Data voor daadkracht

Gegevensbestanden voor veiligheid: observaties en analyse

Rapport van de Adviescommissie Informatiestromen Veiligheid

“The agencies are like a set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications. What is missing is the attending physician who makes sure they work as a team.”

(The 9/11 Commission report, p. 353)

Al weten wij de reden niet,
‘t Is vast op goeden grond geschied.

(A.C.W. Staring, De Hoofdige Boer, 1820)

INHOUDSOPGAVE

INLEIDING

Bij brief van 13 februari 2007 heeft de toenmalige minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens zijn ambtgenoten van Defensie en Justitie opdracht gegeven voor een onderzoek naar de systematiek van de informatiestromen uit (grote) gegevensbestanden in de publieke en private sector ten behoeve van het veiligheidsdomein. In dit onderzoek gaat het om informatiestromen ter ondersteuning van criminaliteitsbestrijding, terrorismebestrijding en crisisbeheersing. Het gaat hierbij om geautomatiseerde databases van zowel publieke als private organisaties. Tot de publieke gegevensbronnen behoren bijvoorbeeld systemen van de Rijksdienst voor het Wegverkeer, het GBA, het Kadaster, UWV, SVB, CWI en de Belastingdienst. Tot de particuliere gegevensbronnen horen o.m. systemen van banken, verzekeraars, hypotheekverstrekkers, BKR, luchtvaartmaatschappijen, telecomaanbieders en makelaars.

De aanleiding voor het onderzoek was dat de genoemde informatiestromen op dit moment op zeer uiteenlopende manieren worden beheerst. Externe bronnen worden steeds vaker en door steeds meer partijen bevraagd. Deze bronnen groeien in aantal en ze bevatten ook steeds meer gegevens. Het aantal partijen in het veiligheidsdomein dat een beroep doet op deze bronnen groeit en het aantal bevragingen lijkt ook sterk te stijgen. Er is daardoor een chaotisch complex van informatiestromen ontstaan. Het onderzoek is bedoeld om meer inzicht te krijgen in dit complex en om na te gaan in hoeverre verbetering nodig, wenselijk en mogelijk is.

Vanwege het bijzondere karakter van het onderwerp is besloten dit onderzoek op te dragen aan een breed samengestelde, onafhankelijke adviescommissie, de voor dit doel in het leven geroepen Adviescommissie Informatiestromen Veiligheid. Voorzitter van de adviescommissie is mr. H. Bosma, tot medio 2005 voorzitter van de concerndirectie van PinkRoccade. Leden van de adviescommissie zijn: mevr. prof. dr. M.G.W. den Boer, wetenschappelijk decaan aan de Politieacademie en bijzonder hoogleraar vergelijkende bestuurskunde aan de Vrije Universiteit, mr. Th.C. de Graaf, burgemeester van Nijmegen en voormalig minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties, mr. J.N. van Lunteren, oud directeur-generaal van de Belastingdienst en drs. W.J.B.M. Stolwijk RA, voorheen algemeen directeur van Interpay Nederland. Namens de opdrachtgevers heeft drs. W.Ph.G. Voogt RI, programmadirecteur informatievoorziening van de Nationaal Coördinator Terrorismebestrijding (NCTb) de vergaderingen van de adviescommissie bijgewoond. Het secretariaat van de adviescommissie is in handen van drs. A.A.M. Horrevorts.

Het initiatief voor het onderzoek is genomen door de Nationaal Coördinator Terrorismebestrijding, die vanuit zijn verantwoordelijkheid het vraagstuk van de

systematiek van de informatievoorziening uit externe databases had gesignaleerd. Op zijn verzoek is de adviescommissie reeds vóór de formele instelling met haar werkzaamheden begonnen.

Onderwerp van onderzoek

Dit onderzoek heeft betrekking op het inwinnen, beheren en uitwisselen van gegevens uit geautomatiseerde bestanden ten behoeve van het veiligheidsdomein (terrorismebestrijding, criminaliteitsbestrijding en crisisbeheersing). Deze omschrijving houdt in dat het onderzoek plaats vindt op een beperkt terrein met een begrensde scope. Een aantal zaken valt daar buiten: het bredere begrip veiligheid, inwinnen van gegevens bij informanten of door observatie en het verlenen van herendiensten aan de overheid door het bedrijfsleven. Ook is de bestaande wetgeving voor de adviescommissie een gegeven bij de toetsing van de systematiek. Om het belang van gegevens en geautomatiseerde gegevensbestanden in perspectief te kunnen plaatsen zal wel een beschrijving worden gepresenteerd van data in samenhang met andere voor het veiligheidsdomein relevante factoren, zoals de ontwikkeling van intelligence.

Verantwoording werkwijze

De eerste fase van het onderzoek van de adviescommissie bestond uit uitvoerige deskresearch en meer dan 90 interviews met betrokkenen en deskundigen, een viertal expertmeetings alsmede drie buitenlandse verkenningen. Omdat de adviescommissie vanwege haar status in deze fase van haar onderzoek geen toegang kon krijgen tot gegevensbestanden van de betrokken diensten, heeft de adviescommissie vooral geprobeerd inzicht te verkrijgen door een groot aantal interviews. Van deze interviews zijn verslagen gemaakt voor intern gebruik, welke in het archief van de adviescommissie worden opgeslagen. Op grond van deskresearch en interviews heeft de adviescommissie een aantal voorlopige observaties en conclusies geformuleerd. In de expertmeetings heeft de adviescommissie vervolgens bij sleutelfiguren en deskundigen getoetst in hoeverre deze voorlopige conclusies correctie of aanvulling behoefden. De resultaten van dit proces vinden hun weerslag in dit rapport. Wat de adviescommissie betreft volgt na deze fase van inventarisatie en analyse een tweede fase waarin zal worden gewerkt aan verdieping en aan verkenning van mogelijke oplossingen voor de gesignaleerde knelpunten in de systematiek.

De adviescommissie heeft haar werkzaamheden kunnen verrichten dankzij de medewerking van veel functionarissen in het veiligheidsdomein, externe deskundigen en andere betrokkenen bij het complexe proces van het inwinnen van gegevens uit externe databases. Op een enkele uitzondering na heeft iedereen op wie de adviescommissie een beroep heeft gedaan, medewerking verleend aan het onderzoek, hetzij in de vorm van een interview of achtergrondgesprek, hetzij door het geven van informatie of door deelname aan een expertmeeting of een brainstormsessie van de adviescommissie.

Wij zijn de betrokken personen dank verschuldigd. Dank zij hen is het inzicht van de adviescommissie in deze complexe materie verdiept. De namen van deze gesprekspartners van de adviescommissie zijn opgenomen in Bijlage 1.

De bedoelde uitzondering betrof twee organisaties. De organisatie van kleine Internet Providers NBIP (Nationale Beheersorganisatie Internet Providers) heeft laten weten dat het niet op haar weg ligt om deel te nemen aan dergelijke activiteiten van de overheid. Op de achtergrond speelde hierbij mee een reeds lang lopend dispuut over de financiële vergoeding voor de bijdragen van deze sector aan het inwinnen van gegevens uit internetverkeer. De inlichtingendienst AIVD bleek in de praktijk (op een individuele uitzondering na) terughoudend in het verlenen van medewerking.

Leeswijzer

De opbouw van ons rapport is als volgt: hoofdstuk 1 geeft een overzicht van de ontwikkelingen rond databases en hun belang voor het veiligheidsdomein. In hoofdstuk 2 geven wij een schets van de systematiek volgens welke de partijen in dat domein gegevens inwinnen uit geautomatiseerde gegevensbestanden. Hoofdstuk 3 bevat een observatie van de knelpunten die wij hebben geconstateerd in deze systematiek. In hoofdstuk 4 trekken wij een aantal conclusies uit deze observaties en in hoofdstuk 5 schetsen wij enkele lijnen voor het vervolg van ons onderzoek en doen wij enkele aanbevelingen voor door de rijksoverheid te ondernemen acties. Dit rapport is niet alleen voorzien van een managementsamenvatting, de meeste hoofdstukken hebben ook een slotparagraaf waarin de belangrijkste punten uit het betreffende hoofdstuk zijn weergegeven.

De titel van ons rapport heeft een drieledige betekenis. In de eerste plaats gaat het om data die nodig zijn voor een daadkrachtig optreden voor het bereiken van veiligheid. In de tweede plaats hoopt de adviescommissie in dit rapport voldoende bouwstenen aan te voeren voor een daadkrachtig debat over het belang van databases voor diezelfde veiligheid: hun omvang, hun inhoud, hun veiligheid en hun toegankelijkheid. In de derde plaats is er daadkracht nodig om de gegevens uit die databases goed toe te passen, goed te delen en zorgvuldig te analyseren. Ook daarvoor hoopt dit rapport de bouwstenen aan te dragen.

MANAGEMENTSAMENVATTING

Iedereen vindt informatie van cruciaal belang voor het werk van inlichtingen- en opsporingsdiensten. Maar de belangrijkste grondstof daarvoor, gegevens of data, en de manier waarop die grondstof wordt verkregen, krijgen nauwelijks aandacht. Wat ontbreekt is systematische, strategische aandacht voor de basis van het inlichtingen- en opsporingswerk. Daardoor verloopt het informatieproces te weinig samenhangend, onvoldoende effectief en zonder doelmatigheidstoets. Dat heeft met een grote mate van waarschijnlijkheid tot gevolg dat op het veiligheidsterrein verbanden over het hoofd worden gezien en kansen worden gemist. Daardoor worden minder resultaten bereikt dan mogelijk zou zijn.

De Adviescommissie Informatiestromen Veiligheid heeft onderzoek gedaan naar de systematiek van het inwinnen van gegevens uit externe databases door inlichtingen- en opsporingsdiensten. Zo'n systematiek blijkt niet te bestaan. Er blijkt eerder een veelheid aan benaderingen te zijn, waarbij elke organisatie zijn eigen systematiek en werkwijze kent. In de praktijk blijven belangrijke elementen van de data buiten beschouwing. Als er in de afgelopen decennia op het gebied van informatie voor het veiligheidsdomein iets fundamenteel veranderd is, is het wel de groei in het aantal databases, in het aantal gegevens dat daarin is opgeslagen en in de mogelijkheden om die databases te bevragen. Toch krijgen die gegevensbestanden en de gegevens die daarin liggen opgeslagen nauwelijks strategische aandacht. Het inwinnen van gegevens is verbrokkeld en sectoraal ingericht. Het ontbreekt aan bestuurlijke aandacht voor het belang van data voor het veiligheidsdomein, voor de consequenties die verbonden zijn aan de groei van omvang en inhoud van gegevensbestanden en voor de toepassing van nieuwe technieken, zoals datamining.

Een aantal direct aan het inwinnen van gegevens gerelateerde onderwerpen behoeft eveneens strategische aandacht. Daartoe behoort de relatie tussen privacy en veiligheid. Bij het zoeken naar gegevens in geautomatiseerde gegevensbestanden kan de privacy van de burgers in het geding raken. Het gevaar is niet denkbeeldig dat de overheid onder verwijzing naar de strijd tegen het terrorisme de bevoegdheden van inlichtingen- en opsporingsdiensten voor het verkrijgen van gegevens uit databases zodanig uitbreidt dat het evenwicht in de balans tussen privacy en veiligheid verdwijnt. Op die manier kan een onwenselijke tegenstelling tussen privacy en veiligheid ontstaan. Het zijn beide kernwaarden die door de overheid beschermd moeten worden en in balans gehouden. Aan dit vraagstuk geeft de overheid te weinig aandacht.

Een ander onderwerp dat aandacht verdient is de veiligheid en beveiliging van de vele gegevensbestanden waarover de overheid beschikt. Ook deze problematiek verdient meer aandacht dan zij nu krijgt.

De adviescommissie heeft een aantal knelpunten geconstateerd rond het proces van inwinnen van gegevens uit externe databases. Zij doen zich voor wel bij de vragers van gegevens, bij de organisaties die deze gegevens moeten leveren en in het proces van bevraging. Deze knelpunten leiden de adviescommissie tot het oordeel dat het totaal aan verschillende systemen om gegevens uit externe gegevensbestanden in te winnen niet voldoet aan de criteria inzake de grondslag, zoals vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid.

Ten aanzien van de grondslag en de vormvereisten stelt de adviescommissie vast dat onvoldoende inzicht mogelijk is in de wetgeving die van toepassing is op het proces van bevraging, onvoldoende duidelijk is of de vormvereisten worden nageleefd en dat er vraagtekens kunnen worden geplaatst bij de mate waarin de bevraging afdoende is afgeschermd tegen onbevoegden.

Aan de normen van maatschappelijke zorgvuldigheid wordt niet voldaan, omdat onvoldoende wordt gestuurd op proportionaliteit en subsidiariteit bij de bevraging. Gegevens over het aantal bevragingen en de groei daarin worden niet centraal bijgehouden. Omdat geen gegevens over aantallen worden bijgehouden, kan ook niet op een deugdelijke wijze maatschappelijk verantwoording worden afgelegd over dit proces.

Aan de eisen van effectiviteit wordt niet voldaan, omdat partijen in het veiligheidsdomein onvoldoende strategisch samenwerken ten aanzien van vraagstukken met betrekking tot het inwinnen van gegevens, ten aanzien van het delen van informatie en ten aanzien van het toepassen van nieuwe technologieën. Door onvoldoende samenwerking worden naar alle waarschijnlijkheid verbanden over het hoofd gezien en kansen in de strijd tegen criminaliteit en terrorisme gemist.

Aan de eisen van doelmatigheid wordt niet voldaan, omdat bij het proces van bevraging sturing op kosten ontbreekt en omdat er sprake is van ondoelmatige bevragingen. Evenmin is er sprake van een doelmatigheidsprikkel voor gegevens vragende partijen.

Op grond van deze conclusies doet de adviescommissie een aantal voorstellen voor een vervolgaanpak. In de volgende fase van haar onderzoek wil de adviescommissie deze punten nader uitwerken. Dit betreft allereerst enkele onderwerpen waar nader onderzoek naar gewenst is. Daarnaast wil de adviescommissie een aantal mogelijkheden onderzoeken welke de onderlinge samenwerking van de partijen in het veiligheidsdomein kunnen versterken. Tot slot zijn er enkele onderwerpen waarover de adviescommissie geen nader onderzoek noodzakelijk acht, maar wel actie door de rijksoverheid.

In dit rapport trekt de adviescommissie de volgende conclusies:

In hoofdstuk 1

1. Gegevens in externe gegevensbestanden hebben in de afgelopen decennia een steeds grotere betekenis voor het veiligheidsdomein gekregen. Desondanks krijgt het proces van inwinnen van gegevens uit die bestanden door inlichtingen- en opsporingsdiensten weinig tot geen bestuurlijke en politieke aandacht.
2. Data zijn een essentieel onderdeel voor de ontwikkeling van intelligence. Binnen de opsporing staat de ontwikkeling van intelligence nog teveel in de kinderschoenen, zowel in Nederland als in andere landen.
3. Criminaliteit met geautomatiseerde gegevensbestanden, zoals identiteitsfraude, komt steeds vaker voor. De voor- en nadelen van deze gegevensbestanden voor veiligheid en onveiligheid verdienen nader onderzoek en discussie.
4. Er is weinig bekend over het gebruik van geautomatiseerde gegevensbestanden voor het veiligheidsdomein in andere landen. Het delen van informatie tussen inlichtingen- en opsporingsdiensten blijkt wereldwijd een groot probleem te zijn. In de Verenigde Staten is de afgelopen jaren het concept van de fusion centers ontwikkeld. De eerste resultaten lijken veelbelovend.

In hoofdstuk 2

5. Er is geen sprake van een eenduidige systematiek waarmee partijen in het veiligheidsdomein gegevens inwinnen uit externe databases. Strategische aansturing en bestuurlijke aandacht daarvoor ontbreken.
6. Er bestaat geen totaaloverzicht van de bestaande wet- en regelgeving met betrekking tot het inwinnen van gegevens uit externe databases. Het is niet mogelijk om inzicht te verkrijgen in consistentie en samenhang van deze wet- en regelgeving.
7. Er is onvoldoende inzicht in het aantal bevragingen dat door de partijen in het veiligheidsdomein wordt verricht. Dat heeft tot gevolg dat maatschappelijke verantwoording over dit proces op dit moment niet mogelijk is.
8. Politieke discussie over voor- en nadelen van toepassing van nieuwe technieken zoals datamining vindt ten onrechte niet plaats.
9. Uitwisseling van gegevens binnen de politie en tussen inlichtingendiensten en politie is nog steeds een moeizaam proces.
10. Uitwisseling van gegevens door middel van verwijsfuncties blijkt in andere maatschappelijke sectoren succesvol te zijn.

In hoofdstuk 3

11. De partijen in het veiligheidsdomein hebben geen gemeenschappelijke visie op het belang van externe gegevensbanken voor de ontwikkeling van informatie en intelligence.
12. De partijen in het veiligheidsdomein werken onvoldoende met elkaar samen bij het inwinnen, delen en analyseren van gegevens uit externe gegevensbanken en bij het zoeken naar toepassingsmogelijkheden van nieuwe technieken.
13. De overheid heeft onvoldoende aandacht voor de zorgpunten die leveranciers van gegevens hebben ten aanzien het aantal bevragingen en de groei daarvan, de vergoeding van de daarvoor te maken kosten en over de terugkoppeling van de met de geleverde gegevens behaalde resultaten.
14. Het risico dat een onbalans tussen privacy en veiligheid ontstaat wordt door de overheid onvoldoende onder ogen gezien.
15. Nut en noodzaak van het fysiek binnenhalen van aantallen databases ten behoeve van het veiligheidsdomein verdienen nader onderzoek.
16. In de discussies over de vertaling van de Europese richtlijn inzake dataretentie in Nederlandse wetgeving toont de rijksoverheid weinig oog voor bezwaren tegen die wetgeving.

In hoofdstuk 4

17. Het complex van deelsystemen voor het inwinnen van gegevens uit externe databases voldoet niet aan daaraan te stellen normen van grondslag en vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid.
18. Aan te stellen normen op het gebied van de grondslag en de vormvereisten wordt niet voldaan, omdat onvoldoende inzicht bestaat in de toepasselijke wet- en regelgeving, de mate waarin inlichtingen- en opsporingsdiensten zich houden aan de geldende regels en omdat de afscherming van de bevraging voor onbevoegden onvoldoende kan worden verzekerd.
19. Aan te stellen normen op het gebied van maatschappelijke zorgvuldigheid wordt niet voldaan omdat onvoldoende inzicht bestaat in proportionaliteit en subsidiariteit en omdat een afdoende inzicht in het aantal bevragingen en de groei daarin ontbreekt. Aan een aantal beleidsvragen die hiermee samenhangen dient de overheid meer aandacht te geven.
20. Aan te stellen normen op het gebied van effectiviteit wordt niet voldaan omdat de betrokken partijen onvoldoende samenwerken bij het inwinnen, gebruiken en delen van gegevens uit externe gegevensbestanden, waardoor verbanden over het hoofd worden gezien en kansen worden gemist.
21. Aan te stellen normen op het gebied van doelmatigheid wordt niet voldaan omdat geen sturing op kosten plaats vindt en er geen sprake is van een doelmatigheidsprikkel voor vragende diensten.

In hoofdstuk 5 doet de adviescommissie de volgende aanbevelingen voor het vervolg:

1. De adviescommissie stelt voor dat een publieke discussie wordt voorbereid over de balans tussen privacy en veiligheid. Doel van deze discussie is om bouwstenen aan te dragen voor een herijking van de balans tussen bevordering van de veiligheid en bescherming van de persoonlijke levenssfeer.
2. De rijksoverheid dient op korte termijn een overzicht op te stellen van alle wet- en regelgeving die van toepassing is op het inwinnen van gegevens uit externe data-

bestanden. De adviescommissie zal nagaan of het wenselijk is in aanvulling op dit overzicht een stelselwet tot stand te brengen voor de bevraging van externe databestanden met een daarop afgestemd toetsingskader.

3. De adviescommissie stelt zich voor in de tweede fase van het onderzoek een nadere verkenning uit te voeren naar de voor- en nadelen van de instelling van een onafhankelijke functionaris voor het toezicht op het inwinnen van gegevens uit externe databases door inlichtingen- en opsporingsdiensten, alsmede naar diens positionering.
4. De adviescommissie stelt zich voor om mogelijke vormen van shared services in het veiligheidsdomein in de tweede fase nader te onderzoeken op nut en haalbaarheid, zoals:
   - Een Intelligent Verwijsknooppunt voor het veiligheidsdomein,
   - Een betrouwbare service provider die zorgt voor inwinnen en verspreiden van gegevens,
   - Fusion centers voor samenwerking en uitwisseling van gegevens,
   - Een expertisecentrum voor de ontwikkeling van nieuwe technologieën.
5. De drie verantwoordelijke ministers worden opgeroepen initiatieven te nemen teneinde de strategische samenwerking binnen het veiligheidsdomein vorm te geven bij het inwinnen, gebruiken en delen van gegevens uit externe databases.
   Ten aanzien van de volgende onderwerpen acht de adviescommissie maatregelen door de rijksoverheid gewenst:
   - Het nemen van verantwoordelijkheid voor afronding van de discussie over de vergoeding van kosten van marktpartijen;
   - Een systeem van terugkoppeling naar het bedrijfsleven van de hoofdlijnen van de resultaten die zijn bereikt met de door het bedrijfsleven verstrekte gegevens;
   - Vergroting van het draagvlak voor de beleidsvoornemens inzake de dataretentie;
   - Een stelsel voor maatschappelijke verantwoording over de bevragingen door de partijen in het veiligheidsdomein uit externe databestanden

1

OVER DATA EN INTELLIGENCE

1.1 Inleiding

Gegevensbestanden staan centraal in dit onderzoek. De gegevens in die bestanden hebben op zichzelf geen waarde voor de veiligheid. Het is de combinatie van data, van gegevens, en de interpretatie daarvan die waarde geven. Dat uit het bevolkingsregister blijkt dat X op een bepaald adres woont, krijgt pas waarde als dit wordt gecombineerd met het gegeven uit de database van de woningcorporatie dat dit een driekamerflat is en het feit dat er volgens bestanden van banken kennelijk nog 20 andere mensen op dat adres bankafschriften ontvangen. Data zijn dan gekoppeld tot informatie. Die informatie kan vervolgens nog meer waarde krijgen, wanneer uit nadere analyse blijkt dat X verdacht wordt van criminele of terroristische activiteiten.

Automatisering van gegevensbestanden heeft in de laatste tien jaar een grote vlucht genomen, zowel binnen de overheid als bij het bedrijfsleven. In dit hoofdstuk wordt nader ingegaan op het belang van gegevensbestanden voor informatie en intelligence in het veiligheidsdomein. Voor de ontwikkeling daarvan blijkt de strijd tegen het internationale terrorisme een grote rol te spelen. Daarom wordt in dit hoofdstuk ook ingegaan op enkele relevante internationale ontwikkelingen.

1.2 Groeiend belang van informatie

Informatie is altijd belangrijk geweest in het veiligheidsdomein. Lange tijd is er weinig beleidsmatige aandacht geweest voor het begrip 'informatie'. Het was immers een integraal onderdeel van de werkprocessen. In het gezaghebbende rapport 'Politie in Verandering' waarmee in 1977 de hoofdlijnen van de politiefunctie werden geschetst, wordt nauwelijks aandacht aan het belang van informatie geschonken. De sociale inbedding van de politie in de samenleving stond centraal en in dat rapport werd de basis gelegd voor het wijkgerichte optreden van de politie.[1] Toen in 2005 een andere generatie korpschefs een nieuwe visie op de politiefunctie ontwikkelde, kreeg informatie een veel belangrijkere positie: *"Informatie is feitelijk de grondstof van het politiebedrijf."* [2] Uitdrukkelijk werd in deze visie aangegeven dat de politie zich in toenemende mate ontwikkelt tot een kennisintensieve uitvoeringsorganisatie. Dit fenomeen zal in de toekomst verder tot ontwikkeling komen. De groei van gegevensbestanden leidt bijvoorbeeld bij de politie tot een sterke toename in het werkaanbod. In 2006 doorzochten de digitaal rechercheurs van de politie 75% meer bestanden dan het daaraan voorafgaande jaar. De politie houdt rekening met een jaarlijkse groei met een factor 1,5 tot 2, hetgeen capaciteitsproblemen tot gevolg heeft.[3]

1 Projectgroep Organisatie Structuren (1977). Politie in Verandering. 's-Gravenhage, Staatsuitgeverij.
2 Raad van Hoofdcommissarissen, Projectgroep Visie op de Politiefunctie, Politie in Ontwikkeling, Den Haag, 2005, pp. 92-93
3 Digitale opsporing komt capaciteit te kort, in: Automatisering Gids, 2 februari 2007

Een aantal ontwikkelingen heeft in de afgelopen jaren het belang van informatie in het veiligheidsdomein meer expliciet gemaakt: de groei van geautomatiseerde databestanden, terroristische aanslagen waarbij achteraf bleek dat veel relevante gegevens beschikbaar waren in gegevensbestanden van de overheid en de ontwikkeling van informatie gestuurd optreden in de opsporing.

Groei van geautomatiseerde databestanden

De eerste ontwikkeling is de groei van het aantal geautomatiseerde gegevensbestanden. Elke dag komen er nieuwe databases bij en ze bevatten daarnaast steeds meer gegevens. Ze zijn niet meer weg te denken uit onze samenleving. Vroeger had men voor een database een mainframe computer nodig, maar de ontwikkeling van de technologie heeft het mogelijk gemaakt dat elk bedrijf, elke overheid of elke burger op de eigen PC een of meer databases kan bijhouden. Iedereen kent de gemeentelijke bevolkingsadministratie (GBA), maar er zijn veel meer gegevensbestanden waar wij dagelijks mee te maken hebben of zullen krijgen, van de bestanden van grootwinkelbedrijven waar gegevens in zijn opgeslagen, de administratie van de creditcard maatschappij tot het komende elektronische patiëntendossier, waarin wordt opgeslagen wat wij mankeren en waarvoor wij een arts bezoeken.

Overheden leggen ook meer en meer bestanden aan, van de eigen gemeente die bijhoudt hoeveel inwoners klagen over bepaalde vormen van dienstverlening tot de Amerikaanse douane die gegevens bijhoudt over de miljoenen mensen die in de afgelopen jaren de Verenigde Staten hebben bezocht. Daarnaast worden bestanden aangelegd over specifieke doelgroepen. Een voorbeeld daarvan is de verwijsindex die het Ministerie van Justitie heeft laten ontwikkelen over Antilliaanse risicojongeren om een betere gegevensuitwisseling over deze groep mogelijk te maken.[4] Ook de beelden die worden opgenomen met beveiligingscamera's in het openbaar domein en vervolgens worden opgeslagen behoren tot dergelijke gegevensbestanden.

Daarnaast zijn er bedrijven die bijzondere databanken exploiteren met gegevens over personen en instellingen die door bedrijven en overheden worden gebruikt. Een voorbeeld daarvan is LexisNexis, een wereldwijde databank met meer dan 5 miljard documenten met gegevens uit meer dan 32.000 bronnen. Ruim 13.000 medewerkers zijn dagelijks bezig om deze databank actueel te houden en aan te vullen.[5] Een ander voorbeeld is World-check, een database met gegevens over personen en instellingen waarvan bekend is dat zij een financieel risico vormen (verdacht of veroordeeld voor fraude, witwassen, terroristische activiteiten etc.). Vooral banken en overheden maken gebruik van deze database.[6]

4 Persbericht van het ministerie van Justitie d.d. 19 december 2006: Verwijsindex Antillianen wordt in gebruik genomen.
5 Zie: www.lexisnexis.com
6 Zie: www.world-check.com

Met de explosieve groei van het aantal bestanden neemt ook de belangstelling van inlichtingen- en opsporingsdiensten toe. Alle vorig jaar opgeslagen digitale gegevens beslaan volgens onderzoek van het Amerikaanse IDC 161 miljard gigabyte, een hoeveelheid gegevens die gelijk staat aan 12 stapels boeken die van hier tot aan de zon reiken. Veel van die informatie wordt verspreid via Internet, de grootste database die er bestaat. In 1996 maakten 46 miljoen mensen gebruik van Internet. Dit aantal is inmiddels gestegen tot 1,1 miljard. Naar verwachting zal dit aantal in de komende drie jaar met nog eens 500 miljoen groeien. Aan deze groei komt voorlopig geen eind.[7]

Ontsluiting van deze gegevens en vooral koppeling van gegevens uit het ene bestand met gegevens uit een ander bestand kunnen zeer interessante gegevens opleveren die bruikbaar zijn voor zowel opsporingsdoeleinden als voor het voorkomen van criminaliteit of terroristische aanslagen. Inlichtingen- en opsporingsdiensten hebben steeds meer belangstelling voor de inhoud van deze bestanden. Voor zowel de eigenaren van deze bestanden als voor de partijen in het veiligheidsdomein is het daarom van het grootste belang dat bestanden correct worden beheerd en steeds actueel zijn.

Gemiste informatie over aanslagen

De tweede ontwikkeling was een direct gevolg van de aanslagen van 11 september 2001 op het World Trade Center in New York en het Pentagon in Washington. Achteraf is gebleken dat over de daders veel bekend was en dat een betere samenwerking tussen inlichtingen- en opsporingsdiensten de aanslagen mogelijk had kunnen voorkomen. Onderzoek door een onafhankelijke commissie toonde aan dat er veel over de daders bekend was, maar dat de beschikbare gegevens niet goed waren geanalyseerd en niet goed waren gecommuniceerd tussen de verantwoordelijke diensten. Kortom, de beschikbare gegevensbestanden waren onvoldoende benut en duidelijke kansen werden gemist: *"Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled. Effective operations were not launched. Often the hand-offs of information were lost across the divide separating the foreign and domestic agencies of the government."*[8] Het niet delen van informatie met elkaar door federale diensten was een belangrijke oorzaak van het falen van de overheid. Veel van deze diensten werken volgens het principe 'need to know'. Dat houdt de veronderstelling in, dat men vooraf kan weten, wat een ander aan informatie nodig heeft. Volgens die commissie moet er veel meer gewerkt worden vanuit het principe 'need to share': actief moet worden nagegaan, welke organisatie nut kan hebben van bepaalde informatie. De balans tussen veiligheid en gedeelde kennis moet in ere worden hersteld, aldus de commissie.[9]
Voorzitter Thomas Kean van die commissie vatte het eindoordeel scherp samen bij de presentatie van het rapport: *"Our intelligence and law-enforcement agencies did not*

7 John F. Gantz, e.a., The Expanding Digital Universe, A Forecast of Worldwide Information Growth Through 2010, uitgave van IDC, maart 2007, p. 7
8 National Commission on Terrorist Attacks Upon the United States, the 9/11 commission report, Washington, July 2004, p. 353
9 Idem, p. 417

manage or share information, or effectively follow leads, to keep pace with a nimble enemy." [10]

Deze conclusies waren des te wranger omdat al veel eerder was gewaarschuwd voor de noodzaak van een betere samenwerking tussen de overheidsdiensten en voor een beter gebruik van de beschikbare informatie. In 1996 had een andere onafhankelijke commissie gewezen op het belang van een goed gebruik van de beschikbare informatie, vooral ook in de strijd tegen internationale criminaliteit, waaronder terrorisme. Om de nieuwe bedreigingen van georganiseerde criminaliteit en terreur het hoofd te kunnen bieden, zouden inlichtingendiensten en politie veel meer moeten samenwerken en informatie moeten uitwisselen: *"While mindful of the potential risks of closer links, the Commission believes that the increasing threats to our national security from global crime require the two communities to work together."* [11] Vooral op het gebied van uitwisseling van informatie tussen inlichtingendiensten en politie zouden veel meer initiatieven moeten worden genomen, aldus die commissie: *"Intelligence must also be integrated more closely with other functions of government, such as law enforcement, to achieve shared objectives."* [12]

Maar 9/11 was niet het enige moment waarop bleek dat de beschikbare informatie tussen inlichtingendiensten en opsporingsdiensten niet goed wordt gedeeld en geanalyseerd. Ook de daders van de bomaanslagen in Madrid en London waren bij de betreffende inlichtingendiensten in het vizier. Uit recent onderzoek blijkt dat bij alle onderzochte 43 aanslagen of pogingen daartoe in West-Europa de dadergroepen in meer of mindere mate bekend waren bij de inlichtingendiensten en in daartoe bestemde databases waren opgenomen.[13] Die informatie was dus op zich wel aanwezig, maar was niet altijd op de goede plaats beschikbaar of er waren niet de goede conclusies uit die gegevens getrokken.

Informatie gestuurd optreden

De derde ontwikkeling is de opkomst in veel landen en ook in Nederland van informatie gestuurd optreden van de politie. Dit verschijnsel is ontwikkeld in de Angelsaksische landen en staat bekend als 'Intelligence Led Policing'. Informatie gestuurde politie (IGP) is een sturingsmodel op grond waarvan het politiewerk gerichter, meer gestructureerd en intelligenter kan worden ingericht. Door goede analyses en daarop gebaseerde heldere keuzes kunnen betere resultaten worden bereikt.[14] Dit nieuwe sturingsmodel was een reactie op toenemende kritiek dat de politie vooral reactief optreedt en niet proactief. Bij informatie gestuurde politie zijn onderzoek en analyse belangrijke

10 De speech is opgenomen op de website van de commissie: http://www.9-11commission.gov/report/911Report_Statement.pdf\
11 Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the twenty-first century An appraisal of U.S. intelligence, Washington, March 1996, p. 43
12 idem, p. XV
13 Wijk, R. de en C. Relk, Doelwit Europa, complotten en aanslagen van moslimextremisten, Amsterdam 2006
14 Inspectie Openbare Orde en Veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, een evaluatie van het project landelijke informatiecoördinatie DNP, Den Haag, 2004, p. 15

Die informatie was op zich wel aanwezig, maar was niet altijd op de goede plaats beschikbaar of er waren niet de goede conclusies uit die gegevens getrokken.

bouwstenen voor het benoemen van veiligheidsproblemen en voor keuzes om deze problemen aan te pakken. Op deze wijze wil de politie meer effectief en meer doelmatig opereren. Goede voorbeelden van deze nieuwe ontwikkelingen zijn het politiekorps Kent dat een voortrekkersrol in de ontwikkeling van de nieuwe aanpak heeft gehad en het politiekorps van New York, dat bekendheid heeft gekregen met de toepassing van geautomatiseerde systemen om criminaliteit beter in beeld te krijgen (CompStat).

In Nederland is informatie gestuurde politie aanvankelijk alleen toegepast in de opsporing. De basis daarvoor is vooral gelegd door het programmabureau Abrio, een landelijk politieprogramma dat tot doel heeft de rechercheprocessen te stroomlijnen. Het programmabureau heeft de hoofdlijnen voor informatie gestuurde opsporing ontwikkeld.[15] Op grond daarvan is vervolgens enkele jaren geleden het begrip informatie gestuurde politie (IGP) geïntroduceerd. Dat begrip neemt een belangrijke plaats in bij de vormgeving van het nieuwe politiemodel: *"Politiewerk is in belangrijke mate kennis gestuurd. Kennis van personen, situaties, normen en processen bepalen wat er gebeurt. De politie streeft ernaar informatie en kennis een grotere rol te laten spelen."* [16] Hoewel in steeds meer korpsen initiatieven worden genomen om informatiegestuurde politie in te voeren, zijn de beleidsdoelstellingen in veel korpsen nog geen dagelijkse praktijk. Goede werkprocessen voor briefing en debriefing zijn nog lang niet overal standaard ingevoerd. Informatie gestuurde politie wordt nog niet in alle regiokorpsen toegepast: *"Het is allemaal nog los zand."* [17] Veel is afhankelijk van mensen, omstandigheden en gevoel voor urgentie bij betrokken medewerkers. Bij bijzondere opsporingsdiensten is de ontwikkeling van informatie gestuurd werken al langer gemeengoed.

1.3 De ontwikkeling van intelligence

Informatie is niet hetzelfde als 'intelligence'. Intelligence is als werkproces en als product vooral een bekend begrip bij de inlichtingendiensten.[18] Bij de politie in de Angelsaksische landen is intelligence in de laatste jaren een begrip geworden en in Nederland wordt van diverse kanten een pleidooi gevoerd om het ook hier in de opsporingsprocessen te hanteren. Onder intelligence verstaat de adviescommissie de combinatie van informatie met analyse en verbinding. Intelligence maakt onderdeel uit van een keten die begint met gegevens (data), welke in een context worden geplaatst en gecombineerd met andere gegevens. Daardoor ontstaat informatie. Vervolgens leidt deze informatie via analyse en onderzoek tot intelligence, de basis voor besluitvorming over te nemen acties (kennis). Intelligence is van cruciaal belang voor besluitvorming, planning, strategieontwikkeling en preventie.

15 Zie voor een overzicht van de ontwikkelingen rond informatie gestuurde politie: Huisman, Aletha, Informatie-Gestuurde Politie: de tijd en moeite waard?!, scriptie bestuurskunde Universiteit Twente, 2006
16 Raad van Hoofdcommissarissen, Projectgroep Visie op de Politiefunctie, Politie in Ontwikkeling, Den Haag, 2005, p. 17
17 Huisman, p.29
18 Ook in de wereld van de inlichtingendiensten verloopt de ontwikkeling van intelligence met vallen en opstaan. Zie hierover bijvoorbeeld: Giliam de Valk , Dutch Intelligence - Towards a Qualitative Framework for Analysis: with case studies on the Shipping Research Bureau and the National Security Service (BVD), proefschrift, Groningen, 2005

In een Amerikaanse studie over de plaats van intelligence in de 21e eeuw werden de navolgende doelstellingen van intelligence onderscheiden:

- ondersteunen van nationaal diplomatiek proces,
- monitoren van internationale verdragen,
- ondersteunen van militaire operaties en de planning daarvan,
- verzamelen van economische gegevens,
- verzamelen van informatie om bedreigingen van de VS in het buitenland tegen te kunnen gaan,
- ondersteuning van opsporing en regelgeving,
- verzamelen en analyseren van gegevens omtrent bedreigingen van het milieu en van de volksgezondheid, en
- de bestrijding van digitale oorlogsvoering (information warfare).[19]

In de wereld van de veiligheidsdiensten omvat het begrip intelligence het geheel van verzamelen en analyseren van gegevens die nodig zijn om de veiligheid van de staat te waarborgen. Er worden verschillende vormen van intelligence onderscheiden, zoals bijvoorbeeld: signals intelligence (SIGINT), intelligence die wordt verkregen uit elektronisch berichtenverkeer, human intelligence (HUMINT), intelligence die wordt verkregen door middel van informanten, en open source intelligence (OSINT). Dit laatste wordt verkregen uit open bronnen, zoals media en Internet. Ook wordt meer en meer gebruik gemaakt van inlichtingen vanuit de gemeenschap, community intelligence.

De wereld van de inlichtingen- en veiligheidsdiensten noemt zich veelal de intelligence-gemeenschap. Daarin ziet zij voor de politie over het algemeen geen plaats, behoudens voor zeer gespecialiseerde diensten, die dicht tegen de veiligheidsdiensten aanzitten. In de VS is de FBI bijvoorbeeld onderdeel van de intelligence-gemeenschap.[20] In het Verenigd Koninkrijk zijn de douane en de onlangs opgerichte Serious Organised Crime Agency (SOCA) in tegenstelling tot de reguliere politie wel onderdeel van wat in dat land wordt genoemd de 'Intelligence Machinery'. [21]

Vooral vanuit de kring van informatiespecialisten en analisten in de opsporing wordt de ontwikkeling van kennis op dit gebied bepleit. Zij benadrukken dat vooral de analyse van het beschikbare materiaal nu bij de politie onvoldoende aandacht krijgt. En juist die analyse maakt het verschil tussen informatie en intelligence. In het analyseproces wordt systematisch gezocht naar informatie, wordt deze onderzocht en vergeleken met andere informatie en dat bepaalt de waarde voor de opsporing. In de analyse vindt een beoordeling van de criminaliteit plaats en wordt de basis gelegd voor strategische

19 Commission on the Roles and Capabilities of the United States Intelligence Community, op. cit., pp. 20-27
20 An Overview of the United States Intelligence Community, uitgave van The Office of the Director of National Intelligence, Washington, 2007
21 National Intelligence Machinery, uitgave van The Stationery Office, September 2006, zie ook www.intelligence.gov.uk

besluitvorming door de leiding van de organisatie. [22] Externe gegevensbestanden spelen bij die systematische analyse een belangrijke rol. Naarmate intelligence een belangrijkere rol in de opsporingsprocessen gaat spelen, groeit ook de behoefte aan gegevens uit externe databases.

