* OUDE GRIFFIE NR.

135703

COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AAN mevrouw mr. Y.E.A.M. Timmerman-Buck,
voorzitter Eerste Kamer der Staten-Generaal
Postbus 20017
2500 EA 's-GRAVENHAGE

GRIFFIE EERSTE KAMER
NR. 140080 *
RUB. VII
28 DEC 2007
DATUM
CS
KOPIE
VERW. 13 2K/AZ /V2.

DATUM 20 december 2007
ONS KENMERK z2007-01381
CONTACTPERSOON mw. mr. V.H. Brouwer
070-8888500
administratie@cbpweb.nl
UW BRIEF VAN 7 november 2007
UW KENMERK HM/eos

ONDERWERP Advies wetsvoorstel 30553

Geachte mevrouw Timmerman-Buck,

Bij brief van 7 november 2007 heeft u het College bescherming persoonsgegevens (CBP) op grond van artikel 17 Kaderwet Adviescolleges verzocht te adviseren over het wetsvoorstel Wijziging van de Wet op 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 (Wijziging van de Wiv 2002, verder: het wetsvoorstel). Uw verzoek volgde op een daartoe strekkend besluit van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin d.d. 30 oktober 2007.

De Wet bescherming persoonsgegevens (Wbp) is niet van toepassing op de verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten, zoals bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (verder: Wiv 2002). Dit geldt evenzeer voor de adviestaak die het CBP is toegekend in artikel 51, tweede lid, Wbp. De verplichting het CBP om advies te vragen is in dezen dan ook niet aan de orde. Het CBP maakt echter graag gebruik van uw uitnodiging om op basis van artikel 17 Kaderwet Adviescolleges te adviseren en zal in dat kader enkele kanttekeningen bij het wetsvoorstel plaatsen die volgens het CBP bij uitstek de aandacht van de Eerste Kamer behoeven bij de behandeling van dit wetsvoorstel, gelet op de aard daarvan en de gevolgen die dit met zich kan brengen. Het CBP voldoet hiermee derhalve aan uw verzoek.

Het wetsvoorstel voorziet, voorzover voor dit advies relevant, in een aantal wijzigingen die in de eerste plaats leiden tot een ruimere toegang tot gegevens bij (bij AMvB te bepalen) bestuursorganen, bepaalde personen en instanties in de vervoers- en financiële sector. Op deze bestuursorganen, personen en instanties komt de plicht te rusten om aan een verzoek tot verstrekking van gegevens te voldoen. Een ruimere toegang tot gegevens wordt tevens gecreëerd door te voorzien in een uitbreiding naar "aanbieders van een communicatiedienst" waar deze categorie eerst "aanbieders van openbare telecommunicatienetwerken en -diensten" betrof. Tot slot wordt de mogelijkheid geautomatiseerde data-analyse uit te voeren met behulp van beschikbaar gestelde geautomatiseerde gegevensbestanden expliciet in de wet opgenomen, evenals de personen wier gegevens het kan betreffen.

BIJLAGEN 1
BLAD 1

Samengevat luidt het advies van het CBP als volgt.

In het streven naar de verbetering van de efficiëntie (van dienstverlening) en klantvriendelijkheid, zijn niet alleen overheidsinstellingen maar ook bedrijven geneigd om steeds meer persoonsgegevens over burgers te verzamelen, te gebruiken en uit te wisselen. Daarnaast worden verplichte bewaartermijnen voor persoonsgegevens opgelegd. In combinatie met verregaande toepassing van ICT bestaat het risico dat de gegevensstromen, ook al worden deze met de beste bedoelingen ingericht, leiden tot een disproportioneel volgen en controleren van de burger. De glazen samenleving die daarmee in het vizier komt, kan een negatieve invloed hebben op het vertrouwen van burgers in de overheid en brengt een zorgvuldige omgang met persoonsgegevens in gevaar.

