Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2006–2007

30 327 Regels inzake de verwerking van politiegegevens (Wet politiegegevens)

F

NADERE MEMORIE VAN ANTWOORD

Ontvangen 8 mei 2007

Graag zeg ik de leden van de PvdA-fractie en de CDA-fractie dank voor de door hen, naar aanleiding van de memorie van antwoord en het nader advies van het College bescherming persoonsgegevens, gestelde nadere vragen inzake het wetsvoorstel. Het is verheugend te constateren dat dit wetsvoorstel in Uw Kamer met de nodige aandacht en belangstelling is ontvangen. Graag beantwoord ik, mede namens mijn ambtgenoten van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie, de door de vaste commissie voor justitie gestelde vragen en ga ik in op de gemaakte opmerkingen.

De leden van de fracties van de PvdA en het CDA hebben gevraagd op welk niveau de informatie doorzoekbaar wordt gemaakt en doorgegeven en vroegen zich af of de minister er zich wel van bewust is dat vaak onzichtbare metadata worden meegezonden, waarvan niet de bedoeling is dat deze worden vrijgegeven. In antwoord hierop kan ik antwoorden dat het wetsvoorstel een juridische grondslag biedt voor het rechtstreeks zoeken van gegevens, die op regionaal of bovenregionaal niveau raadpleegbaar zijn. Het zoeken van de gegevens vindt plaats in de vorm van gegevensvergelijking; ingeval van een hit kunnen de gegevens die overeenkomen en de erbij behorende gegevens worden verwerkt ten behoeve van andere doelen binnen de politietaak. Het wetsvoorstel bevat de nodige waarborgen om te voorkomen dat gevoelige gegevens bij andere politieambtenaren terecht kan komen dan degene die de gegevens nodig heeft ten behoeve van een goede uitvoering van zijn taak. Een belangrijke waarborg betreft de verplichting voor de verantwoordelijke om een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Bijzondere waarborgen gelden voor de ambtenaren van politie die kunnen worden belast met het rechtstreeks zoeken van de gegevens. In het ontwerp Besluit politiegegevens zal worden uitgewerkt welke ambtenaren van politie in aanmerking kunnen komen voor het rechtstreeks zoeken van gegevens. Daarbij zullen ook opleidingseisen gelden. Het vereiste van de instemming van een bevoegde functionaris met de verdere verwerking van de gegevens waarborgt dat vanuit het team of de onderzoeksgroep, waarbinnen de gegevens worden verwerkt, controle bestaat over het verdere gebruik van de gegevens binnen de politie. Tenslotte gelden er verplichtingen tot vastleg-

KST106983
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2007

ging van gegevens (protocollering). Het kan niet bij voorbaat worden uitgesloten dat in sommige documenttypen onzichtbare metadata worden opgeslagen waaruit een technisch vaardig persoon allerlei additionele informatie kan ontlenen, maar gelet op de waarborgen die gelden voor het ter beschikking stellen van gegevens binnen de politie zal het risico dat deze informatie bij onbevoegden terecht komt zich in de praktijk nauwelijks kunnen voordoen. Ten aanzien van de verstrekking van politiegegevens aan derden wordt in het wetsvoorstel voorzien in de mogelijkheid dat gegevens op basis van hit/no hit-bevraging door daartoe aangewezen personen worden geraadpleegd. De categorieën van politiegegevens, aan de hand waarvan de gegevens kunnen worden vergeleken, worden bij algemene maatregel van bestuur aangewezen (artikel 23). Daarbij geldt eveneens dat de verantwoordelijke is gehouden om passende technische en organisatorische maatregelen te nemen teneinde te waarborgen dat uitsluitend de gegevens worden verstrekt die daarvoor in aanmerking komen.

De leden van de fracties van CDA en PvdA hebben gevraagd naar mijn visie over het toenemende multimediale karakter van informatie en hoe in mijn visie wordt omgegaan met het beschikbaar stellen van beeld-, video- en audiomateriaal, en het toelaten van zoekopdrachten hierover. Verder hebben zij gevraagd of binnen de politie voldoende gebruik wordt gemaakt van zogenaamde ontologieën om metadata op een semantische eenduidige manier te benoemen. Tenslotte hebben zij gevraagd of ik van zins ben om in het geval van audio, beeld of video per opvraging een of meerdere unieke identifiers toe te voegen – een zogenaamd digitaal watermerk of een stenografische tag – zodat in geval van lekken media getraceerd kunnen worden naar de bron ervan. In antwoord op de gestelde vragen merk ik op dat het wetsvoorstel van toepassing is op alle persoonsgegevens die worden verwerkt in het kader van de politietaak. Zodra multimediale gegevens te herleiden zijn naar een te identificeren persoon en deze gegevens worden gebruikt in het kader van de uitvoering van de politietaak, vallen deze gegevens dus onder de reikwijdte van het wetsvoorstel. Zoals eerder reeds opgemerkt voorziet het wetsvoorstel in mogelijkheden tot het rechtstreeks zoeken van politiegegevens. Het zoeken kan plaatsvinden door middel van de vergelijking van gegevens op basis van hit/no hit. Daardoor kan worden gewaarborgd dat de raadpleging van andere gegevens slechts plaatsvindt op basis van gegevens die in het onderzoek, van waaruit de gegevens worden bevraagd, reeds zijn verkregen. De gegevensvergelijking is echter niet beperkt tot tekstuele informatie. Ook bij beeld-, audio- en videomateriaal kan op eenzelfde wijze worden gezocht in de beschikbare informatie, die op grond van andere doelen binnen de politietaak wordt verwerkt. Bij beeldmateriaal kan bijvoorbeeld gebruik worden gemaakt van technieken als gezichtsherkenning of ANPR (automatische nummerplaatherkenning). Het toenemend multimediale karakter van informatie is dan ook goed verenigbaar met de opzet van het wetsvoorstel. Het gebruik van ontologieën om metadata op een semantisch eenduidige manier te benoemen is ook binnen de Nederlandse politie in ontwikkeling. Thans worden binnen de Nederlandse politie de mogelijkheden verkend tot het genereren van meta-data uit de vrije teksten van aangiften, verhoren en tapverslagen aan de hand van bepaalde zoeksleutels. Dit betreffen echter experimenten, er is nog geen sprake van een standaardwerkwijze binnen de politie. Voor de politie is het essentieel dat de gegevensverwerking op veilige wijze plaatsvindt. Daarbij wordt ook aandacht besteed aan het traceren van gegevens die in onbevoegde handen zijn gekomen en worden ook technieken beproefd met digitale watermerken, zoals tags en identifiers. De beveiliging van politiegegevens dient te voldoen aan de eisen die zijn neergelegd in de Regeling informatiebeveiliging politie (Regeling van 17 maart 1997, Stcrt. 60) en het ter uitvoering daarvan uitgewerkte stelsel van informatie-