Belangrijke bouwstenen voor de ontwikkeling van intelligence op het gebied van de opsporing zijn genoemd in enkele studies van het Amerikaanse Ministerie van Justitie.[23] Het Department of Justice onderscheidt opsporingsorganisaties naar vier niveaus van intelligence:

- Niveau 1 betreft organisaties die tactische en strategische intelligence producten ontwikkelen, waar niet alleen de eigen dienst gebruik van kan maken, maar ook andere partners in het veiligheidsdomein.
- Niveau 2 betreft organisaties die intelligence ontwikkelen welke gebruikt kan worden voor ondersteuning van eigen onderzoeken. Andere partners in de keten blijven buiten beeld.
- Op niveau 3 functioneren organisaties die geen eigen productie op het gebied van intelligence hebben, maar die gebruik maken van de diensten van andere partijen in de keten.
- Op niveau 4 functioneren de organisaties die geen eigen mensen hebben die kennis hebben van ontwikkeling of toepassing van intelligence.

De meeste politieorganisaties in de VS bevinden zich volgens deze studie nog op het laagste niveau, niveau 4. Veel moet dus nog gebeuren aan de ontwikkeling van een juist stelsel van intelligence op het gebied van opsporing: *"The key to intelligence-led policing is that sufficient interest and training should exist to create a culture of knowledge and intelligence in agencies nationwide."* [24] Zelfs de FBI, die deels inlichtingendienst en deels opsporingsdienst is, presteert onvoldoende op het gebied van de ontwikkeling van intelligence. Een belangrijke oorzaak hiervan is dat analyse heel lang ondergewaardeerd is geweest. Analisten hoorden bij de FBI tot de ondersteunende staf.[25] Dit oordeel over de gebrekkige kennis van veel politiekorpsen wordt gedeeld door de voorzitter van de internationale organisatie van politieanalisten, Lisa M. Palmieri, die een breed overzicht heeft over de ontwikkelingen op het gebied van intelligence: *"Until recently, there were few departments at the state and local levels which were capable of producing intelligence; most often, the analytic component was missing."* [26]

22 U.S. Department of Justice, Bureeau of Justice Assistance: The National Criminal Intelligence Sharing Plan, Washington 2003
23 Zie voor een overzicht: U.S. Department of Justice, Bureau of Justice Assistance, Intelligence-Led Policing: The New Intelligence Architecture, Washington 2005
24 Idem, p. 13
25 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, report to the president, Washington, 2005, p. 455
26 Lisa M. Palmieri, Information vs. Intelligence : What Police Executives Need to Know, uitgave van de International Association of Law Enforcement Intelligence Analysts

Deze woorden zijn ook van toepassing op situatie van de Nederlandse opsporing. De Nederlandse politie heeft wel een visie op het belang van informatiesturing, zoals neergelegd in de nota 'Politie in Ontwikkeling', maar zowel de implementatie van het concept informatie gestuurde politie als de uitwerking op het gebied van intelligence zijn nog niet gerealiseerd. Hoewel al in 2006 een visiedocument is verschenen waarin de visie op informatiesturing is uitgewerkt op het gebied van informatiemanagement en technologie[27], ontbreekt een strategische uitwerking van deze visie op het gebied van de ontwikkeling van intelligence. Een eerste concept voor een systeem van intelligence voor de politie circuleert nu binnen een hiertoe opgerichte werkgroep van de Raad van Hoofdcommissarissen. In een brief aan de Tweede Kamer heeft de voormalige minister van BZK onlangs de ontwikkeling van een nationaal intelligence model aangekondigd. Hij voegde daar aan toe dat de ontwikkeling een concernverantwoordelijkheid van de politie betreft, waarbij ook de departementen en de AIVD betrokken moeten zijn. Deze gewenste ontwikkeling *"behoeft nog de nodige aandacht."* [28]

1.4 De opbouw van intelligence

Het proces van intelligence kent een aantal stappen. De diverse inlichtingen- en opsporingsdiensten hanteren daarbij verschillende onderverdelingen. Allemaal hanteren zij echter het uitgangspunt dat een goede intelligence alleen mogelijk is als de onderliggende gegevens correct en eenduidig zijn. In elke onderverdeling wordt daarom aandacht besteed aan het verkrijgen van de juiste, correcte data.

De Britse onderzoekster Nina Cope[29] onderscheidt de volgende fases in het proces van intelligence: verzameling van data, analyse, prioritering, het ondernemen van actie en evaluatie van de resultaten. Hier begint het proces van intelligence dus bij de gegevens. Volgens haar blijft de ontwikkeling van intelligence bij de politie achter door een gebrek aan kennis bij politiemensen en analisten over de wederzijdse werkprocessen. De Valk[30] maakt een ander onderscheid. Hij benoemt de navolgende onderdelen van het proces: ontwerp van het intelligence-proces, verzameling van gegevens, bewerking en filtering van de gegevens, analyse van de gegevens, opstelling rapportage en verspreiding van de intelligence-resultaten naar de betrokken autoriteiten. Hier begint het proces dus bij de behoeftestelling. In beide onderscheidingen wordt voorbijgegaan aan twee belangrijke onderdelen van het proces: in het ene onderscheid wordt voorbij gegaan aan de planning en de behoeftestelling en in het andere onderscheid aan de evaluatie van het intelligence-proces.

27 Raad van Hoofdcommissarissen, Wenkend Perspectief, strategische visie op politieel informatiemanagement & technologie, Den Haag, 2006
28 Brief van de Minister van BZK aan de Tweede Kamer d.d. 12 februari 2007 betreffende de landelijke coördinatie en uitwisseling van politie-informatie.
29 Nina Cope, Intelligence Led Policing or Policing Led Intelligence? Integrating Volume Crime Analysis into Policing, British Journal of Criminology, vol. 44, 2004, pp. 188-203 (Centre for Crime and Justice Studies)
30 De Valk, op. cit., pp. 12-13

De Verenigde Staten hebben onlangs in een nieuwe strategie de opbouw van intelligence gedefinieerd. Volgens dit beleidsplan kent het proces van intelligence de volgende stappen: planning en sturing, verzameling van gegevens, verwerking, analyse, verspreiding en evaluatie op bruikbaarheid. De meest voorkomende methoden voor het verzamelen van gegevens zijn: surveillance, elektronisch toezicht, informanten, undercover operaties, openbare bronnen (kranten en Internet) en externe databases. Analyse is een sleutelbegrip in intelligence. In de National Intelligence Strategy is verdere versterking van de deskundigheid op dit terrein een van de hoofdpunten voor de komende jaren.[31]

De ontwikkeling van intelligence in de inlichtingendiensten gaat een andere weg dan de ontwikkeling in de opsporingsdiensten. Dat heeft voor een belangrijk deel te maken met verschil in doelstelling en positie van beide soorten diensten. Buiten deze begrijpelijke verschillen zijn er ook belangrijke overeenkomsten in belang en positionering van intelligence binnen die diensten: intelligence is toekomstgericht, komt multidisciplinair tot stand en is een gemotiveerde basis voor besluitvorming. Voor beide geldt als belangrijk uitgangspunt dat de kwaliteit van intelligence in belangrijke mate afhankelijk is van beschikbaarheid en juistheid van data en van een goede interpretatie van die data.

Naast de beschikbaarheid van juiste gegevens is ook analyse van die gegevens een centraal onderdeel van intelligence. Er worden steeds meer methoden en technieken voor analyse ontwikkeld. Voorbeelden van analysetechnieken zijn: misdaadpatronen, gedragsanalyses, daderanalyses, analyse van betalingsstromen, dreigingsanalyses, risicoanalyses en kwetsbaarheidsanalyses.

Met het oog op het belang van intelligence en op de discussie binnen de Nederlandse politie over de ontwikkeling van een eigen model voor de politie en om de noodzaak van het procesmatige karakter te benadrukken, stellen wij de volgende cyclische benadering van het proces intelligence voor:

Intelligence is in deze opvatting geen keten met een begin en een eind, maar een proces. In de eerste fase, behoeftestelling wordt bepaald waarom welke informatie nodig is en op welke wijze die kan worden verkregen. In de volgende fase worden de noodzakelijke gegevens (data) verzameld. Daarna worden de verschillende gegevens bewerkt en gecombineerd tot informatie. Deze informatie wordt geanalyseerd. Dit analyseproces leidt tot intelligence. Dit resultaat wordt vervolgens voorgelegd aan de leiding die beslist over het vervolg en over eventuele verdere verspreiding van de intelligence. De laatste stap in dit proces is de evaluatie. Dan wordt de vraag bezien of de verkregen intelligence voldoet aan de eisen uit de behoeftestelling en waar verbeteringen in het proces kunnen worden aangebracht.

Er is nog een reden waarom wij dit proces op deze manier presenteren. Bestuurlijk en politiek is er voor verschillende onderdelen van het proces van intelligence regelmatig aandacht. Op één uitzondering na: de verzameling van data en de kwaliteit daarvan. Dat onderwerp krijgt in de bestuurlijke en politieke discussie nauwelijks aandacht. En dat is nu juist het enige onderdeel waarop de laatste jaren inhoudelijk veel is veranderd door de opkomst en groei in aantal en omvang van geautomatiseerde gegevensbestanden.

1.5 Veiligheid en privacy

De bescherming van de persoonlijke levenssfeer heeft tal van aspecten:

- Er is allereerst de fysieke privacy, de persoonlijke levenssfeer van het menselijk lichaam. De overheid treedt die levenssfeer binnen bij fouilleringen of inwendige onderzoeken (bij vermeende bolletjesslikkers).
- In de tweede plaats is er de territoriale privacy, de persoonlijke levenssfeer van de verblijfplaats zoals het eigen huis. De overheid kan op deze privacy inbreuk maken door bijvoorbeeld huiszoeking.
- Een derde vorm van privacy is de informationele privacy, de levenssfeer van de gegevens. De overheid kan op deze privacy inbreuk maken door opslag, koppeling en onderzoek van persoonlijke gegevens.
- In de vierde plaats is er de communicatieve privacy, de levenssfeer van de communicatie. De overheid kan op deze privacy inbreuk maken door het aftappen van telefoons en door het bewaren van gegevens over gebruik van telefoon en Internet.

Voor het onderzoek van de adviescommissie zijn vooral de laatste twee vormen van privacy van belang. Door de explosieve groei van de gegevensbestanden en de communicatiemogelijkheden kan de persoonlijke levenssfeer van burgers steeds vaker en steeds indringender in het geding komen. Dit kan zeer zeker het geval zijn bij koppeling van gegevensbestanden of het toepassen van nieuwe zoekinstrumenten, zoals datamining. De enorme groei van databanken en communicatiemogelijkheden en de opkomst van geavanceerde technologie om te zoeken in deze grote hoeveelheid gegevens bieden de inlichtingen- en opsporingsdiensten veel nieuwe mogelijkheden om hun doelstellingen te realiseren. Daarvoor maken zij inbreuk op de persoonlijke levenssfeer van mensen. Een groot zorgpunt voor velen is of daarbij de juiste balans wordt gehandhaafd tussen inbreuk op de levenssfeer van verdachte personen en die van onschuldige mensen.

31 Director of National Intelligence, The National Intelligence Strategy of the United States of America, Transformation through Integration and Innovation, Washington, 2005, p. 12

Tot nu toe is de regering nog niet uitgebreid ingegaan op de groeiende zorgen over mogelijke aantastingen van de persoonlijke levenssfeer door de uitbreiding van de bevoegdheden van inlichtingen- en opsporingsdiensten. Eind januari 2007 heeft de regering gereageerd op zorgen op dit punt vanuit de Eerste Kamer in de memorie van antwoord inzake de nieuwe wet op de politieregister. De minister gaf daarin aan dat er naast de uitbreiding van bevoegdheden gezorgd wordt voor meer waarborgen voor de bescherming van de privacy. Volgens hem is er sprake van een *"nieuw evenwicht."*[32]

1.6 Databases en criminaliteit

Een andere relatie tussen databases en het veiligheidsdomein wordt hier kort even aangestipt, omdat die steeds meer aandacht van zowel inlichtingen- als opsporingsdiensten vraagt. Die relatie valt weliswaar buiten de directe opdracht aan de adviescommissie, maar is daar wel zeer nauw mee verbonden. Deze relatie betreft het misbruik van gegevensbestanden voor criminele activiteiten. De gegevensbestanden worden misbruikt voor identiteitsfraude. Identiteitsfraude is weer de basis voor fraude, oplichting, witwassen en pogingen tot maatschappelijke ontwrichting.

Criminelen proberen in toenemende mate gegevensbestanden te kraken. Zij zoeken via grote databases toegang tot een grote hoeveelheid persoonlijke gegevens om vervolgens met behulp van die gegevens identiteitsfraude te plegen. Identiteitsfraude is vooral in de Verenigde Staten in de afgelopen jaren sterk gegroeid; het is de snelst groeiende vorm van criminaliteit. In 2003 zijn ongeveer 3,25 miljoen Amerikanen slachtoffer geweest van een of andere vorm van identiteitsfraude.[33] Uit onderzoek is gebleken dat vooral databestanden van de overheid hierbij een belangrijke bron van gegevens voor criminelen zijn. In mei 2006 ontdekte het Department of Veterans Affairs dat een computer met persoonlijke gegevens over ongeveer 2,6 miljoen veteranen en actieve militairen was gestolen uit het huis van een medewerker van het ministerie. Naar aanleiding van dit incident heeft een commissie uit het Congres onderzoek gedaan naar de beveiliging van gegevensbestanden bij andere ministeries en agencies. Uit dat onderzoek bleek dat alle onderzochte organisaties in het afgelopen half jaar te maken hadden gehad met verlies van persoonlijke gegevens. Meestal was onbekend welke informatie precies was verdwenen en hoe groot de schade was. Het grootste deel van de incidenten was te wijten aan de daadwerkelijke diefstal van computers of gegevendragers of misbruik van databestanden door eigen medewerkers. [34] Ook andere organisaties in het publieke domein beveiligen hun databases vaak onvoldoende. De Universiteit van Californië moest vorig jaar een brief sturen aan alle 800.000 mensen wier gegevens zij in hun computersysteem hebben opgeslagen (personeel, studenten, oud-studenten) met de mededeling dat een hacker er in was geslaagd om dit computersysteem binnen te dringen en gegevens te stelen.[35]

32 Kamerstuk 30 327, Regels inzake de verwerking van politiegegevens (Wet politiegegevens), nr. C, p. 5
33 Federal Trade Commission, Identity Theft Survey Report, Washington, 2003
34 House Committee on Government Reform, Staff Report, Agency Data Breaches since January 1, 2003, Washington 2006
35 Zie volgende pagina

Ook in Nederland neemt het probleem van identiteitsfraude toe. In 2005 zijn er in Nederland 187.510 paspoorten en nationale identiteitskaarten als gestolen of vermist opgegeven. De vraag komt op hoeveel van deze paspoorten in verkeerde handen terecht zijn gekomen en worden gebruikt voor criminele of terroristische activiteiten. Volgens de regering is hier geen inschatting van te maken.[36] Er is weinig bekend over de omvang van identiteitsfraude in Nederland. De overheid krijgt er wel steeds meer mee te maken:

- Gevangenen blijken niet altijd de personen te zijn, die veroordeeld zijn: uit een steekproef onder gevangen bleek dat 7% ook bekend staat onder een andere identiteit, zodat twijfel bestaat over de juiste identiteit;
- Verdachten staan vaak onder meerdere identiteiten bekend. Van de ruim 1,2 miljoen mensen van wie vingerafdrukken in het politiesysteem HAVANK zijn opgenomen bezitten volgens recent onderzoek ruim 92.000 mensen meerdere identiteiten, variërend van 2 tot 51. Uit vergelijkend onderzoek naar 46 personen die in een ander politiesysteem zijn opgenomen, bleken 33 van de 46 onderzochte personen bekend te staan onder meerdere identiteiten, ook bij de Gemeentelijke Bevolkingsadministratie.[37]
- De Gemeentelijke Bevolkingsadministratie (GBA) beschikt niet altijd over correcte gegevens. Uit een onderzoek van de gemeente Amsterdam naar de juistheid van de GBA-gegevens bleek dat in 7,3% van de adressen fouten voorkomen. Dit cijfer is volgens het ministerie van BZK aanmerkelijk hoger dan volgens onderzoeken in andere gemeenten als landelijk gemiddelde is gemeten, namelijk. 3%. Er is nog geen verklaring voor dit grote verschil gevonden.[38] Overigens is niet duidelijk in hoeveel van deze gevallen het gaat om fouten dan wel om fraude.

Volgens de Utrechtse hoogleraar Grijpink komt identiteitsfraude veel vaker voor dan over het algemeen wordt aangenomen: *"Identiteitsfraude verspreidt zich als een olievlek tot in de kleinste administratieve haarvaten van allerlei maatschappelijke processen waar men de geslaagde primaire identiteitsfraude vaak niet meer kan doorzien."*[39]
De FIOD is een van de weinige organisaties die daarover heeft gepubliceerd. Een onderzoek in 2003 naar identiteitsfraude bij 250 bedrijven bleek dat dit fenomeen op bredere schaal voorkomt dan gedacht. Het leverde de FIOD 7 keer meer op aan achtergehouden belastinggelden dan was ingeschat.[40]

Hoe complex identiteitsfraude is, blijkt uit de gang van zaken rond de invoering van het Burger Service Nummer (BSN). Voor de regering is een van de voordelen van dit nummer om daarmee de kansen op identiteitsfraude te beperken. Tegenstanders van

35 Persbericht van de University of California in Los Angeles (UCLA), d.d. 12 december 2006: UCLA warns of Unauthorized Acces to Restricted Database. Het systeem bevat van deze mensen uitgebreide persoonlijke informatie zoals NAW-gegevens, social security nummers, geboortedatum en contactinformatie. Het systeem bevatte geen bankrekening- of credit card gegevens.
36 Kamerstuk 25 764, reisdocumenten, nr. 28, p. 2
37 Kamerstuk 30 800 VI, begroting voor het ministerie van justitie voor het jaar 2007, nr. 23, p. 2
38 Antwoord van de Minister van Bestuurlijke Vernieuwing in antwoord op vragen uit de Tweede Kamer, Aanhangsel van de Handelingen, vergaderjaar 2006-2007, nr. 399
39 Grijpink, J.H.A.M, Identiteitsfraude en Overheid, Justitiële Verkenningen, 2006, pp. 37-57
40 Franken, L, Literatuuronderzoek Identiteitsfraude 2004, Universiteit Utrecht 2005, p. 30

het wetsontwerp voeren daarentegen juist weer aan dat het Burger Service Nummer die kansen juist versterkt. Voor de Eerste Kamer is die mogelijkheid van fraude een van de gronden om het voorstel met grote aarzeling te bekijken: met het Burger Service Nummer wordt de overheid de regisseur over persoonsgegevens in plaats van de betrokken burger, zo is de vrees van de Eerste Kamer.[41] Ondanks een nadrukkelijke oproep daartoe van de Raad van State gaat de regering het onderwerp identiteitsfraude in discussie over dit wetsontwerp uit de weg. Daardoor is er nog geen antwoord op *"fundamentele vragen die spijtig genoeg in het huidige debat over identificatie en identificatie-instrumenten onbeantwoord blijven."* [42]

Naast identiteitsfraude komen ook andere vormen van criminaliteit met behulp van ICT-technologie steeds vaker voor. Vormen van computercriminaliteit zijn illegale communicatie (voor het verspreiden van criminele gegevens, zoals kinderporno), inbraak in databestanden en beschadiging van ICT-netwerken (onder meer door het verspreiden van virussen). De regering is met het oog hierop begonnen met het opbouwen van een nationale infrastructuur bestrijding cybercrime. Hiertoe behoort ook GOVCERT, het computer emergency response team van de overheid en het Nationaal Meldpunt Cybercrime. Een hieruit ontstaan initiatief tot oprichting van een National High Tech Crime Center (NHTCC) liep al snel op een mislukking uit als gevolg van een onduidelijke aansturing.[43]

De relatie tussen de hier genoemde vormen van criminaliteit en het onderwerp van onderzoek van de adviescommissie is gelegen in het belang van gegevensbestanden voor het veiligheidsdomein: Deze bestanden worden steeds belangrijker voor onze collectieve veiligheid en ieders individuele vrijheid, maar ook voor iedereen die om wat voor reden dan ook inbreuk wil maken op die vrijheid, of daar misbruik van wil maken. Daarom ook is het van belang om meer dan voorheen aandacht te besteden aan zowel veiligheid als onveiligheid van die bron: de gegevensbestanden en aan de manier waarop met die bestanden wordt omgegaan, inclusief de beveiliging van die bestanden, de waarborgen voor de privacy en de mate waarin toegang tot en gebruik van die bestanden geoorloofd is. Het belang van de gegevensbestanden vergt een breder maatschappelijk en politiek debat dan op dit moment wordt gevoerd.

1.7 Internationaal kader

Ten behoeve van haar onderzoek is de adviescommissie nagegaan of er buitenlandse voorbeelden zijn waar Nederland zijn voordeel mee kan doen. Uit een eerste oriëntatie is gebleken, dat er weinig onderzoeksmateriaal voorhanden is met betrekking tot

41 Zie de Kamerstukken 30 312 (met name het nader voorlopig verslag van de Eerste Kamer d.d. 28 februari 2007) en 30380
42 Prins, C., Variaties op een thema: van paspoort- naar identiteitsfraude, Nederlands Juristenblad, 2006, nr. 1
43 Zie kamerstukken 26 671, Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), in het bijzonder de brief van de staatssecretaris van Economische Zaken van 18 mei 2006 inzake het ontwerp van de Nationale Infrastructuur Bestrijding Cybercrime, stuk nummer 24

de systematiek van inwinnen van gegevens uit externe gegevensbestanden. In een volgende fase van het onderzoek zal op dit punt meer verdieping plaats moeten vinden. Nog in het voorjaar van 2007 hoopt de adviescommissie een Europese expertmeeting te beleggen teneinde op dit punt meer inzicht te verkrijgen.
Door middel van deskresearch en werkbezoeken aan twee referentielanden heeft de adviescommissie geprobeerd inzicht te verkrijgen in het internationaal kader voor haar onderzoek. Daartoe heeft zij enkele bezoeken gebracht aan het Verenigd Koninkrijk en de Verenigde Staten met het doel potentiële best practices te identificeren.

Internationale gegevensuitwisseling

Ondanks alle pogingen daartoe, komt de uitwisseling van gegevens tussen Europese inlichtingendiensten nog onvoldoende van de grond. Daarbij spelen twee zaken een rol: de gerichtheid op het eigen belang en het aanboren van nieuwe inlichtingenbronnen. Alle diensten zijn vooral gericht op hun eigen belang en hebben onderling spanning: *"Van een gecoördineerde gezamenlijke aanpak is vooralsnog geen sprake."* [44] Om terroristische aanslagen in de toekomst waar mogelijk te voorkomen boren inlichtingen- en opsporingsdiensten nieuwe bronnen aan om zoveel mogelijk gegevens te kunnen verzamelen.

In het kader van de opsporing neemt de druk toe om gegevens over mogelijke terroristen uit te wisselen. Vooral financiële gegevens blijken daarbij van belang te zijn. Er ontstaat daarom ook meer druk om deze gegevens beter beschikbaar te krijgen: *"In the US and the UK, there will also be pressure for 'real time' financial intelligence to monitor transactions as they happen."* [45] Hieromtrent is overigens al veel publiciteit geweest vanwege de informatie die aan de Amerikaanse overheid is verstrekt door SWIFT, de private organisatie die dagelijks meer dan 10 miljoen internationale transacties verricht voor 8100 banken en financiële instellingen over de hele wereld. Recent werd bekend dat ook Nederlandse banken gegevens over hun klanten verstrekken aan de Amerikaanse overheid. [46] Vanuit dezelfde achtergrond zoekt de Amerikaanse overheid naar mogelijkheden om meer informatie te verkrijgen over mensen die het land binnen willen komen, zoals met het in de pers veel besproken programma voor screening van passagierslijsten van luchtvaartmaatschappijen. Ook andere landen zijn druk doende met soortgelijke programma's, waaronder Nederland. In Engeland bestaat het programma Semaphore, een programma van verschillende departementen dat beoogt onder coördinatie van het Home Office passagiers die het land binnenkomen te screenen en na te gaan of zij een veiligheidsrisico zijn. Via een geautomatiseerd systeem wordt bijgehouden of zij weer tijdig het land hebben verlaten. [47]

44 Cees Wiebes, Geheime diensten moeten over eigen schaduw springen; Inlichtingendiensten dienen bij uitstek het nationale statsbelang, gepubliceerd in de Newsletter van de Netherlands Intelligence Studies Association, www.nisa-inteliigence.nl
45 Wittig, Tim, Not so Legal tender, what next for the financial war on terrorism? In: Jane's Intelligence Review, February 2007, p. 17
46 Zie hierover bijvoorbeeld: "CIA kijkt via achterdeur mee bij banken; monetaire autoriteiten zwegen vier jaar lang tegenover Tweede Kamer", NRC Handelsblad, 10 maart 2007
47 Persbericht van het Home Office van 28 september 2004

Wetenschappelijk onderzoek

Het gebruik van geautomatiseerde gegevensbestanden is vooral in het kader van de terrorismebestrijding nader onderzocht. Onderzoek van het WODC naar het terrorismebeleid in een aantal Westerse landen sinds 2001 geeft aan dat er in alle onderzochte landen in toenemende mate wordt vertrouwd op technologische mogelijkheden om terrorisme te bestrijden. Met behulp van nieuwe zoektechnieken wordt geprobeerd om mogelijke terroristen op te sporen. Het gaat hierbij vooral om geavanceerde technieken om mogelijke terroristen te lokaliseren en te identificeren. Toepassingen van ICT worden daarbij steeds meer gebruikt. Ook worden in alle onderzochte landen steeds meer databases aangelegd met gekoppelde gegevens over burgers. Uit het onderzoek van het WODC blijkt overigens dat de nieuwe technieken vooral leiden tot een overvloed aan data, vaak van matige kwaliteit, waaruit nog maar moeilijk patronen kunnen worden gehaald.[48]

Onderzoek van RAND heeft uitgewezen dat alle West-Europese landen in de afgelopen jaren hun inspanningen op het gebied van inwinnen van gegevens en ontwikkeling van intelligence sterk hebben geïntensiveerd. Binnen deze algemene conclusie vallen wel verschillen tussen de onderzochte landen te signaleren. Sommige landen hebben op dit punt veel meer initiatieven ontplooid dan andere landen. In weer andere landen zijn de bevoegdheden van de inlichtingendiensten sterk uitgebreid. Daarnaast concludeert het onderzoek dat de samenwerking tussen (militaire) inlichtingendiensten en opsporingsdiensten in landen met nationale politie beter verloopt dan die in landen met een meer gedecentraliseerde structuur. Ook in dit rapport wordt gewezen op het belang van de gegevens uit geautomatiseerde databases. Er is meer hoog gekwalificeerd personeel nodig om deze databases te ontsluiten en de informatie daaruit om te zetten in intelligence. In alle onderzochte landen is een gebrek aan daartoe opgeleide medewerkers. [49]

Uit een evaluatie in opdracht van de Europese Commissie van de nationale maatregelen in de strijd tegen het terrorisme is de behoefte gebleken om meer toegang te krijgen tot allerlei databanken. Op grond van deze evaluatie is aan alle lidstaten de aanbeveling gedaan om wetgeving te overwegen die het veiligheidsdiensten mogelijk maakt meer en eerder toegang tot gegevensbanken te krijgen teneinde terroristen, terroristische netwerken en individuen die hen steunen in *"een vroeg stadium te kunnen opsporen en identificeren en aan een profielanalyse te onderwerpen."* [50]

Verenigde Staten

Delen van informatie tussen inlichtingen- en veiligheidsdiensten en opsporingsdiensten, maar ook binnen deze diensten is sinds 9/11 een belangrijk aandachtspunt. Datzelfde geldt voor het delen van informatie door deze diensten met marktpartijen en maatschappelijke organisaties. Bestuurders en politici dringen aan op een beter delen van informatie, zodat criminaliteit en terrorisme beter bestreden kunnen worden. Desondanks leveren al deze pogingen maar moeizaam resultaat op.

In 2005 besteedde een commissie die de aanloop naar de oorlog in Irak onderzocht veel aandacht aan dit onderwerp. De commissie constateerde dat er sinds 2001 meer dan 100 verschillende initiatieven waren geweest om informatie beter te delen, maar dat over het algemeen de vooruitgang onevenwichtig en te gering was geweest: *"Decisions to withhold information are typically based on rules that are neither clearly defined nor consistently applied, with no system in place to hold collectors accountable for in appropriately withholding information."* [51] Volgens deze commissie zijn de gebrekkige resultaten vooral te wijten aan organisatorische, beleidsmatige en culturele obstakels. Vooral onderling wantrouwen blijkt een grote rol te spelen. Dezelfde conclusie trekt de officiële onderzoeksdienst Congressional Research Service (CRS) van het Congres die een inventarisatie heeft gemaakt van de getroffen maatregelen om het delen van informatie te verbeteren.[52]

Het Amerikaanse Congres heeft bij diverse gelegenheden benadrukt dat de inlichtingendiensten meer informatie moeten delen met politiediensten. Deze diensten spelen volgens het Congres een veel belangrijkere rol in de terrorismebestrijding dan veel inlichtingendiensten denken. De inlichtingendiensten maken daarbij een belangrijke inschattingsfout, aldus het Congres: veiligheid hangt voor een groot deel af van agenten in de lokale gemeenschappen. Belangrijk uitgangspunt daarbij is dat de bestrijding van terrorisme alleen goed mogelijk is door zoveel mogelijk gebruik te maken van kennis die aanwezig is bij lokale en regionale politiekorpsen of door deze korpsen kan worden verzameld. De federale overheid heeft op dit moment te weinig aandacht voor dit probleem, waardoor een in potentie grote bron van kennis niet wordt benut. Er is als gevolg daarvan onvoldoende verticale doorstroming van informatie. De kennis zit lokaal en moet daar worden opgehaald en verwerkt. Om die reden heeft het Congres tal van initiatieven genomen om het delen van informatie te bevorderen.[53]

Daarnaast hebben ook diverse thinktanks en onderzoeksorganisaties aangedrongen op betere uitwisseling van informatie. Een belangrijke plaats hierbij is ingenomen door de onafhankelijke Markle Foundation, die drie gezaghebbende rapporten over dit onder-

48 Neve, Rudie, e.a., Eerste inventarisatie van contraterrorismebeleid, Cahier 2006-3 van het WODC, Ministerie van Justitie, Den Haag, 2006, p. 91

49 Linde, Erik van, e.a., Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries, RAND Europe, 2002

50 Besluit van de Raad van ministers van Binnenlandse Zaken en Justitie (Raad JBZ) van 1 en 2 december 2005 tot vaststelling van het Eindrapport over de evaluatie van nationale maatregelen ter bestrijding van het terrorisme: verbetering van de nationale actiemiddelen en vermogens ter bestrijding van het terrorisme, document 12168/3/05 REV 3

51 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, report to the president, Washington, 2005, p. 431

52 Congressional Research Service, Information Sharing for Homeland Security, A Brief Overview, Washington, January 2005, p. 5

53 Voorbeeld hiervan is: Congressman Bennie G. Thompson (sinds begin 2007 voorzitter van de commissie voor Homeland Security), LEAP, a Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing between the Intelligence Community and State, Local and Tribal Law Enforcement, Washington, 2006

werp heeft samengesteld. Ook deze organisatie constateert dat er nog steeds te weinig gebeurt om te komen tot een daadwerkelijk beter delen van relevante informatie. Gebrek aan vertrouwen tussen de betrokken overheidsorganisaties is een van de belangrijkste obstakels. Maar even belangrijk is dat de bevolking er op kan vertrouwen dat de overheid de gegevens die het heeft op de juiste wijze gebruikt en er voor zorgt dat deze op de juiste plaatsen terecht komt en niet elders. Daarom is het belangrijk dat een op te zetten systeem van informatie delen, waarvoor Markle voorstellen doet *"must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate."* [54]

Ondanks deze druk vanuit het Congres en onafhankelijke partijen zit er nog steeds weinig schot in. In 2006 concludeerde de Amerikaanse Rekenkamer, de Government Accountability Office (GAO), dat er bijna vijf jaar na de aanslagen nog steeds geen overheidsbreed beleid was voor het delen van informatie op het gebied van terrorismebestrijding. Er waren wel kleine stapjes gezet, maar nog steeds ontbreekt het aan een geïntegreerde aanpak voor de federale overheid.[55] GAO heeft enkele maanden geleden in een memorandum met aandachtspunten voor het nieuw verkozen congres nogmaals de aandacht voor dit onderwerp gevraagd. Toezicht op dit proces wordt noodzakelijk geacht om te verzekeren dat er daadwerkelijk een begin wordt gemaakt met het delen van informatie: *"Without continued congressional oversight of these issues, the progress and results of the many requirements and initiatives will remain unclear."* [56]

Toch zijn er in de afgelopen jaren wel enkele successen bereikt. Eind vorig jaar heeft de Director of National Intelligence een implementatieplan voor de inrichting van een omgeving voor het delen van informatie aan het Congres toegezonden. In het uitvoerige rapport wordt een gedetailleerde beschrijving gegeven van een mogelijke structuur voor het delen van terrorismegerelateerde informatie tussen partijen binnen de overheid op alle niveaus en met relevante partijen uit de markt en andere maatschappelijke sectoren.[57]

Een andere interessante ontwikkeling is de oprichting van zogenaamde 'fusion centers', waarin overheden van verschillende niveaus samenwerken met inlichtingen- en opsporingsdiensten ter voorkoming van terroristische aanslagen. Een Fusion Center is als volgt gedefinieerd: *"a collaborative effort of two or more agencies that provide resources, expertise and/or information to the centre with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity."* [58]

54 Markle Foundation, Protecting America's Freeom in the Information Age, New York, 2002, p. 31
55 Government Accountability Office (USA), The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information, Washington, March 2006
56 Government Accountability Office (USA), Suggested Areas for Oversight for the 110th Congress, Washington, 17 November 2006, p. 11
57 Program Manager Information Sharing Environment, Implementation Plan, Washington, November 2006
58 Bureau of Justice Assistance e.a., Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New World, Washington, July 2005

De meeste fusion centers zijn vooral gericht op terrorisme en zijn vaak op het niveau van een staat ontstaan zodat er nogal grote verschillen zijn qua omvang, scope en werking tussen deze centers.[59] Namens de adviescommissie is één van deze centers (voor Washington en omgeving) bezocht. Hier wordt heel pragmatisch gewerkt door vertegenwoordigers van landelijke, regionale en lokale inlichtingen- en opsporingsdiensten en in voorkomende gevallen ook met andere betrokken diensten (zoals de rampenbestrijding). Het samenwerken in één ruimte blijkt al een belangrijk middel te zijn om bestaande muren tussen organisaties te slechten. Het ministerie van Homeland Security heeft onderkend dat deze centers succesvol zijn en probeert nu een stroomlijning aan te brengen. Het ministerie doet mee aan de verdere uitbouw van 38 van deze centers en heeft daarvoor een budget van $ 380 miljoen beschikbaar gesteld. De fusion centers zijn samenwerkingsorganen waarin op basis van onderling vertrouwen tussen de betrokken diensten afspraken zijn gemaakt en waarin pragmatisch wordt samengewerkt.
De centers voldoen volgens de eerste analyses in een duidelijke behoefte en zijn een vorm van samenwerking die tegemoet komt aan de politieke wens voor betere informatie-uitwisseling.

Verenigd Koninkrijk

In het Verenigd Koninkrijk betreft een van de initiatieven de oprichting in 2005 van een speciale unit voor zware, georganiseerde criminaliteit. Deze organisatie, the Serious Organised Crime Organisation (SOCA), is een samenwerkingsverband van verschillende opsporingsdiensten, waarin zijn opgegaan de National Crime Squad, de National Criminal Intelligence Service, de delen van Revenue and Customs die te maken hebben met de handel in drugs en daarmee verbonden witwaspraktijken en de onderdelen van de Immigration Service die te maken hebben met mensenhandel. SOCA is een zelfstandig dienstonderdeel dat gefinancierd wordt door het ministerie van Binnenlandse Zaken en onder supervisie staat van een onafhankelijke raad van toezicht. Doelstelling van SOCA is kortweg het terugdringen van de schade die door georganiseerde criminaliteit wordt toegebracht aan de Britse samenleving. De prioriteiten voor SOCA worden vastgesteld door de minister van Binnenlandse Zaken en zijn voor het lopende begrotingsjaar als volgt bepaald: meer resultaten op het gebied van intelligence dan de 'oude' organisaties hebben behaald, bestrijding van de handel in hard drugs en illegale immigratie, alsmede andere vormen van georganiseerde criminaliteit, zoals fraude en computercriminaliteit, en beslaglegging op geld en goederen die door criminele activiteiten zijn verkregen.[60]

Een andere Brits initiatief is de oprichting van SCOPE, een omvangrijk ICT-project dat bedoeld is om inlichtingen- en veiligheidsdiensten in staat te stellen onderling beter samen te werken door middel van de veilige uitwisseling van gegevens binnen een gesloten

59 Zie voor een overzicht dat in 2005 is opgesteld door de National Governor's Association: NGA Center for Best Practices, State Intelligence Fusion Centers: Recent State Actions, Washington, July 2005
60 Serious Organised Crime Agency, SOCA Annual Plan 2006/7, London, 2006

netwerk. Het project loopt al enige jaren en vanwege de technische complexiteit en de beveiligingseisen zijn inmiddels aanzienlijke vertragingen ontstaan. Desondanks wordt het programma met kracht doorgezet omdat er een aantal belangrijke drijfveren voor verandering is: het aanbrengen van verbindingen tussen de verschillende spelers, de snelheid waarmee intelligence moet worden ontwikkeld en verspreid, de noodzaak om systemen beter op elkaar af te stemmen en de wens tot verbetering van de onderlinge samenwerking. [61] Overigens doen van de opsporingsdiensten alleen SOCA en de douane aan dit programma mee. De overige opsporingsdiensten staan te ver van de inlichtingendiensten af.

Tot slot moet hier melding worden gemaakt van een initiatief van het Engelse parlement. De Home Affairs Committee heeft begin dit jaar besloten een vergelijkbaar onderzoek in te stellen als nu wordt uitgevoerd door de adviescommissie.[62] Het betreft een onderzoek naar de invloed van de databases op het overheidsbeleid in het algemeen en het veiligheidsdomein in het bijzonder. De focus ligt op de onderwerpen van het Home Office, zoals identiteitsbewijzen, de nationale DNA Database en het cameratoezicht. In het onderzoek gaat de aandacht uit naar de strategische aspecten, met de bedoeling om basisregels voor de overheid terzake op te stellen. Inmiddels is contact gelegd tussen de adviescommissie en de parlementaire onderzoekscommissie om bevindingen uit te wisselen.