De noodzaak de voorgestelde maatregelen in het belang van de nationale veiligheid in te voeren, is onvoldoende onderbouwd. Omdat de precieze invulling van de in het wetsvoorstel genoemde sectoren alsmede de aard van de gegevens van communicatiediensten onzeker is, kan noch de proportionaliteit noch de subsidiariteit van die invulling beoordeeld worden. Niet is aannemelijk gemaakt dat de huidige bevoegdheden onvoldoende mogelijkheden bieden de taken effectief uit te voeren. Bovendien baart het ontbreken van de proportionaliteit van de maatregelen, afgezet tegen de onduidelijkheid waar het de omvang van de reeds bestaande bevoegdheden betreft, zorgen. Dit terwijl de bij wet gestelde regels ten aanzien van de bescherming van persoonsgegevens opzij gezet worden indien sprake is van een verwerking ten behoeve van de inlichtingen- en veiligheidsdiensten.

De mogelijkheid verantwoordelijken te verplichten op grote schaal gegevens te verstrekken, welke tevens met het oog op data-analyse kunnen worden verwerkt, heeft gevolgen voor de burger, maar ook voor de verantwoordelijken en de diensten. Deze gevolgen zijn niet, althans onvoldoende, onderkend. Bij AMvB wordt een aantal belangrijke elementen binnen dit wetsvoorstel ingevuld, waarover nu nog onduidelijkheid bestaat. De beveiliging van de gegevens is niet expliciet in het wetsvoorstel geregeld. De risico's die data-analyse met zich brengt zijn onderbelicht gebleven.
Juist omdat de risico's en nadelen onvoldoende aan bod zijn gekomen, kan niet beoordeeld worden of de waarborgen een adequaat tegengewicht bieden. Het is evenwel zeker dat het ontbreken van een beveiligingsbepaling en van een evaluatie- en/of horizonbepaling niet bijdraagt aan het benodigde evenwicht.

Het CBP beveelt dan ook aan het wetsvoorstel op bovenstaande opmerkingen nader te beschouwen, met name waar het de noodzaak van de voorgestelde maatregelen betreft. De nadelen en risico's die deze maatregelen meebrengen, zullen beter in kaart moeten worden gebracht. Alleen dan kunnen afwegingen van proportionaliteit en subsidiariteit worden gemaakt en kunnen de maatregelen op hun rechtmatigheid worden beoordeeld en worden voorzien van adequate waarborgen.

DATUM 20 december 2007
ONS KENMERK z2007-01381

Het volledige advies treft u in de bijlage aan. Het CBP is beschikbaar indien nadere toelichting is gewenst.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Een afschrift van deze brief zal worden verstuurd naar de Minister-president, Minister van Algemene Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie en de Minister van Justitie. Voorts wordt een afschrift verzonden aan de voorzitter van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

mw. mr. dr. J. Beuving
collegelid

DATUM 20 december 2007
ONS KENMERK z2007-01381

Bijlage bij de brief van het College bescherming persoonsgegevens van 20 december 2007.

Advies van het College bescherming persoonsgegevens (CBP) over het wetsvoorstel 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 (Wijziging van de Wiv 2002).

1. Inleiding

In Nederland zijn door het kabinet de afgelopen jaren verschillende maatregelen getroffen die ten doel hebben het tijdig onderkennen van terroristische dreigingen en het voorkomen van op handen zijnde terroristische aanslagen. De maatregelen die voortvloeien uit het voorliggende wetsvoorstel dienen om hieraan eveneens een bijdrage te leveren[1].
Niet alleen in de inlichtingen- en veiligheidssfeer zijn maatregelen getroffen. Politie en Justitie hebben de afgelopen jaren meer bevoegdheden toegekend gekregen, waarbij een verschuiving is opgetreden van het creëren van bevoegdheden op het gebied van opsporing en vervolging, naar het creëren van bevoegdheden op het gebied van (criminaliteits)preventie, gestuurd door informatie. De precieze omvang en inhoud van eerdere maatregelen op het gebied van veiligheid is echter onduidelijk[2].