beveiliging. Dit stelsel omvat het zogenaamde basisbeveiligingsniveau Nederlandse politie (BBNP) met gemeenschappelijke betrouwbaarheidseisen en -maatregelen. Deze eisen zijn ook van toepassing op beeld-video- en audiomateriaal dat binnen de politie wordt verwerkt.

De leden van de fracties van de PvdA en het CDA hebben gevraagd of de rol van de privacyfunctionaris ook als pro-actief kan worden gedefinieerd, zodanig dat deze gericht steekproeven kan en mag nemen wanneer gesignaleerd wordt dat er zware of a-typische vormen van gebruik van raadpleging plaatsvinden. Op deze vraag kan bevestigend worden geantwoord. Ingevolge het wetsvoorstel is de verantwoordelijke gehouden passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onrechtmatige verwerking. De verantwoordelijke is verplicht een privacyfunctionaris te benoemen, die namens hem toeziet op de gegevensverwerking en hem adviseert over de naleving van de wet. Het wetsvoorstel voorziet in een verplichting van de verantwoordelijke tot vastlegging van bepaalde gegevens zodat de rechtmatigheid van de gegevensverwerking kan worden gecontroleerd. De vastlegging van de gegevens is geregeld in artikel 32 van het wetsvoorstel. Deze protocolverplichting omvat de vastlegging van verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht. In verband met zijn taak om toe te zien op de gegevensverwerking is de privacyfunctionaris ten allen tijde bevoegd of gerechtigd om steekproeven te nemen bij aanwijzingen van a-typische vormen van gegevensverwerking. Het gebruik van applicaties wordt in logfiles vastgelegd. Daarbij kan gebruik worden gemaakt van zogenaamde gebruikersprofielen, die zijn gebaseerd op het normale gebruik van applicaties door personen die zijn belast met bepaalde werkzaamheden binnen de politie. Door middel van vergelijking van het daadwerkelijke gebruik van de applicaties met de gebruikersprofielen zullen gevallen van oneigenlijk gebruik aan het licht kunnen komen. Een dergelijke handelwijze wordt thans reeds gebruikt bij controle en toezicht op de gegevensverwerking binnen de politie. Bij afwijkend gebruik kunnen stappen worden ondernomen om betrokkene ter verantwoording te roepen.

De leden van de fracties van de PvdA en het CDA hebben gevraagd naar de wijze waarop de ontstaansgeschiedenis en betrouwbaarheid van bepaalde gegevens in een dossier achteraf kunnen worden beoordeeld door zowel diegenen die met politiegegevens werken als door de burger die er het onderwerp van is. Daarbij is ook gevraagd of de kennisneming van de gegevens door betrokkene, dan wel de weigering tot het verlenen van inzage in de gegevensverwerking, wordt gedocumenteerd en zo ja, hoe en waar en hoelang. Tevens is gevraagd of de minister van plan is om hierover expliciet op meta-niveau gegevens te aggregeren teneinde de werking van dit mechanisme te kunnen evalueren of de structurele kwaliteit van bepaalde informatiebronnen ter discussie te stellen. Tenslotte is gevraagd of de argumentatie van een eventuele weigering om de gegevens te corrigeren ook wordt vastgelegd, en zo ja: hoe? In antwoord op de gestelde vragen moet vooraleerst worden opgemerkt dat het wetsvoorstel regels geeft voor de verwerking van gegevens ten behoeve van de uitvoering van de politietaak. De verantwoordelijke is gehouden de nodige maatregelen te treffen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij verbetert of vernietigt politiegegevens of vult deze aan indien hem blijkt dat deze onjuist of onvolledig zijn. Het College bescherming persoonsgegevens is belast met het toezicht. Daarnaast geldt bovendien dat de strafrechtelijke handhaving van de rechtsorde een belangrijk onderdeel van de politietaak vormt. In die gevallen waarin de gegevens worden gebruikt ten behoeve van de opsporing en vervolging van strafbare feiten zullen de ontstaansgeschiedenis en de betrouwbaarheid van bepaalde gegevens ook in een