1.8 Tot slot: dit hoofdstuk in het kort

In dit hoofdstuk is ingegaan op het belang van gegevens en geautomatiseerde gegevensbestanden voor het veiligheidsdomein. Daarbij is ingegaan op enkele beleidsvraagstukken die met dit belang samenhangen.

Informatie speelt in het veiligheidsdomein een steeds grotere rol. Daarvoor kunnen enkele oorzaken worden aangewezen. In de eerste plaats zijn de geautomatiseerde gegevensbestanden in de afgelopen tien jaar exponentieel gegroeid, niet alleen in aantal, maar ook in het aantal gegevens dat zij bevatten. Met deze groei neemt ook het belang van deze bestanden voor de inlichtingen- en opsporingsdiensten toe. Een tweede oorzaak is de ontdekking dat bij recente terroristische aanslagen (New York, Washington, Madrid en London) veel informatie over de daders bekend was bij inlichtingen- en opsporingsdiensten. Door onvoldoende uitwisseling van deze gegevens kwam de informatie niet op de goede plaats terecht en is niet de goede actie ondernomen. Een derde oorzaak is de opkomst van het fenomeen van de informatie gestuurde politie. Informatie moet een steeds centralere rol krijgen in de politieprocessen.

61 Een delegatie van de adviescommissie heeft op 5 december 2005 een bezoek gebracht het programma SCOPE. Zie voorts over dit onderwerp: Intelligence and Security Committee, Annual Report 2005-2006, uitgave van the Stationary Office, London, 2006

62 United Kingdom Parliament, Home Affairs Committee Press Notice, Committee announces inquiry into a surveillance society, 27 maart 2007

De komst van de informatie gestuurde politie hangt samen met de ontwikkeling van intelligence. Onder intelligence verstaan wij de combinatie van informatie met analyse en verbinding. Was intelligence voorheen vooral een proces van de inlichtingendiensten, meer en meer groeit het inzicht dat intelligence ook een centrale rol speelt in de opsporingsprocessen. Een goede toepassing daarvan behoeft nog veel aandacht. Daarvoor is nodig dat een goede analyse wordt gemaakt van het intelligenceproces. In dat proces nemen een juist gebruik van data en de zorg voor de juistheid van die data een belangrijke plaats in. Juist dit element krijgt onvoldoende bestuurlijke aandacht, al hebben zich vooral ten aanzien van dit element in de afgelopen tien jaar de grootste wijzigingen voorgedaan.

Enkele beleidsvraagstukken die bij de toepassing van informatie in het veiligheidsdomein een rol spelen betreffen de verhouding tussen privacy en veiligheid en de misbruik van gegevensbestanden voor criminele activiteiten. Ten aanzien van het eerste vraagstuk wordt geconstateerd dat privacybeschermers en wetenschappers toenemende zorg hebben over een juiste balans tussen privacy en de noodzakelijke inbreuken daarop uit veiligheidsoverwegingen. Ten aanzien van het tweede vraagstuk wordt opgemerkt dat de beveiliging van gegevensbestanden een bredere maatschappelijke en politieke discussie verdient dan op dit moment gebeurt. Vervolgens is in dit hoofdstuk aandacht besteed aan een internationale vergelijking voor zover dat op grond van de beschikbare informatie mogelijk was. Daarbij is vooral gezocht naar best practices, waarvan de oprichting van zogenaamde fusion centers in de Verenigde Staten een voorbeeld is dat nadere bestudering verdient. Ook is gewezen op het onderzoek dat in het Verenigd Koninkrijk door een parlementaire commissie is gestart naar de invloed van databases op het overheidsdomein.

De adviescommissie trekt op grond van het bovenstaande de volgende conclusies:

1. Gegevens in externe gegevensbestanden hebben in de afgelopen decennia een steeds grotere betekenis voor het veiligheidsdomein gekregen. Desondanks krijgt het proces van inwinnen van gegevens uit die bestanden door inlichtingen- en opsporingsdiensten weinig tot geen bestuurlijke en politieke aandacht.
2. Data zijn een essentieel onderdeel voor de ontwikkeling van intelligence. Binnen de opsporing staat de ontwikkeling van intelligence nog teveel in de kinderschoenen, zowel in Nederland als in andere landen.
3. Criminaliteit met geautomatiseerde gegevensbestanden, zoals identiteitsfraude, komt steeds vaker voor. De voor- en nadelen van deze gegevensbestanden voor veiligheid en onveiligheid verdienen nader onderzoek en discussie.
4. Er is weinig bekend over het gebruik van geautomatiseerde gegevensbestanden voor het veiligheidsdomein in andere landen. Het delen van informatie tussen inlichtingen- en opsporingsdiensten blijkt wereldwijd een groot probleem te zijn. In de Verenigde Staten is de afgelopen jaren het concept van de fusion centers ontwikkeld. De eerste resultaten lijken veelbelovend.

2

BESCHRIJVING VAN DE SYSTEMATIEK

2.1 Inleiding

Centraal in de opdracht aan de adviescommissie staat het beschrijven van de systematiek volgens welke inlichtingen- en opsporingsdiensten gegevens verzamelen uit geautomatiseerde gegevensbestanden. Over die systematiek is weinig bekend.
In dit hoofdstuk wordt een schets gegeven. Dat gebeurt in vier stappen.

- Allereerst wordt nagegaan welke diensten en personen informatie (kunnen) vragen uit deze databases.
- Vervolgens wordt ingegaan op de relevante wetgeving.
- De derde stap bestaat uit een beschrijving van de wijze waarop binnen de kaders van deze regelgeving informatie wordt ingewonnen.
- Daarna wordt een vergelijking gemaakt met enkele andere relevante sectoren binnen de overheid.

Op grond van deze vier stappen geeft de adviescommissie vervolgens een karakteristiek van de systematiek.

2.2 De vragers van informatie

De vragers van gegevens in het veiligheidsdomein zijn de inlichtingen- en veiligheidsdiensten, de politie, de Koninklijke Marechaussee en de Bijzondere Opsporingsdiensten. Het aantal bijzondere opsporingsdiensten is in 2006 aanzienlijk teruggebracht en omvat nu nog slechts vier diensten: FIOD-ECD, de Sociale Inlichtingen- en Opsporingsdienst (SIOD), de Algemene Inspectiedienst van het ministerie van LNV en de Inlichtingen- en opsporingsdienst van het ministerie van VROM.[63] Deze bijzondere opsporingsdiensten hebben op het punt van de handhaving een nauwe band met het eigen ministerie, maar werken ten aanzien van de opsporing gelijk de reguliere politie onder aansturing van het openbaar ministerie. In het geval van bijzondere opsporingsdiensten is dit het functioneel parket. De inspectietaken van de bijzondere opsporingsdiensten zijn veelal ondergebracht in andere teams dan de eenheden die belast zijn met de opsporing van strafbare feiten. Binnen de bijzondere opsporingsdiensten bestaan criminele inlichtingen eenheden zoals die ook binnen de reguliere politie bestaan. De regels voor deze eenheden zijn opgesteld in overleg met de ministers van BZK en Justitie. Op deze manier wordt beoogd een zo goed mogelijke gegevensuitwisseling met de politie te realiseren.

Buiten deze inlichtingen- en opsporingsdiensten zijn er nog veel andere bijzondere opsporingsambtenaren die in bepaalde omstandigheden ook informatie aan gegevensbestanden kunnen vragen. Tot deze groep van bijzondere opsporingsambtenaren behoren o.m. gemeentelijke milieuopsporingsambtenaren, parkeercontroleurs, medewerkers van

63 Zie hierover de Kamerstukken 30 182, Vaststelling van regels met betrekking tot de bijzondere opsporingsdiensten en de instelling van het functioneel parket (Wet op de bijzondere opsporingsdiensten)

de Arbeidsinspectie, opsporingsmedewerkers van de douane en medewerkers van de Voedsel- en Warenautoriteit. Dit overzicht lijkt overzichtelijker dan het in werkelijkheid is. Binnen alle genoemde diensten zijn weer onderdelen die meer toegangen hebben tot gegevensbestanden dan andere onderdelen. Sommige gegevensbestanden zijn voor alle opsporingsambtenaren toegankelijk, terwijl de toegang tot andere bestanden aan beperkingen onderhevig is. Het aantal diensten uit het veiligheidsdomein dat vragen aan externe databases kan stellen bedraagt ongeveer 40. Een aantal gegevens leverende organisaties heeft ook daadwerkelijk met alle vragers te maken, zoals de Belastingdienst, de Rijksdienst voor het Wegverkeer (RDW) en het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). De meeste organisaties hebben echter met minder vragende diensten te maken.

2.3 De toepasselijke wetten

De bevoegdheid van de hierboven genoemde diensten om gegevens in te winnen bij externe databases is niet eenduidig geregeld. Er is een grote hoeveelheid wetten dat op deze gegevensverstrekking van toepassing is. Voor de AIVD en de MIVD geldt de Wet op de Inlichtingen- en Veiligheidsdiensten 2002, de WIV. In deze wet wordt omschreven wanneer de betrokken diensten informatie uit externe gegevensbestanden mogen inwinnen.[64] De algemene bevoegdheid tot het verzamelen van gegevens staat in art. 17 van de wet. In dit artikel staat dat de diensten zich voor het verzamelen van gegevens kunnen wenden tot *"eenieder die geacht wordt de benodigde gegevens"* te kunnen verstrekken. De verstrekking gebeurt vervolgens op basis van vrijwilligheid. In de artikelen 28 en 29 staan vergelijkbare bevoegdheden ten aanzien van gegevens over telefoonverkeer en andere vormen van telecommunicatie. Daarnaast kennen de diensten ook een aantal bijzondere bevoegdheden, zoals observeren van personen, het uitvoeren van undercover-operaties en het doorzoeken van besloten plaatsen. Deze bijzondere bevoegdheden vallen buiten de opdracht aan de adviescommissie en blijven hier derhalve buiten beschouwing.

De bevoegdheden van de politie voor het raadplegen van externe gegevensbestanden vinden vooral hun grondslag in het wetboek van strafvordering. In diverse artikelen van het eerste boek hiervan staan bepalingen inzake het raadplegen van bevolkingsadministraties, het doorzoeken van computers, het verkrijgen van financiële gegevens en het doorzoeken van poststukken en van email, alsmede het onderzoeken van het telefoonverkeer van verdachte personen. In dit kader zijn met name ook de bepalingen van belang die betrekking hebben op het vorderen van gegevens. Het betreft de artikelen 126nc tot en met 126ni. Tot de regelingen in deze artikelen horen ondermeer: de bevoegdheid van opsporingsambtenaren tot het vorderen van opgeslagen identificerende gegevens, de bevoegdheid van de officier van justitie tot het vorderen van gegevens met betrekking tot personen die verdacht worden van bepaalde categorieën van misdrijven,

64 Wet van 7 februari 2002, zie voor de parlementaire behandeling: kamerstukken 25 877

de bevoegdheid van de officier van justitie om in bepaalde omstandigheden vertaling af te dwingen van versleutelde gegevens en de bevoegdheid van de officier van justitie om in bepaalde omstandigheden af te dwingen dat bepaalde gegevens in een geautomatiseerd bestand voor een periode van maximaal 90 dagen bewaard blijven. Ook in deze wet zijn bijzondere bevoegdheden opgenomen ten aanzien van ondermeer infiltratie en het doorzoeken van besloten plaatsen.[65] Deze bepalingen blijven hier buiten beschouwing. Daarnaast zijn in de wet bepalingen met bijzondere bevoegdheden opgenomen die betrekking hebben op de opsporing van terroristische misdrijven.[66] Hieronder vallen bepalingen over het vorderen van gegevens. In geval van het vermoeden van een terroristisch misdrijf kunnen opsporingsambtenaren of officieren van justitie gegevens vorderen uit gegevensbestanden. De bepaling is in die zin ruim geformuleerd dat hieronder alle databases vallen behalve de gegevensbestanden die iemand voor zijn persoonlijk gebruik aanhoudt: *"In geval van aanwijzingen van een terroristisch misdrijf kan de opsporingsambtenaar in het belang van het onderzoek van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, vorderen bepaalde opgeslagen gegevens of vastgelegde identificerende gegevens van een persoon te verstrekken."* [67]

Na afronding van het onderzoek moeten de verkregen gegevens worden gewist. Artikel 126dd van de wet opent overigens de mogelijkheid om deze gegevens te bewaren ten behoeve van een ander strafrechtelijk onderzoek of voor de opslag in een register zware criminaliteit.

Bestaande wetten zijn onlangs uitgebreid met mogelijkheden voor inlichtingen- en opsporingsdiensten om gegevens uit externe databases te verkrijgen. De verscherpte strijd tegen het terrorisme ligt aan verschillende van deze wetswijzigingen ten grondslag. Op tal van punten is de wetgeving in de afgelopen jaren aangepast: vorderen gegevens financiële sector (2004), vorderen gegevens telecommunicatie (2004), wet inbeslagneming en doorzoeking (2004), fraude niet-chartaal geldverkeer (2004), bevoegdheden vorderen gegevens (2005), de wet computercriminaliteit II (2006) en de wet opsporing en vervolging terroristische misdrijven (2007).

Overige wetten

Buiten deze generieke wetten op het gebied van de strafvordering zijn er nog tal van andere wetten, waarin bepalingen zijn opgenomen over de bevoegdheid van overheidsdiensten om ten behoeve van het veiligheidsdomein informatie te vragen. In deze bijzondere wetten gaat het vooral om de verplichting van derde partijen om de gevraagde gegevens te verstrekken. Een overzicht van alle relevante wetten op dit punt is overigens niet beschikbaar. De adviescommissie heeft navraag naar een dergelijk overzicht gedaan bij

65 De artikelen 126g tot en met 126ma en 1260 tot en met 126ui
66 De artikelen 126za tot en met 126zu
67 Artikel 126zk

zowel het ministerie van Justitie als het College Bescherming Persoonsgegevens, maar geen van deze instanties beschikte over een dergelijk overzicht. De adviescommissie is daarom niet in staat om een sluitend overzicht te bieden van relevante wettelijke bepalingen. Enkele belangrijke wetten zullen hier kort worden aangeduid:

- De Wegenverkeerswet legt vast dat de Rijksdienst voor het Wegverkeer (RDW) informatie uit het kentekenregister verstrekt aan de autoriteiten die met de uitvoering van die wet zijn belast, alsmede andere daartoe bevoegde autoriteiten. Dit gebeurt overigens op een wijze die door de RDW wordt bepaald.[68]
- De Wet Melding Ongebruikelijke Transacties (MOT) legt de verplichting vast voor eenieder die beroepsmatig een financiële transactie verricht hiervan melding te doen aan een daartoe in het leven geroepen meldpunt als deze transactie als ongebruikelijk aangemerkt moet worden.[69] Dit geldt in het bijzonder voor transacties die gericht zouden kunnen zijn op witwassen, heling van geld of financieren van terrorisme. Het meldpunt analyseert de meldingen en gaat na of de transacties daadwerkelijk als verdacht moeten worden aangemeld. In dat geval worden de transacties doorgemeld aan het openbaar ministerie.
- De Telecommunicatiewet legt de verplichting op aan telecomproviders om hun netwerken open te stellen voor aftappen ten behoeve van doeleinden op het gebied van opsporing of inlichtingendiensten.[70] Deze verplichting strekt tot het mogelijk maken van aftappen van communicatie en tot het verstrekken van gegevens over bepaalde gebruikers. Hiermee samenhangende administratieve en personele kosten worden door de overheid vergoed. Bij deze verplichting wordt verwezen naar de ter zake toepasselijke bepalingen uit de Wet op Inlichtingen- en Veiligheidsdiensten en het Wetboek van Strafvordering.
- De wet Bevordering integriteitbeoordelingen in het openbaar bestuur, kortweg de wet-Bibob[71] geeft bestuursorganen de mogelijkheid te voorkomen dat zij ongewild criminele activiteiten mogelijk maken door het verlenen van een vergunning, het verstrekken van subsidie of het verlenen van een overheidsopdracht. De wet geeft de bestuursorganen de mogelijkheid uitgebreid onderzoek te laten doen door een bureau van het ministerie van Justitie naar de eventuele strafrechtelijke antecedenten van aanvragers van vergunningen of subsidies en potentiële kandidaten voor overheidsopdrachten. Dit bureau heeft toegang tot bronnen die voor de bestuursorganen gesloten zijn en kan op grond van de uit die bronnen verkregen gegevens adviseren tot een al dan niet positieve beschikking. Het bureau kan de verkregen gegevens voor een periode van twee jaar bewaren voor de behandeling van andere verzoeken over betrokkene. Deze gegevens kunnen ook worden gebruikt voor inlichtingen- en opsporingsdiensten. (wet Bibob, art. 20, 3e lid)

68 Wegenverkeerswet, wet van 21 april 1994, art. 43
69 Wet van 16 december 1993, betreffende melding ongebruikelijke transacties bij financiële dienstverlening
70 Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), in het bijzonder hoofdstuk 13 (bevoegd aftappen)
71 Wet van 20 juni 2002, houdende regels inzake de bevordering van integriteitsbeoordelingen door het openbaar bestuur met betrekking tot beschikkingen of overheidsopdrachten (Wet bevordering integriteitsbeoordelingen door het openbaar bestuur)

- De Wet Structuur Uitvoeringsorganisatie Werk en Inkomen heeft uitgebreide bepalingen over informatieverstrekkingen.[72] De bij de uitvoering van deze wet betrokken instanties, CWI, SVB, de Belastingdienst en de UWV, hebben op grond van de wet de verplichting elkaar te informeren en kosteloos gegevens ter beschikking te stellen. Ook kent de wet de verplichting voor deze organisaties om gegevens ter beschikking te stellen aan de minister of aan andere bestuursorganen die dit voor de uitvoering van hun taak nodig hebben. Voor de inlichtingen- en opsporingsdiensten is nog van belang de bepaling (art. 62, 4e lid) dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld aan het gebruik door deze diensten van de elektronische infrastructuur die in het leven wordt geroepen voor de gegevensuitwisseling.
- Niet alle bevragingen of informatiesystemen zijn rechtstreeks gebaseerd op wetgeving. Binnen de strafrechtketen functioneert sinds 1 januari 2006 de Justitiële Informatiedienst. De primaire taak van deze dienst is het verstrekken van een integer en integraal personeelsbeeld van justitiabelen aan daartoe gerechtigden. De dienst beschikt daartoe over een aantal belangrijke databases. Een daarvan is de Verwijs Index Personen, een systeem met verwijzingen die van belang zijn voor alle onderdelen van de strafrechtketen die met dezelfde persoon bezig zijn. Dit systeem is in 2005 meer dan 2 miljoen keer bevraagd. Een ander systeem is het Justitieel Documentatie Systeem, een systeem waarin natuurlijke en rechtspersonen zijn vastgelegd, die op enigerlei wijze met justitie in aanraking zijn gekomen. Het aantal natuurlijke personen dat in systeem zijn opgenomen bedraagt ruim 4 miljoen. De bevragingen door politie op dit systeem worden gelogd, de bevragingen door de AIVD worden niet gelogd.[73]
- Een ander voorbeeld van een regeling die niet rechtstreeks op een wet is terug te herleiden is de verwijsindex voor risicojongeren die in het kader van de WMO is ingevoerd, zonder dat de wet hier een rechtstreekse grondslag voor biedt. [74] Deze verwijsindex brengt signalen van professionals over jongeren in een zo vroeg mogelijk stadium bijeen, zodat hulpverleners in een zo vroeg mogelijk stadium contact met elkaar kunnen opnemen om de hulpverlening op elkaar af te stemmen. Politie en justitie kunnen van deze database gebruik maken.[75]
- Instellingen zoals het Kadaster en de Kamers van Koophandel houden ook registers bij met gegevens die van belang kunnen zijn voor opsporing of nationale veiligheid. Deze gegevensbestanden zijn op grond van de Kadasterwet[76] en de Handelsregisterwet[77] openbaar of grotendeels openbaar. De opsporingsdiensten kunnen hier gelijk andere organisaties of burgers gegevens opvragen, tegen betaling. Alleen het CBS hoeft voor het verstrekken van gegevens op grond van de Wet voor het Centraal Bureau voor de

72 Wet van 29 november 2001, houdende regels tot vaststelling van een structuur voor de uitvoering van taken met betrekking tot de arbeidsvoorziening en socialeverzekeringswetten (Wet structuur uitvoeringsorganisatie werk en inkomen)
73 informatie verstrekt door de Justitiële Informatiedienst.
74 Wet van 29 juni 2006, houdende nieuwe regels betreffende maatschappelijke ondersteuning (Wet maatschappelijke ondersteuning)
75 Factsheet Verwijsindex risicojongeren, uitgave van het ministerie van VWS, juni 2006
76 Wet van 3 mei 1989, houdende regelen met betrekking tot de openbare registers voor registergoederen, alsmede met betrekking tot het kadaster (Kadasterwet)
77 Wet van 8 februari 1996, houdende vereenvoudiging van de Handelsregisterwet en wijziging van enige andere wetten (Handelsregisterwet)

Statistiek niet te betalen voor de verstrekte gegevens. Ook op grond van de Faillissementswet worden allerlei registers bijgehouden die openbaar zijn en waaruit gegevens op verzoek kosteloos en uittreksels tegen betaling aan eenieder beschikbaar worden gesteld.[78]

Wetgeving in voorbereiding

Thans zijn er nog enkele wetsvoorstellen bij het parlement aanhangig die een duidelijke relatie hebben met de bevraging van externe gegevensbestanden. Ten minste één ander wetsvoorstel is in voorbereiding. Daarnaast is er ook een relatie met het in voorbereiding zijnde algemene Burger Service Nummer, waarvoor het wetsontwerp nu in behandeling is bij de Eerste Kamer.

Bij de Eerste Kamer is in behandeling het wetsvoorstel inzake de verwerking en opslag van politiegegevens, als vervanging van de wet op de politieregisters.[79] Het wetsvoorstel beoogt de politie meer mogelijkheden te geven om gegevens te verwerken voor een optimale uitvoering van de politietaak. Het voorstel wil een nieuw evenwicht aanbrengen tussen de bescherming van de privacy van de burger enerzijds en het belang van de rechtshandhaving anderzijds. Er bestaan in de Eerste Kamer nogal wat twijfels over dit wetsontwerp. Ook het College Bescherming Persoonsgegevens heeft kritische kanttekeningen geplaatst bij het wetsvoorstel.[80] De kritiek heeft enerzijds te maken met de veronderstelde link met de terrorismebestrijding, maar ook omdat dit voorstel de weg opent voor de politie om gegevens te verzamelen over personen die niet direct kunnen worden aangemerkt als verdachten. Dit is het gevolg van het nieuwe fenomeen themaverwerkingen, dat de politie de bevoegdheid zou geven om rond een bepaald thema meer gegevens over personen in te winnen en vast te leggen. Volgens een van de grote fracties dreigt een salamitechniek, waarmee elke keer een inbreuk wordt gedaan op het reguliere rechtssysteem. Een samenvattend overzicht van alle wetgeving die in de afgelopen jaren is gerealiseerd in samenhang met nog tot stand te brengen wetgeving wordt daarom noodzakelijk geacht. De Eerste Kamer heeft besloten de schriftelijke discussie met de regering voort te zetten alvorens het wetsontwerp plenair te behandelen.[81]

Bij de Tweede Kamer is in behandeling het wetsvoorstel tot wijziging van de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV), waarin voorstellen worden gedaan om de bevoegdheden van deze diensten om onderzoek te doen naar terroristische en andere gevaren, uit te breiden.[82] Het wetsvoorstel staat bekend als de wet-post Madrid, omdat veel van de voorstellen zijn ontwikkeld naar aanleiding van de bomaanslagen in Madrid op 11 maart 2004. Tot de voorstellen behoren nieuwe vormen van geautomatiseerde

78 Wet van 30 september 1893, op het faillissement en de surséance van betaling (Faillissementswet)
79 Kamerstuk 30 327, Regels inzake de verwerking van politiegegevens (Wet politiegegevens)
80 Advies conceptwetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens), brief van 29 maart 2004, nr. 5274299/04/6
81 Besluit van de Vaste Commissie voor Justitie d.d. 30 januari 2007, het nader voorlopig verslag dateert van 16 maart 2007 (stuk nr. E)
82 Zie notenopsomming volgende pagina

data-analyse (datamining), rechtstreekse toegang tot gegevensbestanden van derden, de verplichting tot het leveren van informatie waar dit vroeger op basis van vrijwilligheid plaatsvonden en de mogelijkheid van rechtstreekse toegang tot politiebestanden. Ook worden de mogelijkheden voor de diensten om gegevens te verzamelen over mensen sterk uitgebreid. Waar in de huidige WIV gegevens worden verstrekt op basis van vrijwilligheid, komt daarvoor een verplichting in de plaats. De verplichting wordt met name opgelegd aan nader aan te wijzen overheidsorganen en bedrijven in de financiële, communicatie- en vervoerssector, voor zover zij al niet op grond van andere wetten tot levering zijn verplicht.

Ook de komende wet op het Burger Service Nummer is van toepassing op de informatieverzameling ten behoeve van het veiligheidsdomein. In de Eerste Kamer is bij de behandeling van het wetsontwerp de stelling opgeworpen dat Burger Service Nummer het nog makkelijker zal maken dat de overheid onbevoegd informatie over burgers verzamelt en voor andere doeleinden gebruikt dan waarvoor de informatie is verstrekt. De mogelijkheid tot koppeling van gegevens zou in strijd zijn met bestaande wetgeving en Europese regelgeving.[83] Het Burger Service Nummer maakt het technisch eenvoudiger om voor de opsporing koppelingen te leggen tussen gegevens in verschillende bestanden. Het Expertise Centrum (HEC) verwacht dat het gebruik van het BSN voor opsporingsdoeleinden spoedig op de politieke agenda zal worden geplaatst.[84] Deze discussie speelt op de achtergrond een rol bij de aarzelingen die de Kamer heeft bij de invoering van dit nummer.

Andere nieuwe wetgeving is minder ver in de voorbereiding van parlementaire behandeling. Dit is de uitvoering van de Europese richtlijn met betrekking tot bewaring van verkeersgegevens op het gebied van telefoonverkeer en gebruik van Internet, de richtlijn inzake de dataretentie.[85] De richtlijn is opgesteld naar aanleiding van de terroristische bomaanslagen in Madrid en Londen en heeft tot doel inlichtingen- en opsporingsdiensten betere mogelijkheden te geven zicht te krijgen op de communicatie van mogelijke verdachten via telefoon, internet of andere vormen van elektronische communicatie. De richtlijn verplicht de lidstaten om zodanige wettelijke voorzieningen te scheppen dat gegevens van verkeer en internet voor een periode van tenminste zes maanden worden bewaard, Tot de te bewaren gegevens behoren bron en bestemming van de communicatie, tijdstip, duur en locatie van de communicatie en de vermoedelijk gebruikte apparatuur. De toegang tot de te bewaren gegevens behoort tot de nationale wetgeving, in Nederland het Wetboek van strafvordering en de WIV.

82 Kamerstuk 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
83 Zie ook: brief van het College Bescherming Persoonsgegevens d.d. 25 oktober 2005, nr. z2005-1198
84 Heemskerk, P., e.a., Naar een goed gebruik van het burgerservicenummer (BSN), Stichting Het Expertise Centrum, Den Haag, 2007, p. 53
85 Zie notenopsomming op de volgende pagina

Voorafgaande aan de vaststelling van de richtlijn heeft de Tweede Kamer al haar twijfels over de richtlijn laten blijken. Op 16 februari 2006 heeft de Tweede Kamer een motie-Dittrich aanvaard waarin wordt uitgesproken dat het ontwerp van de richtlijn onvoldoende tegemoet komt aan de wensen van het Nederlandse parlement. Op grond daarvan werd de regering verzocht niet met de richtlijn in te stemmen.[86] De minister van Justitie schreef vervolgens op 28 februari dat over dit onderwerp overeenstemming bestond tussen het Europees Parlement en de Europese Commissie, waaraan de Europese ministers gebonden zijn: *"Er bestaat daarna geen ruimte meer om de discussie over de inhoud van die voorwaarden weer aan te zwengelen."* [87]

Het ministerie van Economische Zaken heeft een conceptwetsontwerp opgesteld ter uitvoering van de richtlijn en dit concept om commentaar voorgelegd aan een aantal betrokken instanties.[88] Deze instanties hebben overwegend negatief op dit concept gereageerd. De aanbieders van telecomdiensten lieten in hun reactie weten grote zorgen te hebben over de reikwijdte van het voorstel. Hun zorgen omvatten drie hoofdpunten: teveel zaken worden niet in de wet geregeld, maar verwezen naar later op te stellen algemene maatregelen van bestuur, de kosten voor de nieuwe regeling worden eenzijdig bij de aanbieders neergelegd en de negatieve gevolgen op de bedrijfsvoering van de aanbieders vanwege de bestaande privacywetgeving.[89] Een van de belangrijkste punten die in het concept niet worden geregeld is de plaats van opslag van de gegevens, centraal, decentraal of middels een tussenvorm. Een keus uit deze opties heeft belangrijke financiële consequenties, zo is gebleken uit een onderzoek door een extern adviesbureau in opdracht van de minister van Justitie. De duurste variant (decentrale opslag) kost over een periode van 5 jaar in totaal bijna € 158 miljoen, en de minst dure variant (centrale opslag) bijna € 134 miljoen, een verschil van € 24 miljoen.[90] Mede vanwege deze grote financiële consequenties hebben de aanbieders grote bezwaren tegen het achterwege blijven van een duidelijke uitspraak op dit punt, vooral omdat de memorie van toelichting kan worden afgeleid dat het in het voornemen ligt om de kosten voor opslag, ontsluiting, beheer en beschikbaar stellen ten laste te laten komen van het bedrijfsleven. Ook staat in de memorie van toelichting vermeld dat rekening wordt gehouden met een groei van het aantal bevragingen met 20% per jaar. Deze raming wordt overigens niet verder onderbouwd. Er wordt slechts verwezen naar een extern onderzoeksrapport. Dat onderzoeksrapport noemt wel het percentage van 20, maar verwijst als bron naar overleg met de behoeftesteller, het ministerie van Justitie. En daarmee is de cirkel weer rond.

85 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG
86 Kamerstuk 23 490, nr 407
87 Kamerstuk 23 490, nr 408
88 Concept wetsontwerp bewaarplicht telecommunicatiegegevens, Ministerie van Economische Zaken, 2006
89 Gezamenlijke reactie Aanbieders op consultatie Wetsvoorstel Dataretentie, verstuurd aan de minister van Economische Zaken op 18 januari 2007
90 Verdonck, Klooster & Associates bv, Onderzoek naar de nationale implementatie van de Europese richtlijn dataretentie, onderzoek in opdracht van de minister van Justitie, 2006

Het is op dit moment niet mogelijk om een goed overzicht te verkrijgen over het aantal bevragingen aan externe databases.

Ook het College Bescherming Persoonsgegevens heeft in een advies van 22 januari 2007 laten weten bedenkingen te hebben tegen het conceptwetsontwerp.[91] Het College verzet zich tegen de lange bewaartermijn van gegevens, het grote aantal delegatiebepalingen in het wetsvoorstel, de mogelijkheid dat de gegevens kunnen worden gebruikt voor datamining, alsmede tegen de onvoldoende mogelijkheden tot controle op rechtmatig gebruik. Op verschillende onderdelen is het wetsontwerp volgens het CBP in strijd met de Europese richtlijn en zelfs met het Europees verdrag voor de Rechten van de Mens (EVRM).

Overigens heeft de Ministerraad op 30 maart 2007 besloten het wetsontwerp inzake de dataretentie om advies voor te leggen aan de Raad van State. Volgens het persbericht van de Rijksvoorlichtingsdienst is het wetsontwerp op hoofdlijnen gelijk aan het gewraakte conceptwetsontwerp.[92] De discussie over dit onderwerp is dus nog niet ten einde.

Los van deze wetten zijn er nog diverse andere wetsontwerpen in behandeling die te maken hebben met terrorismebestrijding. Wij noemen daarvan als voorbeeld de wet die het mogelijk maakt om bestuurlijke maatregelen te nemen tegen vermeende of potentiële terroristen tegen wie nog onvoldoende bewijzen zijn verzameld voor een strafrechtelijke benadering.[93]

2.4 De wijze van gegevens inwinnen

Ook over de wijze waarop gegevens worden verkregen uit grote databases is geen duidelijk totaalinzicht beschikbaar. De bevraging gebeurt in een aantal gevallen via een rechtstreekse verbinding van de bevragende instantie met het geautomatiseerde gegevensbestand. Dit gebeurt bijvoorbeeld bij de raadpleging van de bestanden van de gemeentelijke bevolkingsadministratie en van de Rijksdienst voor het Wegverkeer (RDW). Soms hebben bepaalde opsporingsdiensten wel rechtstreekse toegang tot bepaalde gegevensbestanden en andere diensten niet. De FIOD-ECD heeft bijvoorbeeld als onderdeel van de Belastingdienst wel (via interne protocollen) rechtstreeks toegang tot de bestanden van die dienst, terwijl andere opsporingsdiensten dat niet hebben. De Belastingdienst heeft met alle instanties die vragen over de inhoud van de bestanden van de Belastingdienst mogen stellen, convenanten afgesloten over de wijze waarop deze bevraging en beantwoording plaatsvindt. Ook komt het voor dat diensten externe gegevensbestanden kopiëren en in eigen huis halen om deze te kunnen onderzoeken en te koppelen met andere bestanden. De politie doet dit soms gericht in opsporingsonderzoeken.

91 College bescherming persoonsgegevens (CBP): Advies inzake het Wetsontwerp implementatie Europese Richtlijn Dataretentie, advies d.d. 22 januari 2007
92 Persbericht ministerraad: Kabinet: bewaarplicht telecommunicatiegegevens anderhalf jaar, 30 maart 2007
93 30 566, Regels inzake het opleggen van beperkende maatregelen aan personen met het oog op de bescherming van de nationale veiligheid en inzake het weigeren of intrekken van beschikkingen met het oog op de bescherming van de nationale veiligheid (Wet bestuurlijke maatregelen nationale veiligheid)

Bij de AIVD is het meer algemeen beleid om externe gegevensbestanden naar 'binnen te halen'. De AIVD beschikt naar eigen zeggen over enige tientallen externe databestanden, sommige groot, andere klein. De inlichtingendiensten krijgen hiertoe nog meer mogelijkheden als de bij de Tweede Kamer aanhangige wijziging van de WIV wordt aangenomen.

Overzicht van bevragingen

Het is op dit moment voor de adviescommissie niet mogelijk om een goed overzicht te verkrijgen over het aantal bevragingen aan externe databases door inlichtingen- en opsporingsdiensten. Bij de politie wordt het niet centraal bijgehouden en over het aantal bevragingen door de AIVD worden om redenen van staatsveiligheid geen mededelingen gedaan. Om diezelfde redenen mogen providers van telefonie en internetdiensten van de AIVD ook geen gegevens verstrekken over het aantal bevragingen dat bij hen is gedaan. Slechts op onderdelen van het proces zijn gegevens summier beschikbaar. Zo blijkt uit het jaarverslag van het Meldpunt Ongebruikelijke Transacties dat er in 2005 ruim 180.000 meldingen zijn gedaan. Het grootste deel hiervan (72%) betreft zogenaamde money transfers, geldtransacties met andere landen. Van alle meldingen zijn er ruim 38.000 als verdacht doorgemeld aan het Openbaar Ministerie, ruim 20% van het oorspronkelijk gemelde aantal ongebruikelijke transacties. Het Meldpunt krijgt geen automatische terugkoppeling van het Openbaar Ministerie over de verdere afhandeling van de verdachte meldingen, zodat exacte cijfers daarover ontbreken. Naar schatting leiden op jaarbasis ongeveer 130 zaken uiteindelijk tot een rechtszaak.

Navraag bij de Nederlandse Vereniging van Banken (NVB) heeft geleerd, dat centraal geen overzicht van het aantal bevragingen wordt bijgehouden. De exacte omvang en de daarmee gepaard zijnde kosten kan alleen door middel van uitvoerig nader onderzoek boven tafel komen, aldus de NVB. Zij tekent daarbij aan dat in bijna alle aspecten van het bankbedrijf door middel van de inzet van systemen of personen forse inspanningen moeten worden verricht ten behoeve van informatievoorziening aan de overheid op het gebied van criminaliteits- en terrorismebestrijding. Volgens onderzoek van CapGemini in opdracht van de NVB is hiermee in totaal op jaarbasis een bedrag van € 480 miljoen gemoeid. Inmiddels zijn met de Nederlandse Bank afspraken gemaakt om de toezichtactiviteiten terug te brengen, zodat een reductie van het genoemde bedrag tot € 320 miljoen kan worden gerealiseerd. Desondanks blijft de hoogte van de kosten die de banken moeten maken een permanente bron van zorg.[94] De scheidend voorzitter van de NVB heeft deze informatieverschaffing door de banken een groot pijnpunt genoemd, vooral omdat de overheid de kosten hiervoor niet vergoedt: "De overheid ziet de banken steeds meer als een verlengstuk van de opsporingsdiensten." [95]

94 Brief van de directeur van de NVB aan de adviescommissie d.d. 19 december 2006
95 Dr P.W. Moerland, Overheid moet het gegeven vertrouwen koesteren, Het Financieele Dagblad, 24 augustus 2006

Het aantal bevragingen bij providers van Internet en telecommunicatie wordt evenmin centraal bijgehouden. Een indicatie kan worden verkregen uit de gegevens van het CIOT. Het CIOT beheert de bestanden die eigenaren van telecommuncatiemiddelen kunnen identificeren. De gegevens uit deze bestanden mogen alleen voor opsporingsdoeleinden of inlichtingenvergaring worden verstrekt. In totaal hebben 42 inlichtingen- en opsporingsdiensten een aansluiting op dit systeem. Telecom- en internetproviders stellen dagelijks geactualiseerde gegevens aan het CIOT ter beschikking. De bevragingen bij het CIOT laten een sterk stijgende lijn zien. Het aantal bevragingen voor telefoniediensten bedroeg in 2003 bijna 722.000. Dit was in 2005 gestegen tot ruim. 1.220.000 en in 2006 tot meer dan 1,8 miljoen. Het merendeel van deze bevragingen komt voor rekening van de politie (93%). De aantallen bevragingen door AIVD (4%) en door bijzondere opsporingsdiensten (3%) zijn beduidend lager.[96] Op basis van de gebruikersgegevens kunnen inlichtingen- en opsporingsdiensten vervolgens de verkeersgegevens opvragen bij de provider. De verkeersgegevens omvatten de gegevens van de telefoongesprekken die gekoppeld zijn aan een gebruiker.

Een apart onderdeel van de bevragingen vormen de taps die op verzoek van inlichtingen- of opsporingsdiensten worden geplaatst op telefoons of internetverkeer. Ook hierover blijken de gegevens moeilijk te verkrijgen. Het onderwerp is aan de orde geweest bij de evaluatie van hoofdstuk 13 van de Telecommunicatiewet. Bij de schriftelijke behandeling van deze evaluatie heeft de Kamer gevraagd om nadere gegevens hierover. In antwoord op deze vragen heeft het kabinet gezegd niet over landelijke gegevens van het aantal justitiële taps op jaarbasis te beschikken. Wel wees het kabinet op de inventarisatie uit 1998 door de tapkamerbeheerders van de regionale korpsen, welke op verzoek van het Overlegorgaan Post en Telecommunicatie was uitgevoerd. Uit deze inventarisatie bleek dat in 1998 ongeveer 10 000 taps zijn geplaatst, waarvan 3000 in het vaste net en 7000 in de mobiele netwerken.[97] Bij de mondelinge behandeling van het onderwerp in de Tweede Kamer heeft de Minister van Justitie onlangs erkend dat een overzicht op dit punt ontbreekt: *“omdat we die cijfers gewoon niet centraal hebben.”* [98] De minister zegde toe door middel van centrale coördinatie van de taps in te toekomst een beter overzicht mogelijk te maken.