Aan de andere kant bestaat bij instellingen binnen het bedrijfsleven, maar ook binnen de overheid, de neiging om in het kader van efficiëntie (van dienstverlening) en klantvriendelijkheid met gebruikmaking van de technologische ontwikkelingen steeds meer gegevens van burgers te verzamelen, te gebruiken en uit te wisselen, veelal voor goede doeleinden. Tevens wordt de verplichting gecreëerd gegevens gedurende een bepaalde tijd te bewaren, zoals ingevolge de Wet implementatie Europese Richtlijn Dataretentie in de telecommunicatiesector. Hierdoor ontstaan grote hoeveelheden opgeslagen gegevens.
Het risico bestaat dat de gegevensstromen, ook al worden deze met de beste bedoelingen ingericht, door de combinatie van de omvang van de bestanden met de verregaande toepassingsmogelijkheden van ICT leiden tot een disproportioneel volgen en controleren van de burger. De glazen samenleving die daarmee in het vizier komt, kan een negatieve invloed hebben op het vertrouwen van burgers in de overheid en brengt een zorgvuldige omgang met persoonsgegevens in gevaar.

De bevoegdheden voor de inlichtingen- en veiligheidsdiensten (verder: de diensten) persoonsgegevens in te winnen, terwijl de verantwoordelijke tot het verstrekken daarvan verplicht is, worden door middel van dit wetsvoorstel uitgebreid. Omdat dit wetsvoorstel er weer één extra is bovenop alle andere maatregelen die de afgelopen tijd zijn genomen, dient in de eerste plaats de noodzaak daartoe gedegen te zijn onderbouwd. Vervolgens dient het

[1] TK, 2005-2006, 30 553, nr. 3, p. 3
[2] Zie ook: Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse, Rapport van de Adviescommissie Informatiestromen Veiligheid (april 2007), p. 39 e.v.

wetsvoorstel voldoende waarborgen te bevatten om de risico's die het met zich brengt, te beperken. In dat kader zal het wetsvoorstel in het navolgende worden bezien.

2. Inhoud van het wetsvoorstel

Het wetsvoorstel Wijziging op de Wiv 2002 (verder: het wetsvoorstel) strekt ertoe bij te dragen aan de vergroting van de doelmatigheid en doeltreffendheid van de uitvoering van de taken die in de Wiv 2002 aan de diensten is opgedragen. Aanleiding hiervoor is dat in een aantal situaties de Wiv 2002 onnodig beperkend is bij de toepassing van de in de wet geregelde bijzondere bevoegdheden, of onvoldoende expliciet is waar het gaat om de toepassing van bepaalde methodieken voor gegevensverwerking, zoals data-analyse en de mogelijkheden tot het verkrijgen van rechtstreekse toegang tot bepaalde gegevensbestanden, aldus de Memorie van Toelichting[3].

Met dit doel voorziet het wetsvoorstel onder meer in de volgende maatregelen:
- een ruimere toegang tot gegevens bij (bij AMvB te bepalen) bestuursorganen, bepaalde personen en instanties in de vervoers- en financiële sector, waarbij op alle de plicht komt te rusten om aan een verzoek van de diensten tot verstrekking van gegevens te voldoen (de artikelen 17a en 29a van het wetsvoorstel);
- de reeds bestaande verplichtingen tot gegevensverstrekking in de sfeer van telecommunicatie wordt aangepast aan ontwikkelingen in die sector, met name op het vlak van internet: er wordt voorzien in een uitbreiding naar "aanbieders van een communicatiedienst" (de artikelen 28 en 29 van het wetsvoorstel);
- een explicitering in de wet van de mogelijkheid geautomatiseerde data-analyse uit te voeren met behulp van het rechtstreeks beschikbaar stellen van geautomatiseerde gegevensbestanden alsmede explicitering van de personen wier gegevens het kan betreffen (de artikelen 12a, 13, vijfde lid, 17, derde lid, 17a, derde lid en 29b van het wetsvoorstel).