strafzaak aan de orde kunnen komen. De rechter zal op basis van de ingebrachte bewijsmiddelen moeten beoordelen in hoeverre deze aanleiding geven tot een veroordeling van de verdachte dan wel tot het nemen van een andere rechterlijke beslissing. Dit betekent dat het ook voor het openbaar ministerie en de politie van belang is om zich reeds in de fase van de opsporing, ter voorbereiding op mogelijke strafvervolging, rekenschap te geven van de ontstaansgeschiedenis en betrouwbaarheid van de gebruikte gegevens. De noodzaak daartoe komt specifiek tot uitdrukking in de regels die gelden voor de verwerking van gegevens door de criminele inlichtingen eenheden binnen de politie. Op grond van de Regeling criminele inlichtingen eenheden worden de herkomst en betrouwbaarheid van de gegevens aangeduid in een CIE-informatierapport. De officier van justitie draagt, onverlet de verantwoordelijkheid van de verantwoordelijke, zorg voor een deugdelijke vastlegging van gegevens over informanten. Verder kent het wetsvoorstel de verplichting voor de verantwoordelijke tot het periodiek laten verrichten van privacy audits. Bij de uitvoering van een dergelijke audit wordt door een onafhankelijke auditor getoetst of de organisatie adequaat is ingericht om in voldoende mate tegemoet te komen aan de wettelijke bepalingen over de verwerking van politiegegevens. Hiertoe behoren voorschriften over de juistheid en nauwkeurigheid van de verwerkte gegevens, overeenkomstig artikel 4 van het wetsvoorstel. Buiten het bovengenoemde geval, waarin de gegevens in een strafzaak worden gebruikt, kan de betrokkene de ontstaansgeschiedenis en betrouwbaarheid van de gegevens toetsen door middel van kennisneming van de hem betreffende politiegegevens, op grond van artikel 25 van het wetsvoorstel. Het wetsvoorstel voorziet niet in een expliciete verplichting voor de verantwoordelijke om het feit, dat de burger kennis heeft genomen van de hem betreffende politiegegevens en daar al dan niet correcties in heeft laten aanbrengen, te documenteren. De waarborgen voor een juiste en nauwkeurige gegevensverwerking, die uit het wetsvoorstel voortvloeien, zijn op zich reeds afdoende en noodzaken niet tot een dergelijke aanvullende vastlegging van gegevens. Wel zal de afhandeling van een verzoek om kennisneming door de betrokkene in de administratie van de politie doorgaans worden gedocumenteerd, zodat de wijze van afhandeling kan worden verantwoord jegens het College bescherming persoonsgegevens of de rechtbank, ingeval de betrokkene zich tot de betreffende instantie wendt. Ook de argumentatie van een eventuele weigering om gegevens te corrigeren zal in de administratie worden vastgelegd. Aldus wordt een overzicht gehouden van de gevallen waarin het recht op kennisneming is uitgeoefend en de afhandeling daarvan. Aggregatie van deze gegevens op meta-niveau maakt het mogelijk de werking van dit mechanisme te kunnen evalueren. Zo bevat het rapport van de Raad van Advies voor de CIE, waarnaar is verwezen in de memorie van toelichting van het wetsvoorstel (Kamerstukken II, 2005–2006, 30 327, nr. 3, pag. 84) cijfers omtrent de aantallen verzoeken om kennisneming gedurende de jaren 2000 tot en met 2002.

De leden van de fracties van de PvdA en het CDA hebben verwezen naar hetgeen in de memorie van antwoord is opgemerkt over de vermelding van herkomst en wijze van verkrijging van gegevens en hebben gevraagd of ik van mening ben dat de extra werklast van beperkte omvang is, omdat herkomst en wijze van verkrijging veelal uit de geregistreerde gegevens kunnen worden afgeleid. Ook hebben zij gevraagd of het bevorderen van een zorgvuldig gebruik van gegevens dan niet ruimschoots opweegt tegen de beperkte extra werklast. Tenslotte hebben zij gevraagd hoe ik tot die conclusie ben gekomen en of het niet zo is dat op ieder moment in de tijd het er wel degelijk toe doet hoe deze gegevens worden beoordeeld, en dat het achteraf veel gemakkelijker is om het gebruik van een dergelijk systeem af te schaffen wanneer de hypothese van de minister bewaarheid blijkt dan het omgekeerde. In antwoord op de

gestelde vragen merk ik vooraleerst op dat in het wetsvoorstel wordt bepaald dat bij de gerichte vormen van gegevensverwerking – dit betreft de verwerking als geregeld in de artikelen 9, 10 en 12 – de herkomst van de gegevens en de wijze van verkrijging worden vermeld. Een dergelijk vereiste geldt echter niet voor de niet gerichte verwerking van persoonsgegevens in het kader van de uitvoering van de dagelijkse politietaak, als geregeld in artikel 8 van het wetsvoorstel. Deze verwerking omvat alle gegevens die de politie in het kader van de basispolitiezorg verzamelt, zoals telefonische meldingen of vragen van burgers, mutaties naar aanleiding van de surveillance, aangiften van eenvoudige strafbare feiten en dergelijke. Doorgaans zal de herkomst en wijze van verkrijging van de gegevens kunnen worden afgeleid uit de betreffende mutaties, processenverbaal of signaleringen. Gelet op het minder ingrijpende karakter van de gegevensverwerking acht ik het evenwel niet proportioneel om de politie bij voorbaat te verplichten om voor alle gegevens, die in dat verband worden verwerkt, de herkomst en de wijze van verkrijging van de gegevens ook nog apart te vermelden. Een verplichting zou immers betekenen dat de betreffende gegevens op uniforme en controleerbare wijze worden vastgelegd. De extra werklast die daaraan verbonden is laat zich niet goed overzien maar zal, gelet om de omvang van de gegevensverwerking, aanzienlijk kunnen zijn juist voor die gevallen waarin deze informatie uit de geregistreerde gegevens niet goed is af te leiden. Het wetsvoorstel bevat bovendien reeds de nodige waarborgen voor een zorgvuldig gebruik van de gegevens, zoals in het voorgaande aan de orde kwam. De zorgvuldige vastlegging van opsporingsinformatie impliceert dat de herkomst van de gegevens wordt vastgelegd. De bewijspositie in een eventuele strafzaak is in hoge mate afhankelijk van een zorgvuldige vastlegging van gegevens. In de applicaties, die binnen de politie worden gebruikt ten behoeve van de opsporing van strafbare feiten, is daarom een afzonderlijk veld opgenomen om de herkomst van gegevens vast te leggen. Daar waar de aard van het incident vereist dat de herkomst van gegevens wordt vastgelegd, wordt de herkomst van de gegevens ook bij de uitvoering van andere taken van de politie vastgelegd.