De Nationale Beheerorganisatie voor Internet Providers (NBIP) heeft vorig jaar in een persbericht informatie gegeven over het aantal taps en de kosten daarvan. De NBIP is een organisatie die vooral de kleinere providers verenigt, in totaal 44 met ongeveer 1,5 miljoen eindgebruikers. Bij deze providers is sprake van een gering aantal taps (geschat voor 2006: 31, met in totaal 66 tapmaanden). Een van de belangrijkste taken van de NBIP is het verzorgen van de technische apparatuur voor de taps omdat dit de draagkracht van

96 Gegevens van het ministerie van Justitie.
97 Kamerstukken, 30 517, nr. 27
98 persbericht van nieuws.nl d.d. 29 maart 2007: `Internettelefoon mag worden afgetapt`

de individuele kleinere providers te boven gaat. Volgens het persbericht kost een tap ruim € 9.450,00, waarin geen rekening is gehouden met de administratieve en overige kosten van de providers. Het persbericht voegt hier zonder verder commentaar aan toe: *“Zoals bekend hanteert de overheid een vergoeding van € 13,13 voor het plaatsen van een tap.”* [99]

Het gebrekkige aantal gegevens over de bevragingen maakt het moeilijk om een goed inzicht te verkrijgen in de groei daarvan. Navraag door de adviescommissie bij providers levert als beeld op dat het aantal bevragingen naar verkeersgegevens in de afgelopen jaren sterk tot zeer sterk toeneemt, maar dat het aantal taps slechts een geringe stijging vertoont. Naar men mag aannemen houdt de groei van het aantal bevragingen van verkeersgegevens gelijke tred met de groei van het aantal bevragingen inzake gebruikersgegevens bij het CIOT.

Nieuwe technieken: datamining

Voor de bevraging van deze gegevensbestanden maken inlichtingen- en opsporingsdiensten meer en meer gebruik van nieuwe technieken, zoals datamining. Datamining is een techniek om interessante en toepasbare informatie te halen uit grote hoeveelheden gegevens (databases en datawarehouses). Met behulp van datamining kunnen de gegevens in deze gegevensbestanden worden geanalyseerd en kunnen nuttige en relevante verbanden worden gedetecteerd. Op basis daarvan kunnen trends worden ontdekt en kunnen beslissingen worden voorbereid voor een verdere aanpak. Datamining is een verzameling van technieken waarmee het zoekproces in de grote databases op een zeer snelle wijze kan worden uitgevoerd. Voorbeelden van deze technieken zijn het opzetten van neurale netwerken (waarbij voorspellingen worden gedaan op basis van historische gegevens) en clustering (waarbij gemeenschappelijke kenmerken worden gezocht in verzamelingen ongelijksoortige gegevens). Alle inlichtingen- en opsporingsdiensten in Nederland hebben ieder voor zich initiatieven genomen om datamining toe te passen. Ook de IND wil vormen van datamining toepassen om de eigen bestanden beter te kunnen onderzoeken. Datamining kan behulpzaam zij bij het geautomatiseerd zoeken naar bruikbare kennis die zich in de almaar groeiende stroom van gegevensbestanden schuilhoudt.

De techniek staat voor het veiligheidsdomein nog steeds in de kinderschoenen en niet iedereen is overtuigd van de waarde daarvan. Daarnaast zijn er zorgen over de mate waarin datamining de privacy van burgers aan kan tasten. Het College Bescherming Persoonsgegevens (CBP) heeft zorgen over de toepassing van datamining en vindt dat dit alleen met grote waarborgen kan worden toegestaan. Vooral het gebruiken van gegevensbestanden met fouten kan te snel leiden tot de verkeerde uitkomst. Vaak zal de politie niet voor de kwaliteit van de gegevens in kunnen staan omdat de bestanden door anderen zijn

99 Nationale Beheerorganisatie voor Internet Providers (NBIP), de stichting NBIP voortvarend het vijfde jaar in, persbericht d.d. 10 oktober 2006

opgesteld. [100] Op grond van de wet mogen AIVD en MIVD volgens de minister van Justitie datamining toepassen, als het maar niet om zogenaamde 'fishing expeditions' gaat: *"Deze term suggereert dat zonder vooropgezet doel en zonder dat daartoe concrete aanleiding bestaat gegevensbestanden worden doorzocht. Iedere gegevensverwerkende activiteit van de dienst dient conform artikel 12 van de WIV 2002 te geschieden voor een bepaald doel en noodzakelijk te zijn voor een goede taakuitvoering van de diensten."* [101]
Uit onderzoek is gebleken dat de Nederlandse wetgeving niet is toegesneden op datamining, zowel vanuit het oogpunt van privacy als vanuit het oogpunt van de toepassing bij de opsporing. Om datamining toe te kunnen passen in de opsporing is volgens dit onderzoek een *"ingrijpende aanpassing"* van bestaande regelgeving noodzakelijk.[102]

De discussie over de toepassing van nieuwe technieken zoals datamining vindt in Nederland nog niet op politiek of bestuurlijk niveau plaats. Noch over de wijze van toepassing, noch over de samenwerking op dit punt door de daarvoor in aanmerking komende diensten, maar evenmin over eventuele grenzen aan de toepassing van datamining. In de Verenigde Staten is deze discussie al een stuk verder.

Een deel van deze discussie gaat over de vraag wat datamining precies is. Het is immers een containerbegrip waaronder uiteenlopende technieken worden gevat. Er zijn dus ook veel verschillende definities in omloop. Zoals deze van een tegenstander: *"Torturing data until it confesses... and if you torture it enough, you can get it to confess to anything."* [103] De Amerikaanse Rekenkamer (GAO) hanteert een meer waardevrije definitie: *"The application of database technology and techniques - such as statistical analysis and modelling - to uncover hidden patterns and subtle relations in data and to infer rules that allow for the prediction of future results."* [104] Volgens deze Rekenkamer wordt datamining door de Amerikaanse overheid toegepast voor een aantal uiteenlopende doeleinden. Van de 128 federale organisaties gaven 52 aan vormen van datamining te gebruiken of binnenkort te gaan gebruiken. De belangrijkste redenen waren: verbeteren van dienstverlening, ontdekken van fraude, misbruik of verspilling, het analyseren van wetenschappelijke informatie, het managen van personeelszaken, het onderzoeken van criminele activiteiten, het analyseren van intelligence en het ontdekken van terroristische activiteiten. Volgens GAO zijn er diverse privacyaspecten aan datamining die verder moeten worden onderzocht. Een van de belangrijkste daarvan is dat foute gegevens in een gegevensbank ertoe kunnen leiden dat personen via datamining worden geselecteerd als (potentiële) verdachten terwijl daar feitelijk geen aanleiding voor is. GAO bepleit daarom nader

100 Advies van het CBP inzake het conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven d.d. 22 december 2004, nr. z2004-1529
101 Antwoord van de minister van Justitie op vragen van het kamerlid De Wit (SP), Aanhangsel Handelingen vergaderjaar 2004-2005, nr. 2324
102 Dr. R. Sietsma. Gegevensverwerking in het kader van de opsporing, toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy, proefschrift Leiden, 2007, p. 417
103 Zoals geciteerd door Jeff Jonas, in What is datamining?, http://jeffjonas.typepad.com
104 General Accounting Office, report on datamining, Washington, 4 mei 2004

onderzoek. Ook de onderzoeksdienst van het Congres kwam tot de conclusie dat toepassing van datamining binnen de overheid, in het bijzonder voor veiligheidsdoeleinden een aantal knelpunten met zich brengt die tot een oplossing moeten worden gebracht: de borging van de kwaliteit van de gegevens, problemen met de koppeling van verschillende gegevensbestanden, gebruik van gegevens voor een ander doel dan waarvoor zij zijn aangeleverd ('mission creep') en mogelijke inbreuken op de privacy.[105] Enkele Amerikaanse onderzoekers hebben onlangs gesteld dat datamining bij de bestrijding van terrorisme slechts een beperkte rol kan spelen, omdat er onvoldoende patronen zijn om deze techniek te kunnen toepassen: *"The statistical likelihood of false positives is so high that predictive data mining will inevitably waste resources and threaten civil liberties."* [106] Volgens deze onderzoekers zal datamining falen als er geen gegevens bekend zijn over terroristen, hun plannen en hun methoden.

Deze kritische rapporten hebben ertoe geleid dat de Senaatscommissie voor Juridische Zaken begin 2007 een hoorzitting heeft gehouden over de toepassing van datamining bij de overheid. Door tal van deskundigen en belangengroepen zijn tijdens deze hoorzitting de mogelijke problemen rond datamining onderstreept. Van verschillende kanten is gepleit voor nadrukkelijke goedkeuring door het Congres van dataminingprogramma's.[107] De commissie heeft nog geen conclusies getrokken, maar senator Edward Kennedy heeft al laten weten dat een nadrukkelijker toezicht door het Congres noodzakelijk is: *"Today, we face the unsettling prospect that there are no clear rules for the government's national security actions or data collection."* [108]

2.5 De wijze van gegevens uitwisselen

Uitwisseling van gegevens tussen inlichtingen- en opsporingsdiensten is al jaren aangemerkt als een moeizaam proces en ook binnen de politie verloopt de uitwisseling van gegevens niet vlekkeloos. Continu doen partijen pogingen om hierin verbetering te brengen. Deze pogingen hebben weliswaar succes, maar de vooruitgang is minder dan waarop mag worden gerekend. De Algemene Rekenkamer heeft op dit punt al diverse malen aangegeven dat de samenwerking veel te wensen overlaat: *"Er bestaat derhalve geen zekerheid over de volledigheid van relevante informatie op centraal niveau."* [109]

Uitwisseling binnen de politie

De Raad van Hoofdcommissarissen kent vier portefeuillehouders die zich op een of andere manier met informatie bezig houden: Informatiemanagement, Intelligence,

105 Congressional Research Service, Data Mining and Homeland Security: an Overview, Washington, January 2006
106 Jonas, Jeff, and Jim Harper, Effective Counterterrorism and the Limited Role of Predictive Data Mining, Policy Analysis, no. 584, December 11, 2006, pp. 1-12
107 Van de hoorzitting is geen verslag beschikbaar, maar links naar de verschillende inbrengen kunnen worden gevonden op: http://jeffjonas.typepad.com
108 Edward Kennedy, Statement on balancing privacy and security: the privacy implications of government data mining programs, Washington, January 10, 2007
109 Kamerstuk 28 845, uitwisseling van opsporings- en terrorisme-informatie, p. 34

Criminele Samenwerkingsverbanden en Opsporing. Elke portefeuillehouder is vanuit zijn eigen invalshoek betrokken bij de ontwikkeling van de politiële informatiefunctie. De Inspectie Openbare Orde en Veiligheid heeft geconstateerd dat er op het hoogste niveau van de Nederlandse politie geen board of portefeuillehouder is, die het gehele terrein van informatiehuishouding tot zijn verantwoordelijkheid rekent. De nadruk ligt teveel op de informatietechnologie en te weinig op de content, de informatie, aldus de Inspectie. [110]

Oorspronkelijk was de informatie-uitwisseling en coördinatie bij de politie georganiseerd langs thematische lijnen: openbare orde informatie, criminele informatie, terreurinformatie en voetbalinformatie. Er was geen uniform, landelijk systeem. Vooral op het gebied van openbare orde was de uitwisseling van informatie slecht geregeld. Nadat rond een aantal incidenten (mond- en klauwzeer, 9/11) en evenementen (Euro 2000) de behoefte was gebleken aan een landelijk systeem, startte in 2002 het project landelijke informatiecoördinatie (LIC). Dat project beoogde een permanente voorziening te bouwen, die het mogelijk moest maken dat de informatiestromen tussen de korpsen en met de landelijke diensten doelgericht en efficiënt zouden kunnen verlopen. Het nieuwe systeem kent de volgende opbouw: op landelijk niveau is een Nationaal Informatie Knooppunt (NIK) ingericht bij de dienst Nationale Recherche Informatie. Elk korps heeft een Regionaal Informatie Knooppunt (RIK). De informatie die langs deze lijn wordt uitgewisseld staat bekend als de NIK-RIK-lijn. Deze lijn is bedoeld voor landelijke informatie en heeft een verplichtend karakter. Als via deze lijn aan de korpsen om informatie wordt gevraagd, zijn zij verplicht tot medewerking. Het vragende korps stelt in samenwerking met het NIK een strategiedocument op met een daarbij behorend informatiebehoefteplan. Dit plan wordt vervolgens bij de korpsen uitgezet die zorg dragen voor het aanleveren van de gevraagde informatie. Het proces kent de navolgende fases: bepalen van de informatiestrategie, coördinatie inwinnen informatie, ontvangen en vastleggen van informatie, analyseren en interpreteren van informatie en het verstrekken van informatie.

De Inspectie Openbare Orde en Veiligheid (IOOV) heeft twee onderzoeken verricht naar het functioneren van dit systeem van coördinatie en uitwisselen van gegevens, in 2004 en in 2006. [111] Uit deze onderzoeken blijkt dat bij elk proces via de RIK-NIK-lijn informatie uit gegevensbestanden van het korps wordt ontsloten. Slechts in een kwart van de gevallen wordt informatie gevraagd aan wijkagenten of aan informatierechercheurs. In vrijwel alle gevallen worden ook de regionale infodesk, de criminele inlichtingen eenheid en de regionale inlichtingendienst bevraagd. Voor een goede uitwisseling van informatie is een systeem van briefen en debriefen essentieel. Die systemen functioneren nog onvoldoende. In 2004 hadden 3 van de 26 korpsen op dit punt nog geen beleid

110 Inspectie Openbare Orde en veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, ontwikkelingen sinds rapportage 2004, Den Haag, 2006

111 Inspectie Openbare Orde en veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, een evaluatie van het project landelijke informatiecoördinatie DNP, Den Haag, 2004 en: Landelijke coördinatie en uitwisseling van politie-informatie, ontwikkelingen sinds rapportage 2004, Den Haag, 2006

ontwikkeld, terwijl van de korpsen die wel een beleid hadden, de helft dat beleid nog niet had geïmplementeerd. De Inspectie noemde deze situatie zorgelijk en sprak het vermoeden uit dat nu niet alle relevante informatie wordt ingezameld. [112] In 2006 was wel sprake van verbetering, maar: *"De praktijk blijkt weerbarstiger dan gedacht."* [113] De Inspectie constateerde dat de algemene tendens er een is van verdergaande integratie van informatiefuncties en het benoemen van informatie als een eigenstandig proces. Wel zijn alle korpsen hier *"te veel ieder op hun eigen wijze mee bezig."* [114]

Uitwisseling tussen inlichtingendiensten en politie

De uitwisseling tussen inlichtingendiensten en de politie loopt formeel via de lijn van de regionale inlichtingendiensten (RID). De regionale inlichtingendiensten hebben tot taak openbare orde-informatie te verzamelen alsmede informatie op het gebied van de nationale veiligheid. Voor deze veiligheidsinformatie functioneren de regionale inlichtingendiensten onder de verantwoordelijkheid van de AIVD. Deze dienst bepaalt welke informatie door de RID aan derden kan worden doorgegeven. Op deze terreinen hebben de medewerkers van de RID dus een andere verantwoordelijkheid dan andere medewerkers van het korps. Zij hebben een zogenaamde art. 60 aanwijzing.[115] Dat houdt in dat zij op grond van art. 60 van de WIV onder het gezag staan van de AIVD. Het is hen verboden om opsporingshandelingen te verrichten. De verhouding tussen de RID en de rest van het korps waar zij werkzaam zijn, staat vaak onder spanning. De uitwisseling van gegevens verloopt dan ook vaak moeizaam. Volgens het rapport van de inspectie uit 2004 bestaat er veel onvrede over het functioneren van de RID'en. Zij willen te vaak en soms ten onrechte geen informatie delen met de regionale informatie coördinator, terwijl zij daar wel over beschikken. [116] Dit probleem bestaat anno 2006 nog steeds en is in een opzicht complexer geworden: korpsen die hun informatieorganisatie beter willen stroomlijnen en in het kader van de informatie gestuurde politie effectiever en doelmatiger willen inrichten, lopen aan tegen de eis van de AIVD dat de regionale inlichtingendienst een eigenstandige positie binnen het korps moet hebben. De Inspectie noemt deze constructie gekunsteld. Bepaalde informatie zal de ene keer worden gebruikt voor opsporing, de andere keer voor terreurbestrijding en weer een andere keer voor handhaving van de openbare orde: *"Het strikt gehanteerde onderscheid tussen de twee soorten RID-informatie leidt in de praktijk van de korpsen tot, wat sommige korpsen noemen, een onwerkbare situatie."* [117] De Inspectie roept op tot het zoeken naar een bevredigende oplossing voor zowel de korpsen als de AIVD. Die oplossing zal volgens de Inspectie binnen de kaders van de wettelijke mogelijkheden moeten zijn gericht op een doelgerichte aanpassing van de cultuur.

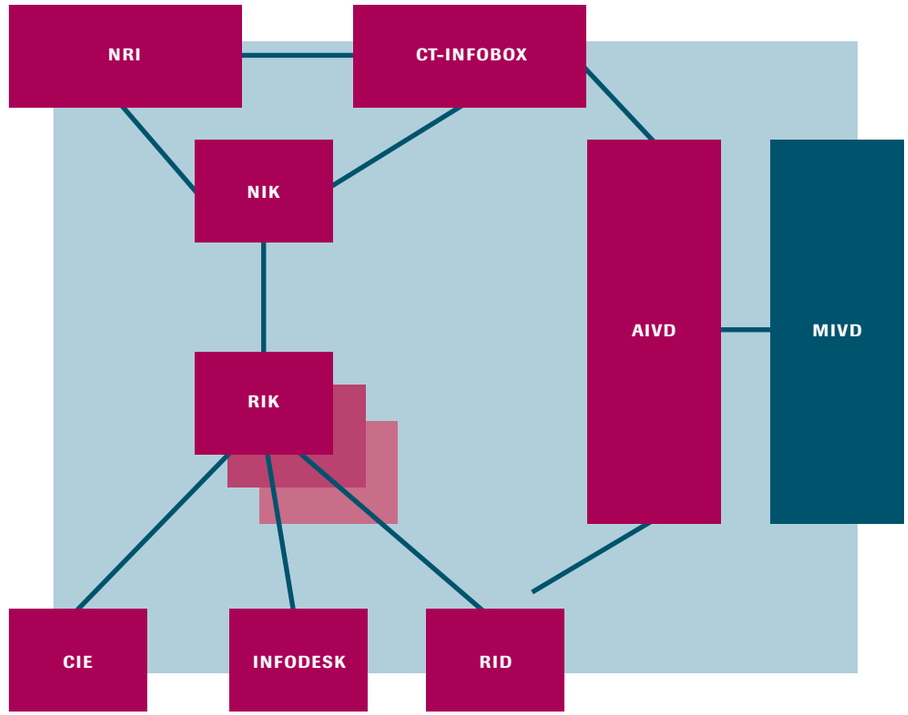
112 IOOV, 2004, p. 42
113 IOOV, 2006, p. 17
114 IOOV, 2006, p. 28
115 Uit artikel 60, derde lid: "werkzaamheden worden verricht onder verantwoordelijkheid van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en overeenkomstig de aanwijzingen van het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst."
116 IOOV, 2004, p. 55
117 IOOV, 2006, p. 22

Mede vanwege de kritiek op het functioneren van de uitwisseling van informatie tussen betrokken diensten is in 2004 besloten tot de oprichting van de Contra-Terrorisme Infobox, de CT-Infobox. Hierin werken partijen uit het veiligheidsdomein samen in de bestrijding van het terrorisme, in het bijzonder het islamitisch terrorisme. De CT-Infobox is een bijzonder samenwerkingsverband van respectievelijk AIVD, IND, KLPD, MIVD, OM en sinds kort ook de FIOD-ECD, dat ressorteert onder de AIVD en daardoor is onderworpen aan het regime van de WIV. Dat betekent onder meer dat alle informatie die wordt ingebracht in de CT-Infobox daarmee AIVD-gegevens zijn geworden. Dit samenwerkingsverband heeft tot doel het leveren van informatie over netwerken en personen die op de een of andere wijze zijn betrokken bij (islamitisch) terrorisme en daaraan te relateren radicalisering. Via raadpleging, consultatie en multidisciplinaire analyse wordt binnen de CT-Infobox een snelle beoordeling mogelijk op grond waarvan eventuele maatregelen kunnen worden getroffen. De CT-Infobox brengt zelf geen informatie naar buiten. De bestaande procedures blijven daarvoor onverkort van kracht. De CT-Infobox adviseert slechts aan de deelnemende partijen over de wenselijkheid tot verstrekking van gegevens. De minister van BZK heeft aan de Tweede Kamer laten weten dat de eerste resultaten van de CT-Infobox veelbelovend zijn en aan de verwachtingen van de deelnemende diensten voldoen.[118]

Onlangs heeft de commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten over het functioneren van de CT-Infobox gerapporteerd. De commissie heeft geconstateerd, dat er nog de nodige onduidelijkheden zijn in positie en functioneren van de CT-Infobox die een nadere regeling behoeven. Er zal volgens de commissie veel meer wettelijk moeten worden geregeld. Zo wringt het dat de CT-Infobox een samenwerkingsverband is, maar wel ondergeschikt is aan de AIVD: *"Naar het oordeel van de commissie zou in een nadere wettelijke regeling meer de nadruk kunnen en moeten worden gelegd op de samenwerking binnen de CT-Infobox."* [119] Minister Ter Horst heeft de Tweede Kamer laten weten dit advies van de commissie van toezicht over te zullen nemen: *"Hoewel ik van mening ben dat er thans op een zodanig constructieve wijze in de CT Infobox wordt gewerkt dat dit ook positieve effecten heeft op de samenwerking van de betrokken organisaties buiten de box ben ik gaarne bereid de commissie in dezen te volgen."* [120]

De Nationaal Coördinator Terrorismebestrijding (NCTb) heeft geconstateerd, dat op een aantal onderdelen de samenwerking tussen partijen die betrokken zijn bij de bestrijding van terrorisme verbeterd moet worden. Daartoe heeft de NCTb in 2006 het programma VIA gestart, Verbetering terrorisme- en criminaliteitsbestrijding door information awareness. In dit programma wordt door NCTb samengewerkt met de AIVD, het KLPD en het NFI om een aantal instrumenten te ontwikkelen die de onderlinge samenwerking verder kunnen ondersteunen. Het programma bestaat uit drie gerelateerde deelprojecten. Twee deelprojecten hebben tot doel om na te gaan in hoeverre nieuwe technologie en modellen waarde kunnen toevoegen aan criminaliteits- en terrorismebestrijding. Dit gaat om de deelprojecten patroonherkenning en kennisontwikkeling in modellen. Het derde deelproject, Verbetering CT-Infobox, betreft het ontwikkelen van een nieuw informatiesysteem voor de CT-Infobox die de analyseprocessen kan versnellen. Het totale programma duurt vier jaar en kost volgens de oorspronkelijke raming € 12 miljoen. Het programma VIA heeft volgens mededeling van de NCTb nog niet tot concrete resultaten kunnen leiden.

Het model voor uitwisseling binnen de politie en tussen de politie en inlichtingendiensten kan als volgt grafisch worden weergegeven, waarbij de bijzondere opsporingsdiensten en de Koninklijke Marechaussee buiten beschouwing blijven omdat deze relaties veelal gerelateerd zijn aan concrete zaken die in onderzoek zijn. Het model geeft de navolgende informatiestromen weer:



Verklaring van de afkortingen:
CIE = Criminele Inlichtingen Eenheid
NIK = Nationaal Informatie Knooppunt
NRI = Nationale Recherche Informatie
RIK = Regionaal Informatie Knooppunt

NIK en RIK worden aangestuurd door een Nationaal Informatie Coördinator (NIC) respectievelijk een Regionaal Informatie Coördinator (RIC).

118 Kamerstukken 29 754, Terrorismebestrijding, nr. 21, p. 3. Zie ook stuknummer 29 over de juridische positie van de CT-Infobox en het oordeel van het College Bescherming Persoonsgegevens daarover.
119 Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), Toezichtsrapport inzake de Contra Terrorisme Infobox (rapport nr. 12)Den Haag, 2007, p. 30
120 Kamerstukken 29 924, Toezichtverslagen AIVD en MIVD, nr. 16, p. 2

Ook op regionaal niveau zijn vergelijkbare initiatieven ontplooid om te komen tot betere afstemming en informatie-uitwisseling op het gebied van terrorismebestrijding. In verschillende regio's zijn daarvoor specifieke overlegvormen tussen inlichtingendiensten en de politie ontwikkeld. Inmiddels is door de Raad van Hoofdcommissarissen besloten tot een meer uniforme aanpak, waarbij wordt voort geborduurd op de aanpak die is ontwikkeld door de noordelijke korpsen. Het gaat hier om de zogenaamde regionale CT-Infoboxen, ofwel de Regionale Informatie Box Radicalisme en Islamitisch Terrorisme. Deze boxen bestaan uit twee delen, het coördinatieoverleg en het informatieoverleg. Het coördinatieoverleg bestaat uit de regionaal informatiecoördinator en het hoofd van de Regionale Inlichtingendienst. In het informatieoverleg, dat wordt voorgezeten door een medewerker van de RID die fungeert als coördinator van de regionale informatiebox, kunnen verder zitting hebben vertegenwoordigers van de criminele inlichtingeneenheid, de vreemdelingenpolitie, de regionale infodesk, de financiële recherche en (in overleg met de AIVD) andere onderdelen van de politie, bijvoorbeeld de sociale recherche. De analysewerkzaamheden vinden plaats bij de RID door de coördinator, een strategisch analist en een documentalist. Sturing van dit proces is een complex thema. Wanneer er immers over zaken wordt gesproken die het werk van AIVD raken moeten de gespreksdeelnemers beschikken over de zogenaamde artikel 60 status van de WIV. Dit geldt evenwel slechts voor een beperkt aantal mensen binnen het korps. Informatie van de AIVD wordt alleen met toestemming van de AIVD in het proces van regionale infobox ingebracht. Er is een belangrijk verschil tussen de landelijke en de regionale box. De landelijke box werkt onder gezag en verantwoordelijkheid van de AIVD. De regionale box werkt onder gezag en verantwoordelijkheid van de korpschef.

2.6 Vergelijking met andere sectoren

Om een goed beeld te kunnen krijgen over het functioneren van de systematiek van inwinnen van gegevens, heeft de adviescommissie nagegaan in hoeverre inwinnen of delen van informatie in aanpalende sectoren leerpunten voor het veiligheidsdomein op kan leveren. Daartoe komen twee sectoren meer in het bijzonder in aanmerking. Dit zijn de sector van de sociale zekerheid en de sector van de volksgezondheid.

De sociale zekerheid

In de sector van de sociale zekerheid is werkzaam de Stichting Inlichtingenbureau, een kleine non-profit organisatie die wordt gefinancierd door het ministerie van SZW. De stichting heeft tot taak de gegevensuitwisseling tussen de gemeenten en andere partijen in de keten werk en inkomen te bevorderen. De stichting levert samenloopsignalen aan gemeenten, die op grond hiervan onderzoek naar eventuele fraude of oneigenlijke gebruik kunnen starten.[121]

121 Zie voor meer informatie: www.inlichtingenbureau.nl

Al de partijen in deze sector hebben hun eigen gegevensbestanden en afspraken voor het bevragen van deze bestanden. Daarnaast zijn er ook afspraken over informatie-uitwisseling, waar ook opsporingsdiensten en -ambtenaren gebruik van maken. Voor de gegevensuitwisseling zijn twee instanties van belang, het Bureau Keteninformatisering Werk en Inkomen (BKWI), en het SZW-Informatieknooppunt (IKP). Het BKWI ondersteunt de samenwerking tussen gemeenten, de Centrale organisatie Werk en Inkomen (CWI), het Uitvoeringsinsituut WerknemersVerzekeringen (UWV) en de Sociale Verzekeringsbank (SVB).[122] Deze organisaties zijn ketenpartners in het domein van werk en inkomen. Recentelijk zijn daar de Arbeidsinspectie (AI) en de Sociale Inlichtingen en Opsporingsdienst (SIOD) bij gekomen. Het BKWI biedt voorzieningen waarmee deze organisaties hun gegevens op een efficiënte en betrouwbare manier met elkaar kunnen delen. Suwinet is de voorziening die het mogelijk maakt gegevens met elkaar uit te wisselen. Dankzij deze voorziening kan ook de 1-loket functie voor deze sector worden ingevuld. Alle gegevens blijven bij de eigenaar, maar de partners kunnen door middel van Suwinet-Inkijk in de bestanden van de partners kijken op grond van een functiegebonden autorisatiesysteem. Medewerkers hebben afhankelijk van hun functie en taak toegang tot die onderdelen van de bestanden die voor hun taak nodig zijn. Het BKWI beheert het maken van afspraken tussen de partners over de inhoud van die gegevens en de manier waarop de uitwisseling kan worden aangepakt. Ook bij de inrichting en verbetering van lokale samenwerking tussen de ketenpartijen ondersteunt en adviseert het BKWI.
Alle bevragingen worden standaard gelogd en maandelijks geanonimiseerd aan de betrokken partij toegezonden. Als er aanleiding is om een bepaalde serie bevragingen nader uit te zoeken, dan kan worden aangegeven welke medewerker welke bevragingen heeft gedaan. Hiervoor is een aparte procedure afgesproken die loopt via het eigen security management. De systematiek wordt elk jaar geaudit door externe EDP-auditors.

Naast deze voorziening bestaat nog het Informatieknooppunt van het ministerie van SZW, het IKP. Dit knooppunt is het scharnierpunt voor controle- en toezichtinformatie voor het domein werk en inkomen, met het SIOD als opsporingsdienst.

De gezondheidszorg

In de gezondheidszorg wordt al enkele jaren met wisselend succes gewerkt aan een betere geautomatiseerde toegankelijkheid van gegevensbestanden. Belangrijke bestanden zijn het patiëntendossier, het medicatiedossier, een waarneemdossier voor huisartsen en een geautomatiseerd declaratiesysteem. Deze projecten worden aangestuurd door NICTIZ, het Nationaal ICT Instituut in de Zorg.[123] Centraal onderdeel in deze ontwikkelingen wordt gevormd door het landelijk schakelpunt, een soort verkeerstoren die de uitwisseling van patiëntinformatie regelt tussen zorginstellingen. Via het landelijk schakelpunt kunnen zorgverleners informatie opvragen uit computers van andere zorgverleners. Het landelijke

122 Zie voor meer informatie: www.bkwi.nl
123 Zie voor meer informatie: www.nictiz.nl

schakelpunt is begin dit jaar aan de opdrachtgever opgeleverd. Er zijn dus nog geen ervaringen met dit schakelpunt opgedaan.

Kenmerkend voor beide domeinen is dat niet gekozen is voor een centrale opslag van gegevens, maar voor de inrichting van een geautomatiseerde verwijsfunctie, die de professionals in de keten verwijst naar de juiste plaats waar de informatie is opgeslagen. Autorisatie van toegang tot bestanden is gebaseerd op functie-eisen en een daarop aangepast beveiligingsniveau (role-based). Verwijsindexen worden overigens in het veiligheidsdomein ook toegepast, maar alleen voor de eigen dienst of organisatie.

Buitenland

In Nederland is in het verleden in dit kader regelmatig gewezen op het voorbeeld van de Belgische kruispuntbanken, welke sinds een jaar of 10 bestaan. Er is er een voor de sociale zekerheid en een voor het verkeer tussen overheid en ondernemingen. Deze banken zijn onderdeel van de strategie van de Belgische overheid op het vlak van e-government. Belangrijke doelstellingen zijn: terugdringen van administratieve formaliteiten, optimale dienstverlening en grotere doelmatigheid. Belangrijk kenmerk is voorts dat burgers en ondernemingen maar één keer hun persoonlijke of bedrijfsgegevens hoeven op te geven of te wijzigen. Binnen het netwerk van betrokken instellingen is de Kruispuntbank de centrale motor en verwijsindex. Iedere instelling in het netwerk is verantwoordelijk voor de opslag en het bijwerken van de informatie in haar gegevensbank. Op basis van strikte machtigingen kunnen andere instellingen uit het domein via het netwerk de informatie uit de verschillende gegevensbanken raadplegen. De Kruispuntbank bevat geen inhoudelijke informatie, maar slechts verwijzingsgegevens. De belangrijkste verwijsindexen zijn: het personenrepertorium (wie-waar-hoe-wanneer), de toegangsmachtigingtabel (wie krijgt wat) en de beschikbaarheidstabel (wat is waar beschikbaar).[124]

2.7 Duiding van de systematiek

Het meest opvallend aan de systematiek van inwinnen van gegevens in het veiligheidsdomein is dat er in feite geen sprake is van een systematiek, maar meer van een serie uiteenlopende systematieken. Elke partij heeft immers zijn eigen systematiek. De grote hoeveelheid toepasselijke wetgeving draagt ook al niet bij aan de totstandkoming van een heldere systematiek voor het veiligheidsdomein. Er zijn immers zoveel wetten van toepassing op het inwinnen en leveren van gegevens dat het vrijwel onmogelijk is om een goed overzicht te krijgen van de relevante wetgeving. Dat er nog veel nieuwe wetgeving in voorbereiding is, maakt dit alles nog complexer. Wat ontbreekt is een helder toetsingskader waaraan bevragingen door inlichtingen- en opsporingsdiensten moeten voldoen. In een dergelijk kader zou de wettelijke basis voor de bevraging verder kunnen worden uitgewerkt. Ook kunnen daarin voorwaarden worden gesteld aan het proces van bevraging.

124 Zie voor meer informatie: www.ksz-bcss.fgov.be

Het meest opvallend aan de systematiek van inwinnen van gegevens is dat er in feite geen sprake is van één systematiek.
Elke partij heeft immers zijn eigen systematiek.

Het is evenmin goed mogelijk om een overzicht te krijgen van het aantal malen dat externe databases per jaar worden geraadpleegd. De AIVD verschaft deze gegevens niet en de politie registreert deze gegevens niet centraal. Uit wel beschikbare bronnen en uit informatie van leveranciers van gegevens kan de conclusie worden getrokken dat het aantal bevragingen in de afgelopen jaren een sterke groei laat zien. Voor de komende jaren wordt eveneens uitgegaan van een sterke groei. In dit verband kan worden gewezen op het concept wetsontwerp voor de dataretentie. Dit concept gaat, zoals hiervoor opgemerkt, uit van een jaarlijkse toename van het aantal vragen met 20%.

Ook al betreft het vragen aan geautomatiseerde gegevensbestanden, de vragen worden vanuit het veiligheidsdomein vrijwel altijd gesteld door menselijke tussenkomst. Waar wel sprake is van een rechtstreekse toegang tot gegevensbestanden, betreft het bestanden die volledig toegankelijk zijn voor inlichtingen- en opsporingsdiensten, zoals de bevolkingsadministratie en het kentekenregister. Hierin kan verandering komen als het nu voorliggende wetsontwerp tot wijziging van de WIV wet wordt. Op grond van de voorgestelde wetswijziging kan de AIVD rechtstreekse toegang krijgen tot een lijst van bestanden die nog nader moet worden bepaald.

2.8 Tot slot: dit hoofdstuk in het kort

Het is moeilijk gebleken om een goed inzicht te verkrijgen in de wijze waarop de bevragingen vanuit externe geautomatiseerde gegevensbestanden plaats vindt. Er is geen totaaloverzicht van de wet- en regelgeving die van toepassing is op het inwinnen van gegevens uit bedoelde databases. Dat overzicht is ook moeilijk aan te leveren, omdat de relevante wetgeving divers is, van veel ministeries afkomstig en tot stand gekomen vanuit zeer uiteenlopende achtergronden. Het aantal wetten heeft de afgelopen jaren ook een sterke groei gekend vanwege de uitbreiding van bevoegdheden van inlichtingen- en opsporingsdiensten in de strijd tegen het terrorisme.

Het is niet alleen moeilijk gebleken om inzicht te verkrijgen in de relevante wetgeving, er blijkt ook geen duidelijk inzicht te bestaan in de hoeveelheid vragen die vanuit het veiligheidsdomein richting de externe databases worden gesteld. Binnen de overheid worden de bevragingen niet bijgehouden of worden zij niet extern beschikbaar gesteld. Ook het aantal taps dat de overheid plaatst op telefoongesprekken of e-mailcontacten wordt tot heden niet bijgehouden.

Ten aanzien van de toepassing van nieuwe technologieën werken de organisaties in het veiligheidsdomein weinig samen. Elke partij probeert een goede toepassing te vinden voor het gebruik van nieuwe technologische mogelijkheden zoals datamining. Samenwerking of het uitwisselen vindt nauwelijks plaats. Bestuurlijke aandacht voor de toepassing van deze nieuwe technologieën is in tegenstelling tot bijvoorbeeld de Verenigde Staten afwezig.

Uitwisseling is meer algemeen een woord dat niet vooraan staat in het denken van de verschillende partijen in het veiligheidsdomein. Het uitwisselen van gegevens is een moeizaam proces, zowel tussen de inlichtingendiensten aan de ene kant en de opsporingsdiensten aan de andere kant, als binnen de politie. Hoewel op beide fronten wordt gewerkt aan verbetering, moet toch worden geconstateerd, dat de praktijk weerbarstiger is dan gedacht.

Wanneer de situatie in het veiligheidsdomein wordt vergeleken met andere maatschappelijke sectoren, valt op dat in de andere sectoren in ieder geval conceptueel vormen van samenwerking zijn ontstaan, waar vanuit een erkenning van eenieders verantwoordelijkheid vormen van samenwerking worden ontwikkeld, die als uitgangspunt hebben dat gegevens voor andere partners in de keten beschikbaar worden gesteld.

Op grond van het bovenstaande trekt de adviescommissie de navolgende conclusies:

1. Er is geen sprake van een eenduidige systematiek waarmee partijen in het veiligheidsdomein gegevens inwinnen uit externe databases. Strategische aansturing en bestuurlijke aandacht daarvoor ontbreken.
2. Er bestaat geen totaaloverzicht van de bestaande wet- en regelgeving met betrekking tot het inwinnen van gegevens uit externe databases. Het is niet mogelijk om inzicht te verkrijgen in consistentie en samenhang van deze wet- en regelgeving.
3. Er is onvoldoende inzicht in het aantal bevragingen dat door de partijen in het veiligheidsdomein wordt verricht. Dat heeft tot gevolg dat maatschappelijke verantwoording over dit proces op dit moment niet mogelijk is.
4. Politieke discussie over voor- en nadelen van toepassing van nieuwe technieken zoals datamining vindt ten onrechte niet plaats.
5. Uitwisseling van gegevens binnen de politie en tussen inlichtingendiensten en politie is nog steeds een moeizaam proces.
6. Uitwisseling van gegevens door middel van verwijsfuncties blijkt in andere maatschappelijke sectoren succesvol te zijn.

3

3.1 Inleiding

In dit hoofdstuk worden de knelpunten geïnventariseerd die de adviescommissie is tegengekomen bij de verkenning van het systeem van inwinnen van gegevens door het veiligheidsdomein. Deze inventarisatie wordt gepresenteerd aan de hand van de volgende onderverdeling:

1. Allereerst worden de knelpunten geschetst die de adviescommissie heeft gesignaleerd aan de vraagkant.
2. Vervolgens komen de knelpunten van de leveranciers aan de orde.
3. Daarna worden enkele knelpunten in het proces beschreven.

In het volgende hoofdstuk, hoofdstuk 4, komen de conclusies aan de orde die uit deze knelpunten kunnen worden getrokken.