3. Toepassing van de Wbp

Ingevolge (het huidige) artikel 17, derde lid, Wiv 2002 zijn de wettelijke voorschriften voor de verantwoordelijke voor een gegevensverwerking niet van toepassing op een verstrekking gedaan ingevolge een verzoek van de diensten. De wetgever heeft met deze bepaling niet alleen beoogd het vereiste van verenigbaar gebruik of de protocolplicht te omzeilen, maar hij heeft tevens het oog gehad op verplichtingen van de verantwoordelijke jegens een toezichthouder als het CBP[4]. Uitsluiting van de Wbp en aanpalende wetgeving voor dergelijke verwerkingen heeft echter, zeker nu het wetsvoorstel expliciet voorziet in rechtstreekse verstrekkingen aan de diensten zonder menselijke tussenkomst aan de zijde van de verantwoordelijke, de volgende consequenties.

[3] TK, 2005-2006, 30 553, nr. 3, p. 3
[4] TK 1997-1998, 25 877, nr. 3, p. 23-24

De transparantie van de gegevensverwerkingen voor de burgers die het betreft wordt ondergraven zodra sprake is van een verstrekking van gegevens aan één van de diensten. Niet wordt vastgelegd welke gegevens worden verstrekt, noch kan de burger zijn rechten op basis van de Wbp laten gelden tegenover de verantwoordelijke waar het de aan de diensten verstrekte gegevens betreft. Daarvoor moet uitgeweken worden naar de daartoe strekkende bepalingen in de Wiv 2002.

De verantwoordelijke is in het geval van een verplichte verstrekking niet gerechtigd naar aanleiding van het verzoek van de diensten een afweging te maken tussen het belang van de burger de gegevens niet te verstrekken en het algemeen belang deze wel te verstrekken. Evenmin kan een verantwoordelijke de integriteit en kwaliteit van de gegevens garanderen indien hij verplicht wordt gesteld alle gegevens te verstrekken, nu hij ook die op de Wbp gebaseerde afweging niet kan maken. Niet in de laatste plaats doet zich de vraag voor of, indien enerzijds de Wbp niet van toepassing is en anderzijds deze verstrekkingsverplichting geldt, dit impliceert dat een verantwoordelijke met een beroepsgeheim geen beroep meer kan doen op zijn geheimhoudingsplicht.

Het CBP kan ingevolge artikel 2, tweede lid, onder b, Wbp geen invulling geven aan zijn bevoegdheden waar het het toezicht betreft op de verwerking van persoonsgegevens bij de verstrekkende verantwoordelijken wanneer sprake is van een verwerking door, maar ook ten behoeve van de diensten. Het is aan de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) om toe te zien op de rechtmatigheid van het deel van de verwerking van persoonsgegevens dat *ten behoeve van* de diensten plaatsvindt.

4. Noodzaak

In de Memorie van Toelichting bij het wetsvoorstel wordt aangegeven dat de Wiv 2002 thans onnodig beperkend is bij de toepassing van reeds in de wet geregelde bijzondere bevoegdheden, of "onvoldoende expliciet waar het gaat om de (mogelijkheden tot) toepassing van bepaalde methodieken voor gegevenverwerking, zoals data-analyse en de mogelijkheid tot het verkrijgen (c.q. verlenen) van rechtstreekse toegang tot bepaalde gegevensbestanden. Een aanpassing en aanvulling van de wettelijke regeling met betrekking tot deze en enkele andere onderwerpen, zou wezenlijk kunnen bijdragen aan een effectiever en efficiënter functioneren van de diensten"[5]. De verschillende aanslagen die hebben plaatsgevonden, waaronder die op Theo van Gogh, "hebben bovendien meer dan ooit duidelijk gemaakt dat de mogelijkheden tot het tijdig onderkennen van terroristische dreigingen en het waar mogelijk voorkomen van op handen zijnde terroristische aanslagen dienen te worden vergroot"[6]. De diensten worden, zo vervolgt de Memorie van Toelichting, door middel van de voorgestelde maatregelen beter in staat gesteld hun taken uit te voeren.

