelijkheid thans ook expliciet in de wet op te nemen teneinde zodoende de kenbaarheid te vergroten en de toepassing ervan op onderdelen met extra waarborgen te omgeven.

Hiervoor heb ik er voorts al op gewezen dat de verplichting tot gegevensverstrekking die het wetsvoorstel introduceert niet zozeer ingegeven is door de wens over meer gegevens en bestanden te beschikken als wel om de nadelen van vrijwillige gegevensverstrekking te ontlopen. Er is dan ook geen sprake van de hooggespannen verwachtingen waar het CBP voor waarschuwt, maar van een reële inschatting van mogelijkheden tot verbetering gebaseerd op de huidige ervaringen. Het lijkt mij goed om op deze plaats aan de hand van enkele voorbeelden inzicht te geven in het belang van geautomatiseerde data-analyse voor een goede taakuitvoering.

Op aanbeveling van de Commissie-Oord (veiligheid burgerluchtvaart) en na wijziging daartoe van de Wet veiligheidsonderzoeken is thans de zogeheten dynamisering van het veiligheidsonderzoek mogelijk gemaakt. Zoals bekend dienen personen die werken op het beveiligde gebied van Schiphol een veiligheidsonderzoek te ondergaan, waarbij onder meer wordt gekeken naar de justitiële antecedenten van de persoon door raadpleging van het Justitieel Documentatiesysteem (JDS). De dynamisering maakt het mogelijk om periodiek (bijvoorbeeld een keer per maand) de justitiële gegevens (en de politiegegevens) van de in het beveiligde gebied werkzame personen te checken. Dit betekent dat er dus periodiek vele tienduizenden personen dienen te worden nageslagen in de desbetreffende bestanden van politie en justitie. Dat kan alleen nog maar door toepassing van geautomatiseerde data-analyse. Aan de hand van de in de Beleidsregel veiligheidsonderzoeken voor de burgerluchthaven expliciet genoemde strafbare feiten worden daartoe criteria aangewezen. Via een daartoe te ontwikkelen data-mining applicatie wordt aan de kant van de AIVD een geautomatiseerd selectiemechanisme toegepast waardoor alleen die personen worden uitgeselecteerd die voldoen aan de vooraf gestelde criteria. De aldus geselecteerde personen worden vervolgens aan een nader onderzoek onderworpen ter beantwoording van de vraag of de feiten en omstandigheden inderdaad zodanig zijn, dat tot intrekking van de verklaring van geen bezwaar, en daarmee van de toegangspas tot het beveiligde gebied, dient te worden overgegaan. De resultaten van geautomatiseerde data-analyse leiden dus nimmer automatisch tot conclusies, maar vormen het startpunt voor verder onderzoek.

Een ander voorbeeld betreft de voorlegging van visumaanvragen. De AIVD krijgt van het ministerie van Buitenlandse Zaken jaarlijks ongeveer 21 000 visumaanvragen voorgelegd. Dit zijn visumaanvragen van de landen op de 5A-lijst, een bijlage bij de Gemeenschappelijke Visuminstructies van de Beneluxlanden. Als over een aanvrager bij de dienst informatie aanwezig is die relevant is voor de beslissing over de aanvraag, dan brengt de dienst daarover een ambtsbericht uit aan het ministerie van Buitenlandse Zaken. Dit dient binnen vijf werkdagen te gebeuren. Het zal duidelijk zijn dat de zoekslag die noodzakelijk is voor het binnen zo korte termijn beschikbaar krijgen van de mogelijk voor de aanvraag relevante informatie alleen mogelijk is door het toepassen van geautomatiseerde data-analyse. Hierbij is het mogelijk dat de dienst de gegevens die verstrekt worden ten behoeve van deze visumaanvragen doorzoekt aan de hand van profielen. Ter illustratie kan genoemd worden het profiel van personen afkomstig uit een risicogebied, binnen een bepaalde leeftijdscategorie en met een technische achtergrond. Dat betekent uiteraard geenszins dat personen die voldoen aan een dergelijk profiel automatisch niet meer in aanmerking kunnen komen voor een visum. De uitkomst van het profielonderzoek zal slechts de basis vormen voor verder onderzoek naar de achtergrond en mogelijke beweegredenen van die groep personen om een visum voor Nederland aan te vragen.