In dit hoofdstuk ligt het accent op de knelpunten. Dat wil uiteraard niet zeggen dat er alleen maar knelpunten zijn. Er gaat immers veel goed op het gebied van data, informatie en intelligence in het veiligheidsdomein. Aan die goede ontwikkelingen wil de adviescommissie zeker niet voorbij gaan. Uit de goede ontwikkelingen kunnen een paar leerpunten worden ontleend:

1. Allereerst blijkt met name bij de bijzondere opsporingsdiensten dat een thematische aanpak over het algemeen tot gevolg heeft dat ook veel strategischer wordt gekeken naar de noodzakelijke gegevens en naar de manier waarop die gegevens kunnen worden verkregen.
2. In de tweede plaats blijkt dat de samenwerking bij het inwinnen en delen van informatie beter verloopt naarmate de betrokken partijen elkaar meer vertrouwen.
3. Geconstateerd kan worden dat binnen veel van de betrokken organisaties initiatieven worden gestart om te komen tot oplossing van knelpunten. Het zoeken is nu naar de samenhang tussen deze initiatieven en naar de meest levensvatbare daaronder.
4. Het aanwijzen van de meest levensvatbare initiatieven en deze vervolgens snel tot ontwikkeling brengen vraagt sturing door de leiding van de organisatie.

3.2 Knelpunten aan de vraagkant

De vraagzijde bestaat uit de inlichtingendiensten AIVD, MIVD, de regionale politiekorpsen, het KLPD, de Koninklijke Marechaussee en de bijzondere opsporingsdiensten en de bijzondere opsporingsambtenaren die werkzaam zijn bij andere overheidsdiensten.

Visie en strategie

Allereerst valt op dat de partijen in het veiligheidsdomein geen gemeenschappelijke visie hebben op het belang van databanken voor de ontwikkeling van informatie en intelligence. De politie noemt informatie een kernpunt van beleid, maar de concrete uitwerking

van dit kernpunt is in de ontwikkeling van beleid ten aanzien van informatietechnologie veel verder dan de ontwikkeling van beleid ten aanzien van intelligence. Dat roept de vraag op of in de ontwikkeling van intelligence wel voldoende aandacht kan worden geschonken aan de rol van databanken. Overleg over dit onderwerp met de inlichtingendiensten vindt evenmin op strategisch niveau plaats. Dat betekent dat de leiding van deze organisaties de groeiende betekenis van geautomatiseerde gegevensbestanden voor hun primaire processen en voor de ontwikkeling van intelligence beter moet onderkennen en onderstrepen. Vooral bij een strategische aanpak van dit onderwerp kan de samenwerking veel beter. Dit geldt niet alleen voor de relatie opsporings- en inlichtingendiensten, maar ook binnen het domein opsporing en binnen de politie zelf.

Op het punt van de ontwikkeling van visie en strategie ten aanzien van samenwerking in de keten data - informatie - intelligence hebben de betrokken departementen een belangrijke initiërende en stimulerende rol. Zij hebben die rol vooral in situaties en momenten dat de partners in de veiligheidsketen onvoldoende zicht hebben op het belang van het totaal, maar vooral op het belang van de eigen positie. Die rol komt evenwel niet uit de verf. De redenen daarvoor vallen buiten de scope van ons onderzoek. Wij volstaan met de signalering dat een gezamenlijk en eensgezind optreden van de departementen op het gebied van de strategie van veiligheid een positieve stimulans zal hebben op de strategische samenwerking van de uitvoerende diensten. Wij zeggen dat met nadruk, maar ook met enige zorg omdat wij in de afgelopen maanden op dit punt een onvoldoende gevoel voor urgentie hebben geproefd.

Op het punt van de uitvoering valt eveneens op dat de samenwerking tussen opsporings- en inlichtingendiensten vooral operationeel van aard is en weinig strategisch. Op zaaksniveau worden gegevens uitgewisseld, soms in het kader van de landelijke of regionale CT-Infobox soms door middel van de regionale inlichtingendienst. Ook bij de politie kan de ontwikkeling van de strategische samenwerking op het gebied van het inwinnen van informatie nog een stevige impuls gebruiken. Deze observatie is door veel gesprekspartners op verschillende niveaus uit de betrokken organisaties gemaakt. Vooral vanuit de politie wordt geklaagd over het gebrek aan strategische samenwerking met de inlichtingendiensten. Weliswaar signaleren de meeste gesprekspartners verbetering, maar deze verbetering is nog niet in alle echelons doorgedrongen en is nog onvoldoende strategisch verankerd. Verbetering op strategisch niveau kan betere kaders bieden voor de tactische en operationele samenwerking, zodat ook daar verbetering kan ontstaan.

Enkele voorbeelden van deze observaties zijn: de samenwerking binnen de CT-Infobox is operationeel en niet strategisch; elke organisatie onderstreept het belang van informatiesturing, maar werkt niet samen met anderen bij de ontwikkeling van intelligence; debriefing wordt allerwegen als een essentieel onderdeel van informatiesturing gezien, maar is in veel korpsen nog geen standaard onderdeel van de werkprocessen; het overleg

over de inrichting van de regionale CT-Infoboxen gaat niet over de resultaten die met die samenwerking kunnen worden gerealiseerd maar over afbakening van posities en bevoegdheden.

Het proces van inwinnen en delen van gegevens kan dus als suboptimaal en zelfs onvoldoende worden gekenschetst. Door de gebrekkige samenwerking tussen de vragende partijen is dit proces onvoldoende effectief en onvoldoende efficiënt. Doordat partijen onvoldoende met elkaar samenwerken, vooral op strategisch terrein hebben zij alleen zicht op hun eigen proces en op hun eigen pogingen om in dat proces verbetering aan te brengen. Zij hebben daardoor onvoldoende zicht op het totale proces, op de overlap met andere bevragingen en op de beoordeling die hierop wordt gegeven door de informatieleverende partijen. Daardoor ontbreekt bij hen het inzicht dat de resultaten van het proces suboptimaal zijn. Niet voor niets werd in veel gesprekken door vragende partijen opgemerkt dat men van mening was dat men toch zo goed zijn best deed. Als er al dingen fout of minder goed gaan, ligt dat toch vooral aan een andere partij. Met alleen zicht op de eigen koker ontbreekt het zicht op het totaal en blijft het suboptimale karakter van het totaal achter de horizon.

Inwinnen van informatie

Bij het daadwerkelijk inwinnen van gegevens uit externe geautomatiseerde databases wordt niet samengewerkt. Elke partij maakt zijn eigen afspraken met beheerders van databases, soms zonder duidelijke wettelijke basis. Sommige vragende diensten hebben convenanten met leveranciers over inhoud en proces van informatieverstrekking, andere diensten baseren zich alleen op wettelijke bepalingen. Er is dus geen sprake van een eenduidige systematiek. Ook hier geldt dat inlichtingendiensten niet samenwerken met de politie en dat ook de samenwerking binnen de politie voor verbetering vatbaar is. Alle politiekorpsen hebben hun eigen procedures en afspraken. De NRI heeft geen zicht op de deugdelijkheid of kwaliteit van deze procedures. De informatie uit databases wordt soms online verkregen (zoals uit de database van de RDW) soms door tussenkomst van daartoe geautoriseerde functionarissen bij de informatieleverende partij (zoals bij telecombedrijven). Deze gebrekkige samenwerking binnen de opsporing heeft tot gevolg dat dezelfde informatie soms meerdere malen wordt gevraagd. Ook ontstaat soms twijfel of de wijze waarop de informatie wordt gevraagd voldoende professioneel is. Deze twijfel is in verschillende gesprekken door vertegenwoordigers van informatieaanbieders geuit. Volgens hen komt het veelvuldig voor, dat de vraagstelling onvoldoende specifiek is, niet leiden kan tot de gewenste informatie, onzorgvuldigheden bevat of voorbij gaat aan de inhoudelijke deskundigheid van de aanbieders. Ook is bij herhaling geconstateerd dat dezelfde vraag binnen korte tijd door vier verschillende diensten is gesteld.

Dat het vrijwel onmogelijk is gebleken om goed zicht te krijgen op het aantal bevragingen dat wordt gedaan door inlichtingen- en opsporingsdiensten en op de daad-

werkelijke groei daarvan, is een aanwijzing te meer dat er geen eenduidige systematiek bestaat voor deze bevragingen. Er kan immers geen systematiek zijn als er geen zicht bestaat op de inhoud daarvan - en kennelijk onvoldoende behoefte om dat inzicht te verkrijgen.

Iedereen constateert dat de bevragingen in de afgelopen jaren sterk zijn gegroeid, maar een cijfermatige onderbouwing daarvan kan alleen op onderdelen worden verkregen. De cijfers van CIOT en MOT laten zien dat er daadwerkelijk sprake is van een flinke groei. De inschattingen in het conceptontwerp dataretentie over een jaarlijkse groei van 20% geven aan dat ook de rijksoverheid rekening houdt met een forse groei[125]. De AIVD houdt de feitelijke gegevens voor zich om redenen van staatsveiligheid en de politie houdt de bevragingen niet bij, noch centraal, noch decentraal. Zelfs over het aantal taps dat door inlichtingen- en opsporingsdiensten wordt geplaatst, een middel dat met veel juridische waarborgen is omgeven, kan de regering geen duidelijkheid bieden. In antwoord op vragen uit de Tweede Kamer heeft minister Brinkhorst van Economische Zaken vorig jaar aangegeven dat er geen landelijke gegevens beschikbaar zijn van het aantal justitiële taps op jaarbasis.[126] Uitzondering hierop is een onderzoek uit 1998 bij de regionale tapkamers, waaruit bleek dat er in 1998 ongeveer 10.000 taps zijn geplaatst, waarvan 3000 in het vaste net en 7000 in het mobiele net. Dit betreft dus niet de taps die ten behoeve van de AIVD zijn geplaatst. Door de invoering van de wet Bijzondere Opsporingsbevoegdheden in 2000 is de kring van personen waar een tap kan worden geplaatst, aanzienlijk uitgebreid. Er is dus geen zicht in hoeverre het aantal taps sinds 1998 is uitgebreid.

Het aantal en de omvang van de databases waaruit gegevens kunnen worden geput nemen in hoog tempo toe. Het aanbod aan informatie groeit dus navenant en als gevolg daarvan ook de behoefte aan informatie. Ook hier geldt immers dat aanbod vraag schept. Het technisch beheren van deze informatiemogelijkheden vraagt nieuwe instrumenten en nieuwe specialismen. Bij het zoeken daarnaar vindt elke betrokken partij in het veiligheidsdomein zijn eigen wiel uit. Datamining, patroonherkenning en profiling zijn in dit verband relevante begrippen. Op deze punten wordt door de vragers van informatie slechts in beperkte mate samengewerkt. Het project VIA van de NCTb in samenwerking met AIVD, NFI en KLPD geeft aanzetten tot deze samenwerking, maar de resultaten daarvan zijn nog niet zichtbaar. De schaarse kennis die er op dit gebied aanwezig is, wordt door deze gebrekkige samenwerking ondoelmatig benut. Dit geldt ook voor de steeds schaarser wordende kennis van nieuwe informatietechnologieën. Met het aantrekken van de economie wordt het voor het veiligheidsdomein steeds moeilijker om deze kennis uit de markt aan te trekken. Inlichtingendiensten en opsporingsdiensten beconcurreren elkaar op dit punt in plaats van dat zij met elkaar samenwerken.

125 Zie Memorie van Toelichting concept wetsontwerp inzake bewaarplicht van telecommunicatiegegevens, ministerie van Economische Zaken, Den Haag, 2006

126 Zie voor de antwoorden: kamerstuk 30 517, nr. 2, pp 7-8

Dit maakt het proces niet alleen onvoldoende effectief, maar ook onvoldoende efficiënt. Elke partij pleegt immers zijn eigen afspraken te maken, zijn eigen vorm van contact of bevraging te organiseren en erop toe te zien dat het proces professioneel is ingericht. Nog ondoelmatiger is dat elke partij probeert op eigen kracht het steeds sneller verlopende proces van technologische vernieuwing bij te houden. Dit gebrek aan samenwerking is kostbaar in zowel de inzet van financiële en personele middelen als ook in de termijnen waarop resultaten worden bereikt.

Het delen van informatie

De werelden van opsporing en inlichtingendiensten groeien naar elkaar toe. Vroeger waren de inlichtingendiensten gericht op het weren van bedreigingen van de staatsveiligheid die vooral van buiten kwamen. Dat stond relatief ver af van de wereld van de opsporing die zich bezig hield met al dan niet georganiseerde criminaliteit in eigen land. Het fenomeen van het moderne terrorisme heeft dat veranderd en de werelden van inlichtingendiensten en opsporing dichter bij elkaar gebracht. Het mondiale terrorisme waar wij nu mee te maken hebben, is gericht op maatschappelijke ontwrichting en gebruikt daarvoor criminele instrumenten. Een op het oog door gewone criminelen uitgevoerde overval kan dus zeer wel bedoeld zijn om geld binnen te halen ter voorbereiding van een terroristische aanslag. Uit onderzoek van de politie is bijvoorbeeld gebleken dat van de jongeren die gesignaleerd staan voor radicalisering 75% eerder met de politie in aanraking is geweest vanwege criminele activiteiten.

Naarmate de politie meer pro-actief dan reactief werkzaam wil zijn, zal zij meer gebruik gaan maken van instrumenten zoals die voorheen vooral in de wereld van de inlichtingendiensten werden gebruikt. Daarnaast is voor een succesvolle bestrijding van terrorisme in toenemende mate een rol voor de politie weggelegd. Uit onderzoek blijkt dat met name de plaatselijke politie een belangrijke rol kan spelen in het voorkomen van terroristische aanslagen door gebruik te maken van hun lokale netwerken voor het delen van relevante informatie met bewoners en voor het verzamelen van gegevens die voor de strijd tegen het terrorisme van belang zijn.[127] Hoewel de werelden van de inlichtingendiensten en de opsporingsdiensten dus naar elkaar toegroeien, trekken deze diensten zelf vaak nog niet samen op.

De adviescommissie wil zeker niet ontkennen dat er sprake is van verbetering, zoals diverse gesprekspartners hebben aangegeven. Desondanks heeft de adviescommissie moeten constateren dat het onderling vertrouwen kennelijk nog onvoldoende groot is. In de gevoerde gesprekken werden over en weer veel verwijten geuit en werd de mate van elkaars professionaliteit ter discussie gesteld. De onderlinge cultuur is er nog lang niet een van elkaar helpen en elkaar opzoeken. Het gevoel van urgentie voor onderlinge

127 Police Executive Research Forum, Local Law Enforcement's Role in Preventing and Responding to Terrorism, Washington 2001

samenwerking leeft nog onvoldoende breed. De verhouding tussen AIVD en politie wordt nog teveel gekenmerkt door wederzijdse verwijten en te weinig door het besef dat zij partners zijn in het veiligheidsdomein en doelstellingen hebben die in elkaars verlengde liggen. Deze constatering is niet nieuw en ook niet specifiek Nederlands.

Het gebrek aan samenwerking tussen inlichtingen- en opsporingsdiensten komt in alle landen voor. Ondanks pogingen van bestuurders en wetgevers om hier verandering in aan te brengen, blijft de samenwerking onder de maat. Door de globalisering van de criminaliteit en de groei van het wereldwijde terrorisme zijn de werelden van de inlichtingendiensten en de opsporingsdiensten dichter bij elkaar gekomen en hebben de betrokken diensten ook veel meer met elkaar te maken. Dat heeft spanningen opgeroepen die nog steeds bestaan. Volgens een Amerikaanse regeringscommissie zijn er drie oorzaken voor deze spanningen.

- De belangrijkste oorzaak is dat opsporingsdiensten klagen over de gebrekkige informatievoorziening door de inlichtingendiensten.
- Een tweede oorzaak is dat inlichtingendiensten zich vaak verschuilen achter buitenlandse afspraken of bronnen.
- Een derde bron van conflict is gegroeide praktijk van opsporingsdiensten om een eigen internationaal netwerk op te bouwen en steeds meer liaisons in het buitenland te stationeren. Ook op dit vlak loopt de informatiewisseling moeizaam.[128]

De Commissie-Havermans, die een bestuurlijke evaluatie heeft uitgevoerd van het functioneren van de AIVD, heeft gewezen op de moeizame positie van deze dienst in de veiligheidsketen en op de negatieve oordelen die de ketenpartners hierover hebben. Deze commissie signaleerde dat er veel beelden bestaan over de AIVD als een verkokerde en bureaucratische organisatie: *"Het belangrijkste beeld is dat de AIVD niet gepercipieerd wordt als een organisatie die ervan doordrongen is dat hij daadwerkelijk deel uitmaakt van een keten. Bovendien wordt de AIVD door de ketenpartners onvoldoende gezien als een partner. In de keten wordt de nadruk gelegd op het belang van het uitwisselen van informatie en op het feit dat de AIVD juist in dat opzicht in gebreke blijft."* [129] Duidelijk is dat de dienst deze kritiek ter harte heeft genomen en veel investeert in verbetering van de relatie met de andere partners in de veiligheidsketen. De kaders daarvoor zijn aangegeven in het kabinetsstandpunt naar aanleiding van het rapport van de commissie: uitwisseling moet beter, maar het moet passen binnen de wettelijke kaders, afspraken met buitenlandse zusterdiensten en bronnen alsmede de modus operandi moeten worden beschermd.[130]

128 Commission on the Roles and Capabilities of the United States Intelligence Community, pp.41-42
129 Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst ("Commissie-Havermans"): De AIVD in verandering, November 2004, p. 44
130 29 876, nr. 3, Regeringsstandpunt inzake Rapport van de Commissie Bestuurlijke Evaluatie AIVD, p. 4

Wij hebben echter moeten constateren dat de pogingen tot verbetering door de AIVD nog niet in alle opzichten succesvol zijn geweest. Vooral op het punt van uitwisselen en delen van informatie bestaan fricties. Er wordt onvoldoende informatie gedeeld tussen inlichtingendiensten en opsporingsdiensten. Er zijn aanzetten voor verbetering gedaan, maar zij hebben nog onvoldoende resultaat. Volgens verschillende gesprekspartners bij de politie heeft de AIVD nog onvoldoende invulling gegeven aan de adviezen van de commissie-Havermans om meer informatie te verstrekken en beter samen te werken met de andere diensten in het veiligheidsdomein. Het volgende citaat uit het rapport van deze commissie doet volgens deze gesprekspartners nog steeds opgeld: *"De samenwerking tussen de AIVD en anderen op het terrein van terrorismebestrijding dient sterk te worden verbeterd, zowel ten aanzien van de informatieuitwisseling en de informatie-analyse als ten aanzien van de operationele consequenties die daaruit voortvloeien."* [131] De samenwerking tussen de betrokken partijen in de CT-Infobox wordt verschillend beoordeeld. De ene gesprekspartner is van mening dat dit proces goed loopt, terwijl de andere gesprekspartner aangeeft van mening te zijn dat de AIVD in dit samenwerkingsverband te weinig coöperatief is en de indruk wekt zich te willen terugtrekken. Alle partijen erkennen dat de samenwerking nog in de kinderschoenen staat en dat verdere ontwikkeling noodzakelijk is.

Overal in de wereld bestaat een politieke en bestuurlijke wens tot betere samenwerking tussen deze diensten en tot een betere uitwisseling van informatie. In Nederland is dat naar aanleiding van het rapport van de Commissie-Havermans nog eens nadrukkelijk onderstreept. Die samenwerking en uitwisseling zullen er echter niet vanzelf komen, maar alleen als politieke en bestuurlijke leiding nadrukkelijk daarop gaan en blijven sturen. De natuurlijke neiging van mensen die beschikken over geheime informatie is immers om te proberen alle risico's voor schending van dat geheim volledig uit te sluiten. Dat is echter onmogelijk. Daarom moet een goed systeem van risicobeheersing afdoende zijn. En juist daar zullen de politieke en bestuurlijke sturing en ondersteuning zich op moeten richten.

3.3 Knelpunten aan de leverancierskant

Er zijn veel partijen die informatie leveren aan het veiligheidsdomein, soms op basis van een wettelijke verplichting, soms op basis van vrijwilligheid. In het onderzoek van de adviescommissie zijn vertegenwoordigers betrokken van diverse belangrijke leveranciers uit zowel de private sector, zoals banken en telecomproviders, als uit de publieke sector, zoals gemeenten en rijksdiensten. Uit de reacties van deze partijen valt een aantal duidelijke hoofdlijnen te onderkennen. Toch zullen er ongetwijfeld partijen zijn die geen knelpunten of andere knelpunten ervaren. De adviescommissie heeft er naar gestreefd om vooral een beeld te krijgen van de belangrijkste knelpunten. Meer was

131 Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst (Commissie-Havermans): De AIVD in verandering, Den Haag, 2004, p. 205.

ook niet mogelijk, al was het maar omdat er ook leveranciers zijn die onbekend blijven omdat hun afspraken met inlichtingen- of opsporingsdiensten niet openbaar gemaakt kunnen worden.

Omvang en kosten

Partijen die informatie moeten leveren klagen in toenemende mate over het proces van inwinning van informatie. Dit proces groeit in hun ogen sterk wat betreft omvang en complexiteit van vraagstelling en de tegemoetkoming door het Rijk in de te maken kosten is volgens hun onvoldoende. De stijging van de kosten wordt voor een deel veroorzaakt door de groei in het aantal bevragingen en door de complexiteit daarvan en voor een deel omdat de overheid steeds vaker vraagt om gegevens die bedrijven uit eigen bedrijfseconomische overwegingen niet bij zouden houden. Deze klachten komen niet alleen uit het private domein (vooral banken, telecom en internetproviders) maar ook uit het publieke domein (bijvoorbeeld RDW). De discussie over de hoogte van de vergoedingen loopt al enkele jaren en partijen zijn er nog steeds niet in geslaagd om tot een bevredigende oplossing te komen. In de telecomsector heeft dit inmiddels tot een tweetal gerechtelijke procedures geleid en de bankenwereld heeft berekend dat de jaarlijkse kosten voor de gegevenslevering aan het veiligheidssector ongeveer € 320 miljoen bedraagt.[132]

Deze discussie over de financiële vergoeding klemt temeer omdat het aantal bevragingen door politie en inlichtingendiensten in de afgelopen jaren sterk is toegenomen en er geen eind aan de groei lijkt te komen. Precieze gegevens over alle sectoren ontbreken, maar op deelterreinen is de groei wel degelijk duidelijk. Wordt bijvoorbeeld gekeken naar het aantal gemelde ongebruikelijke financiële transacties in het kader van de Wet MOT, dan is een sterke groei waarneembaar: Het aantal gemelde transacties nam toe van 76.085 in 2001 tot 181.623 in 2005, een stijging met meer dan 150% in 4 jaar. [133] Alle respondenten aan de kant van de verstrekkers van gegevens geven aan dat het aantal bevragingen in de afgelopen 5 jaar sterk is gegroeid. Deze trend blijkt ook uit de gegevens van de RDW. Op jaarbasis verricht de RDW 154,7 miljoen verstrekkingen uit het kentekenregister aan de partijen in veiligheidsdomein. De RDW mag voor deze verstrekkingen geen kosten in rekening brengen. Volgens berekeningen die de RDW op verzoek van de adviescommissie heeft gemaakt, bedragen de rechtstreekse kosten voor deze leveringen tussen de € 2,5 en 4 miljoen op jaarbasis. De indirecte kosten van de RDW (voor inrichting van de database voor deze verstrekkingen, van de technische infrastructuur en van de organisatie) bedragen volgens de RDW tenminste een drievoud van dit bedrag.

De klachten van de leverende partijen op dit punt vallen in twee hoofdlijnen uiteen. In de eerste plaats zijn inlichtingen- en opsporingsdiensten volgens hen onvoldoende bereid om te praten over een meer doelmatige inrichting van de zoekprocessen waarbij meer rekening wordt gehouden met de bedrijfsvoering van de leverende partijen. De tweede hoofdlijn is de hoogte van de vergoeding voor de geleverde informatie. Met name ten aanzien van deze tweede hoofdlijn komen partijen in de sector van de telecommunicatie steeds scherper tegenover elkaar te staan. Er lopen twee rechtzaken tegen de staat over de vergoeding van kosten voor het leveren van informatie en voor het aftappen. In de ene zaak, die gaat over de vergoeding van kosten voor het aftappen (aangespannen door XS4ALL) heeft de rechter onlangs uitspraak gedaan. Er zitten in die uitspraak aanknopingspunten voor nieuw overleg, aldus de sector. Een belangrijk aanknopingspunt is dat de rechter in zijn uitspraak op onderdelen ernstige kritiek uit op de Staat. De rechtbank overweegt dat een op zichzelf rechtmatig overheidsbesluit er niet toe mag leiden dat onevenredig nadelige gevolgen daarvan (dat wil zeggen buiten het normale bedrijfsrisico vallend) ten laste van een beperkte groep komen. Zij dienen gelijkelijk over de gemeenschap te worden verdeeld. Het toebrengen van onevenredige schade noemt de rechtbank onrechtmatig. De rechtbank kan op grond daarvan de Staat ook niet volgen in diens stelling dat het logisch is om de kosten van het aftappen bij de marktpartijen te leggen. De eis van XS4ALL wordt echter toch afgewezen, omdat de verplichting tot aftappen is gebaseerd op de Telecommunicatiewet. Toetsing van de wet is aan de rechter niet toegestaan en daarom wordt de eis afgewezen.[134] XS4ALL overweegt om hoger beroep aan te tekenen, maar is aldus een persbericht naar aanleiding van het vonnis gesterkt in de overtuiging dat de Staat ten aanzien van de vergoeding van tapkosten een verkeerde weg bewandelt: *“De rechtbank is het zo te zien principieel met ons eens dat dit soort kosten niet bij providers maar bij de overheid thuis horen. Dat is een belangrijk signaal naar het parlement bij de invoering van de bewaarplicht.”* [135]

De andere rechtszaak is aanhangig gemaakt door KPN en Vodafone (namens de sector) en heeft te maken met de hoogte van de vergoeding voor werkzaamheden. Deze zaak wordt behandeld door de bestuursrechter in Rotterdam en spitst zich toe op door het Rijk niet betaalde rekeningen. De uitspraak wordt in het voorjaar van 2007 verwacht. De achtergrond van die zaak is de volgende: vanaf medio jaren ‘90 vergoedde de Staat de kosten voor werkzaamheden van Internet en telecomproviders, zoals het aanleveren van gegevens en het aftappen. Over de hoogte van de vergoeding vond jaarlijks overleg plaats tussen de Staat en de betrokken partijen. In 2005 heeft de Staat dit eenzijdig gewijzigd. Sindsdien stelt zij eenzijdig jaarlijks de hoogte van de vergoedingen vast. Een handeling waarvoor in het verleden een bedrag van € 110 werd vergoed, krijgt bijvoorbeeld nu als vergoeding niet meer dan € 13.

Onenigheid over de hoogte van de financiële vergoeding speelt ook een rol bij de voorbereiding van de Nederlandse wetgeving over de invoering van de dataretentie. Volgens het conceptwetsontwerp zullen de telecomaanbieders (in totaal ongeveer 300

132 Zie hiervoor in paragraaf 2.4.
133 Jaaroverzicht 2005 van het Meldpunt Ongebruikelijke Transacties (MOT)
134 Vonnis van de rechtbank ‘s-Gravenhage, d.d. 21 februari 2007, zaaknummer 239632/HA ZA 05-1009
135 Persbericht van XS4ALL d.d. 21 februari 2007: http://www.xs4all.nl/nieuws/bericht.php?id=857&taal=nl&msect=Nieuws

bedrijven in Nederland) verantwoordelijk zijn voor de kosten die gemaakt moeten worden voor de opslag van de gegevens, de investeringen die benodigd zijn om de (verkeers-) gegevens te ontsluiten, de kosten van het beheer van de systemen, en het beschikbaar maken en stellen van de gegevens ten behoeve van de behoeftestellers. De bedrijven verzetten zich tegen deze lastenverhogingen.

De discussies over de kostenvergoedingen verzieken de sfeer tussen overheid en de sector van de telecombedrijven. Er is nauwelijks meer sprake van overleg, zodat er ook over de uitvoering van de praktijk van gegevensverstrekking tal van onduidelijkheden bestaan. Zo zijn er op dit moment geen concrete procesafspraken over onder meer de volgende punten:

- de tijd waarop de aanbieders beschikbaar moeten zijn voor het verschaffen van informatie (zoals 's nachts),
- de termijn waarbinnen moet worden gereageerd op een verzoek om informatie,
- de termijn waarbinnen een mondeling verzoek wordt opgevolgd door de (verplichte) schriftelijke bevestiging,
- de feiten waarover de sector uit eigen beweging informatie zou moeten of kunnen geven (bijvoorbeeld kinderporno).

Een punt wat hierbij ook een rol speelt is dat de Internetproviders dagelijks van alle Internetgebruikers een IP-adres moeten aanleveren. Met name de mensen die gebruik maken van een inbelverbinding krijgen elke keer dat zij inbellen een nieuw IP-adres toegewezen. Toch hoeft per abonnee maar één IP-adres per dag te worden aangegeven.

Nu is er nauwelijks meer sprake van een goed overleg tussen sector en overheid. Bij dit overleg zijn 4 departementen betrokken, maar het enige departement dat niets met de inhoud van het inwinnen van informatie en met het aftappen te maken heeft, is het aanspreekpunt voor de sector: Economische Zaken. Toen Telecom nog onder Verkeer en Waterstaat viel was er een overlegorgaan tussen de Staat en de sector ingericht, het Overleg Post en Telecom. Omdat Economische Zaken geen geformaliseerd overleg wilde, wordt nu alleen nog maar informeel overleg gevoerd, waaraan de andere drie overige betrokken departementen niet meer deelnemen. De nieuwe staatssecretaris van Economische Zaken heeft inmiddels aan de Tweede Kamer toegezegd dat er een nieuwe vorm van overleg zal worden opgezet, waarbij ook de opsporingsdiensten betrokken zullen worden.[136]

De manier waarop sector en overheid met elkaar omgaan wordt treffend duidelijk gemaakt door de beoordeling van de evaluatie van het aftappen. Vorig jaar is er in opdracht van de minister van Economische Zaken een evaluatie uitgevoerd naar de werking van hoofdstuk 13 van de Telecommunicatiewet (het hoofdstuk over aftappen).

136 Mededeling tijdens het Algemeen Overleg van 28 maart 2007

De conclusie van de onderzoekers van de universiteit van Tilburg en een extern adviesbureau was dat het huidige systeem voor dit moment met een aantal aanpassingen zou kunnen voldoen, maar dat dit systeem niet toekomstvast is en snel aan de nieuwe technologische ontwikkelingen moet worden aangepast. Deze evaluatie is door minister Brinkhorst naar de Kamer gestuurd met als hoofdconclusie dat de wet goed functioneert: *"Het is verheugend, dat het evaluatierapport concludeert dat de beleidsuitgangspunten adequaat zijn vertaald in wetgeving en dat het doel van het beleid is bereikt."* [137]
De telecombedrijven benadrukken een heel andere conclusie uit het rapport. Die conclusie houdt in dat het huidige beleid en regelgeving niet adequaat zijn voor de toekomst: *"De ontwikkelingen in techniek en markt die wij signaleren veroorzaken diverse problemen die de doeltreffendheid en de doelmatigheid onder druk zetten."* [138] De technologische ontwikkelingen op het gebied van de telecom zullen ertoe leiden dat er steeds meer gaten vallen in de aftapbaarheid die niet te dichten zijn met de huidige beleidsuitgangspunten en de huidige wetgeving. Daarom zullen keuzes gemaakt moeten worden in beleid en wetgeving, wil men het instrument aftappen ten minste in redelijke mate kunnen behouden. Grondige aanpassing van de bestaande regelgeving is dus nodig.[139]

De positieve toon van de kabinetsbrief ligt dus niet geheel in lijn met de conclusies van het externe onderzoeksrapport. Het negeren van de kritische kanttekeningen bracht de leider van het onderzoek er toe om in een persbericht van de universiteit op te merken dat het kabinet de moeilijkheden rondom aftappen van nieuwe technische apparatuur onderschat.[140] De Tweede Kamer heeft op 28 maart 2007 met het nieuwe kabinet overleg gevoerd over dit rapport en de problemen rond het aftappen. In dat overleg hebben de bewindslieden toezeggingen gedaan over hervatting van het overleg met de sector en over een beter inzicht in het aantal telefoontaps.

Niet alleen in de sector van de telecom hebben de klachten geleid tot spanningen en irritaties tussen het bedrijfsleven en de overheid. Ook uit andere sectoren zijn klachten gekomen over de geringe bereidheid van de rijksoverheid om aandacht aan de problemen op dit gebied te schenken. Het is opvallend dat zich hieronder ook overheidsinstellingen bevinden, met name zelfstandige bestuursorganen en verzelfstandigde diensten.
De antwoorden van de overheid op deze klachten van de gegevens leverende partijen zijn over het algemeen formalistisch van aard: de verplichting staat in de wet en men heeft zich maar aan de wettelijke regelingen te houden. Deze formalistische houding wordt soms vergezeld van een bijna emotionele oproep: het bedrijfsleven zou zich meer bewust moeten zijn van de eigen rol in de strijd die de samenleving moet voeren tegen criminaliteit en terrorisme.

137 Kamerstuk 30 517, nr. 1, p. 1. Het evaluatierapport is als bijlage bij dit Kamerstuk gevoegd: Koops, B.J., Bekkers, R.N.A., Bongers, F.J., & Fijnvandraat, M. (2006). Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet. Tilburg, 2005
138 P. 74.
139 Koops, B.J., Bekkers, R.N.A., Bongers, F.J., & Fijnvandraat, M. (2006). Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet. Tilburg: TILT & Dialogic
140 Persbericht van de Universiteit van Tilburg d.d. 13 april 2006: Aftapproblemen door kabinet onderschat

Terugkoppeling

Een andere klacht is dat de informatie leverende partijen niet of nauwelijks zicht hebben op wat er gebeurt met de door hen verstrekte gegevens. Zij ervaren deze levering als eenrichtingsverkeer; zij leveren wel, maar krijgen er niets voor terug. De aanbieders stellen dat het achterwege blijven van enige feedback het gevoel voedt dat de levering vooral een bureaucratische actie is waarvan nauwelijks een bijdrage kan worden gezien aan de strijd tegen criminaliteit of terrorisme. Met name de banken wijzen erop dat de financiële sector jaarlijks met aanzienlijke kosten ongeveer 180.000 ongebruikelijke transacties meldt, maar dat er uiteindelijk slechts ongeveer 130 zaken bij de rechter aanhangig worden gemaakt, minder dan 0,1%. Het ontgaat de banken volledig welke waarde hun meldingen hebben gehad voor de bestrijding van criminaliteit of terrorisme. Betere feedback helpt de leveranciers van informatie ook om hun eigen taken op dit vlak beter te doen. Verzekeringsmaatschappijen merken bijvoorbeeld op dat de politie wel medewerking vraagt bij het opsporen van verzekeringsfraude, maar de verzekeringsbedrijven onvoldoende in staat stelt om dubieuze claims af te wijzen. Dit is voor de sector een groot probleem, omdat deze per jaar meer dan € 900 miljoen schade lijdt door fraude. Het Verbond van Verzekeraars stelt dat dit bedrag aanzienlijk kan worden teruggebracht door een betere terugkoppeling van informatie door de politie. Nu kan volgens inschattingen maar 5 tot 8 % van de fraude door particulieren daadwerkelijk worden bewezen.
Het Verbond van Verzekeraars heeft vorig jaar een eigen Deltaplan vastgesteld met maatregelen voor de sector om de fraude terug te dringen. Betere informatie-uitwisseling met politie en justitie maakt onderdeel uit van dit plan.[141] Wel zijn inmiddels afspraken gemaakt over een betere afhandeling door het Openbaar Ministerie van fraudemeldingen door verzekeringsbedrijven. Bij vermoeden van fraude doen zij altijd aangifte bij een meldpunt van het OM.

De leveranciers van informatie tekenen aan, dat bestuurders en politici wel oog hebben voor hun wens tot betere terugkoppeling, maar dat dit in de praktijk door politie en inlichtingendiensten niet wordt uitgevoerd. Er wordt in dit verband op gewezen dat diverse ministers (Donner, Remkes, Korthals Altes) in het recente verleden wel degelijk de politieke uitspraak hebben gedaan dat de inhoudelijke feedback vanuit het veiligheidsdomein richting het bedrijfsleven moet verbeteren.

Ook overheidsdiensten klagen over de gebrekkige terugkoppeling. Voorbeelden hiervan zijn de sector van de sociale zekerheid en de IND. Deze diensten klagen vooral over terugkoppeling door de AIVD.

Mate van gezamenlijkheid

De klachten van de informatie leverende partijen kennen nog een diepere dimensie. De overheid stelt al enkele jaren dat de vorming van de netwerksamenleving tot gevolg

141 Verbond van Verzekeraars, Deltaplan aanpak fraude bij schadeverzekeringen, Den Haag, februari 2006

Zij ervaren deze levering als eenrichtingsverkeer; zij leveren wel, maar krijgen er niets voor terug.

heeft dat hiërarchische lijnen tussen overheid en samenleving vervagen en dat de overheid haar taken veel meer dan vroeger in samenwerking met marktpartijen en civil society moet uitvoeren. Op veel terreinen onderneemt de overheid dan ook pogingen om samen met markt en civil society maatschappelijke vraagstukken aan te pakken. In dat kader doet zij ook regelmatig een oproep aan het bedrijfsleven over te gaan tot maatschappelijk verantwoord ondernemen. Het motto van het kabinet-Balkenende IV ('Samen werken, samen leven') verwoordt deze oproep tot gezamenlijkheid heel stellig. Maar op het terrein van de veiligheid is volgens de informatie leverende marktpartijen een omgekeerde trend waarneembaar. Daar trekt de overheid zich terug op haar eigen stellingen en geeft zij aan zich als enige verantwoordelijk te achten voor het bestrijden van criminaliteit en terrorisme. Het bedrijfsleven mag wel helpen, maar elke vorm van gezamenlijkheid lijkt te ontbreken. Vooral in de strijd tegen terrorisme is dat een onhoudbare stelling, aldus deze critici. Deze dreiging is immers zo divers en kan op zoveel plaatsen tot uitdrukking komen dat een effectieve bestrijding alleen mogelijk is in samenwerking met bedrijven en burgers. Bedrijven weten waar de zwakke plekken zitten, terwijl burgers eerder symptomen van radicalisering of ander afwijkend gedrag opmerken. De informatie die de NCTb heeft gegeven aan bedrijven om zich beter voor te bereiden op een mogelijke terroristische aanslag wordt niet ervaren als een vorm van samenwerking, maar als een vorm van voorlichting.[142] Deze groep critici wijst er ook op dat de overheid niet de kennis heeft welke in het bedrijfsleven beschikbaar is op terreinen als risicomanagement en profilering van risicogroepen.[143] Uit deze kritiek blijkt dat de pogingen vanuit de overheid om het bedrijfsleven meer te betrekken bij de strijd tegen het terrorisme door het bedrijfsleven nog te weinig worden ervaren als een poging tot gezamenlijk optrekken.

3.4 Knelpunten in het proces

In het proces van gegevens vragen en leveren kunnen eveneens knelpunten worden onderscheiden. Deze knelpunten betreffen soms zowel de vragers als de verstrekkers van gegevens, maar hebben ook te maken met aandachtspunten die worden aangedragen door wetenschappers of zij die anderszins betrokken zijn bij dit proces.

Toezicht op het inwinnen van gegevens

Het toezicht op het inwinnen van gegevens uit externe databases is niet eenduidig geregeld. Alle instanties die de bevoegdheid hebben om deze gegevens in te winnen vallen onder verschillende toezichtregimes.