De leden van de fracties van de PvdA en het CDA hebben gevraagd welke authenticatiemechanismes ik voor ogen heb, indien het systeem «op afstand» bevraagd wordt en hebben de garantie gevraagd dat toegang vanaf thuiswerkplekken, alsook vanaf mobiele werkplekken is uitgesloten bij alle betrokken partijen. Wie toegang heeft tot welke applicatie wordt bepaald door de rol van de functionaris in het werkproces. Bij die rol horen bepaalde bevoegdheden en autorisaties. Het verstrekken van autorisaties is in de verschillende regio's strikt geregeld voor de administratieve procedures rond iedere afzonderlijke applicatie. Het is binnen de Nederlandse politie geen algemeen beleid om thuis werkplekken te scheppen. In de gevallen waarin dit – bij uitzondering – wel mogelijk is, zijn stringente eisen gesteld op het gebied van de beveiliging van gegevens. In de uitvoering van de dagelijkse politietaak maakt de politie gebruik van mobiele dataterminals in de auto, en in sommige regio's loopt een proef met personal digital assistance (*pda's*). Ook daarbij zijn technische en organisatorische beveiligingsvoorzieningen getroffen overeenkomstig de huidige stand der techniek en passend bij het betreffende werkproces.

Onder verwijzing naar de mogelijkheid om schriftelijk politiegegevens op te vragen en daarvan schriftelijke mededeling te doen, in artikel 25 van het wetsvoorstel, hebben de leden van de fracties van de PvdA en het CDA gevraagd naar de controle op de authenticiteit van een persoon om te voorkomen dat door middel van misbruik van het recht op kennisneming informatie met een potentieel privacyschendend karakter in handen kan komen van derden. Hoe is de minister van plan om te authenticeren of de

persoon die de politiegegevens aanvraagt en ontvangt ook de persoon is waarover de betreffende informatie is verzameld? Hoe voorkomt de minister dat bijvoorbeeld studenten die samenwonen in een studentenhuis of partners op zoek naar het aantonen van overspel dit gaan gebruiken als mechanisme om anders niet toegankelijke informatie te verkrijgen teneinde de betreffende persoon te benadelen? In antwoord op de gestelde vragen moet worden opgemerkt dat het niet tot de politietaak behoort om gegevens te verzamelen over overspel of andere intieme gedragingen van personen, het ligt dan ook niet voor de hand dat dergelijke informatie bij de politie beschikbaar is. Wel verzamelt de politie gegevens over de betrokkenheid van personen bij strafbare feiten. Inderdaad is het denkbaar dat dergelijke gegevens interessant kunnen zijn voor derden, bijvoorbeeld werkgevers die de betrouwbaarheid van hun personeelsleden willen toetsen. Het recht op kennisneming is daarvoor echter niet bedoeld. De verantwoordelijke dient zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker. Dit is vastgelegd in artikel 26 van het wetsvoorstel. Daarvoor kan gebruik worden gemaakt van wettige identificatiemiddelen als het paspoort of het rijbewijs. Het vereiste van de vaststelling van de identiteit van de verzoeker zal in de praktijk in de weg staan aan telefonische verstrekking van de gegevens. Ingeval een verzoek om kennisneming aan de politie wordt gericht door de wettelijke vertegenwoordiger van de betrokkene, op grond van artikel 26, tweede lid, van het wetsvoorstel, geldt de verplichting tot vaststelling van de identiteit van de wettelijk vertegenwoordiger. Hoewel dit niet expliciet wettelijk is geregeld volgt uit de wettelijke bepalingen dat de bevoegdheid van de wettelijk vertegenwoordiger om als zodanig op te treden deugdelijk moet worden vastgesteld. Hiertoe kan bijvoorbeeld een uittreksel uit het geboorteregister worden verlangd van ouders die optreden namens hun kind. Bij een voogd die optreedt namens een kind of een curator die optreedt namens een onder curatele gestelde kan respectievelijk om een uittreksel uit het voogdijregister of het curateleregister worden verzocht.

De leden van de fracties van het CDA en de PvdA concluderen uit de memorie van antwoord dat gegevens elk half jaar worden gecontroleerd en eventueel verwijderd. Zij vroegen of het omgekeerde proces, waarbij informatie wordt verwijderd behalve wanneer er expliciete redenen worden aangegeven om dat niet te doen, niet daarboven te verkiezen is. Deze vraag beantwoord ik graag als volgt. Zoals in de memorie van toelichting aan de orde kwam is in het wetsvoorstel de verwerking van gegevens rond personen ten aanzien van wie er aanwijzingen bestaan van betrokkenheid bij handelingen die kunnen wijzen op bepaalde ernstige schendingen van de rechtsorde, de zogenaamde themaverwerking, met strikte waarborgen omgeven. De gegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens inderdaad elk half jaar gecontroleerd. Het betreft hier een gegevensverwerking die, vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer, ingrijpend kan zijn voor de betrokkene. Anders dan bij de gerichte gegevensverwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval, staat niet zozeer de gebeurtenis of situatie centraal. De gegevensverwerking heeft een meer pro-actieve functie, ter verkrijging van een goede informatiepositie. Daarbij kan het noodzakelijk zijn om gedurende een langere periode gegevens te verwerken omtrent personen die betrokken zijn bij handelingen die relevant kunnen zijn voor en kunnen wijzen op het beramen of plegen van misdrijven die een ernstig gevaar voor de rechtsorde opleveren. Hierbij wordt gedacht aan terroristische misdrijven en aan mensenhandel en mensensmokkel. Bij dergelijke misdrijven zijn veelal groeperingen betrokken waarvan de leden elkaar reeds langere tijd kennen en die zeer goed zijn afgeschermd voor de buitenwereld. Een gedurende een langere periode op te bouwen brede