[5] TK, 2005-2006, 30 553, nr. 3, p. 3)
[6] idem

Aandacht is besteed aan artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet (GW) teneinde de verruiming van de bevoegdheden van de diensten te kunnen rechtvaardigen waar deze inbreuk maken op de bescherming van de persoonlijke levenssfeer van burgers[7]. Artikel 10 GW stelt dat behoudens bij of krachtens de wet een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, terwijl artikel 8 EVRM slechts dan een beperking op het recht op privacy toestaat indien dit bij wet is voorzien en deze beperking in een democratische samenleving noodzakelijk is in het belang van - in dit geval - de nationale veiligheid.

Bij de beoordeling van de noodzaak van de voorgestelde maatregelen in het belang van de nationale veiligheid, dient naar het oordeel van het CBP de vraag centraal te staan of is aangetoond dat de reeds bestaande bevoegdheden voor het beoogde doel, te weten de vergroting van de doelmatigheid en doeltreffendheid van de uitvoering van de taken die de diensten is opgedragen, niet voldoen. Dit betreft niet alleen de voorgestelde bevoegdheid verantwoordelijken te verplichten gegevens desgevraagd te verstrekken, maar eveneens de bevoegdheid via rechtstreekse verbindingen gegevensbestanden binnen te halen ten behoeve van data-analyse, terwijl deze data-analyse alle burgers kan betreffen.

De onderbouwing van de noodzaak in het belang van de nationale veiligheid om ruimere toegang te verkrijgen tot gegevens bij bestuursorganen en bij bepaalde personen en instanties, op welke tevens de plicht komt te rusten om aan een verzoek tot verstrekking van gegevens te voldoen, houdt feitelijk niet meer in dan dat thans geen sprake is van een dekkend informatiestelsel. Ter vergelijking wordt in de Memorie van Toelichting aangegeven dat uitsluitend met betrekking tot de klassieke aanbieders van openbare telecommunicatienetwerken en -diensten dit wel het geval is. De Minister van Binnenlandse Zaken en Koninkrijksrelaties (verder: de Minister) zet dit eveneens uiteen in het nader rapport: het is onwenselijk dat gegevens slechts (enkele uitzonderingen daargelaten) op basis van vrijwilligheid ter beschikking kunnen komen, terwijl de vrijwillige arrangementen op basis waarvan verstrekkingen plaatsvinden elk individueel voldoen, maar als geheel niet voorzien in de informatie waaraan de diensten in het kader van hun goede taakuitvoering behoefte hebben[8].

Het CBP acht op grond van het voorgaande de noodzaak van de voorgestelde maatregelen in het belang van de nationale veiligheid onvoldoende onderbouwd. Zeker waar het de (eveneens door de Raad van State in zijn advies gesignaleerde) opmerking betreft dat bestaande vrijwillige arrangementen elk individueel wel zouden voldoen, in relatie tot de opmerking van de Minister tijdens de algemene beraadslaging in de Tweede Kamer van het wetsvoorstel dat het opstellen van vrijwillige convenanten veel administratieve lasten veroorzaakt[9]. Dit klemt des te meer nu in de Nota naar aanleiding van het verslag aangegeven wordt dat het invoeren van een verstrekkingsverplichting voor enkele specifieke categorieën "wenselijk" is, alsmede dat het

[7] TK, 2005-2006, 30 553, nr. 3, p. 19 e.v.
[8] Advies Raad van State en Nader Rapport, TK, 2005-2006, 30 553, nr. 4, p. 2
[9] TK 9, 9-552, 4 oktober 2007

"wenselijk" is dat de informatie die wordt aangeleverd volledig is met het oog op data-analyse[10]. Wenselijk is echter iets anders dan noodzakelijk. Gelet op het voorgaande lijken niet zozeer proportionaliteit en subsidiariteit afgewogen, maar lijkt veeleer sprake te zijn van meer praktische overwegingen. Dit blijkt ook uit het volgende.