De huidige toezichthouders hebben over het algemeen een andere focus dan de bevraging van externe databases. Zij hebben slechts bevoegdheden voor een deel van het onderhavige werkterrein. De Inspectie Openbare Orde en Veiligheid (IOOV) heeft bevoegdheden ten aanzien van de politie, niet ten aanzien van bijzondere opsporingsdiensten en de Koninklijke Marechaussee. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft bevoegdheden ten aanzien van de AIVD en de MIVD. De Koninklijke Marechaussee valt als onderdeel van de krijgsmacht onder het toezicht van de Inspecteur-Generaal voor de krijgsmacht. De vier bijzondere opsporingsdiensten vallen onder het toezichtsregime van het departement waartoe zij behoren en kennen dus geen vorm van extern toezicht. Geen van de genoemde toezichtorganen heeft voldoende mandaat om voor alle betrokken diensten na te gaan of de bevraging voldoet aan daaraan te stellen normen.

In dit kader heeft de adviescommissie een korte verkenning gemaakt van de bestaande situatie in enkele andere landen: Het Verenigd Koninkrijk, de Verenigde Staten, België, Duitsland, Frankrijk, Canada en Nieuw-Zeeland.

Het Verenigd Koninkrijk kent Commissioners die verantwoordelijk zijn voor het toezicht op de inlichtingen- en veiligheidsdiensten, de Interception of Communications Commissioner en de Intelligence Services Commissioner. Zij onderzoeken de wijze waarop de diensten hun bevoegdheden toepassen en onder meer of de bevragingen van externe databases en eventuele telefoontaps correct worden uitgevoerd en voldoen aan eisen van proportionaliteit en subsidiariteit. Als de Commissioner tot de conclusie komt dat een bevraging niet voldoet aan de daaraan te stellen eisen, ziet hij erop toe dat alle verkregen informatie wordt vernietigd en niet verder wordt gebruikt door de dienst die de bevraging heeft verricht. De Commissioners brengen jaarlijks verslag uit aan de minister-president, die deze verslagen voorlegt aan het parlement, in de vorm van een openbaar verslag en een vertrouwelijke bijlage met operationele details. Daarnaast bestaat er nog een Investigatory Powers Tribunal, waar iedereen kan klagen over de behandeling door de diensten of over de aantasting van hun privacy. Ook buitenlanders kunnen een klacht bij dit tribunaal indienen. Het tribunaal onderzoekt alle klachten en kan in voorkomende gevallen schadevergoeding toekennen. Van dat laatste is het overigens tot nu toe nog niet gekomen.[144]

In de VS bestaat sinds enkele jaren het Office of the Director of National Intelligence, dat verantwoordelijk is voor de aansturing van de inlichtingendiensten. Binnen dit bureau bestaat de functie van inspecteur-generaal als toezichthoudende functie. Deze interne toezichthouder houdt intern audits en onderzoeken naar de effectiviteit en doelmatigheid van de programma's en operaties van de organisaties die onder de Director of National Intelligence vallen. Hij is verantwoordelijk voor het onderzoek naar fraude, misbruik en verspilling. Ook doet hij onderzoek naar de prestaties van de verschillende organisatieonderdelen. Hij kan aanbevelingen doen ter verbetering van de effectiviteit en

142 Zie bijvoorbeeld de brochure "Wat kan uw bedrijf ondernemen tegen terrorisme, handreiking voor bedrijven", uitgave van de NCTb, november 2006.

143 Een pleidooi voor het beter betrekken van het bedrijfsleven bij terrorismebestrijding is ook gedaan door vertegenwoordigers van het Amerikaanse Department of Homeland Security op een door PWC in Den Haag georganiseerd symposium over veiligheid op 2 november 2006.

144 National Intelligence Machinery, uitgave van The Stationery Office, September 2006, zie ook www.intelligence.gov.uk

doelmatigheid van de Amerikaanse intelligence community. Hij heeft de bevoegdheid om onderzoek te doen naar het proces van gegevens inwinnen in externe databases. De functie van inspecteur-generaal komt op meer Amerikaanse departementen voor. Deze functionaris heeft een onafhankelijke positie en kan rechtstreeks aan het Congres rapporteren.[145]

België kent als vormen van onafhankelijk toezicht op de inlichtingendiensten een vast comité van toezicht en een Dienst Enquêtes. Duitsland kent de zogenaamde G10-Kommission, een onafhankelijke commissie van toezicht. Frankrijk kent de Commission Nationale du Controle des Interceptions de Sécurité (vooral voor het toezicht op het aftappen) en de Commission Nationale de l'Informatique et des Libertés. Deze laatste commissie ziet toe op de databases van de overheid. Daarbij ziet de commissie er op toe dat bij het beheer van deze databases de privacy van de burgers niet wordt geschonden. De databases van de inlichtingen- en veiligheidsdiensten vallen ook onder het toezicht van deze commissie. Canada kent een Security Intelligence Review Committee, een inspector general en een commissioner voor het toezicht op een inlichtingendienst van het ministerie van Defensie. Deze Inspector General heeft een meer algemene taak en gaat ondermeer na of de inlichtingendienst zich houdt aan het operationele beleid en of de activiteiten die daarvan worden afgeleid rechtmatig en doelmatig zijn. Ook Nieuw-Zeeland kent een Inspector General die onderzoek kan doen naar enig onderwerp dat betrekking heeft op het rechtmatig handelen van de inlichtingendiensten. Toetsing van besluiten inzake het aftappen van telefoons is een nadrukkelijk onderdeel van het takenpakket. [146]
Uit dit korte overzicht mag worden afgeleid dat een toezichthouder voor het toezicht op onderdelen van het proces van gegevens inwinnen in internationaal opzicht geen vreemde eend in de bijt is.

Privacy en veiligheid

Het College Bescherming Persoonsgegevens (CBP) wijst bij herhaling op het belang van een goede bescherming van de persoonlijke gegevens van de burgers. Volgens het CBP komen in het kader van veiligheid algemeen aanvaarde maatschappelijke principes in toenemende mate in gevaar, vooral door het steeds sterker groeiende gebruik van technologische hulpmiddelen. Zorgen heeft het CBP over ondermeer de opslag van telecommunicatiegegevens en de snelle toepassing van op repressie gerichte activiteiten. Het CBP concludeert: "Zorgen om terrorisme, onveiligheid en maatschappelijke misstanden bij burgers, bestuurders, politici en beleidsmakers hebben ertoe geleid dat de regels voor de bescherming van persoonsgegevens in het publieke debat als zondebok of als obstakel worden afgedaan." [147]

144 National Intelligence Machinery, uitgave van The Stationery Office, September 2006, zie ook www.intelligence.gov.uk
145 An Overview of the United States Intelligence Community, uitgave van The Office of the Director of National Intelligence, Washington, 2007
146 Clingendael Centrum voor Strategische Studies TNO, Democratische Controle Inlichtingen- en Veiligheidsdiensten, Den Haag, 2005
147 College Bescherming Persoonsgegevens, jaarverslag 2005, Den Haag, 2006, p. 23

Het CBP heeft bij tal van wetsontwerpen die de laatste jaren zijn ingediend om de bevoegdheden van inlichtingen- en opsporingsdiensten uit te breiden, kritische kanttekeningen geplaatst. De Europese organisatie van privacytoezichthouders heeft onlangs eveneens gewaarschuwd voor een afglijden van de huidige democratische rechtstaat naar een controlestaat waarin overmatige vormen van toezicht de persoonlijke vrijheden van de burgers teveel inperken. Toezicht is goed om onze veiligheid beter te garanderen en de samenleving soepeler te laten functioneren, maar een teveel aan toezicht belemmert de democratie in diezelfde samenleving, aldus een onderzoeksrapport waarop de Europese privacytoezichthouders zich baseren: *"Surveillance is two-sided, and its benefits must be acknowledged. Yet at the same time risks and dangers are always present in large-scale systems and of course power does corrupt or at least skews the vision of those who wield it."* [148]
De Europese toezichthouders hebben afgesproken om in onderlinge samenwerking te bezien of de traditionele methoden van toezicht gezien de nieuwe technieken nog voldoende effectief zijn en hoe zij eventueel moeten worden aangepast.

Niet alleen de toezichthouders maken zich zorgen over de toenemende inbreuken op de privacy van burgers. Ook in de wetenschappelijke wereld neemt de onrust toe over de groei in de bevoegdheden van inlichtingen- en opsporingsdiensten. Desondanks wordt de discussie in een te kleine kring gevoerd, zo wordt geconstateerd in een recente studie van het Rathenau Instituut in samenwerking met onderzoekers van de Universiteit van Tilburg. Privacy lijkt in de bredere discussie nauwelijks een rol te spelen. De onderzoekers schetsen een aantal trends, die noodzaken tot een verdieping en verbreding van de discussie: steeds vaker wordt onderzoek gedaan naar mensen op wie geen verdenking berust, in toenemende mate wordt een verkenning gedaan op basis van risicoprofielen op grond waarvan mogelijke verdachten in kaart worden gebracht, wettelijke beperkingen worden steeds vaker opgeheven en opsporingsdiensten krijgen meer mogelijkheden om eigenstandig onderzoek uit te voeren. Zij krijgen daarbij steeds meer de beschikking over persoonsgegevens die voor een ander doel zijn verzameld en tot slot worden andere partijen steeds vaker gedwongen tot medewerking.[149] Het merendeel van de geschetste ontwikkelingen wordt mogelijk gemaakt door databestanden: de toegang daartoe, de koppeling van bestanden en de toepassing van nieuwe technologieën om deze bestanden te doorzoeken. De auteurs wijzen erop dat het totaal aan maatregelen in toenemende mate een bedreiging vormt voor de privacy van de burgers, zonder dat zij goed kunnen overzien wat er op dit vlak allemaal gaande is: *"De optelsom van een reeks maatregelen kan, zeker op de lange termijn, grotere gevolgen hebben dan die maatregelen afzonderlijk doen vermoeden. Elke inbreuk op de privacy - gerechtvaardigd of niet - maakt elke volgende inbreuk gemakkelijker. Is één steen uit de muur gewrikt, dan is het eenvoudiger om een volgende los te halen."* [150] Daarom ook bepleiten de auteurs een verbreding van de discussie,

148 Surveillance Studies Network, A Report on the Surveillance Society, report for the Information Commissioner, London, 2006, p. 2
149 Vedder, Anton, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut, 2007; Studie 49, pp. 36-37
150 Idem, p. 65

vooral ook over het cumulatieve effect van alle maatregelen: elke maatregel op zich kan nodig of gewenst zijn, maar het totaal aan inbreuken zou wel eens een onaanvaardbaar resultaat tot gevolg kunnen hebben.

Ook hoogleraar Bart Jacobs, directeur van het Institute for Computing en Information Sciences van de Radboud Universiteit Nijmegen, maakt zich zorgen over de toenemende aantasting van de privacy door de ontwikkelingen op het gebied van criminaliteits- en terrorismebestrijding. Hij stelt dat de overheid de burgers steeds minder vertrouwt, haar Big Brother rol steeds nadrukkelijker invult en de burgers steeds meer in de breedte in de gaten houdt en controleert. Op het gebied van de opsporing van strafbare feiten ziet Jacobs een zorgwekkende revolutie. Vroeger werden eerst mogelijke verdachten geselecteerd en daarover werd informatie verzameld om op grond daarvan na te gaan wie de dader was. Tegenwoordig wordt volgens Jacobs eerst een grote hoeveelheid informatie over burgers verzameld en vervolgens wordt nagegaan of zich daarbinnen mogelijke verdachten bevinden. Op die manier wordt volgens hem teveel informatie over onschuldige burgers verzameld, waardoor het wettelijk evenwicht zoals dat wordt beoogd door de Wet Bescherming Persoonsgegevens uit het oog verloren: *"Vroeger waren de surveillancecapaciteiten beperkt en werden alleen diegenen in de gaten gehouden die eerst als verdachten gekenmerkt werden. Dat laatste gebeurde, in juridische termen, op basis van een redelijk vermoeden. Tegenwoordig kan iedereen in de gaten gehouden worden en hoeft surveillance niet meer om praktische redenen beperkt te worden tot verdachten."* [151]

Deze zorgen over privacy en de relatie tussen privacy en veiligheid brachten de Tilburgse hoogleraar Corien Prins tot de stelling, dat een nieuwe discussie nodig is over alle aspecten die samenhangen met de verschillende identiteiten die een individu kan hebben. De huidige wetgeving kent nauwelijks instrumenten voor transparantie, toetsing en controle van identiteiten. Voor Prins is de vraag relevant *"of het huidige wettelijke regime voor privacybescherming nog wel voldoende is geëquipeerd om burgers de noodzakelijke bescherming te bieden in een maatschappij waarin identificatie en 'identiteiten' centraal lijken te komen te staan."* [152]

Het evenwicht tussen veiligheid en privacy komt volgens steeds meer deskundigen en belanghebbenden in gevaar door de steeds grotere mogelijkheden voor inlichtingen- en opsporingsdiensten om toegang te krijgen tot externe gegevensbestanden. De sterke uitbreiding van bevoegdheden voor het veiligheidsdomein gaan niet gelijk op met versterking van de bescherming van de persoonlijke levenssfeer voor burgers op wie geen verdenking van criminaliteit of terrorisme berust. Op die manier ontstaat onbalans tussen privacy en veiligheid, aldus de hoofdlijn van de critici. Een Amerikaanse adviescommissie die onderzoek heeft gedaan naar privacybescherming in de strijd tegen terrorisme haalde

151 Jacobs, Prof. dr. B.P.F., De menselijke maat in ICT, webboek, te raadplegen op: http://www.cs.ru.nl/B.Jacobs, p. 92, zie ook p. 102
152 Prins, J.E.J., Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy, Justitiele Verkenningen, 2004, nr. 8, p. 45

in dit verband een uitspraak aan van Benjamin Franklin die waarschuwde tegen *"sacrificing essential liberty to purchase a little temporary safety,"* [153]

Volgens de adviescommissie kan er niet aan worden ontkomen dat in het belang van de veiligheid of de opsporing van terroristische of criminele activiteiten inbreuken op de privacy van burgers moeten worden gepleegd. Deze inbreuken hebben daartoe ook een wettelijke grondslag. Veel burgers accepteren deze inbreuken: cameratoezicht is een algemeen geaccepteerd verschijnsel geworden en uit veel onderzoeken blijkt steun voor privacybeperkende maatregelen in de strijd tegen terrorisme. Meer algemeen geven burgers vrijwillig informatie die in steeds meer databases wordt opgeslagen. Er is weinig publieke tegenstand tegen het vooraf verstrekken van gegevens door passagiers die per vliegtuig vertrekken naar de Verenigde Staten.

Desondanks wordt de vraag steeds pregnanter of de privacy van burgers in het huidige stelsel van gegevens inwinnen niet te zeer in het geding komt. Vroeger richten de inlichtingen- en opsporingsdiensten zich op verdachte personen, nu richten zij zich op hele groepen en gaan vervolgens na of daar mogelijk verdachte personen onder zouden kunnen zitten. Burgers kunnen ineens ergens van verdacht worden, niet omdat zij iets hebben gedaan, maar omdat zij passen in een bepaald profiel. De overheid wijst daarbij op het draagvlak dat er onder burgers bestaat voor deze inbreuken als dat leidt tot betere veiligheid. De vraag is of dan niet te gemakkelijk aan zorgen voor onnodige inbreuken op de privacy voorbij wordt gegaan.

De adviescommissie signaleert dat er in toenemende mate sprake is van een scherpe tegenstelling tussen privacy aan de ene kant en veiligheid aan de andere kant. De aanhangers van de privacywaarden vinden dat de overheid in het algemeen en het veiligheidsdomein in het bijzonder doorschieten in het aantasten van privacy op grond van veiligheidsoverwegingen. De overheid en het veiligheidsdomein daarentegen vinden dat de aanhangers van privacy overdrijven in hun klachten omdat de burgers inbreuken op de privacy graag over hebben voor veiligheid. In deze verscherping van de tegenstellingen wordt meer en meer de zakelijkheid en evenwicht in rederingen uit het oog verloren. Er dreigt een wederzijdse ridiculisering van standpunten.

Die groeiende tegenstelling is onnodig en zelfs contraproductief. Het gevaar is immers niet denkbeeldig dat het huidige draagvlak onder de burgers voor inbreuken op de privacy om veiligheidsredenen radicaal omslaat als bijvoorbeeld zou blijken dat deze inbreuken niet het gewenste effect heeft of als zou blijken dat een overheidsorganisatie of medewerkers misbruik maken van de verkregen gegevens. Het ligt naar de mening van de adviescommissie op de weg van de overheid om zich in te spannen voor een herstel van

153 Technology and Privacy Advisory Committee (TAPAC), Safeguarding Privacy in the Fight against Terrorism, Washington, March 2004, p. 61

evenwicht tussen privacy en veiligheid. Er heeft altijd een zekere mate van spanning bestaan tussen de waarden privacy en veiligheid en die spanning zal altijd blijven bestaan. Maar het is juist de taak van de overheid om te zorgen dat beide waarden met elkaar in evenwicht zijn. Een overheid die in toenemende mate het verwijt krijgt dat zij een van beide waarden uit het oog dreigt te verliezen, moet zich zorgen maken.

Daarbij mag niet uit het oog worden verloren dat technologische ontwikkelingen de privacy enerzijds in gevaar kunnen brengen, maar anderzijds ook weer kunnen beschermen door toepassing van daarop gerichte technieken. Technologie kan dus ook helpen om het evenwicht weer te herstellen. Deze dubbele functie van de technologie, de transparantie van netwerken, de anonimiteit van contacten via netwerken en het gebruik daarvan door criminelen voor ondermeer identiteitsfraude doen in toenemende mate de behoefte ontstaan aan een discussie over de vraag wat nu de beste verhouding is tussen privacy en veiligheid.[154] Wat de juiste balans ook is, die balans zal niet kunnen ontstaan zonder draagvlak onder de bevolking.

Binnenhalen van databases

Met name de inlichtingendiensten halen in toenemende mate externe databases binnen. Ook de politie maakt gebruik van deze werkwijze. Dat betekent dat men afspraken maakt met de eigenaar van externe databases om deze in kopie volledig over te hevelen naar het overheidsdomein. Regelmatig worden dan ook updates van het totale bestand geleverd om er voor te zorgen dat de dienst niet zoekt in verouderde gegevens. De AIVD heeft op dit vlak op grond van de WIV ruimere bevoegdheden dan de politie en maakt hier ook gebruik van. De dienst beschikt thans over 'tientallen' databases in eigen beheer. Met uiteenlopende organisaties in het private en publieke domein zijn hieromtrent afspraken gemaakt. De mogelijkheden terzake zullen binnenkort nog verder worden uitgebreid wanneer de bij de Tweede Kamer aanhangige wijziging van de WIV in het Staatsblad komt. Volgens het huidige voorstel kunnen organisaties worden verplicht geautomatiseerde gegevensbestanden af te staan aan de dienst.[155] Vooruitlopend hierop heeft de AIVD al contact gelegd met verschillende overheidsdiensten om gegevensbestanden af te staan. Dit geldt ondermeer voor uitvoerende diensten van Verkeer en Waterstaat en van Justitie. Ook heeft de AIVD enkele maanden geleden een brief aan de Raad van Hoofdcommissarissen gezonden met het verzoek aan alle korpsen om rechtstreekse, geautomatiseerde toegang te verkrijgen tot een aantal politiesystemen, in het bijzonder opsporingssystemen. De dienst wil deze toegang voor de uitvoering en ondersteuning van haar taken. De vertrekking van gegevens kan hetzij online hetzij door levering van het gehele bestand geschieden. Het verzoek van de AIVD is nog in behandeling bij de Raad van Hoofdcommissarissen, maar een aantal korpsen heeft al medewerking toegezegd.[156]

154 Zie bijvoorbeeld hierover: Marcus H. Sachs, P.E.: national security policy aspects of future computing capabilities, uitgave van SRI International, 6 november 2006
155 Kamerstuk 30 553
156 Brief van de AIVD aan de Board Opsporing van de Raad van Hoofdcommissarissen d.d. 21 december 2006, nr. 2741394/01

Een overheid die in toenemende mate het verwijt krijgt dat zij één van beide waarden uit het oog dreigt te verliezen, moet zich zorgen maken.

Als argument voor het binnenhalen van deze databases wordt aangegeven dat men deze databases uitgebreid wil onderzoeken. Men wil deze in eigen beheer kunnen koppelen met andere databases. Ook wil men daarop vormen van datamining toepassen.[157] Uit veiligheidsoverwegingen moet worden voorkomen dat de eigenaar van deze databases of medewerkers van dat bedrijf inzicht zouden kunnen krijgen in het zoekproces of in het object van onderzoek. Bevragingen van databases worden immers gelogd en zijn dus voor de beheerders van de gegevens te zien. Dit proces kan volgens de AIVD onvoldoende worden afgeschermd. De procedure van het binnenhalen van databases is nodig om de authenticiteit van gegevens te waarborgen, hetgeen vooral nodig is in het verkeer van de AIVD met andere, buitenlandse inlichtingendiensten. Men moet kunnen waarborgen dat de gegevens authentiek zijn en dat de geheimhouding is gewaarborgd. Tot slot wordt als argument aangevoerd, dat bevraging op locatie geen afdoende alternatief is omdat de verbinding tussen de database en de AIVD niet afdoende kan worden beveiligd.

Daar tegenover wordt door deskundigen op het gebied van beveiliging van ICT-toepassingen opgemerkt dat het binnenhalen van grote gegevensbestanden een valkuil is die uiteindelijk leidt tot een voor de veiligheidsdiensten onbeheersbare situatie. De argumentatie daarvoor is dat het in toenemende mate complexer wordt om dit groeiende aantal uiteenlopende databases die ook in omvang steeds verder toenemen te kunnen beheersen. Het is voor overheidsdiensten op termijn onmogelijk om deze databases tegen maatschappelijk aanvaardbare kosten te beheersen. Bestanden zijn bovendien moeilijk up te date te houden omdat allerlei informatie snel veroudert, met name de informatie die niet relevant is voor het primaire doel van de oorspronkelijke bestanden. Volgens deze deskundigen is het zeer goed mogelijk om zoekprocessen in de databases bij de eigenaar zelf uit te voeren op een zodanige wijze dat dit kan worden afgeschermd voor derden of voor gebruikers binnen die organisatie. Hiervoor kunnen duidelijke procedures en protocollen worden afgesproken. Andere deskundigen merken op hun beurt weer op dat dergelijke beveiligingsconstructies kunnen worden omzeild.

Het betreft hier dus een complex vraagstuk met diverse aspecten, waarover deskundigen kennelijk verschillend oordelen. De adviescommissie heeft hierover een rondetafelgesprek met enkele uiteenlopende deskundigen belegd om de verschillende stellingen nader te onderzoeken. De AIVD heeft geen medewerking aan dit gesprek willen verlenen.

In dit gesprek met wetenschappers en beveiligingsdeskundigen uit het bedrijfsleven hebben de experts verschillende kanttekeningen geplaatst bij een beleidslijn om gegevensbestanden naar binnen te halen:

- In de eerste plaats was men van mening dat het verzenden van informatie door gebruik van bestaande technologie zeer goed te beveiligen is.

157 Het hiervoor bedoelde wetsontwerp tot wijziging van de WIV geeft de inlichtingendiensten expliciet toestemming voor datamining.

- In de tweede plaats is het vanuit een oogpunt van beheersbaarheid belangrijk om een goed onderscheid te maken tussen soorten databases en het gebruik daarvan. Daarmee hangt samen de mate van beveiliging van een gegevensbestand en de versleuteling van de gegevens.
- In de derde plaats zijn databases ongelijk van structuur, technologische samenstelling, systematiek van beheer en van de wijze waarop de gegevens actueel worden gehouden. Het verzamelen van grote aantallen databases brengt daarom in toenemende mate grote beheersproblemen met zich mee.
- In de vierde plaats bestaan er alternatieve mogelijkheden van bevraging die voldoen aan de beveiligingseisen van de inlichtingendiensten en niet de beheersproblemen met zich brengen van het vergaren van vele verschillende databases. De alternatieve mogelijkheden hebben te maken met onder meer encryptie en bevraging van decentrale kopieën van databases in een afgesloten omgeving.

De adviescommissie heeft uit dit gesprek met de deskundigen de voorlopige conclusie getrokken dat er voor de inlichtingendiensten meer veilige opties open staan dan het binnenhalen van uiteindelijk onbeheersbaar veel gegevensbestanden. De adviescommissie hoopt in de tweede fase van haar onderzoek de discussie over dit onderwerp met de AIVD voort te kunnen zetten.

Informatie delen met openbaar bestuur

Het delen van informatie speelt ook tussen de inlichtingen- en veiligheidsdiensten en gezagsdragers in het openbaar bestuur. Verschillende burgemeesters hebben in de afgelopen jaren geklaagd over slechte informatievoorziening vanuit deze diensten. Dit gebeurde op basis van incidenten zoals een onderzoek naar de Hofstadgroep in Amsterdam, de inval van een arrestatieteam in Utrecht en de aanhouding van enkele vermeende terroristen in Den Haag. Mede naar aanleiding van deze incidenten heeft de minister van BZK een werkgroep ingesteld met als taak te onderzoeken of de gegevensverstrekking aan burgemeesters door landelijke diensten verbeterd moet worden. De werkgroep concludeerde dat er niet zozeer behoefte was aan nieuwe regelgeving dan aan verandering van de cultuur: *“Een wijziging van de thans bestaande bestuurscultuur zal moeten bijdragen aan een verbetering in de samenwerking tussen betrokkenen.”* [158] De werkgroep is op dit moment doende na te gaan of er inmiddels sprake is van verbetering in de cultuur en van een grotere wil tot onderlinge samenwerking en vertrouwen. De adviescommissie verwijst ter zake naar het komende verslag van deze werkgroep.

De dataretentie

Een zorgpunt voor de adviescommissie is de wijze waarop de rijksoverheid omgaat met de problematiek van de dataretentie. Het betreft hier de uitvoering van de Europese

158 Werkgroep gegevensverstrekking lokaal bestuur “Werkgroep-Holtslag”, Vaste Verbindingen, rapportage aan de minister van BZK, Den Haag, 2005, p. 14 Het standpunt van de minister naar aanleiding van dit rapport is opgenomen in: Kamerstuk 29 876, nr. 9 inzake de gegevensverstrekking door landelijke diensten aan het lokaal bestuur

richtlijn met betrekking tot de opslag van persoons- en verkeersgegevens op het gebied van telefonie en internet. [159] Deze richtlijn moet op 1 september 2007 zijn vertaald in Nederlandse wetgeving. Daarbij zal nog een beslissing moeten worden genomen over de wijze waarop deze gegevens zullen worden opgeslagen. Over die vraag dreigt een heftige strijd te ontbranden tussen de overheid en de betrokken bedrijven. Daarbij gaat het om de vraag of de gegevens zullen worden opgeslagen bij de bedrijven of bij de overheid en bovenal wie voor de kosten van deze opslag opdraait. Volgens onderzoek kan het om bedragen gaan van meer dan € 100 miljoen per jaar. Het conceptwetsontwerp voor de invoering van de dataretentie in Nederland heeft scherpe kritiek van het betrokken bedrijfsleven opgeroepen. Deze kritiek is niet alleen ontstaan vanwege de problematiek van de kostenverdeling, maar ook vanwege belangrijke onderdelen die niet in het wetsontwerp zijn geregeld en worden overgelaten aan nadere regelgeving. Daar zitten zaken bij die van groot belang zijn voor zowel de opsporing als voor de bedrijfsvoering van de providers. Zaken die nog niet zijn geregeld, betreffen ondermeer de wijze van aanlevering (batch of real time), de termijn van de beantwoording en de mate waarin de uitvoering van de richtlijn de huishouding van de providers zou kunnen verstoren. In het verlengde daarvan merken de providers op dat de technologische ontwikkelingen op het gebied van telefonie zo snel gaan dat het risico niet denkbeeldig is dat bestaande verplichtingen op het gebied van dataretentie snel zullen worden achterhaald door de technologische actualiteit.

De richtlijn heeft overigens ook ernstige kritiek gekregen van organisaties op het gebied van privacybescherming. Peter Hustinx, de European Data Protection Supervisor, noemde de richtlijn *"far to weak on essential safeguards."* [160] Ook het Nederlandse College Bescherming Persoonsgegevens heeft in een recent advies op hoofdpunten kritiek op het concept ontwerp uitgesproken. [161] De Leidse hoogleraar en CDA-senator Hans Franken heeft onlangs namens zijn fractie eveneens bezwaren tegen het wetsontwerp aangetekend: *"De voordelen ervan wegen niet op tegen de enorme inbreuk op de privacy. Het middel is te zwaar voor de resultaten die het oplevert. En de consument draagt de kosten. Bovendien kan je met verkeersgegevens profielen opstellen van het gedrag van mensen, waarmee sprake is van inbreuk op de persoonlijke levenssfeer."* [162] Niet uit het oog mag daarbij worden verloren dat ook de Tweede Kamer heeft aangegeven niet enthousiast te zijn over de voornemens met betrekking tot dataretentie.[163]

159 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.

160 Peter J. Hustinx, Human rights and public security: change for a compromise, or continuity of safeguards?, Conference on Public Security and Data Protection, Warsaw, 11 May 2006

161 College bescherming persoonsgegevens (CBP): Advies inzake het Wetsontwerp implementatie Europese Richtlijn Dataretentie, advies d.d. 22 januari 2007

162 Middel is te zwaar voor wat het oplevert, NRC Handelsblad, 23 januari 2007

163 Motie-Dittrich, zie noot 86

Het dataretentieprobleem beperkt zich overigens niet tot de aanbieders van telecomdiensten, maar geldt ook voor de zoekdiensten op Internet. Zoekmachines als Google, Yahoo en Microsoft bewaren ook gegevens over het zoekgedrag van surfers op Internet. Deze gegevens worden bewaard voor eigen gebruik, maar worden ook ter beschikking gesteld aan opsporingsinstanties. Google laat zich hierbij leiden door de wetgeving van het betrokken land: in China worden gegevens verstrekt volgens de Chinese wetten en in Nederland volgens de Nederlandse wetten. Google zegt de gegevens voor drie doeleinden te bewaren: verbeteren van de service aan de gebruikers en het bestrijden van fraude, aanbrengen van voorzieningen voor privacybescherming en in de derde plaats om te voldoen aan de wettelijke regels ten aanzien van dataretentie.[164] Veel privacybeschermers vinden de mededeling van Google een stap in de goede richting, maar volgens anderen horen bedrijven als Google deze gegevens in het geheel niet te bewaren.[165]

Tegen de achtergrond van de eerder geschetste verhoudingen tussen de overheid en de sector van de telecom en tegen de achtergrond van de groeiende tegenstellingen tussen privacy en veiligheid is de kans groot dat de parlementaire besluitvorming over de uitvoering van de Europese richtlijn niet eenvoudig zal zijn. Onverkorte handhaving van het voorliggende wetsontwerp zal spanningen oproepen. Het onderwerp verdient dan ook beduidend meer bestuurlijke aandacht dan het nu krijgt. Mogelijk zal de Raad van State die zich thans over het wetsontwerp buigt die bestuurlijke aandacht geven.

3.5 Tot slot: dit hoofdstuk in het kort

Een belangrijke observatie is dat de partijen in het veiligheidsdomein geen gemeenschappelijke visie hebben op het belang van databanken voor de ontwikkeling van informatie en intelligence. Hoewel alle betrokken partijen het belang van informatie onderkennen, geven zij onvoldoende aandacht aan een van de belangrijkste basiselementen voor informatie en intelligence: de groeiende hoeveelheid gegevens die in steeds meer gegevensbestanden ligt opgesloten. En dus hebben zij ook geen op die visie gebaseerde strategie ten aanzien van het benaderen van deze bestanden, het inwinnen van gegevens en het benutten van deze gegevens.

Hiermee hangt samen dat de partijen in het veiligheidsdomein ondanks pogingen tot verbetering te weinig samenwerken met elkaar op het gebied van inwinnen, gebruiken en delen van gegevens uit deze databases. Dat maakt het proces suboptimaal. Dat blijkt ook uit het feit dat het vrijwel onmogelijk is om goed zicht te krijgen op het aantal bevragingen en taps op telefoons en internet. Gegevens vragende partijen houden dit niet bij of verstrekken de gegevens niet. Bij afwezigheid van dit inzicht kan de leiding van de betrokken organisaties ook niet sturen op effectiviteit of doelmatigheid van de bevragingen.

164 Google Log retention Policy FAQ, 14 maart 2007: http://216.239.57.110/blog_resources/google_log_retention_policy_faq.pdf

165 Zie bijvoorbeeld: CNet, Google adding search privacy protections, http://news.com.com/Google+adding+search+privacy+protections/2100-1038_3-6167333.html?tag=nefd.lede

Bij het inwinnen van gegevens uit deze bestanden willen inlichtingen- en opsporingsdienten gebruik makan van nieuwe technologieën zoals datamining. Ook op dit vlak kan veel beter worden samengewerkt. Hier is sprake van een situatie dat elke partij zijn eigen wiel uitvindt. Bij het delen van informatie werken partijen eveneens te weinig met elkaar samen. Hoewel representanten van het veiligheidsdomein claimen dat er zeker sprake is van een opgaande lijn, zijn successen van samenwerking op dit terrein onvoldoende bekend. De adviescommissie is van mening dat op het gebied van samenwerking bij het inwinnen, gebruiken en delen van informatie meer politieke en bestuurlijke sturing noodzakelijk is.
Leveranciers van informatie signaleren drie categorieën van knelpunten.

- In de eerste plaats zijn zij van mening, dat het aantal bevragingen te sterk toeneemt, terwijl de vergoeding van kosten die de bedrijven daarvoor moeten maken onvoldoende door de overheid worden vergoed.
- In de tweede plaats ervaren zij het proces van gegevens verstrekken als een eenrichtingsverkeer: zij krijgen van de overheid niets terug voor hun inspanningen, in die zin dat de overheid onvoldoende duidelijk maakt wat zij heeft gedaan met de verkregen inlichtingen. Met andere woorden: hebben de inspanningen van de leveranciers op hoofdlijnen geleid tot successen op het gebied van opsporing of voorkoming van criminele of terroristische activiteiten.
- In de derde plaats zijn zij van mening, dat de overheid het bedrijfsleven veel meer en beter kan betrekken bij het bestrijden van criminaliteit en terrorisme. Zij beschikken immers over kennis en vaardigheden die de overheid niet heeft.

In het proces van gegevens inwinnen kunnen ook enkele knelpunten worden onderkend. Een belangrijk knelpunt is de groeiende onbalans in de verhouding tussen privacy en veiligheid. Er beginnen hier twee kampen te ontstaan die onvoldoende begrip hebben voor de argumenten van de andere partij. Voor de overheid zijn zowel privacy als veiligheid belangrijke waarden. Daarom moet de overheid ook zorgen voor een goede balans tussen beide waarden. Organisaties en deskundigen op het gebied van privacy krijgen steeds meer het gevoel dat de overheid de balans uit het oog verliest.

Enkele andere knelpunten in het proces die nadere aandacht verdienen zijn het feitelijk binnenhalen van tientallen externe databases door inlichtingendiensten. Bij nut en noodzaak van dit beleid worden door beveiligingsdeskundigen vraagtekens gezet.
Een ander knelpunt waar de adviescommissie op is gewezen is de informatievoorziening door de inlichtingendiensten aan de gezagsdragers in het openbaar bestuur. Een werkgroep van het ministerie van BZK doet hiernaar nader onderzoek. Tot slot is de uitvoering van de Europese richtlijn met betrekking tot de dataretentie (het bewaren van verkeersgegevens met betrekking tot telefonie en internet) aangemerkt als een knelpunt. Zorgpunt voor de adviescommissie is of de overheid wel voldoende aandacht heeft voor de vele bezwaren die leven bij deskundigen, privacyorganisaties en in de politiek.

Op grond van het bovenstaande trekt de adviescommissie de volgende conclusies:

1. De partijen in het veiligheidsdomein hebben geen gemeenschappelijke visie op het belang van externe gegevensbanken voor de ontwikkeling van informatie en intelligence.
2. De partijen in het veiligheidsdomein werken onvoldoende met elkaar samen bij het inwinnen, delen en analyseren van gegevens uit externe gegevensbanken en bij het zoeken naar toepassingsmogelijkheden van nieuwe technieken.
3. De overheid heeft onvoldoende aandacht voor de zorgpunten die leveranciers van gegevens hebben ten aanzien van het aantal bevragingen en de groei daarin, de vergoeding van de daarvoor te maken kosten en over de terugkoppeling van de met de geleverde gegevens behaalde resultaten.
4. Het risico dat een onbalans tussen privacy en veiligheid ontstaat wordt door de overheid onvoldoende onder ogen gezien.
5. Nut en noodzaak van het fysiek binnenhalen van aantallen databases ten behoeve van het veiligheidsdomein verdienen nader onderzoek.
6. In de discussies over de vertaling van de Europese richtlijn inzake dataretentie in Nederlandse wetgeving toont de rijksoverheid weinig oog voor bezwaren tegen die wetgeving.

4

4.1 Inleiding

Hoewel het inwinnen van informatie uit grote externe databases een sterk technologisch aspect heeft, is er geen sprake van een automatiseringsprobleem. Het enige vraagstuk met technologische aspecten dat de adviescommissie is tegengekomen, heeft betrekking op het binnenhalen van externe databases door inlichtingen- of opsporingsdiensten. De adviescommissie bepleit op dit punt nader onderzoek.

De conclusies die de adviescommissie wel heeft getrokken liggen op strategisch, organisatorisch, financieel en cultureel gebied. Strategisch omdat de samenwerking op het strategische niveau onvoldoende is, organisatorisch omdat het proces op deelniveau is ingericht, financieel omdat er een dispuut over kostenvergoedingen loopt dat een bedreiging vormt voor de informatieverstrekking en de juistheid daarvan, en cultureel omdat samenwerken en delen van informatie allerminst behoren tot de cultuur van de betrokken organisaties en de mensen die daarin werkzaam zijn.

4.2 Een veelheid aan systematieken

De adviescommissie heeft tot opdracht gekregen onderzoek te doen naar 'de systematiek' van informatiestromen uit geautomatiseerde gegevensbestanden naar het veiligheidsdomein. Uit de analyse van de adviescommissie is gebleken dat er geen sprake is van een systematiek, wel van systematieken. Elke organisatie kent zijn eigen systematiek en werkwijze. Onderlinge afstemming vindt zelden plaats en als het al plaats vindt is het afstemming over operationele zaken. De organisaties hebben geen gezamenlijke visie of strategie ten aanzien van het belang van externe gegevensbestanden, de manier waarop deze bestanden benaderd moeten worden en hoe moet worden omgegaan met de gegevens die uit deze bestanden worden verkregen. Dit heeft tot gevolg dat er geen duidelijk beeld kan zijn over relevante onderdelen van het proces van inwinnen van gegevens: het aantal bevragingen, de groei daarin, de toepasselijke wetgeving, de wijze waarop de wetgeving wordt uitgevoerd en geïnterpreteerd, de wijze waarop de gegevens worden ingewonnen en de professionaliteit waarmee dit proces is ingericht. Het ontbreekt op dit terrein aan een helder systeem van governance en toezicht.

De adviescommissie heeft niet kunnen constateren dat er vanuit de beleidsdepartementen veel aandrang bestaat om verandering in deze situatie aan te brengen.

De adviescommissie heeft vervolgens nagegaan of deze verzamelde systematieken voldoen aan daaraan te stellen normen. Zij heeft deze vraag niet bevestigend kunnen beantwoorden. Het totaal aan deelssystemen dat wordt gehanteerd voldoet niet aan de

daaraan te stellen normen inzake vormvereisten en van maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid. Deze conclusie zal in de volgende paragrafen aan de hand van deze normen nader worden toegelicht.