In de tweede plaats suggereert het CBP een groot risico voor de burger omdat niet gegarandeerd is dat de kwaliteit van de gegevens van dien aard is dat daaruit conclusies kunnen worden getrokken die overeenkomen met de werkelijkheid. Het risico op valse positieve en valse negatieve uitkomsten is aanzienlijk.

Ik ben het met het CBP eens dat aan data-analyse als zodanig, en zeker aan het gebruik van profielen, het risico is verbonden dat het teveel valse treffers oplevert. Dat zou kunnen inhouden dat personen onterecht als target kunnen worden aangemerkt. Bij de data-analyse door de diensten is het echter nooit de computer die bepaalt of iemand een target is. De resultaten die worden verkregen door de data-analyse zijn namelijk niet definitief, maar worden gebruikt ter advisering of ondersteuning van verder onderzoek. Na het uitvoeren van data-analyse zal altijd verder onderzoek plaatsvinden, waarbij de uitkomsten van de data-analyse verder worden vergeleken met aanvullende informatie. In alle gevallen is er sprake van een menselijke beoordeling alvorens de uitkomsten van data-analyse verder worden gebruikt.

In de derde plaats wijst het CBP op het gevaar van de zogenaamde function creep, waarbij technologieën die aanvankelijk gericht waren op een bepaalde doelgroep, in casu degenen die een gevaar vormden voor de nationale veiligheid, gaandeweg worden toegepast op (bijna) iedereen, terwijl anderzijds verzamelde gegevens voor een bepaald doel, voor een ander doel verstrekt en verwerkt worden. Daarbij wijst het CBP erop dat in het wetsvoorstel wordt geëxpliciteerd (artikel 13, vijfde lid) dat data-analyse een ieder kan betreffen.

Hoewel ik met het College het gevaar van function creep vermag in te zien, ben ik van mening dat de activiteiten van de inlichtingen- en veiligheidsdiensten met zoveel wettelijke waarborgen, waaronder onafhankelijk toezicht op de rechtmatigheid, zijn omgeven, dat dit gevaar nu juist in dit geval een uiterst hypothetisch karakter heeft. Zo dient, zoals ik al eerder heb aangegeven, alle gegevensverwerking door de diensten, dus ook de data-analyse, te voldoen aan de eisen die zijn neergelegd in artikel 12 van de WIV 2002. Dat betekent dat gegevensverwerking slechts plaats vindt voor een bepaald doel, noodzakelijk voor een goede uitvoering van de WIV 2002 of de Wet veiligheidsonderzoeken (WVO), in overeenstem-

ming met de wet en op behoorlijke en zorgvuldige wijze. De gegevens die worden geanalyseerd zijn onderzocht op hun betrouwbaarheid en eventueel voorzien van bronvermelding.

Het is echter onvermijdelijk dat bij het verzamelen en doorzoeken van externe gegevensbestanden ten dienste van de goede taakuitvoering van de inlichtingen- en veiligheidsdiensten, ook gegevensverwerking plaats vindt met betrekking tot personen waarop het onderzoek van de dienst zich niet richt. Onder meer onder toepassing van data-analysetechnieken kunnen deze personen er uit worden gefilterd, zodat alleen die personen resteren waarvoor de dienst belangstelling heeft. Wat vroeger handmatig gebeurde kan nu – gelukkig – op geautomatiseerde wijze. Niettemin worden met betrekking tot deze onverdachte personen ook hun gegevens verwerkt overeenkomstig de definitie die in artikel 1. onderdeel f, WIV 2002 van gegevensverwerking wordt gegeven: elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Tot nog toe wordt de grondslag voor deze verwerking gevonden in artikel 13, eerste lid, onderdeel e, WIV 2002 (personen wier gegevens noodzakelijk zijn ter ondersteuning van een goede taakuitvoering door de dienst). Nu in het wetsvoorstel wordt voorgesteld een expliciete wettelijke basis te geven aan de geautomatiseerde data-analyse door de diensten, wordt ook voorzien in een aanvulling van artikel 13 die buiten twijfel stelt in het kader van die data-analyse ook persoonsgegevens van onverdachte personen verwerkt kunnen worden. Daartoe is artikel 13, vijfde lid, in het wetsvoorstel opgenomen.