Het opleggen van een informatieverplichting zal gelden voor alle tot een bepaalde categorie behorende bestuursorganen alsmede instanties binnen de vervoers- en financiële sector die bij AMvB zullen worden aangewezen. Nut en noodzaak van de voorhanden zijnde gegevens zullen leidend zijn bij de aanwijzing van deze categorieën[11]. De eis van de rechtsgelijkheid brengt, naar het oordeel van de regering, met zich dat de informatieverplichting voor alle tot een bepaalde categorie behorende instanties geldt[12]. Waar het dan vervolgens de afweging van de proportionaliteit betreft, wordt opgemerkt dat "een informatieverplichting naar zijn aard een bevoegdheid [is] die minder ingrijpend is in de persoonlijke levenssfeer van burgers dan het verkrijgen van gegevens door middel van de toepassing van andere bijzondere bevoegdheden, zoals de inzet van agenten of het aftappen van gesprekken met een technisch hulpmiddel"[13]. Hier lijkt voorbij te zijn gegaan aan de omstandigheden dat een informatieverplichting zoals voorgesteld per definitie meer gegevens van meer burgers zal betreffen, alsmede een groter aantal verantwoordelijken dan voorheen het geval was, en dat bovendien ook nog sprake zal kunnen zijn van rechtstreekse toegang tot de gegevensbestanden ten behoeve van data-analyse, met alle risico's die daarmee samen gaan. Daarnaast is thans niet duidelijk welke categorieën van bestuursorganen en personen en instellingen binnen de vervoers- en financiële sector, alsmede welke gegevens binnen de communicatiesector het betreft, zodat op dat punt proportionaliteit noch subsidiariteit kunnen worden afgewogen.
Van een minder ingrijpende toepassing voor burgers is dan ook naar het oordeel van het CBP geen sprake. Zoals het CBP in 2001 reeds heeft opgemerkt[14] geldt ook hier dat een proportioneel gebruik van de voorgestelde bevoegdheden sterk dient te worden aangezet, terwijl daarvoor nadere begrenzingen noodzakelijk zijn. Het CBP achtte een grotere terughoudendheid op zijn plaats bij het opleggen van meewerkingsverplichting van de voor de verwerking van persoonsgegeven verantwoordelijke instanties. Deze opmerking is nog steeds actueel.

De reeds bestaande bevoegdheden, in samenhang bezien met eerdere maatregelen die strekken tot het vorderen van gegevens in zijn algemeenheid, lijken niet per definitie ontoereikend te zijn. Complicerend in dit verband is evenwel dat "geen totaaloverzicht van bestaande wet- en regelgeving met betrekking tot het inwinnen van gegevens uit externe databases"[1] bestaat[15]. Dit is een belangrijk gegeven omdat op basis van die bestaande wet- en regelgeving en de bevoegdheden die daaruit voortvloeien bezien dient te worden of de bestaande bevoegdheden

[10] TK, 2006-2007, 30 553, nr. 7, p. 7
[11] TK, 2005-2006, 30 553, nr. 3, p. 9
[12] TK, 2006-2007, 30 553, nr. 7, p. 8
[13] idem
[14] Advies op het Rapport Commissie Strafvorderlijke gegevensvergaring (z2001-00735), 18 oktober 2001, p. 1
[15] Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse, Rapport van de Adviescommissie Informatiestromen Veiligheid (april 2007).

voldoen, en zo nee, op welke punten niet. In dit geval geldt de vraag of ondanks optimale inzet van de reeds bestaande bevoegdheden het niet mogelijk is gebleken om op effectieve wijze de veiligheid te beschermen.