4.3 Grondslag en vormvereisten

Allereerst valt op dat het niet mogelijk is gebleken om een goed inzicht te verkrijgen in alle voor het bevragen van externe gegevensverzamelingen relevante wetgeving. Een overzicht bestaat niet. Het is opvallend dat niemand in staat is gebleken de adviescommissie te voorzien van een overzicht van wetten die van toepassing zijn op de bedoelde systematiek van gegevens inwinnen, met aan de ene kant de bevoegdheden en verplichtingen van inlichtingen- en opsporingsdiensten en aan de andere kant de bevoegdheden en verplichtingen van verstrekkers van gegevens. Zeker in het licht van de sterke groei van de bevoegdheden van de inlichtingen- en opsporingsdiensten tegenover de groei van de verplichtingen van de leveranciers van gegevens, heeft de adviescommissie daarom begrip voor critici die beweren dat er in toenemende sprake is van onbalans. Door het ontbreken van dit overzicht ontneemt de overheid zichzelf immers een goede mogelijkheid om op basis van feiten weerwoord te geven aan deze critici.

Door het ontbreken van het inzicht in het juridisch kader is er ook geen inzicht in de vormvereisten die aan de bevraging worden gesteld. Daarmee wordt ook onduidelijk in hoeverre inlichtingen- en opsporingsdiensten zich aan die vormvereisten houden. Het is gebleken dat hier van eenduidigheid geen sprake is. Soms worden deze vormvereisten bepaald door de leverende partij (zoals bij de Belastingdienst) en soms hangt het van toevalligheden af of betrokken partijen zich houden aan de vormvereisten. Een van de telecomproviders waarmee de adviescommissie heeft gesproken, gaf aan dat dit bedrijf gemiddeld een keer per week wordt gebeld door een opsporingsdienst met een verzoek om gegevens zonder een daartoe noodzakelijke last van de officier van justitie. Omdat de FIOD-ECD gemakkelijker toegang heeft tot de bestanden van de Belastingdienst, komt het voor dat deze dienst gevraagd wordt om een vertegenwoordiger af te vaardigen in onderzoekteams van andere diensten zodat gemakkelijker aan fiscale gegevens kan worden gekomen. Aangezien vrijwel altijd de bevraging van externe databases verloopt via een menselijke interface, is onduidelijk in hoeverre de vormvereisten altijd worden gevolgd. Het toezicht op de bevragingen is derhalve in de praktijk gebrekkig.

In het verlengde hiervan ligt de afscherming van het proces van bevraging voor onbevoegden. Deze afscherming kan niet altijd worden verzekerd. Voor een deel komt dit door de menselijke interface. Niemand kan garanderen dat de contactpersonen bij de leverende diensten geen informatie aan derden verschaffen. Een ander risico voor de bevraging ligt in onzorgvuldigheid aan de kant van de informatie vragende partijen. Het blijkt voor te komen dat informatievragen met de daarbij behorende lastgeving van de officier van justitie via een publieke fax worden verzonden.

Het toezicht op de bevragingen is in de praktijk gebrekkig.

4.4 Maatschappelijke zorgvuldigheid

Om te voldoen aan de eisen van maatschappelijke zorgvuldigheid moet het stelsel van gegevens inwinnen voldoen aan eisen ten aanzien van proportionaliteit en subsidiariteit en moet er afdoende verantwoording worden afgelegd. Daarbij is bepalend of er sprake is van een helder en evenwichtig beleid ten aanzien van het bevragingsproces. Ook is hierbij van belang in hoeverre de informatie vragende partijen rekening houden met de positie van de partijen die geacht worden gegevens te verstrekken.

Beleidsvragen

De groei van databases roept in toenemende mate een aantal beleidsvragen op, waar de overheid nog een antwoord op moet geven. Veiligheid van de burgers is daarbij een kernbegrip. Die veiligheid kan op vele manieren in gevaar worden gebracht.

- In de eerste plaats door fouten in de opslag van gegevens. Elke beheerder van gegevensbestanden heeft een bijzondere verantwoordelijkheid voor de juistheid van deze gegevens. Die verantwoordelijkheid wordt niet altijd waargemaakt, sterker nog: zelfs het meest primaire overheidsbestand, de gemeentelijke bevolkingsadministratie, bevat veel onvolkomenheden. Naarmate het belang van gegevensbestanden toeneemt, wordt het dus ook steeds belangrijker dat deze bestanden, en zeker de overheidsbestanden, juiste gegevens bevatten.
- In de tweede plaats wordt de veiligheid van de burger in gevaar gebracht door mogelijke inbreuken van buiten op deze bestanden. Dat de overheid op dit vlak vaak niet afdoende bewust is van de risico's op dit vlak is in meerdere rapporten van de Algemene Rekenkamer gebleken.[166] Uit recent Amerikaans onderzoek is gebleken dat vorig jaar bij alle onderzochte federale departementen of agencies vertrouwelijke persoonsgegevens zijn verdwenen. Steeds vaker zijn criminele organisaties er op uit om deze gegevens te pakken te krijgen en ze vervolgens te gebruiken voor vele vormen van fraude. Eerder in dit rapport is aangegeven dat dit de snelst groeiende vorm van criminaliteit in de Verenigde Staten is. Vergelijkbare cijfers voor Nederland ontbreken, maar zouden voor een goed beeld van de beveiliging van persoonsgegevens door de Nederlandse overheid wel beschikbaar moeten komen.
- Een derde risico wordt gevormd door het gebruik van de gegevensbestanden: welke gegevens mogen er in en wie mogen er gebruik van maken. Met name het College Bescherming Persoonsgegevens is op dit punt alert, maar constateert dat de grenzen voor toegang onder het mom van veiligheid worden opgerekt. Dat heeft als onbedoelde consequentie dat binnen organisaties de discipline ten aanzien van beheer en toegang verslapt.
- Het vierde risico wordt gevormd door de toepassing van moderne technieken zoals bijvoorbeeld datamining. Deze technieken zijn nog in ontwikkeling en een ongeclausuleerde toepassing daarvan kan ongewenste gevolgen hebben. Een publiek debat over voor- en nadelen van toepassing van datamining in Nederland heeft tot nog toe niet plaats gevonden, maar wel zijn alle partijen inmiddels in enigerlei vorm begonnen met het toepassen daarvan.
- Een vijfde risico is dat de overheid door onvoldoende aandacht voor het onderwerp van de gegevensbestanden, bestaande of nieuwe databases over het hoofd ziet en dus ook geen acht kan slaan op mogelijkheden of beperkingen van deze onbekende databases.

Veiligheid en privacy zijn daarbij sleutelbegrippen. Het evenwicht tussen die twee begrippen staat van nature onder spanning. Maar in toenemende mate dreigt deze spanning te groot te worden en dreigt een onbalans te ontstaan tussen privacy en veiligheid, allebei kernwaarden die door de overheid gewaarborgd moeten worden. Deze kernwaarden moeten met elkaar in balans zijn en het is een taak van de overheid om te zorgen voor die balans. Afwezigheid van die balans heeft het risico in zich dat op termijn het draagvlak bij de burgers voor het veiligheidsbeleid zal verdwijnen als dat teveel inbreuk maakt op de privacy van de burger. Een veiligheidsbeleid zonder draagvlak bij de burgers is gedoemd te mislukken. De overheid lijkt op dit moment teveel uit te gaan van het huidige vertrouwen en te weinig oog te hebben voor de dreigende onbalans.

Maatschappelijke verantwoording

Het is moeilijk om goed zicht te krijgen op de vraag of het systeem van gegevens inwinnen voldoet aan de eisen van proportionaliteit en subsidiariteit. Dat wordt veroorzaakt doordat daarvoor noodzakelijke gegevens onvoldoende worden bijgehouden of beschikbaar worden gesteld. Uit de gegevens die wel beschikbaar zijn, blijkt dat het aantal bevragingen in de afgelopen jaren een grote vlucht heeft genomen.

Het is in dit verband zorgelijk dat er zo slecht wordt bijgehouden hoe vaak er gebruik wordt gemaakt van rechtsmiddelen die een sterke inbreuk zijn op de privacy van burgers, zoals het aftappen van telecommunicatie. Dit middel is zozeer door procedures van zorgvuldigheid omgeven, dat een bijhouden van het aantal taps een logisch onderdeel van de procedure behoort te zijn. Telecombedrijven zijn door de overheid verplicht om geen mededelingen te doen over het aantal taps.[167] Dat de gegevens hierover door de AIVD niet worden verstrekt om redenen van staatsveiligheid, is voor de adviescommissie geen overtuigend argument. Het moet immers mogelijk zijn een maatschappelijke discussie te voeren over totale aantallen en over de mate waarin deze aantallen groeien (of afnemen).

Uit het feit dat er onvoldoende inzicht bestaat in de mate waarin externe databases worden bevraagd, moet de conclusie worden getrokken dat de overheid daarom geen goed beeld kan hebben van proportionaliteit en subsidiariteit. In ieder geval wordt het

166 Zie voor een recente rapportage: Kamerstuk 30 505, Grip op informatievoorziening, IT Governance bij ministeries, maart 2006

167 Besluit van 28 oktober 2003, houdende regels betreffende door aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten te treffen beveiligingsmaatregelen ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie (Besluit beveiliging gegevens aftappen telecommunicatie), art. 6

onmogelijk gemaakt om over die punten een publieke discussie te voeren. Er bestaat dus geen sluitend systeem van maatschappelijke verantwoording.

De informatie leverende partijen

Met leveranciers van informatie en andere relevante partijen in het private en publieke domein kan meer en beter informatie worden gedeeld. Er is over het algemeen te weinig begrip voor de begrijpelijke vraag van derde partijen om meer informatie en over terugkoppeling over de waarde die gegeven informatie heeft gehad voor het proces van opsporing. Natuurlijk kan niet alle informatie worden verstrekt, daarover bestaat geen misverstand, maar nu is er sprake van het andere uiterste. De overheersende mening in het veiligheidsdomein is dat de leveranciers van informatie 'gewoon' hun wettelijke verplichtingen moeten nakomen en de gevraagde gegevens moeten leveren en verder niet zeuren. Een dergelijke houding gaat voorbij aan gerechtvaardigde vragen en zorgen van andere partijen, maar vooral ook aan de gezamenlijke verantwoordelijkheid van overheid en markt en civil society voor veiligheid. Leveranciers van gegevens kunnen belangrijke bijdragen daaraan leveren.

Er loopt al geruime tijd een discussie over de vergoeding van de kosten die het bedrijfsleven moet maken voor het aanleveren van gegevens. Deze discussie loopt vooral met banken, telecomproviders en internetproviders. Dit al jaren slepende proces verziekt de sfeer en draagt er aan bij dat het bedrijfsleven steeds minder geneigd is om gevraagd of ongevraagd informatie te leveren. Ook neemt de bereidheid af om de overheid te informeren over nieuwe ontwikkelingen die van invloed kunnen zijn op het proces van gegevens inwinnen.

De rijksoverheid geeft te weinig blijk van het besef dat het een inhoudelijk belang heeft bij een coöperatieve houding van het bedrijfsleven. De opstelling van de overheid lijkt vooral ingegeven door financiële overwegingen. Het kabinet gaat een inhoudelijk debat uit de weg. Een voorbeeld daarvan geeft het kabinet in een reactie op de Raad van State, die in haar advies op de aanhangige wijziging van de WIV aandrong op volledige kostenvergoeding bij het verstrekken van informatie. In zijn reactie geeft het kabinet weliswaar aan, dat als uitgangspunt geldt een vergoeding van de daadwerkelijke kosten. Maar als vervolgens wordt aangegeven dat dit inhoudt dat alleen de personeels- en administratiekosten worden vergoed, gaat het kabinet voorbij aan de inhoudelijke discussie over dit onderwerp.[168] Daarmee wordt onrecht gedaan aan de achterliggende problematiek en aan de toenemende bezwaren bij het bedrijfsleven tegen de hoogte van de vergoeding. Teveel neemt de overheid de houding aan, dat de verplichting tot levering van informatie berust op de wet en dat bedrijven dus moeten leveren. Dat is een miskenning van het probleem. De bestaande bezwaren leiden bij sommige marktpartijen tot evidente vormen van tegenwerking en obstructie. Tegenwerking is daarmee een impliciet veiligheidsrisico. De inlichtingen- en opsporingsdiensten krijgen mogelijk niet de goede informatie, of zij krijgen vervuilde informatie of niet nuttige hulp bij het zoeken naar de goede informatie.

De adviescommissie heeft er begrip voor dat de overheid op tal van terreinen de hulp van marktpartijen inroept bij het uitvoeren van haar taken. Dat gebeurt op tal van gebieden, niet alleen het veiligheidsdomein. Het betreft hier voornamelijk de zogenaamde herendiensten die van het bedrijfsleven worden gevraagd. In het kader van het terugdringen van de administratieve lasten wordt alom geprobeerd deze kosten terug te dringen. Op het veiligheidsdomein wordt deze meer algemene discussie overheerst door de problematiek van de vergoeding van de kosten die het bedrijfsleven moet maken voor de levering van gegevens aan het veiligheidsdomein. In plaats van terugdringen van deze kosten, is veeleer sprake van toename daarvan.

De overheid voert op dit punt geen heldere lijn. Enerzijds accepteert zij wel dat de betrokken partijen recht hebben op een vergoeding, maar zij laat anderzijds onduidelijkheid bestaan over het soort kosten dat wordt vergoed en over de hoogte van de vergoeding. Er zijn twee belangrijke overwegingen die hierbij naar het oordeel van de adviescommissie een rol spelen. In de eerste plaats is de overheid gehouden om er voor te zorgen dat de bevraging doelmatig plaats vindt en niet meer vraagt van de gegevens leverende partijen dan redelijkerwijs van hen mag worden gevraagd. In de tweede plaats moet de overheid ervoor waken dat de lasten van de bevraging niet bij een onevenredig kleine groep terecht komen. De rechter heeft naar het gevoelen van de adviescommissie een belangrijke vingerwijzing gegeven voor een oplossing van het nu bestaande probleem.[169] Hij heeft in een recente uitspraak over de problematiek van de vergoedingen gesteld dat het toebrengen van onevenredige schade door de Staat op dit punt moet worden aangemerkt als een onrechtmatige daad. De adviescommies verwacht dat de twee genoemde overwegingen voor beide partijen een voldoende leidraad kunnen zijn om het inmiddels al veel te lang slepende conflict tot een oplossing te brengen.

4.5 Effectiviteit

De samenwerking tussen de partijen in het veiligheidsdomein blijft op het punt van data, informatie en intelligence veelal beperkt tot samenwerking op zaaksniveau en heeft daarom veelal een operationeel karakter. Er bestaat geen gemeenschappelijke strategische visie ten aanzien van deze onderwerpen. Dit gebrek aan een strategische visie ten aanzien van data en gegevensbestanden en hun belang voor informatie en intelligence geldt voor de partijen die het veiligheidsbeleid moeten uitvoeren, inlichtingen- en opsporingsdiensten, ieder voor zich en allen in gezamenlijkheid. Er vindt over dit strategische onderwerp ook geen onderling overleg plaats. Natuurlijk wordt het belang van informatie en

168 Kamerstuk 30 553, nr. 4, Advies Raad van State en Nader Rapport, p. 5

169 Zie ook paragraaf 3.3 en in het bijzonder noot 130

intelligence erkend, wat mist is de rol van data en gegevensbestanden hierbij en met name de beleidsmatige vragen die deze bestanden oproepen, zoals op het gebied van de privacybescherming en gegevensbescherming. De adviescommissie heeft niet kunnen nagegaan of deze visie op de betrokken departementen wel bestaat. Zij heeft alleen geconstateerd dat op dit onderwerp vanuit de departementen geen sturing plaats vindt.

Geautomatiseerde gegevensbestanden zijn in de afgelopen 10 tot 20 jaar in belang voor het veiligheidsdomein enorm toegenomen. Binnen dat domein bestaat geen breed gedragen beeld over de omvang en de gevolgen van deze groei, over de complexiteit van gegevensbestanden en evenmin over de grenzen die deze complexiteit oproept voor het gebruik. In alle recente strategische documenten van inlichtingen- en opsporingsdiensten staat het belang van informatie en intelligence voorop. De rol die de geautomatiseerde gegevensbestanden daarbij spelen, blijft buiten beschouwing. Dat is des te opvallender omdat deze bestanden in feite het enige onderdeel van het informatieproces vormen dat in de afgelopen jaren daadwerkelijk is veranderd. Omvang, complexiteit en inhoudelijke betekenis van deze bestanden zullen in de komende jaren nog verder toenemen. Dit vraagt om een heldere strategische visie van de overheid hoe met deze gegevensbestanden moet worden omgegaan en in hoeverre die gegevensbestanden gebruikt kunnen en mogen worden voor het veiligheidsdomein.

Door het ontbreken van deze gemeenschappelijke strategische visie op het belang van de gegevensbestanden kunnen de diensten ook niet ten volle effectief gebruik maken van deze bestanden. Vooral door een betere samenwerking bij de ontwikkeling van deze visie kan de effectiviteit van het proces worden vergroot.

Ook op andere onderdelen van het proces van gegevens inwinnen uit externe gegevensbestanden wordt te weinig samengewerkt. Dit geldt vooral voor het delen van gegevens. Er bestaat in het veiligheidsdomein een breed probleem ten aanzien van het delen van informatie. Dit geldt voor het delen van informatie tussen inlichtingen- en opsporingsdiensten, maar ook voor het delen van informatie binnen de opsporingsdiensten en binnen politiekorpsen. Ondanks alle pogingen om verbetering aan te brengen, moet toch worden geconcludeerd dat het delen van informatie kennelijk een bijzonder moeizaam proces is dat zeker niet vanzelf verloopt. Dienstleidingen van betrokken organisaties stellen dat er op dit vlak in de afgelopen jaren veel is verbeterd, maar op de niveaus waarop dit delen van informatie daadwerkelijk moet gebeuren, blijkt elke dag weer dat de praktijk weerbarstig is. Bij veel van de daar werkzame medewerkers leeft niet het gevoel dat delen van informatie noodzakelijk is. Zij zijn opgeleid in de cultuur dat informatie macht is en dus zo weinig mogelijk moet worden gedeeld. Een tweede cultuurelement wordt bepaald door het principe ‘need to know’. Met andere woorden: degene die beschikt over de informatie, bepaalt wie de informatie nodig heeft. Dat is een heel ander principe dan het principe ‘need to share’: degene die over de informatie beschikt,

moet actief nadenken met wie hij de informatie moet delen.[170] De oude cultuur bestaat nog op veel plaatsen, omdat dit altijd de overheersende leidraad voor het werken is geweest, een cultuur waar veel mensen in de wereld van de inlichtingen en opsporingen in zijn opgevoed.

Delen van informatie gaat overigens uit van eigendom van informatie. Dat is een merkwaardige veronderstelling binnen landsgrenzen waar alle inlichtingen- en opsporingsdiensten uiteindelijk werken voor een en dezelfde overheid. De onderzoekscommissie naar intelligence voorafgaande aan de oorlog in Irak heeft zich erg gestoord aan diensten die zich verzetten tegen het delen van informatie omdat die ‘hun eigendom zou zijn’ en zij alleen informatie willen afstaan als daar een tegenprestatie tegenover staat. Niet de diensten zijn eigenaar van die informatie, maar de federale overheid aldus de onderzoekscommissie. Zij verwerpt het idee van eigendom, ook al leeft dit heel sterk bij de inlichtingendiensten: *“Officials are fiduciaries who hold the information in trust for the nation.”* [171] Het begrip eigendom van informatie komt overigens in Nederland ook heel vaak voor en het wordt zowel in de inlichtingen- als de opsporingswereld als een argument gebruikt om informatie niet aan anderen te geven, ook al hebben die anderen de bewuste informatie voor hun eigen werk nodig. De eigenaar van informatie geeft de informatie alleen als de ander daar een tegenprestatie tegenover stelt: quid pro quo. Als die tegenprestatie niet komt of niet van waarde is, wordt de informatie niet verstrekt. Het loutere argument dat een dergelijk eigendomsbegrip usance is in de internationale wereld van de inlichtingendiensten, mag ons inziens geen rol spelen in de Nederlandse verhoudingen tussen inlichtingen- en opsporingsdiensten. Het belemmert de effectiviteit van het primaire proces van alle inlichtingen- en opsporingsdiensten.

Een ander gebied waarop partijen bij het inwinnen van gegevens onvoldoende samenwerken, is het toepassen van nieuwe technologieën, zoals bijvoorbeeld datamining. Hier vindt elke partij zijn eigen wiel uit. Betere samenwerking bij het opzetten van systemen voor de nieuwe technologie zal leiden tot veel betere resultaten.

Omdat elke partij zijn eigen systeem volgt voor het inwinnen van gegevens uit externe gegevensbestanden en omdat elke partij gericht is op de eigen aanpak, leeft er onvoldoende besef dat er sprake is van een suboptimaal systeem dat bij een betere inrichting substantieel meer en betere resultaten op zou kunnen leveren. Door de verbrokkelde aanpak is het onvermijdelijk dat verbanden over het hoofd worden gezien en kansen in de strijd tegen criminaliteit en terrorisme worden gemist. Dat is op zich een veiligheidsrisico, waarvan de omvang overigens moeilijk kan worden gekwantificeerd.

170 De WIV gaat overigens nog steeds uit van het “need to know” principe, zie artikel 35.

171 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, report to the president, Washington, 2005, p. 430

4.6 Doelmatigheid

Het proces van inwinnen van gegevens uit externe databases is in verschillende opzichten niet doelmatig. Voor deze stelling heeft de adviescommissie een aantal argumenten:

1. Het is onmogelijk te sturen op kosten, omdat er geen inzicht is in het aantal bevragingen.
2. Er bestaat geen inzicht in en verantwoording over de sterke groei in het aantal bevragingen.
3. Omdat de kosten voor de bevragingen veelal worden gedragen door de leverancier van de gegevens, bestaat er bij de vragende diensten een onvoldoende prikkel om het proces van gegevens inwinnen doelmatig in te richten en uit te voeren.
4. In de gevoerde gesprekken zijn regelmatig voorbeelden aangedragen van ondoelmatige bevragingen.

Uit de wijze waarop de verschillende partijen dit inwinnen hebben ingericht, blijkt dat doelmatigheid in het geheel geen kwestie van overweging is of zelfs maar kan zijn. Aangezien er geen gezamenlijke visie of strategie is ten aanzien van dit belangrijke onderdeel van de processen die moeten leiden tot intelligence, komen vragen ten aanzien van doelmatigheid niet aan de orde. Er vindt geen sturing plaats op kosten. Er bestaat geen centraal inzicht in de kosten. Er vindt ook geen verantwoording plaats over de gemaakte kosten. Deze kosten zijn over het algemeen versleuteld in andere begrotingen. Als er geen inzicht mogelijk is in het totaal aantal bevragingen kan er ook geen inzicht bestaan in de kosten en in de vraag of deze kosten terecht zijn gemaakt.

Dat het proces ondoelmatig is, blijkt ook uit de ongecontroleerde groei van het aantal bevragingen, waarvoor niemand een echte verklaring heeft. Gewezen kan worden op de sterke groei in het aantal bevragingen aan telecomproviders en op de ongemotiveerd sterke groei van 20% in het aantal bevragingen dat in het kader van de dataretentie voor de komende jaren wordt voorzien. Gegevens leverende partijen worden volgens hen regelmatig bestookt met vragen die in hun ogen niet doelmatig zijn, maar die wel zorgen voor een kostbaar zoekproces in de geautomatiseerde gegevensbestanden van de leveranciers. In ieder geval kan worden opgemerkt dat de stijging van het aantal gegevens dat wordt ingewonnen uit externe gegevensbestanden veel groter is dan de stijging in het aantal opgeloste misdrijven.

Omdat de gegevens vragende partijen vaak niet of zeer weinig hoeven te betalen voor de gegevens, worden zij ook niet geconfronteerd met de financiële gevolgen van hun vragen. Er bestaat derhalve geen doelmatigheidsprikkel bij de vragende partijen. Zij worden op die manier niet gestimuleerd om na te gaan of de bevraging doelmatiger (en mogelijk effectiever) op een andere manier kan worden gedaan. Een goed voorbeeld daarvan is de gegevensverstrekking door de RDW aan het veiligheidsdomein. Volgens opgave van de RDW is daarmee een bedrag gemoeid van tussen de € 10 en € 16 miljoen.

Dat het proces ondoelmatig is, blijkt uit de ongecontroleerde groei van het aantal bevragingen, waarvoor niemand een echte verklaring heeft.

Omdat de RDW zelf voor deze kosten opdraait, stelt niemand in het veiligheidsdomein zich de vraag of een aantal van 154,7 miljoen verstrekkingen op jaarbasis een doelmatigheidstoets zou kunnen doorstaan. Als de overheid op dit punt al met een doelmatigheidsvraag wordt geconfronteerd is dat in de discussies met het bedrijfsleven over de hoogte van de vergoeding die het Rijk zou moeten geven voor het aanleveren van gegevens, met name in de sectoren van de banken en de telecomproviders. Maar dat is een andere doelmatigheid dan de afweging tussen inspanning en opbrengst.

Tijdens de door de adviescommissie gevoerde gesprekken zijn veel voorbeelden gegeven van ondoelmatige bevraging: meervoudige bevraging door verschillende diensten, bevraging zonder formele grondslag en bevraging die een evident te grote hoeveelheid gegevens oplevert en dus onnodig veel bewerking. Verschillende gesprekspartners uit zowel de private als de publieke sector hebben daarvan voorbeelden gegeven.

4.7 Tot slot: dit hoofdstuk in het kort

In dit hoofdstuk heeft de adviescommissie haar analyse weergegeven naar aanleiding van de observaties die zij heeft gedaan tijdens haar onderzoek. In de allereerste plaats concludeert de adviescommissie dat er geen sprake is van een eenduidige systematiek van gegevens inwinnen uit externe gegevensbestanden voor het veiligheidsdomein. Elke partij heeft zijn eigen systematiek en werkwijze. Onderlinge afstemming vindt zelden plaats. De partijen in het veiligheidsdomein hebben geen gezamenlijke strategie ten aanzien van het belang van databases voor de keten data - informatie - intelligence en ten aanzien van de manier waarop met dat belang moet worden omgegaan. Zij worden daarin door de betrokken departementen onvoldoende gestimuleerd.

In het verlengde hiervan constateert de adviescommissie dat dit totaal aan deelsystemen voor het inwinnen van gegevens uit externe databases niet voldoet aan daaraan te stellen normen voor vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid.

Aan de normen op het gebied van vormvereisten of de grondslag voor de bevraging wordt niet voldaan omdat onvoldoende inzicht mogelijk is in de wetgeving die van toepassing is op het proces van bevraging, onvoldoende duidelijk is of de vormvereisten in voldoende mate worden nageleefd en omdat er vraagtekens kunnen worden gezet bij de mate waarin de bevraging afdoende is afgeschermd tegen personen die niet bevoegd zijn.

Aan de normen van maatschappelijke zorgvuldigheid wordt niet voldaan, omdat er onvoldoende inzicht bestaat in de mate waarin bij de bevraging eisen ten aanzien van proportionaliteit en subsidiariteit worden nageleefd. Daarbij speelt mee dat gegevens ten aanzien van het aantal bevragingen en de groei daarin niet worden bijgehouden. Daar wordt dus niet op gestuurd. Dan kan er ook niet voldoende aandacht zijn voor vraagstukken met betrekking tot proportionaliteit en subsidiariteit. Omdat er geen gegevens over aantallen worden bijgehouden kan er ook niet op een deugdelijke wijze maatschappelijk verantwoording worden afgelegd over het proces van bevraging.

Aan de eisen van effectiviteit wordt niet voldaan, omdat de betrokken partijen in het veiligheidsdomein onvoldoende samenwerken ten aanzien van strategische vraagstukken met betrekking tot het inwinnen van gegevens. Ook wordt onvoldoende samengewerkt ten aanzien van het delen van informatie en ten aanzien van het toepassen van nieuwe technologieën. Door onvoldoende samenwerking worden verbanden over het hoofd gezien en kansen in de strijd tegen criminaliteit en terrorisme gemist. Dat is op zich een veiligheidsrisico.

Aan de eisen van doelmatigheid wordt niet voldaan, omdat er bij het proces van bevraging geen sturing is op kosten. Evenmin is er sprake van een doelmatigheidsprikkel voor gegevens vragende partijen. Een ander draait immers voor de kosten op.

Op grond van het bovenstaande trekt de adviescommissie de volgende conclusies:

1. Het complex van deelsystemen voor het inwinnen van gegevens uit externe databases voldoet niet aan daaraan te stellen normen van grondslag en vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid.
2. Aan te stellen normen op het gebied van de grondslag en de vormvereisten wordt niet voldaan, omdat onvoldoende inzicht bestaat in de toepasselijke wet- en regelgeving, de mate waarin inlichtingen- en opsporingsdiensten zich houden aan de geldende regels en omdat de afscherming van de bevraging voor onbevoegden onvoldoende kan worden verzekerd.
3. Aan te stellen normen op het gebied van maatschappelijke zorgvuldigheid wordt niet voldaan omdat onvoldoende inzicht bestaat in proportionaliteit en subsidiariteit en omdat een afdoende inzicht in het aantal bevragingen en de groei daarin ontbreekt. Aan een aantal beleidsvragen die hiermee samenhangen dient de overheid meer aandacht te geven.
4. Aan te stellen normen op het gebied van effectiviteit wordt niet voldaan omdat de betrokken partijen onvoldoende samenwerken bij het inwinnen, gebruiken en delen van gegevens uit externe gegevensbestanden, waardoor verbanden over het hoofd worden gezien en kansen worden gemist.
5. Aan te stellen normen op het gebied van doelmatigheid wordt niet voldaan omdat geen sturing op kosten plaats vindt en er geen sprake is van een doelmatigheidsprikkel voor vragende diensten.

5

5.1 Inleiding

Het onderzoek van de adviescommissie is opgedeeld in twee fases. In de huidige eerste fase maakt de adviescommissie een beschrijving van de systematiek van inwinnen van gegevens uit externe gegevensbestanden voor zover deze bestaat en gaat zij na in hoeverre deze systematiek verbetering behoeft. In de tweede fase zal het accent vooral liggen op mogelijkheden voor verbetering. In dit hoofdstuk geeft de adviescommissie een aanduiding van de onderwerpen die in de volgende fase aan de orde kunnen komen. Over deze aanbevelingen en over de wijze waarop aan deze aanbevelingen gevolg zal worden gegeven, zal overleg plaats vinden tussen de opdrachtgevers, de drie betrokken departementen, en de adviescommissie.

In dit hoofdstuk zal allereerst worden ingegaan op een aantal onderwerpen waarvan de adviescommissie zich voorstelt deze in een volgende fase verder uit te diepen. Vervolgens komen enkele onderwerpen aan de orde, welke kunnen ondersteunen bij een verdere verbetering van de samenwerking tussen de partijen in het veiligheidsdomein, de inlichtingen- en opsporingsdiensten. Tot slot worden enkele onderwerpen benoemd waarbij de regering de terzake noodzakelijke acties kan ondernemen.

5.2 Verdieping

Privacy en veiligheid

De maatschappelijke discussie over de juiste balans tussen privacy en veiligheid moet op een hoger niveau worden getild. De discussie vindt nu in te beperkte kring plaats en heeft de neiging te verzanden in een stellingenoorlog waar partijen steeds minder geneigd zijn om naar de argumenten van de ander te luisteren. De wijze waarop data-mining en andere nieuwe technologieën in het veiligheidsdomein worden toegepast hoort naar onze mening onderdeel van deze discussie te zijn, omdat aspecten van privacy daarbij nadrukkelijk aan de orde zijn. De discussie is ook en misschien juist wel nodig omdat een breed gedragen veiligheidsbeleid staat of valt met een goede balans tussen privacy en veiligheid. Het brede draagvlak komt in gevaar als de bevoegdheden van inlichtingen- en opsporingsdiensten zover worden uitgebreid dat de negatieve gevolgen daarvan voor de privacy van de burger te groot worden. Diverse onderzoekers en politici (vooral uit de Eerste Kamer) geven aan dat de grens in zicht is en volgens sommigen al overschreden.

De discussie moet worden gevoerd op een wijze die voor alle partijen aanvaardbaar is en ontdaan van elementen die zouden kunnen wijzen op een zekere mate van voor-ingenomenheid. De betrokken departementen noch het College Bescherming Persoons-

gegevens zijn op dit moment de aangewezen instanties om deze discussie voor te bereiden; zij zijn immers partij geworden in deze discussie.

Aanbeveling

De adviescommissie stelt voor dat een publieke discussie wordt voorbereid over de balans tussen privacy en veiligheid. Doel van deze discussie is om bouwstenen aan te dragen voor een herijking van de balans tussen bevordering van de veiligheid en bescherming van de persoonlijke levenssfeer.

De werkzaamheden zullen zich vooral richten op het inhoudelijk voorbereiden van de discussie: welke elementen spelen een rol, welke standpunten zijn ingenomen, welke technologische aspecten moeten worden onderscheiden en hoe heeft het privacybegrip zich in de afgelopen jaren ontwikkeld.

Wetgeving en toetsingskader

De adviescommissie heeft geconstateerd dat er geen overzicht beschikbaar is van toepasselijke wetgeving ten aanzien van bevoegdheden en verantwoordelijkheden op het gebied van inwinnen en verschaffen van gegevens ten behoeve van het veiligheidsdomein. De hierop betrekking hebbende regelgeving is verspreid over een groot aantal verschillende wetten die tot de verantwoordelijkheid behoren van uiteenlopende departementen. Er bestaat in ieder geval een duidelijke behoefte aan een duidelijk overzicht van alle op dit punt relevante wet- en regelgeving. Door het opstellen van een dergelijk overzicht kan ook de vraag worden beantwoord of de bestaande systematieken met elkaar in evenwicht zijn en of verantwoordelijkheden en bevoegdheden een consistent en logisch geheel vormen. Het is in de visie van de adviescommissie aan de minister van Justitie om zorg te dragen voor de totstandkoming van een dergelijk overzicht.

In een volgende fase wil de adviescommissie dit onderwerp nader uitdiepen en daarbij ook nagaan of het aanbeveling verdient in aanvulling op bedoeld overzicht de genoemde bevoegdheden en verantwoordelijkheden onder te brengen in één overzichtelijke stelselwet, waarin duidelijk staat omschreven onder welke voorwaarden inlichtingen- en opsporingsdiensten gegevens mogen inwinnen uit externe gegevensbestanden en wat terzake rechten en plichten zijn van beheerders van deze bestanden. Daarbij zou ook in kunnen worden gegaan op de vraag in hoeverre deze beheerders uit eigen beweging informatie moeten verstrekken aan de inlichtingen- en opsporingsdiensten.

Een onderwerp dat dan ook aan de orde zal komen is de vraag in hoeverre het wenselijk is een toetsingskader op te stellen van normen waaraan bevraging door inlichtingen- en opsporingsdiensten van deze externe bestanden moet voldoen. Gedacht kan worden aan vormvereisten, normen van maatschappelijke zorgvuldigheid en normen van effectiviteit en doelmatigheid. Tot de vereisten inzake grondslag en vorm kunnen

Een onderwerp dat aan de orde zal komen is de vraag in hoeverre het wenselijk is een toetsingskader op te stellen van normen waaraan bevraging door inlichtingen- en opsporingsdiensten van deze externe bestanden moet voldoen.

eisen behoren ten aanzien van de bevraging, de gebruikte technieken en procedures en de afscherming van de bevraging voor onbevoegden. Tot de normen van maatschappelijke zorgvuldigheid kunnen behoren eisen ten aanzien van proportionaliteit en subsidiariteit en eisen ten aanzien van het draagvlak bij de maatschappij en de leverende partijen alsmede eisen ten aanzien van de openbare verantwoording over de inwinning en de daarbij bereikte resultaten. Tot de normen op het gebied van effectiviteit en doelmatigheid kunnen eisen behoren ten aanzien van de maatschappelijke kosten, de resultaten van de vraagstelling, het voorkomen van dubbele of meervoudige bevraging, de toepassing van het need-to-share principe en de toepassing van nieuwe technologieën.

Aanbeveling

De rijksoverheid dient op korte termijn een overzicht op te stellen van alle wet- en regelgeving die van toepassing is op het inwinnen van gegevens uit externe databestanden. De adviescommissie zal nagaan of het wenselijk is in aanvulling op dit overzicht een stelselwet tot stand te brengen voor de bevraging van externe databestanden met een daarop afgestemd toetsingskader.

Toezicht op raadpleging databases

In de beraadslagingen van de adviescommissie is de vraag aan de orde gekomen of het wenselijk is de aanstelling te bepleiten van een onafhankelijk toezichthouder op de gegevensinwinning uit externe gegevensbestanden bij zowel overheid als bedrijfsleven door inlichtingen- en opsporingsdiensten. De discussie is mede beïnvloed door pleidooien in de pers voor de instelling van een inspecteur-generaal voor de AIVD.[172] De adviescommissie blijft buiten de discussie over het toezicht op de AIVD, maar heeft wel geconstateerd dat een vorm van onafhankelijk toezicht, toegespitst op de raadpleging van externe databases door inlichtingen- en opsporingsdiensten, een positieve bijdrage kan leveren aan de wijze waarop dit proces wordt uitgevoerd, de daarbij behorende zorgvuldigheid en op de wijze waarop de privacy van de betrokken personen wordt beschermd. Het zou ook het draagvlak voor de bevraging bij betrokken leveranciers en bij de burgers kunnen vergroten. Tijdens de gevoerde gesprekken en expertmeetings is gebleken dat het idee van een onafhankelijk toezichthouder op de raadpleging van de externe databases in brede zin positief werd onthaald. Wel werd daarbij als belangrijke randvoorwaarde gesteld dat een dergelijke functionaris alleen effectief toezicht kan houden als deze ook daadwerkelijk onafhankelijk van de departementen wordt gepositioneerd.

Aanbeveling

De adviescommissie stelt zich voor in de tweede fase van het onderzoek een nadere verkenning uit te voeren naar de voor- en nadelen van de instelling van een onafhankelijke functionaris voor het toezicht op het inwinnen van gegevens uit externe databases door inlichtingen- en opsporingsdiensten, alsmede naar diens positionering.

172 Frank Kuitenbrouwer, Inspecteur-generaal goed voor AIVD, NRC Handelsblad, 6 februari 2007

5.3 Samenwerking

In de tweede fase wil de adviescommissie ook enkele mogelijkheden onderzoeken die een betere samenwerking van de inlichtingen- en opsporingsdiensten bij het inwinnen en delen van gegevens uit externe databases kunnen ondersteunen. Centraal hierbij staat de mogelijke inrichting van enkele shared services voor dit proces.

Een mogelijke shared service wordt gevormd door de instelling van een centrale verwijsindex voor de verschillende partijen in het veiligheidsdomein. Deze verwijsindex zou - zoals gelijksoortige verwijsindexen in de sectoren sociale zekerheid en volksgezondheid - geen inhoudelijke informatie dienen te bevatten. Maar wel gegevens over personen en organisaties die in een of ander onderzoek zijn betrokken en gegevens over de dienst die belast is met dit onderzoek. Hiermee kunnen dubbelingen worden voorkomen, kan snel contact worden gelegd tussen functionarissen die met eenzelfde soort onderzoek bezig zijn en kan onderlinge interferentie worden voorkomen. Als dit systeem op een goede manier wordt ingericht kan het ook bijdragen een betere identificatie van subjecten. Op dit moment kennen alle diensten wel een eigen vorm van een verwijsindex, maar deze hebben vooral een interne functie. Op het gebied van criminaliteitsonderzoek bestaat sinds enkele jaren het systeem VROS (Verwijzingsindex Recherche Onderzoeken en Subjecten), maar dit heeft niet de plaats weten te verkrijgen van algemene verwijsindex. Mogelijk kan dit systeem wel een basis vormen voor een meer algemene verwijsindex voor het veiligheidsdomein. Nader onderzoek moet hierin duidelijkheid brengen.