De CTIVD ziet er op toe dat de verwerking van (persoons)gegevens op rechtmatige wijze wordt uitgevoerd. De CTIVD beschikt over alle daartoe vereiste bevoegdheden. Voor de goede orde voeg ik hieraan toe dat de CTIVD, overeenkomstig de wettelijke regeling, naar aanleiding van de door haar verrichte onderzoeken openbare toezichtsrapporten opstelt die aan de beide kamers der Staten-Generaal worden aangeboden. Gezien de aard van het werk van de diensten kunnen evenwel niet alle onderzoeksbevindingen openbaar gemaakt worden. Het gaat dan met name om gegevens die zicht geven op door de diensten aangewende middelen in concrete aangelegenheden, door de diensten aangewende geheime bronnen en het actueel kennisniveau van de diensten. Deze gegevens kunnen echter wel ter vertrouwelijke kennisname aan de commissie voor de inlichtingen- en veiligheidsdiensten van de Tweede Kamer worden meegedeeld. Daardoor kunnen de betrokken ministers ook over de onderzoeksbevindingen waarin deze gegevens voorkomen politieke verantwoording afleggen.

Waarborgen voor de burger

Het CBP geeft aan dat onvoldoende inzichtelijk is met welke waarborgen de gegevensverstrekking ten behoeve van de diensten is omgeven, maar dat in ieder geval het wettelijk verankerd toetsingskader van artikel 31 WIV 2002 en de verplichting een verslag te maken van de uitoefening van een bijzondere bevoegdheid (artikel 33 WIV 2002) niet van toepassing zijn op de verruiming van de verstrekking door bestuursorganen.

Nadat ik in het voorafgaande de wettelijke waarborgen waarmee de gegevensverstrekking ten behoeve van de diensten is omgeven al uitvoerig heb toegelicht, volsta ik op dit punt met een bespreking van de door het CBP gesignaleerde manco's.

De artikelen 31 en 33 van de WIV 2002 gelden voor de inzet van bijzondere bevoegdheden door de diensten. De bevoegdheid van het voorgestelde artikel 17a wordt niet aangemerkt als bijzondere bevoegdheid en is derhalve niet in paragraaf 3.2.2. van de WIV 2002 geplaatst. De reden hiervoor is dat artikel 17a gericht is op informatieverstrekking binnen de overheid. Gezien de verhoudingen binnen de overheid ligt het niet voor de hand te regelen dat de verstrekking van gegevens die bij het ene orgaan aanwezig zijn en die noodzakelijk zijn voor de taakuitvoering van een ander overheidsorgaan plaats vindt door de inzet van een bijzondere bevoegdheid. Ook in de huidige wet zijn de bestaande verplichtingen voor overheidsorganen (leden van het openbaar ministerie in artikel 61 WIV 2002 en ambtenaren van politie, douane en Koninklijke marechaussee in artikel 62 WIV 2002) om gegevens die voor een dienst van belang zijn aan de betreffende dienst te verstrekken niet in de vorm van een bijzondere bevoegdheid van de diensten geregeld. Daarnaast dient opgemerkt te worden dat momenteel artikel 17 reeds de bevoegdheid schept voor de diensten om bij de uitvoering van hun taak of ter ondersteuning van een goede taakuitvoering aan bestuursorganen te verzoeken gegevens te verstrekken. De artikelen 31 en 33 zijn ook nu niet van toepassing indien van deze bevoegdheid gebruik wordt gemaakt. Artikel 17a voegt hier slechts aan toe dat bestuursorganen kunnen worden aangewezen welke verplicht worden gesteld aan een dergelijk verzoek te voldoen. De enkele reden dat artikel 17a een verplichting creëert, noopt niet tot het van toepassing verklaren van het toetsingskader van artikel 31 en de verslagverplichting van artikel 33 op deze bevoegdheid. De eerder vermelde eisen aan de gegevensverwerking van artikel 12 en 13 WIV 2002 zijn uiteraard ook bij toepassing van artikel 17a onverkort van toepassing.