informatiepositie is nodig om hierop zicht te kunnen krijgen. De gegevensverwerking zal dan ook gedurende een langere periode moeten kunnen plaatsvinden. Het vereiste van de halfjaarlijkse controle van de gegevens beoogt een extra waarborg te bieden dat de gegevens slechts worden verwerkt voorzover dat nodig is voor het doel van de verwerking. Het omgekeerde proces, waarbij de gegevens na een periode van een half jaar worden geschoond, behalve wanneer er expliciete redenen worden aangegeven om dat niet te doen, verhoudt zich minder goed met de aard van de verwerking, die er door wordt gekenmerkt dat gedurende een langere periode gegevens moeten kunnen worden verwerkt ten behoeve van het verkrijgen en behouden van een goede informatiepositie op het betreffende terrein. Gelet op het feit dat het vereiste van de doelbinding voorwaardelijk is voor de rechtmatigheid van de gegevensverwerking, zal het eindresultaat van de voorgestelde werkwijze overigens niet wezenlijk verschillen van dat wanneer wordt uitgegaan van het beginsel dat de gegevens worden verwijderd tenzij er redenen zijn om dat niet te doen.

De leden van de fracties van de PvdA en het CDA hebben om een reactie gevraagd op de opvatting dat elke verwerking van persoonsgegevens door een Bijzondere opsporingsdienst in het kader van diens opsporingstaak onder de reikwijdte van dit wetsvoorstel dient te vallen en uitdrukkelijk dient te worden uitgesloten van de Wet bescherming persoonsgegevens (WBP). Bij gelegenheid van de memorie van antwoord heb ik reeds uiteengezet dat de gegevensverwerking door de Bijzondere opsporingsdiensten (BOD-en) exclusief gericht is op de strafrechtelijke handhaving van de rechtsorde terwijl de gegevensverwerking door de politie, die is gericht op de uitvoering van de politietaak als bedoeld in de artikelen 2 en 6 van de Politiewet 1993, meer taken omvat (Kamerstukken I, 2006–2007, 30 327, C).
Thans zijn de meer algemeen geldende regels van de WBP toepassing op de gegevensverwerking door de BOD-en. Deze situatie heeft niet zozeer consequenties voor het niveau van bescherming ten aanzien van de gegevensverwerking door de BOD-en. Wel moet worden vastgesteld dat dit regime minder geëigend is voor de specifieke behoeften van de BOD-en. Het ligt dan ook in de rede dat het wetsvoorstel waar nodig van toepassing is op de gegevensverwerking door de BOD-en. Het wetsvoorstel voorziet hier reeds in voor wat betreft de verwerking van gegevens ten behoeve van criminele inlichtingeneenheden en met betrekking tot informanten. Daartoe is het bepaalde omtrent de gegevensverwerking op grond van de artikelen 10, eerste lid, onder a, en artikel 12 van overeenkomstige toepassing op de gegevensverwerking door BOD-en. Voor de andere onderdelen van het bij of krachtens dit wetsvoorstel bepaalde kan daartoe worden besloten bij algemene maatregel van bestuur op voordracht van Onze Ministers en Onze Minister wie het mede aangaat. Eenzelfde situatie geldt thans ten aanzien van de toepassing van de regels van de Wet politieregisters betreffende de toepassing van de regels voor de bijzondere politieregisters op de BOD-en. In artikel 13c van de Wet politieregisters is namelijk vastgelegd dat het bij of krachtens deze wet bepaalde betreffende de bijzondere politieregisters, op voordracht van Onze Ministers en Onze Minister wie het mede aangaat, van toepassing kan worden verklaard op de daarbij aan te wijzen registers van een BOD. Anders dan de gegevensverwerking ten behoeve van de uitvoering van de politietaak wordt de gegevensverwerking door de BOD-en op deze onderdelen niet expliciet uitgesloten van de reikwijdte van de WBP. Op dit punt kan de regeling van het wetsvoorstel gelden als een lex specialis ten opzichte van de meer algemene regeling van de WBP.

De leden van de fracties van de PvdA en het CDA hebben gevraagd naar mijn mening over de stelling dat op zich waardevolle gegevens zonder indicatie omtrent de betrouwbaarheid in de toekomst onbruikbaar kunnen