Naar de mening van de adviescommissie kan een Intelligent Verwijsknooppunt voor het Veiligheidsdomein een aantal voordelen combineren: vergroten van de onderlinge samenwerking, identificatie van individuen die bij meerdere partijen in het veiligheidsdomein in onderzoek of behandeling zijn en daarom in aanmerking komen voor een gecombineerde aanpak en toetsing van identiteit van personen. Ook kan deze verwijsindex mogelijk een rol spelen bij de aanpak van veelplegers of van personen die voor overlast zorgen. In de eerste verkennende gesprekken over een dergelijke verwijsindex is de adviescommissie gebleken dat bij diverse betrokken partijen interesse bestaat voor een verdere uitwerking van deze mogelijkheid voor verbetering van de onderlinge samenwerking.

Een andere mogelijke shared service kan wellicht worden gevonden in de opzet van een betrouwbare service provider ten behoeve van de inlichtingen- en veiligheidsdiensten. Externe partijen leveren hun informatie aan bij een gecertificeerde overheidsorganisatie die zorgt voor verdere verspreiding van de informatie naar de diensten binnen de overheid die deze informatie nodig hebben en voor bewaking van de kwaliteit van dit verdelingsproces. Onderdeel van de werkzaamheden kan zijn de zorg voor tijdelijke opslag van gegevens en voor tijdige en deugdelijke vernietiging. Ook kan een dergelijke organisatie er voor zorgen dat vertrouwelijke bedrijfsgegevens uit het bedrijfsleven niet bij concurrenten

terecht komen. Nu zijn er al enkele kleinere organisaties binnen de overheid die zich met delen van dit takenpakket bezig houden. Voorbeelden daarvan zijn CIOT (voor telecomgegevens), JID (voor justitiële gegevens) en MOT (voor financiële gegevens). Onderdeel van het onderzoek in de tweede fase kan ook zijn of er toegevoegde waarde kan worden gevonden in het op laten gaan van deze kleinere organisaties in een nieuwe shared service organisatie. Daarbij kan ook in ogenschouw worden genomen de wijze van opslag van gegevens voor de dataretentie inzake telefonie en internet.

Een derde mogelijkheid is de oprichting van fusion centers naar het voorbeeld van de Amerikaanse organisaties die in de afgelopen jaren zijn opgericht. Er zijn twee soorten fusion centers mogelijk. Een mogelijkheid is een regionale samenwerking van inlichtingen- en opsporingsdiensten op het vlak van criminaliteits- en terrorismebestrijding. Aan dergelijke fusion centers zou kunnen worden deelgenomen door vertegenwoordigers van AIVD, politie, bijzondere opsporingsdiensten, Koninklijke Marechaussee en douane. Ook zou een liaison van het bestuur deel kunnen nemen om snel te zorgen voor het leggen van relaties naar de juiste bestuurlijk niveaus. Een andere mogelijke inrichting van de fusion centers is sectoraal. Zo kan worden overwogen om per vitale sector (bijvoorbeeld nutsvoorzieningen, infrastructuur, betalingsverkeer) een fusion center in te richten waarin inlichtingen- en opsporingsdiensten overleggen met vertegenwoordigers van de desbetreffende sector overleggen over mogelijke bedreigingen voor die sector en over manieren waarop aan die bedreigingen het hoofd kan worden geboden.

Een vierde mogelijke shared service is een verdere professionalisering van de wijze waarop gegevens worden ingewonnen en verwerkt. Trefwoorden hierbij zijn datamining, profiling en patroonherkenning. Uit het onderzoek tot nu toe is gebleken dat op deze terreinen nog onvoldoende samenwerking plaats vindt en dat de diensten in het veiligheidsdomein op dit onderwerp elkaar eerder beconcurreren dan ondersteunen. Een shared service, bij voorbeeld in de vorm van een expertisecentrum, waarin de ontwikkeling van deze nieuwe technologieën plaats vindt kan voor versnelling zorgen. De daadwerkelijke toepassing van deze technologieën valt uiteraard onder de verantwoordelijkheid van de onderscheidene diensten. Wellicht kan hierbij worden voortgebouwd op de ervaringen die op dit moment worden opgedaan in het project VIA dat onder auspiciën van de NCTb plaats vindt.

In dit kader wil de adviescommissie ook de nadere discussie betrekken met de AIVD over nut en noodzaak van het fysiek binnenhalen van externe databases voor het doen van eigen onderzoek. Naar dit gebruik zijn door deskundigen tegenover de adviescommissie vraagtekens geplaatst. Zoals eerder vermeld wil de adviescommissie het gesprek over dit onderwerp met de AIVD voortzetten. Mogelijk kan het genoemde expertisecentrum hierbij een rol gaan spelen.

Aanbeveling

De adviescommissie stelt zich voor om mogelijke vormen van shared services in het veiligheidsdomein in de tweede fase nader te onderzoeken op nut en haalbaarheid, zoals:

- **Een Intelligent Verwijsknooppunt voor het veiligheidsdomein,**
- **Een betrouwbare service provider die zorgt voor inwinnen en verspreiden van gegevens,**
- **Fusion centers voor samenwerking en uitwisseling van gegevens,**
- **Een expertisecentrum voor de ontwikkeling van nieuwe technologieën.**

5.4 Het Rijk aan zet

Tot slot zijn er enkele onderwerpen waarover naar de mening van de adviescommissie geen nadere verkenning nodig is, maar waar het Rijk aan zet is om tot verbetering te komen. Dit geldt allereerst het initiatief dat de drie verantwoordelijke departementen, BZK, Defensie en Justitie kunnen nemen om het proces van strategische samenwerking binnen het veiligheidsdomein vorm te geven op het gebied van het inwinnen, gebruiken en delen van gegevens uit externe databases.

Naast deze meer algemene opmerking is het Rijk naar het gevoelen van de adviescommissie op de volgende punten aan zet:

- Het eerste onderwerp betreft de kwestie van de vergoeding van de kosten voor het aanleveren van gegevens aan het veiligheidsdomein door partijen in de markt. Dit probleem betreft vooral de banken en de providers op het gebied van telecom en Internet. De huidige patstelling is contraproductief en heeft tot gevolg dat bedrijven steeds minder bereid zijn om de gevraagde gegevens te verstrekken. Dit belemmert het proces van de inlichtingen- en veiligheidsdiensten. De adviescommissie is van mening dat een systeem van gegevens inwinnen dermate doelmatig moet zijn ingericht dat de te maken kosten voor het bedrijfsleven tot een minimum worden beperkt. Ook mag niet uit het oog worden verloren dat een financiële prikkel de inlichtingen- en opsporingsdiensten kan stimuleren om de vraag richting de externe gegevensbank beter in te richten. Belangrijkste punt is echter dat de rijksoverheid haar verantwoordelijkheid pakt en de discussie met het bedrijfsleven weer start om te zorgen dat aan deze slepende discussie een eind komt.

- Het tweede onderwerp is de terugkoppeling over de resultaten die zijn behaald met behulp van de gegevens die zijn verkregen uit externe databases. Dit betreft niet alleen databases van marktpartijen, maar ook die van de overheid. Een dergelijke terugkoppeling kan het draagvlak bij deze leverende partijen voor medewerking vergroten, kan bijdragen aan een verlaging van de kosten van het bedrijfsleven en geeft invulling aan toezeggingen die in het verleden aan het bedrijfsleven zijn gedaan. Dit onderwerp is vooral een kwestie van sturing en organisatie en kan binnen niet al te lange tijd zijn gerealiseerd.

- In de derde plaats zal het Rijk initiatieven kunnen nemen om de discussie over de invoering van de dataretentie in goede banen te leiden. Het gepubliceerde concept-wetsontwerp heeft grote bezwaren opgeroepen in zowel de betrokken sector als bij het College Bescherming Persoonsgegevens. Ook in het parlement is het regerings-voornemen gestuit op forse bedenkingen. Het vraagstuk van de kosten voor de opslag en levering van gegevens speelt hierbij eveneens een belangrijke rol. Veel telecom-deskundigen vragen zich daarnaast af of de verplichting tot dataretentie inmiddels niet is ingehaald door de praktijk van de technologische vernieuwing. Het verdient naar de mening van de adviescommissie aanbeveling om, gelet op deze standpunten, de merites van het wetsvoorstel aan een nader onderzoek te onderwerpen en te overwegen of een andere benadering van dit onderwerp niet op een breder draagvlak kan rekenen.

- In de vierde plaats moet het mogelijk zijn om op een meer gestructureerde wijze maat-schappelijk verantwoording af te leggen over de hoeveelheid bevragingen die inlichtingen- en veiligheidsdiensten doen bij externe gegevensbestanden en over het aantal malen dat per jaar telefoons worden afgetapt. Nu worden gegevens niet bijgehouden of geheim gehouden. De argumentatie daarvoor is onvoldoende. Een openbare discussie over het aantal bevragingen en het aantal telefoontaps alsmede de groei in de tijd daarvan moet mogelijk worden gemaakt. De adviescommissie adviseert de betrokken departementen daarom ervoor te zorgen dat de hierop betrekking hebbende gegevens beter worden bijgehouden en geadministreerd en dat daarover jaarlijks op een inzich-telijke manier openbaar verslag wordt gedaan.[173] De meest eenvoudige manier daarvoor is een jaarlijkse rapportage van de betrokken ministers aan de Tweede Kamer. Mogelijk kan de toezichthouder waarvan eerder in dit hoofdstuk sprake was, in de toekomst een rol spelen in dit verantwoordingsproces.

Aanbeveling

De drie verantwoordelijke ministers worden opgeroepen initiatieven te nemen teneinde de strategische samenwerking binnen het veiligheidsdomein vorm te geven bij het inwinnen, gebruiken en delen van gegevens uit externe databases.

Ten aanzien van de volgende onderwerpen acht de adviescommissie maatregelen door de rijksoverheid gewenst:

- **Het nemen van verantwoordelijkheid voor afronding van de discussie over de vergoeding van kosten van marktpartijen;**
- **Een systeem van terugkoppeling naar het bedrijfsleven van de hoofdlijnen van de resultaten die zijn bereikt met de door het bedrijfsleven verstrekte gegevens;**
- **Vergroting van het draagvlak voor de beleidsvoornemens inzake de dataretentie;**
- **Een stelsel voor maatschappelijke verantwoording over de bevragingen door de partijen in het veiligheidsdomein uit externe databestanden.**

173 De minister van Justitie heeft onlangs al aangegeven dat verbetering op dit punt mogelijk is door de in gang gezette centralisatie van het aftappen bij de KLPD. Het aftappen door de AIVD moet ook in de verantwoording worden meegenomen.

De drie verantwoordelijke ministers worden opgeroepen initiatieven te nemen teneinde de strategische samenwerking binnen het veiligheidsdomein vorm te geven bij het inwinnen, gebruiken en delen van gegevens uit externe databases.

BIJLAGE 1

OVERZICHT GEVOERDE GESPREKKEN

In onderstaand overzicht zijn de namen opgenomen van personen met wie door of namens de adviescommissie gesprekken ten behoeve van deze rapportage zijn gevoerd. Met sommige personen zijn meerdere gesprekken gevoerd. Ook zijn opgenomen de personen die deel hebben genomen aan de expertmeetings van de adviescommissie. Niet zijn opgenomen de personen die informeel achtergrondinformatie hebben gegeven en de personen van buitenlandse diensten en instellingen die zijn geraadpleegd tijdens drie fact finding trips naar het Verenigd Koninkrijk en de Verenigde Staten.

Vragers van informatie

P.J. Aalbersberg, *korpschef van politie IJsselland*
Afdelingshoofd Open Bronnen Informatie, *AIVD*
drs. E.S.M Akerboom, *korpschef van politie Brabant-Noord*
M.A. Beuving, *bevelhebber Koninklijke Marechaussee*
Dr. J.Th Bijman, *directeur CIOT, ministerie van Justitie*
S.B. Bloemsma EMPM, *Politieacademie-KLPD*
mr. H. van Brummen, *lid van het college van procureurs-generaal*
mw. Drs. J.C.L.J. Denis, *directeur werkproces Regulier IND*
A.L. Driessen, EMPM, *Hoofd Dienst Nationale Recherche*
Mr. H.J.E. Hambeukers, *officier van justitie, functioneel parket*
A.D. Heil, *lid korpsleiding politieregio Utrecht*
Mr. J.M.H.M. Hermans, *hoofd FIOD-ECD*
C.J. Heijsman, *korpschef van politie Utrecht*
E.C. Hogervorst MBA, *programmamanager terrorisme politie Amsterdam-Amstelland*
S. van Hulst, *hoofd AIVD*
H. de Jong, *directeur politie, Rotterdam-Rijnmond*
Drs. J. Kapsenberg, *oud-plaatsvervangend korpschef politie Amsterdam-Amstelland*
drs H. Karreman, *directeur bedrijfsvoering politie Rotterdam-Rijnmond*
B.A. Lutken, *lid commissie van toezicht inlichtingen- en veiligheidsdiensten (CTIVD)*
Medewerker afdeling Strategie, Planning en Control, *AIVD*
H.E.N.A. Meijer EMPM, *directeur operatiën Koninklijke Marechaussee*
J.H. ter Mors, *waarnemend hoofd dienst Nationale Recherche Informatie KLPD*
W. Paulissen, *plv. korpschef Brabant-Midden-West*
H. Schönfeld MCM, *Hoofd bedrijfsvoering en bedrijfsprocessen politie Amsterdam-Amstelland*
drs. J. Sikkel, *plv. directeur MIVD*
mr. A.L. Speijers, *officier van Justitie, hoofd onderzoek en expertise, functioneel parket*
H. Stiekema, *CIO Politie Brabant Zuid-Oost*
Mw. J. van de Streek, *Hoofd Meldpunt Ongebruikelijke Transacties (MOT)*

mevr. Mr. L. Veringmeier MPA, *programmamanager gemeente Rotterdam*
R. Vestjens, *MIVD*
J.A.J.T. Vissers, *plv. korpschef politie Rotterdam-Rijnmond*
C.Chr. van de Waal, *politie Brabant-Noord*
A.A.M. Wezenberg, *directeur fraudebestrijding van de IND*
mr. A. van Wijk, *Landelijk Parket*
P.J. van Zunderd, *Korpschef KLPD*

Leveranciers van informatie
Drs. H.G.M. Blocks, *directeur Nederlandse Vereniging van Banken*
Drs. S. Broers, *directeur Bestuurszaken, gemeente Den Haag*
J.A.F. van der Bruggen, *adjunct-directeur RDW*
mevrouw drs. Th.A.J. Burmanje, *voorzitter Raad van Bestuur Kadaster*
H. van der Giessen, *directiesecretaris CAIW Holding*
A. van Leeuwen, *beveiligingsexpert @Home*
Mr. W. Louwman, *Kadaster*
Dr.mr. E.C. MacGilvray, *security Nederlandse Vereniging van Banken*
drs. L. Muusse, *consultant Essent Kabelcom, thans @home*
P. Nijenhuis, *hoofd relatiemanagement van de Justitiële Inlichtingendienst*
W.A.J.M. Rovers, *Lid MT Belastingdienst*
Drs. E. Stoové, *voorzitter Raad van Bestuur Sociale Verzekeringsraad (SVB)*
J. van der Tuuk, *manager Strategie en Externe Ontwikkelingen RDW*
drs A.B. Volkers, *secretaris criminaliteitsbeheersing en veiligheid VNO NCW*
G.A. Wabeke, *manager Justitieel Aftappen & Monitoren KPN*
J. van Wesemael, *directeur dienst Sociale Zaken, gemeente Den Haag*
mr. A.H. Westerman, *adviseur veiligheid en criminaliteitsbeheersing Verbond van Verzekeraars*

Betrokken beleidsdepartementen
drs A.H.C. Annink, *secretaris-generaal van Defensie*
Mw. E. Y. Bogerman, *directeur van de Directie Informatisering van het ministerie van Justitie*
mr. M. Gazenbeek, *directeur juridische zaken, ministerie van Defensie*
Mr. T.H.J. Joustra, *Nationaal Coördinator Terrorismebestrijding (NCTb)*
L.A. Nieuwenhuizen, *hoofd Informatiebeleid, DGV, ministerie van BZK*
drs F.D. Ossewaarde, *hoofd afdeling informatie van de directie POI Rijk van BZK*
drs H.W.M. Schoof, *directeur-generaal Veiligheid, ministerie van BZK*
mr. J.J. Stam, *directeur instrumentatie rechtspleging & rechtshandhaving, ministerie van Justitie*
Mr. J. van der Vlist, *directeur-generaal rechtspleging en rechtshandhaving*
C. Willemse, H. Hoijtink en W. Borst, *medewerkers DGRR van het ministerie van Justitie*
dr H.J.M. van Zon, *directeur Innovatie- en Informatiebeleid Openbare Sector, ministerie van BZK*

Deskundigen en stakeholders
drs G.J. van Boven, *directeur Nationaal ICT Instituut in de Zorg (NICTIZ)*
prof. mr. Y. Buruma, *hoogleraar strafrecht, Radbout Universiteit, Nijmegen*
J. Butcher, *beveligingsexpert Fox-IT, Delft*
Dr. ir. S.R. Choenni, *hoofd statistische informatievoorziening en beleidsanalyse, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie*
mr. M.J. Cohen, *burgemeester van Amsterdam en korpsbeheerder van de politieregio Amsterdam-Amstelland*
drs W.J. Deetman, *burgemeester van Den Haag en korpsbeheerder van de politieregio Haaglanden*
mw. mr dr A. W. Duthler, *partner van Duthler Associates*
mw. Dr. C. van Eck, *beleidsmedewerker directie beleid en strategie NCTb*
ir. A.W.A. Erkens, *Directeur Kennis en Analyse, NCTb*
prof. dr. H. Franken, *hoogleraar Informatierecht, Universiteit van Leiden*
mw. drs J.A.M. Hilgersom, *directeur-generaal Sociale Verzekering bij ministerie van SZW*
prof. M.J. van den Hoven, *hoogleraar ethiek, TU Delft,*
Prof. dr. B.P.F. Jacobs, *Nijmeegs instituut voor informatica en informatiekunde, Radbout Universiteit, Nijmegen*
drs. O.M. Kinkhorst, *directeur stichting Inlichtingenbureau*
mr. A.W. Kist, *lid raad van bestuur AFM*
mr. J. Kohnstamm, *voorzitter van het College Bescherming Persoonsgegevens*
M. van der Marel, *directeur FOX-IT, Delft*
E. Moonen, *senior inspecteur, Inspectie Openbare Orde en Veiligheid, ministerie van BZK*
Ir H.I.M. Nieuwenhuis MBA, *director Getronics PinkRoccade*
R. Oord, *commissie beveiliging en publieke veiligheid Schiphol*
Prof. dr. S. Peters, *hoogleraar informatie en strategie, Vrije Universiteit*
Mw. Prof.mr. J.E.J. Prins, *hoogleraar Recht en informatisering, Universiteit van Tilburg*
Mw. drs O.F. Scheidel, *senior projectleider NCTb*
E. Schreuders, partner, *Net2Legal Consultants, Den Haag*
drs L.J.E. Smits, *directeur Het Expertise Centrum*
N. Spekking, *deskundige telecom, CapGemini*
Prof. dr. Ir. H.C.A. van Tilborg, *hoogleraar wiskunde, cryptologie, technische universiteit Eindhoven*

BIJLAGE 2

GERAADPLEEGDE LITERATUUR

Documentatie uit en over Nederland

- Adviescommissie Coördinatie ICT Rampenbestrijding: 'De Vrijblijvendheid Voorbij' Op naar een effectieve multidisciplinaire informatievoorziening bij grootschalig gezamenlijk optreden in onze gedecentraliseerde eenheidsstaat, maart 2005
- Albers, P., Een proces van macht, shared services organisaties bij het Rijk, Zoetermeer, 2006
- Algemene Rekenkamer: terugblik op 2005, de pp. 20-30
- Brinkman, L.C., De organisatie van de veiligheid op rijksniveau nader bezien, advies van 13 oktober 2006, ministerie van BZK
- Clingendael Centrum voor Strategische Studies TNO, Democratische Controle Inlichtingen- en Veiligheidsdiensten, Den Haag, 2005
- College Bescherming Persoonsgegevens, brief aan de Tweede Kamer inzake het wetsontwerp Burger Service Nummer d.d. 25 oktober 2005, nr. z2005-1198
- College Bescherming Persoonsgegevens (CBP), jaarverslag 2005, Den Haag, 2006
- College bescherming persoonsgegevens (CBP): Advies inzake het Wetsontwerp implementatie Europese Richtlijn Dataretentie, advies d.d. 22 januari 2007
- Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst (Commissie-Havermans): De AIVD in verandering, November 2004
- Commissie Strafvorderlijke gegevensvergaring in de Informatiemaatschappij (Commissie-Mevis), Gegevensvergaring in strafvordering, Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, mei 2001
- Commissie Toegangsbeheer Schiphol (Commissie-Oord), Veiligheid en beveiliging door één deur, Rapportage over het toegangsbeheer en het passensysteem, Den Haag, juni 2005
- Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, Toezichtrapport naar de door de AIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot oktober 2005, rapport d.d. 31 mei 2006, nr. 9a.
- Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), Toezichtsrapport inzake de Contra Terrorisme Infobox, rapport d.d. 21 februari 2007, nr. 12
- Duthler, Anne-Wil, Met recht een TTP!, uitgave 11 in de ITER reeks, 1998
- Erasmus Universiteit: onderzoek 'Wie wat bewaart, die heeft wat', Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer, juni 2005
- Franken, L, Literatuuronderzoek Identiteitsfraude 2004, Universiteit Utrecht 2005, p. 30
- Gemengde Commissie Veiligheid en Rechtsorde, de zgn. Commissie Brinkman: Meer samenhang en slagkracht, betere informatie, minder beleidsdrukte, september 2005
- Gezamenlijke reactie Aanbieders op consultatie Wetsvoorstel Dataretentie, verzonden aan de minister van Economische Zaken op 18 januari 2007

- Grijpink, J.H.A.M, Identiteitsfraude en Overheid, Justitiële Verkenningen, 2006, pp. 37-57
- Heemskerk, P., e.a., Naar een goed gebruik van het burgerservicenummer (BSN), Stichting Het Expertise Centrum, Den Haag, 2007
- Hoekstra, D.J. e.a., XBRL taxonomieën voor beginners en doeners, rapport in opdracht van de stichting XBRL Nederland, 2006
- Huisman, Aletha, Informatie-Gestuurde Politie: de tijd en moeite waard?!, scriptie bestuurskunde Universiteit Twente, 2006
- Inlichtingenbureau, Stichting, Jaarverslag 2005, Den Haag, 2006
- Inspectie Openbare Orde en Veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, een evaluatie van het project landelijke informatiecoördinatie DNP, Den Haag, 2004
- Inspectie Openbare Orde en veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, ontwikkelingen sinds rapportage 2004, Den Haag, 2006
- Justitiële Verkenningen, Inlichtingendiensten, 2004, nr. 3
- Kenniscentrum PPS, Samenwerking tussen overheden ter voorbereiding op Publiek Private samenwerking, versie van januari 2005
- Jacobs, Prof. dr. B.P.F., De menselijke maat in ICT, web-boek, te raadplegen op: http://www.cs.ru.nl/B.Jacobs
- Koops, B.-J., e.a., Veiligheid en privacy in 2030: twee toekomstscenario's, Tilburg, januari 2005
- Koops, B.J., e.a., Aftapbaarheid van telecommunicatie, Een evaluatie van hoofdstuk 13 Telecommunicatiewet, Tilburg, 2005
- Kuitenbrouwer, F., Inspecteur-generaal goed voor AIVD, NRC Handelsblad, 6 februari 2007
- Meldpunt Ongebruikelijke Transacties, Jaaroverzicht 2005 en vooruitblik 2006 Meldingen Ongebruikelijke Transacties, 2006
- Minister van BZK, brief inzake Rapportage Intensivering Civiel-Militaire Samenwerking, d.d. 24 mei 2006
- Ministerie van Economische Zaken, concept wetsontwerp inzake bewaarplicht van telecommunicatiegegevens, met memorie van toelichting, Den Haag, 2006
- Nationale Beheerorganisatie voor Internet Providers (NBIP), de stichting NBIP voort-varend het vijfde jaar in, persbericht d.d. 10 oktober 2006
- National High Tech Crime Center, Verantwoording Project High Tech Crime, februari 2006
- Netherlands Intelligence Studies Association, diverse nieuwsbrieven (http://www.nisa-intelligence.nl/)
- Neve, Rudie, e.a., Eerste inventarisatie van contraterrorismebeleid, Cahier 2006-3 van het WODC, Ministerie van Justitie, Den Haag, 2006
- Olsthoorn, P., Cybercrime-eenheid in de knop gebroken, Netkwesties, 24 augustus 2006
- Onderzoeksgroep Inlichtingen en Veiligheid Defensie, Inlichtingen en Veiligheid Defensie: Kwaliteit, Capaciteit en Samenwerking, Den Haag, 2006

- Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime', Den Haag, maart 2006
- Overzicht uitvoeringsorganisaties en inspectiediensten waarbij ambtenaren werkzaam zijn met opsporingsbevoegdheden en van de reikwijdte van die bevoegdheden, uitgave van het ministerie van justitie, 2005
- Polderman, A, Nederland en de Europese Informatie-uitwisseling, de sterren stevig voor anker, Den Haag 2004
- Prins, J.E.J., Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy, Justitiele Verkenningen, 2004, nr. 8, pp. 34-47
- Prins, C., Variaties op een thema: van paspoort- naar identiteitsfraude, Nederlands Juristenblad, 2006, nr. 1
- Projectgroep Organisatie Structuren, Politie in Verandering, 's-Gravenhage 1977
- Raad van Hoofdcommissarissen, Projectgroep Visie op de Politiefunctie, Politie in Ontwikkeling, Den Haag, 2005
- Raad van Hoofdcommissarissen, Wenkend Perspectief, strategische visie op politieel informatiemanagement & technologie, Den Haag, 2006
- Sietsma, dr. R.: Gegevensverwerking in het kader van de opsporing, toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy, proefschrift Leiden, 2007
- Stratix Consulting 'Bewaren Verkeersgegevens door Telecommunicatieaanbieders' Augustus 2003
- Teepe, W., Reconciling Information Exchange and confidentiality, a formal approach, proefschrift, universiteit van Groningen, 2007
- TNS NIPO: Verkennend onderzoek terrorisme, augustus 2005
- Valk, Giliam de, Dutch Intelligence - Towards a Qualitative Framework for Analysis, proefschrift, Rijksuniversiteit Groningen, 2005
- Vedder, Anton, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut, 2007; Studie 49
- Verdonck, Klooster & Associates bv, Onderzoek naar de nationale implementatie van de Europese richtlijn dataretentie, onderzoek in opdracht van de minister van Justitie, oktober 2006
- Werkgroep gegevensverstrekking lokaal bestuur 'Werkgroep-Holtslag', VasteVerbindingen, rapportage aan de minister van BZK, Den Haag, 2005
- Wiebes, C., Geheime diensten moeten over eigen schaduw springen; Inlichtingendiensten dienen bij uitstek het nationale staatsbelang, gepubliceerd in de Newsletter van de Netherlands Intelligence Studies Association, www.nisa-inteliigence.nl
- Wijk, R. de en C. Relk, Doelwit Europa, complotten en aanslagen van moslimextremisten, Amsterdam 2006

Buitenlandse documentatie

- AFCEA, Lessons Learned: Building a New National Intelligence Partnership, 2006-08-21
- An Overview of the United States Intelligence Community, uitgave van The Office of the Director of National Intelligence, Washington, 2007
- Association of Chief Police Officers, Retention guidelines for nominal records on the police national computer, Winchester, 2006
- Barger, Deborah G., Toward a Revolution in Intelligence Affairs, Santa Monica, 2005
- Bureau of Justice Assistance, Principles and promises, BJA's plan for the future, Washington, z.j.
- Bureau of Justice Assistance: The National Criminal Intelligence Sharing Plan, Washington 2003, revised in 2005
- Bureau of Justice Assistance, Intelligence-led policing, the New Intelligence Architecture, Washington, 2005
- Bureau of Justice Assistance e.a., Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New World, Washington, July 2005
- Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the twenty-first century An appraisal of U.S. intelligence, Washington, March 1996
- Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, report to the president, Washington, 2005
- Congressional Research Service, The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project, Washington, August 2004
- Congressional Research Service, Information Sharing for Homeland Security, A Brief Overview, Washington, January 2005
- Congressional Research Service, Data Mining and Homeland Security: an Overview, Washington, January 2006
- Congressional Research Service, Terrorist Watchlist Checks and Air Passenger Prescreening, Washington, September 2006
- Cope, Nina, Intelligence Led Policing or Policing Led Intelligence? Integrating Volume Crime Analysis into Policing, British Journal of Criminology, vol. 44, 2004, pp. 188-203 (Centre for Crime and Justice Studies)
- Council of the European Union, The European Union Counter-Terrorism Strategy, Brussels, November 2005
- Department of Homeland Security, National Infrastructure Protection Plan (NIPP), Washington, z.d. (summary)
- Department of Justice, The National Criminal Intelligence Sharing Plan, Solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence, Washington, October 2003
- Director of National Intelligence, Information Sharing Environment, Interim Implementation Plan, Washington 2005

- Director of National Intelligence, The National Intelligence Strategy of the United States of America, Transformation through Integration and Innovation, Washington, 2005
- Director of National Intelligence, An overview of the United States intelligence Community, Washington, 2007
- Federal Trade Commission, Identity Theft Survey Report, Washington, 2003
- Gantz, John F., e.a., The Expanding Digital Universe, A Forecast of Worldwide Information Growth Through 2010, uitgave van IDC, maart 2007
- Global Justice Information Sharing Initiative (Global) Advisory Committee, Guiding Principles and Strategic Vision of the Global Justice Information Sharing Initiative, Washington, z.j.
- Government Accountability Office (USA), Data Mining, Federal Efforts Cover a Wide Range of Uses, Washington, May 2004
- Government Accountability Office (USA), Overview of Department of Homeland Security Management Challenges, Washington, April 2005
- Government Accountability Office (USA), The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information, Washington, March 2006
- Government Accountability Office (USA), Homeland Security, Progress Continues, but Challenges Remain on Department's Management of Information Technology, Statement of Randolph C. Hite, Director Information Technology Architecture and Systems Issues, March 29, 2006
- Government Accountability Office (USA), Information sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information, Washington, April 2006
- Government Accountability Office (USA), Suggested Areas for Oversight for the 110th Congress, Washington, 17 November 2006
- Hollywood, John, Diane Snyder, Kenneth McKay and John Boon, Out of the Ordinary, Finding Hidden Threats by Analyzing Unusual Behavior, Santa Monica, 2004
- Homeland Security Advisory Council, Homeland Security Information Sharing between Government and the Private Sector, Washington, 2005
- House Committee on Homeland Security Democratic Staff, Beyond Connecting the Dots, A Vital Framework For Sharing Law Enforcement Intelligence Information, Washington, z.j. (vermoedelijk 2005)
- House Committee on Government Reform, Staff Report, Agency Data Breaches since January 1, 2003, Washington 2006
- Hustinx, Peter J., Human rights and public security: change for a compromise, or continuity of safeguards?, Conference on Public Security and Data Protection, Warsaw, 11 May 2006
- Identity Theft Resource Center, Identity Theft: The Aftermath 2004, San Diego, 2005
- Information Sharing Council (ISC), Implementation Plan For the Information sharing Environment Electronic Directory Services - People & Organizations, Washington, March 2006

- Intelligence and Security Committee (ISC), Intelligence Oversight, London, 2002
- Intelligence and Security Committee (ISC), Annual Report 2004-2005, uitgave van the Stationary Office, London, April 2005
- Intelligence and Security Committee (ISC), Annual Report 2005-2006, uitgave van the Stationary Office, London, June 2006
- Jonas, Jeff, and Jim Harper, Effective Counterterrorism and the Limited Role of Predictive Data Mining, Policy Analysis, no. 584, December 11, 2006, pp. 1-12
- Linde, Erik van, e.a., Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries, RAND Europe, 2002
- Markle Foundation, Protecting America's Freedom in the Information Age, new York, 2002
- Markle Foundation, Creating an Trusted Information Network for Homeland Security, New York, 2003
- Markle Foundation, Mobilizing Information to Prevent Terrorism, Accelerating Development of a Trusted Information Sharing Environment, New York, 2006
- McNamara, Thomas E., Statement for the Record, Building on the Information Sharing Environment: Addressing Challenges of Implementation, May 10, 2006
- National Commission on Terrorist Attacks Upon the United States, the 9/11 commission report, Washington, July 2004
- National Intelligence Machinery, uitgave van The Stationery Office, September 2006, zie ook www.intelligence.gov.uk
- NGA Center for Best Practices, State Intelligence Fusion Centers: Recent State Actions, Washington, July 2005
- NIEM Program Management Office, Introduction to the National Information Exchange Model, Washington, 2006
- Palmieri, Lisa M., Information vs. Intelligence : What Police Executives Need to Know, uitgave van de International Association of Law Enforcement Intelligence Analysts
- Police Executive Research Forum, Local Law Enforcement's Role in Preventing and Responding to Terrorism, Washington 2001
- Police Executive Research Forum, Protecting your community from terrorism, een serie van white papers, verschenen tussen 2003 en 2006
- Program Manager Information Sharing Environment, Interim Implementation Plan, Washington, December 2005
- Program Manager Information Sharing Environment, Implementation Plan, Washington, November 2006 (http://www.ise.gov/docs/ISE-impplan-200611.pdf)
- Secretary of State, Review of intelligence on weapons of mass destruction: implementation of its conclusions, London, March 2005
- Serious Organised Crime Agency, SOCA Annual Plan 2006/7, London, 2006
- Serious Organised Crime Agency, The United Kingdom Threat Assessment of serious organised crime, London, 2006
- Stolen lives, Technology and easy credit give identity thieves an edge, New York Times, 30 mei 2006

- Surveillance Studies Network, A Report on the Surveillance Society, report for the Information Commissioner, London, 2006
- Technology and Privacy Advisory Committee (TAPAC), Safeguarding Privacy in the Fight against Terrorism, Washington, March 2004
- Thompson, Bennie G., LEAP, a Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing between the Intelligence Community and State, Local and Tribal Law Enforcement, Washington, 2006
- Vries, Gijs de, The Fight Against Terrorism - Five Years After 9/11, Annual European Foreign Policy Conference, London School of Economics & King's College London, 30 June 2006
- Wittig, Tim, Not so Legal tender, what next for the financial war on terrorism? In: Jane's Intelligence Review, February 2007, p. 17

Kamerstukken en andere officiële documenten

- 23 490, Ontwerpbesluiten Unie-verdrag, de nummers 407 en 408, motie-Dittrich, respectievelijk brief van de minister van Justitie inzake de bewaring van verkeers-gegevens, alsmede stuk nummer AW, brief aan de Eerste Kamer over dataretentie
- 25 764, reisdocumenten
- 25 877 Wet op de inlichtingen en veiligheidsdiensten
- 26 671, Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatie-technologie (computercriminaliteit II)
- 27 925, Bestrijding internationaal terrorisme
- 28 059, Wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie)
- 28 845, nrs 1-2, rapport van de Algemene Rekenkamer inzake uitwisseling van opsporings- en terrorisme-informatie
- 29 200, VII, nr. 61, brief inzake voorgenomen wetswijziging van de WIV
- 29 441 Wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens)
- 29 628, politie
- 29 754, terrorismebestrijding
- 29 876, nr. 3, Regeringsstandpunt inzake Rapport van de Commissie Bestuurlijke Evaluatie AIVD
- 29 876, nr. 8 (met bijlage) onderzoek democratische controle inlichtingen- en veiligheidsdiensten.
- 29 876, nr. 9 inzake de gegevensverstrekking door landelijke diensten aan het lokaal bestuur.
- 29 876, nr. 10 inzake het jaarplan van de AIVD

- 29 924, Toezichtverslagen AIVD en MIVD
- 30 164, Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven
- 30 171, Herstel van wetstechnische gebreken en leemten alsmede aanbrenging van andere wijzigingen van ondergeschikte aard in diverse wetten op het terrein van het Ministerie van Justitie (Reparatiewet II Justitie)
- 30 182, Vaststelling van regels met betrekking tot de bijzondere opsporingsdiensten en de instelling van het functioneel parket (Wet op de bijzondere opsporingsdiensten)
- 39 312 Algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het burgerservicenummer (Wet algemene bepalingen burgerservicenummer)
- 30 315, Gebruik van grenscontroles bij terrorismebestrijding
- 30 327, Regels inzake de verwerking van politiegegevens (Wet politiegegevens)
- 30 380 Regels inzake het gebruik van het burgerservicenummer in de zorg (Wet gebruik burgerservicenummer in de zorg)
- 30 505, Grip op informatievoorziening, IT Governance bij ministeries, rapport van de Algemene Rekenkamer
- 30 517, Evaluatie van hoofdstuk 13 van de Telecommunicatiewet
- 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
- 30 566, Regels inzake het opleggen van beperkende maatregelen aan personen met het oog op de bescherming van de nationale veiligheid en inzake het weigeren of intrekken van beschikkingen met het oog op de bescherming van de nationale veiligheid (Wet bestuurlijke maatregelen nationale veiligheid)
- 30 800 VI, begroting voor het ministerie van justitie voor het jaar 2007
- 30 821, brief inzake nationale veiligheid
- Aanhangsel van de Handelingen, vergaderjaar 2004-2005, nr. 2324
- Aanhangsel van de Handelingen, vergaderjaar 2006-2007, nr. 399
- Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG
- Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 1998, nr. 610
- Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002), Staatsblad 2002, nr. 148
- Wet van 29 mei 2006 tot vaststelling van regels met betrekking tot de bijzondere opsporingsdiensten en de instelling van het functioneel parket (Wet op de bijzondere opsporingsdiensten, Staatsblad, 2006, nr. 285

- Besluit van 28 oktober 2003, houdende regels betreffende door aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten te treffen beveiligingsmaatregelen ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie (Besluit beveiliging gegevens aftappen telecommunicatie)
- Besluit van 3 augustus 2004, houdende aanwijzing van de gegevens over een gebruiker en het telecommunicatie-verkeer met betrekking tot die gebruiker die van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst kunnen worden gevorderd (Besluit vorderen gegevens telecommunicatie)
- Besluit van de Raad van ministers van Binnenlandse Zaken en Justitie (Raad JBZ) van 1 en 2 december 2005 tot vaststelling van het Eindrapport over de evaluatie van nationale maatregelen ter bestrijding van het terrorisme: verbetering van de nationale actiemiddelen en vermogens ter bestrijding van het terrorisme, document 12168/3/05 REV 3

Vertrouwelijke informatie

Diverse partijen hebben aan de adviescommissie vertrouwelijke gegevens ter beschikking gesteld. Deze informatiebronnen worden hier niet vermeld. De bedoelde stukken zijn opgenomen in het archief van de adviescommissie dat na afronding van de werkzaamheden ter beschikking wordt gesteld aan de Minister van Justitie.

Colofon

Dit rapport is opgesteld door de Adviescommissie Informatiestromen Veiligheid in opdracht van de ministers van BZK, Defensie en Justitie.

De tekst van dit rapport kan worden geraadpleegd op: www.nctb.nl

De commissie bestaat uit:
mevr. prof. dr. M.G.W. den Boer
mr. H. Bosma, voorzitter
mr. Th. C. de Graaf
drs. A.A.M. Horrevorts, secretaris
mr. J.N. van Lunteren
drs. W.J.B.M. Stolwijk RA

Contact met de adviescommissie kan worden opgenomen via de secretaris:
a.a.m.horrevorts@nctb.nl

Vormgeving
Richard Sluijs

Foto omslag
Hollandse Hoogte

Druk
Deltahage