Dit gegeven alsmede de door de Tweede Kamer op 27 november 2007 aangenomen motie van het lid Pechtold, waarin opgemerkt wordt dat de meeste anti-terrorismemaatregelen geen horizonbepaling en evaluatiemoment kennen, wijzen erop dat de wetgever geen zicht heeft op (de effectiviteit van) bestaande bevoegdheden. De vraag die zich in dit kader voordoet is dan ook wie het overzicht heeft over welke informatiestromen uit grote gegevensbestanden, waar, waarom en door wie in het kader van de nationale veiligheid worden opgevraagd en verwerkt en hoe in de beveiliging daarvan is voorzien. Vervolgens dient de vraag te worden beantwoord of inzicht kan worden gegeven in de mate waarin en in de effectiviteit waarmee via profilering en datamining van bulkgegevens, van grote daartoe opgevraagde bestanden met gegevens van veelal onverdachte mensen gebruik wordt gemaakt.

In het licht van het vorenstaande adviseert het CBP het wetsvoorstel kritisch te beschouwen. Het vermoeden dat de informatievergaring niet dekkend is of de wens structureel de beschikking te hebben over actuele gegevens, is naar het oordeel van het CBP niet voldoende om de noodzaak van deze maatregelen in het belang van de nationale veiligheid aannemelijk te maken.

5. Consequenties van de voorgestelde maatregelen

In groter verband bezien bevatten de voorgestelde maatregelen risico's en gevolgen voor de verantwoordelijken, voor de diensten en bovenal voor de burger.

5.1 Aanwijzing bij AMvB
Voor bestuursorganen, de sector vervoer alsmede de sector financiële diensten is bepaald dat de nadere bepaling van categorieën van personen en instellingen waarop een verplichting kan komen te rusten gegevens te verstrekken, bij AMvB geschiedt. Ten aanzien van communicatiediensten, die gelijkgeschakeld worden met telecommunicatiediensten waarvoor een verplichting gegevens desgevraagd te verstrekken reeds bestond, kan in een AMvB een nadere aanduiding van te verstrekken gegevens worden aangegeven.

Het principe van kenbaarheid is met het voornemen bij AMvB nadere invulling te geven aan het wetsvoorstel in dit geval geenszins gediend. Het betekent immers niet alleen onduidelijkheid voor de sectoren die het betreft, maar ook voor de burger, terwijl de Minister aanzienlijke speelruimte heeft om invulling te geven aan deze categorieën. Bovendien schuilt hierin het risico dat de drempel de categorieën uit te breiden, lager ligt dan indien deze zouden zijn neergelegd in het wetsvoorstel zelf.

Nut en noodzaak van de voorhanden zijnde gegevens voor een goede taakuitvoering van de diensten dienen bij de aan te wijzen categorieën aanwezig te zijn[16]. Nu de noodzaak van de

[16] TK, 2005-2006, 30 553, nr. 3, p. 9

voorgestelde maatregelen zelf onvoldoende is onderbouwd, geeft de stelling dat nut en noodzaak van de bij de aan te wijzen categorieën dienstverleners voorhanden zijnde gegevens bepalend dient te zijn, weinig vertrouwen.

5.2 Beveiliging

In het wetsvoorstel is geen bepaling opgenomen met betrekking tot het beveiligingsniveau bij de verantwoordelijken, noch voor de gegevensverstrekking door de verantwoordelijke door middel van menselijke tussenkomst, noch wanneer deze plaatsvindt zonder menselijke tussenkomst aan de zijde van de verstrekkende verantwoordelijke (zijnde de mogelijkheid van rechtstreekse toegang tot geautomatiseerde gegevensbestanden). Slechts ten aanzien van de aan te wijzen bestuursorganen worden bij AMvB nadere regels gesteld met betrekking tot de ter zake door het bestuursorgaan te treffen technische en organisatorische maatregelen.