blijken of, erger nog, dat waardeloze gegevens een eigen leven kunnen gaan leiden. Deze leden van deze fracties vroegen of het extra werk dat indicatiestelling oplevert op de lange termijn niet juist meer arbeid zal besparen en minder nadelige gevolgen zal hebben voor de uitvoering van de politietaak en de belangen van betrokkenen. In het voorgaande en bij gelegenheid van de memorie van antwoord heb ik reeds uiteengezet welke bezwaren zijn verbonden aan een algemene verplichting voor de politie tot het vermelden van een indicatie rond de betrouwbaarheid van de verwerkte gegevens (Kamerstukken I, 2006–2007, 30 327, C, pag. 3 en 20/21). Naar aanleiding van de gestelde vragen merk ik aanvullend op dat een indicatie van de betrouwbaarheid van gegevens geen eeuwigheidswaarde heeft. Het zou een misverstand zijn te veronderstellen dat politiegegevens die op een zeker moment worden voorzien van een indicatie omtrent hun betrouwbaarheid, bijvoorbeeld doordat de gegevens als betrouwbaar, minder betrouwbaar of niet-betrouwbaar worden aangemerkt, voortaan steeds aan de gestelde indicatie zullen blijven voldoen. Het werk van de politie is er juist bij uitstek op gericht om de betrouwbaarheid van gegevens vast te stellen. Daarbij passen geen zekerheden vooraf maar zal altijd aan de hand van de beschikbare gegevens moeten worden geprobeerd om een zo betrouwbaar en nauwkeurig mogelijk beeld te vormen van het verloop van gebeurtenissen en van de betrokkenheid van personen daarbij. Het zal in de praktijk dan ook vrijwel onvermijdelijk zijn dat gegevens in een later stadium van een onderzoek nieuwe inzichten worden verkregen omtrent de kwaliteit van de gegevens, bijvoorbeeld doordat gegevens minder betrouwbaar blijken dan eerder werd aangenomen of dat andersom gegevens die aanvankelijk van weinig belang leken, later van cruciale waarde blijken. Een indicatie omtrent de betrouwbaarheid van politiegegevens zal dan kunnen leiden tot schijnzekerheid en daarmee tot risico's voor het verloop van het onderzoek van de politie. De stelling dat op zich waardevolle gegevens zonder indicatie omtrent de betrouwbaarheid in de toekomst onbruikbaar kunnen blijken deel ik dan ook niet. Vanwege de mogelijke risico's voor de uitvoering van de politietaak meen ik juist dat een indicatie van de betrouwbaarheid van politiegegevens slechts in die gevallen verantwoord is waarin strikte waarborgen gelden voor een bepaald gebruik van de gegevens. In het geval van de verwerking van gegevens door de criminele inlichtingen eenheden zijn die waarborgen daadwerkelijk aanwezig. Het argument van de efficiency, dat indicatiestelling op langere tijd arbeid kan besparen, acht ik niet van zodanig belang dat dit opweegt tegen de nadelen voor de uitvoering van de politietaak en de belangen van betrokkenen.

De leden van de fracties van de PvdA en het CDA hebben gevraagd of ik kan onderschrijven dat het vervallen van de geïnstitutionaliseerde bescherming ten aan zien van gegevens omtrent onverdachte personen onverlet laat dat waarborgen voor een terughoudend gebruik geboden zijn en of ik bereid ben die waarborgen te bieden. De beide vragen worden door mij bevestigend beantwoord. In de memorie van antwoord ben ik reeds in gegaan op de noodzaak voor de politie om gegevens omtrent onverdachte personen te kunnen verwerken ten behoeve van een goede uitvoering van de politietaak (Kamerstukken I, 2006–2007, 30 327, C, pag. 3/5). Het verwerken van dergelijke gegevens dient echter met strikte waarborgen te zijn omgeven. In het wetsvoorstel worden die waarborgen ook geboden. In de eerste plaats is een dergelijke verwerking slechts mogelijk voorzover dit noodzakelijkheid is voor de uitvoering van de politietaak. Daarbij is de gegevensverwerking gebonden aan bepaald omschreven doelen binnen de politietaak, waarbij specifieke termijnen gelden voor de duur van de verwerking. Ingeval de gegevens bijvoorbeeld worden verwerkt ten behoeve van de dagelijkse uitvoering van de politietaak, kunnen de gegevens gedurende een periode van één jaar breed worden verwerkt. Daarna zijn de gegevens gedurende vier jaar toeganke-

lijk op basis van vergelijking of – ingeval van bredere zoekvragen – voor speciaal daartoe geautoriseerde ambtenaren van politie. Raadpleging zonder dat daartoe een deugdelijke aanleiding bestaat, is niet toegestaan. De gegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de dagelijkse uitvoering van de politietaak, en worden in ieder geval uiterlijk vijf jaar na de datum van de eerste verwerking verwijderd. Ingeval de gegevens worden verwerkt ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde, worden de gegevens verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking en uiterlijk vijf jaar na de datum van de laatste verwerking die blijkt geeft van de noodzaak tot verwerking van de gegevens. Daarbij is wettelijk vastgelegd omtrent welke categorieën van onverdachte personen de gegevensverwerking kan plaatsvinden. Verwijderde gegevens kunnen uitsluitend bij hoge uitzondering nog worden gebruikt voor operationele doeleinden (artikel 14, derde lid). Tenslotte gelden de nodige waarborgen ten aanzien van de controle en het toezicht, dit betreft onder meer de aanwijzing van een privacyfunctionaris, die namens de verantwoordelijke toeziet op de gegevensverwerking, en het periodiek doen verrichten van privacy audits. Het in het wetsvoorstel gekozen systeem van specifieke doelen binnen de politietaak met het oog waarop politiegegevens kunnen worden verwerkt, de op die doelen toegesneden termijnen voor de verwerking van de gegevens, de autorisaties voor de toegang tot de gegevens, de wettelijke vastlegging van de categorieën van personen omtrent wie politiegegevens kunnen worden verwerkt en het toezicht – zoals de verplichting tot het periodiek doen verrichten van privacy audits – vormen naar mijn mening afdoende waarborgen voor een zorgvuldige verwerking van gegevens van onverdachte personen, ten behoeve van een goede uitvoering van de politietaak.