Het CBP wijst ten aanzien van de gegevensverstrekking en de data-analyse op het feit dat het wetsvoorstel niet is voorzien van een evaluatie- en/of een horizonbepaling. Het CBP geeft voorts aan dat een evaluatiebepaling meer evenwicht zou scheppen tussen de eventuele risico's of nadelen van data-analyse en bepaalde waarborgen, zoals beveiliging van de gegevens. Ik ben het met het CBP eens dat een evaluatiebepaling in beginsel een geschikt middel is om na enkele jaren de balans op te maken van nut en noodzaak voorzover nieuwe bevoegdheden worden gecreëerd in relatie tot de daarbij voorziene waarborgen. Wat betreft het opnemen van een evaluatiebepaling in onderhavig wetsvoorstel heb ik echter mijn twijfels en wel om de volgende redenen. Hierboven is reeds aangegeven dat data-analyse een bestaande bevoegdheid betreft die in onderhavig voorstel wordt geëxpliciteerd. Daarnaast is reeds aan de orde geweest dat ik me bewust ben van de risico's en nadelen die aan data-analyse kunnen kleven, maar dat deze door de wijze van analyse die de diensten hanteren geenszins aan de orde zijn. Tot slot is al ingegaan op de hoge mate van beveiliging die door de diensten gehanteerd wordt. Ik kan derhalve niet direct meegaan in de suggestie van het CBP dat een evaluatiebepaling nodig zou zijn om een vermoed gebrek aan evenwicht in onderhavige voorstellen te herstellen.

Wat betreft het opnemen van een horizonbepaling wil ik graag het volgende opmerken. Een dergelijke bepaling zou leiden tot tijdelijke werking van de wijzigingsvoorstellen. Hiervoor is slechts aanleiding als de achterliggende verschijnselen, die nopen tot de wijzigingen, van voorbijgaande aard zijn. Op dit moment is niet te voorzien of de huidige dreiging ten aanzien van de nationale veiligheid, en daarmee de noodzaak tot de nu voorgestelde wijzigingen, zal afnemen. Daarbij komt dat het opnemen van een horizonbepaling niet voor de hand ligt gezien het systeem van de WIV 2002; ook in de huidige wet is immers geen horizonbepaling opgenomen. Een opname van een horizonbepaling wat betreft de huidige

uitbreiding van enkele bevoegdheden en voornamelijk de explicitering van bestaande bevoegdheden ligt mijns inziens derhalve niet in de rede.

Dit betekent echter geenszins dat de toepassing in de praktijk van onderhavige wijzigingsvoorstellen niet kritisch zullen worden bezien. Ook in dit verband wil ik graag wijzen op het feit dat de inlichtingen- en veiligheidsdiensten onder controle staan van de CTIVD. Dit college is onder meer belast met het toezicht op de rechtmatigheid van de taakuitvoering van de diensten. Op basis van artikel 80 WIV 2002 brengt het college hierover jaarlijks verslag uit aan beide kamers der Staten-Generaal en aan de betrokken ministers. Dit brengt derhalve met zich mee dat zonodig ook met betrekking tot het uitvoeren van data-analyse, dan wel de gegevensverwerking door of ten behoeve van de diensten, aan Uw Kamer en de Tweede Kamer der Staten-Generaal gerapporteerd wordt.

Tot slot

We bevinden ons in een wereld die snelle ontwikkelingen kent op het gebied van mobiliteit, informatisering, communicatie, terwijl voorheen vaststaande grenzen vervagen of verdwijnen (Schengen, globalisering). Deze ontwikkelingen zijn een teken van vooruitgang en modernisering en bieden volop kansen. Deze mogelijkheden en kansen hebben ook een schaduwzijde. Zij bieden ook ruimte voor activiteiten die een bedreiging vormen voor de nationale veiligheid, zoals terrorisme en spionage. Wij willen geen risico's nemen met de nationale veiligheid. Daartoe is het noodzakelijk dat de inlichtingen- en veiligheidsdiensten, die tot taak hebben de nationale veiligheid te beschermen, ook in staat gesteld worden op deze snelle ontwikkelingen in te spelen. Het onderhavige wetsvoorstel beoogt daartoe een bijdrage te leveren. Bij alle overwegingen die er verder te maken zijn mogen we die doelstelling niet uit het oog verliezen.

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