De leden van de fracties van de PvdA en het CDA hebben gevraagd welke leemte de themaverwerking moet opvullen bij de effectieve opsporing van in het bijzonder terroristische, maar ook andere «commune» misdrijven tegen de achtergrond van verschillende andere wetsvoorstellen. Zij hebben tevens gevraagd hoe de themaverwerking zich verhoudt tot de uitbreiding van strafbaarstellingen en het verruimen van het toepassingsbereik van strafvorderlijke onderzoeksbevoegdheden en gevraagd om opheldering van de verhouding van het criterium voor een themaverwerking tot de strafvorderlijke aanwijzingen. Tenslotte hebben zij gevraagd of het verschil in de gevolgen van terroristische aanslagen, gegeven het maatschappij ontwrichtend oogmerk, en andere commune vormen van criminaliteit, zoals mensensmokkel en -handel, niet dusdanig evident is dat themaverwerkingen niet voor de opsporing van laatstgenoemde misdrijven open te stellen dienen te zijn. De gestelde vragen beantwoord ik als volgt. De themaverwerking voorziet in de leemte dat thans geen daarop toegesneden wettelijke grondslag bestaat voor het langdurig verwerken van gegevens van personen die betrokken zijn bij handelingen die kunnen wijzen op het beramen of plegen van misdrijven die een ernstig gevaar voor de rechtsorde opleveren. Zoals in het voorgaande aan de orde kwam, is een dergelijke verwerking van gegevens nodig om de politie een toereikende informatiepositie te verschaffen om de betreffende misdrijven effectief te kunnen aanpakken. Bij dit type misdrijven moet, gelet op de ernst van de delicten, het conspiratieve en ondoordringbare karakter van de betrokken dadergroepen en de mogelijk ernstige maatschappelijke consequenties van het handelen van deze groepen, vanuit bepaalde beschikbare informatie gerechercheerd worden naar concrete misdrijven. Dit kan bijdragen aan de voorkoming, opsporing en vervolging van deze misdrijven.
Over de verhouding tot de uitbreiding van strafbaarstellingen en de verruiming van strafvorderlijke onderzoeksbevoegdheden kan worden

vermeld dat, anders dan die uitbreiding en verruiming, het wetsvoorstel politiegegevens niet voorziet in bevoegdheden voor de politie tot het verzamelen en inwinnen van informatie. Het wetsvoorstel voorziet alleen in wettelijke regels voor de verwerking van gegevens die de politie heeft verkregen bij de uitvoering van de politietaak. Dit kan de dagelijkse uitvoering van de politietaak betreffen maar ook het verrichten van een opsporingsonderzoek. Door de uitbreiding van de bevoegdheden op het gebied van de opsporing en vervolging van terroristische misdrijven kunnen ten behoeve van de opsporing van terroristische misdrijven reeds in geval van een aanwijzing van een terroristisch misdrijf bijzondere opsporingsbevoegdheden worden toegepast. De gegevens die hierdoor worden verkregen, dienen te worden verwerkt met toepassing van artikel 9 van het wetvoorstel. Voldoen de gegevens tevens aan de criteria van artikel 10, eerste lid, onder b, dan mogen zij tevens op grond van dat wetsartikel worden verwerkt.

Over de verhouding van de themaverwerking tot de strafrechtelijke aanwijzing kan worden vermeld dat voor de themaverwerking het niet behoeft te gaan om personen die als verdachte van of betrokkene bij misdrijven worden gezien, dan wel ten aanzien van wie aanwijzingen bestaan dat zij verdachte zijn van of betrokken zijn bij misdrijven, maar dat het voldoende is dat het gaat om personen die betrokken zijn bij handelingen die relevant kunnen zij voor en kunnen wijzen op het beramen of plegen van misdrijven die een ernstig gevaar voor de rechtsorde opleveren. Deze personen behoeven dus niet zelf te zijn betrokken bij het beramen of plegen van deze misdrijven. Evenmin is vereist dat er aanwijzingen bestaan van een terroristisch misdrijf. Het wetsvoorstel introduceert een nieuwe wettelijke grondslag, die ruimer is dan de andere grondslagen, om een ruimere verwerking van gegevens mogelijk te maken. Deze gegevensverwerking strekt ertoe om de politie een toereikende informatiepositie te verschaffen voor de strafrechtelijke handhaving van bepaalde ernstige misdrijven.
Op de noodzaak om de themaverwerking ook mogelijk te maken voor mensensmokkel en -handel, ben ik reeds ingegaan in de memorie van antwoord. Deze misdrijven brengen ernstige risico's voor personen met zich mee, tasten de territoriale en economische integriteit van een staat aan en leveren aldus een ernstig gevaar op voor de rechtsorde. Zij kunnen bovendien alleen effectief worden aangepakt als de politie over een brede relevante informatiepositie beschikt. Bij dit type misdrijven wordt doorgaans geen aangifte gedaan en is er bij de betrokkenen veelal geen bereidheid om verklaringen af te leggen. Daarom moet vanuit brede beschikbare relevante informatie onderzoek worden gedaan en worden doorgerechercheerd naar het concrete misdrijf. Pas na analyse kan worden bezien of er inderdaad sprake is van een misdrijf en kan verder onderzoek er toe leiden dat betrokkene bij het beramen of plegen van die misdrijven in beeld komen. Het is op zich voorstelbaar dat de maatschappelijke impact van een terroristische aanslag zeker op kortere termijn zwaarder zal kunnen zijn dan bij mensenhandel en mensensmokkel. De Dover-zaak heeft echter uitgewezen dat ook gevallen van georganiseerde mensensmokkel of -handel ernstige consequenties kunnen hebben voor het leven van de betrokken slachtoffers en de samenleving ernstig kunnen schokken. Ook op de langere termijn zullen dergelijke misdrijven ernstige gevolgen kunnen hebben voor de integriteit van de maatschappij omdat mensen in gevaarlijke en mensonwaardige situaties worden gebracht door uitbuiting ten behoeve van geldelijk gewin van de betrokken groeperingen.

De leden van de fracties van de PvdA en het CDA hebben gevraagd naar de richtinggevende normen voor nadere beperking van hergebruik en verstrekkingsmogelijkheden van gegevens, die worden verwerkt op grond

van artikel 10, eerste lid, onder b in een themaverwerking. Ook hebben zij gevraagd welke beperkingen gelden voor het gebruik van gegevens in een themaverwerking voor andere doelen binnen de politietaak. In antwoord op de gestelde vragen merk ik vooraleerst op dat de verwerking van gegevens ten behoeve van de zogenaamde thema's, op grond van artikel 10, eerste lid, onderdeel b, uitsluitend kan plaatsvinden voor bepaalde categorieën van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. In de memorie van antwoord is aangegeven dat hierbij wordt gedacht aan de terrorisme en de mensenhandel/mensensmokkel (Kamerstukken I, 2006–2007, 30 327, C, pag. 7).

Tijdens de reguliere verwerking van de gegevens kan blijken dat deze ook van belang kunnen zijn voor andere doelen binnen de politietaak. Indien daartoe op grond van de aard of inhoud van de gegevens aanleiding bestaat, dan kunnen deze verder worden verwerkt ten behoeve van die andere doelen. Dit is geregeld in artikel 10, vijfde lid, van het wetsvoorstel. Het initiatief daartoe is echter voorbehouden aan de speciaal daartoe geautoriseerde politieambtenaren die met deze gegevensverwerking zijn belast; in het eerdergenoemde ontwerp voor een Besluit politiegegevens zal voor de ter beschikking stelling van deze gegevens een uitzondering worden gemaakt op de in het wetsvoorstel neergelegde verplichting voor de verantwoordelijke tot het ter beschikking stellen van deze gegevens aan personen die deze gegevens behoeven voor de uitvoering van hun taak (artikel 15). De gegevens kunnen wel worden betrokken in het rechtstreeks vergelijken van politiegegevens op grond van artikel 11 van het wetsvoorstel. Daarbij zal echter gelden dat de overeenkomende gegevens niet zichtbaar zijn voor de daartoe geautoriseerde politieambtenaar, die is belast met het uitvoeren van de gegevensvergelijking. De functionaris die reeds is betrokken bij de gegevensverwerking en die, op grond van artikel 11, tweede lid, van het wetsvoorstel, moet instemmen met de verdere verwerking zal een signaal kunnen krijgen dat er overeenkomende gegevens zijn gevonden bij de gegevensvergelijking. De functionaris zal dan zelf de afweging moeten maken of de gegevens verder mogen worden verwerkt. Daarmee kan worden gewaarborgd dat de gegevens alleen dan ter beschikking worden gesteld voor verdere verwerking voor andere doelen binnen de politietaak wanneer daarvoor op grond van de aard en inhoud van die gegevens aanleiding bestaat. Zoals door mij aangegeven in de memorie van antwoord wordt hiermee, in combinatie met het in het ontwerp voor een Besluit politiegegevens uit te werken systeem voor autorisaties en de in dat besluit op te nemen verplichting dat de tot deze verwerking bevoegde politieambtenaren werkzaam zijn bij een daartoe ingerichte eenheid die specifiek is belast met deze gegevensverwerking, voorzien in toereikende waarborgen voor een zorgvuldige verwerking van gegevens in het kader van de themaverwerkingen.

De verstrekking van politiegegevens aan derden wordt op hoofdlijnen in het wetsvoorstel geregeld, dit betreft de artikelen 18, 19 en 20. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de categorieën van gegevens die worden of kunnen worden verstrekt (artikel 21). De themaverwerking kan betrekking hebben op personen die niet als verdachte van of betrokkene bij misdrijven kunnen worden gezien maar om personen die betrokken zijn bij handelingen die relevant kunnen zijn voor en kunnen wijzen op het beramen of plegen van misdrijven die een ernstig gevaar voor de rechtsorde opleveren. De gevoeligheid van de gegevensverwerking noodzaakt tot grote terughoudendheid ten aanzien van de gegevensverstrekking aan derden. Er is immers nog niet gebleken van mogelijke betrokkenheid van personen bij strafbare feiten. Hieruit vloeit tevens voort dat het belang van derden bij de verstrekking van dergelijke gegevens niet zal opwegen tegen het belang van de betrokken personen bij bescherming van de gegevens die op hen betrekking

hebben. In het ontwerp voor een Besluit politiegegevens, dat thans in voorbereiding is, zal dan ook worden vastgelegd dat deze gegevens niet aan derden worden verstrekt tenzij op basis van een expliciete basis in de wet of het besluit.

De gegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. De gegevens worden verwijderd uiterlijk vijf jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de gegevens voor het wettelijk vastgelegde doel. Daarna worden de gegevens op grond van artikel 14 gedurende een periode van vijf jaar bewaard met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd. In bijzondere gevallen is hergebruik van de gegevens binnen de politie dan nog mogelijk op grond van artikel 9 of 10 van het wetsvoorstel, voorzover dat noodzakelijk is met het oog op een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval of ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde. Hierbij gaat het om uitzonderlijke gevallen, wanneer er dringende redenen bestaan om de gegevens opnieuw beschikbaar te stellen voor concrete operationele doeleinden en moet op voorhand duidelijk zijn voor welk doel de gegevens moeten worden teruggehaald en om welke gegevens het gaat. Om te voorkomen dat te snel naar dit middel wordt gegrepen is een daartoe strekkende opdracht van het bevoegd gezag vereist.

De minister van Justitie,
E. M. H. Hirsch Ballin