Teneinde de integriteit en kwaliteit van de te verstrekken gegevens ten behoeve van de verdere analyses te kunnen bewaken, is goede beveiliging noodzakelijk. Dit is niet alleen in het belang van de diensten, maar ook in het belang van de burger; onjuiste gegevens of gegevens die onvolledig zijn kunnen immers een vertekend beeld geven. Daarnaast dient opgemerkt te worden dat voor de verwerking van gevoelige gegevens, wegens de aard van die gegevens, een hoger beschermingsniveau nodig is.
Hoewel artikel 13 Wbp een passend beveiligingsniveau voorschrijft voor de verwerking van gegevens door de verantwoordelijke, lijkt ook dit artikel niet van toepassing te zijn bij een verstrekking ten behoeve van de diensten. Het CBP constateert dan ook een manco in het wetsvoorstel.

5.3 Data-analyse

Bedrijven en instellingen, zowel in de publieke als in de private sector, hebben de neiging om steeds meer persoonsgegevens te verzamelen, te gebruiken en uit te wisselen. Daarnaast worden ook wettelijke verplichtingen geschapen om gegevens gedurende een bepaalde periode te bewaren. Het wetsvoorstel schept de mogelijkheid voor de diensten om rechtstreekse geautomatiseerde toegang te verkrijgen tot de gegevens die bij de aangezochte persoon of instantie berusten: hiermee wordt een *on line- en real time* verbinding bedoeld, waarbij zonder menselijke tussenkomst gegevens verstrekt kunnen worden[17]. Op deze wijze kan een grote hoeveelheid gegevens vergaard worden uit externe databases, mede ten behoeve van data-analyse. Deze combinatie leidt tot consequenties die niet of niet voldoende lijken te zijn onderkend.

In de eerste plaats heeft deze combinatie tot gevolg dat de diensten steeds meer gegevens zullen moeten analyseren om de eenvoudige reden dat steeds meer gegevens beschikbaar zijn; zoeken naar een speld in een hooiberg. Het is niet aannemelijk dat de effectiviteit van het doorzoeken van informatie hiermee gediend is. Gewaarschuwd dient dan ook te worden voor de hooggespannen verwachtingen van technologische toepassingen en de verplichting die op verantwoordelijken kan worden gelegd. Dit geldt evenzeer voor de volgende punten.

[17] TK, 2005-2006, 30 553, nr. 3, p. 27

In de tweede plaats is niet gegarandeerd dat de kwaliteit van de gegevens die worden binnengehaald, van dien aard is dat daaruit, op zichzelf of in samenhang met andere gegevens bezien, conclusies kunnen worden getrokken die overeenkomen met de werkelijkheid. Hierin schuilt een groot risico voor de burger. Gegevens kunnen immers in een andere context dan waarin zij verzameld zijn of bewaard worden, een volstrekt onjuist beeld geven van die burger of groep burgers. Het risico op valse positieve en valse negatieve uitkomsten is aanzienlijk. Dit is schadelijk voor die betreffende burger(s), maar ook schadelijk voor de samenleving als geheel omdat hierdoor het vertrouwen van de burgers in de overheid wordt aangetast. De vraag is dan ook, gelet op die mogelijke onwenselijke gevolgen, of het middel data-analyse reeds voldoende is ontwikkeld voor gebruik in het veiligheidsdomein.

Data-analyse bergt in de derde plaats ook het risico van zogenaamde function creep in zich: enerzijds worden technologieën die aanvankelijk gericht waren op een bepaalde doelgroep, in casu degenen die een gevaar vormden voor de nationale veiligheid, gaandeweg toegepast op (bijna) iedereen, terwijl anderzijds verzamelde gegevens voor een bepaald doel ten behoeve van een ander doel verstrekt en verwerkt worden. In het wetsvoorstel wordt geëxpliciteerd dat data-analyse een ieder kan betreffen (artikel 13, vijfde lid in het wetsvoorstel). Binnen de Artikel 29-werkgroep is in het kader van de Richtlijn Dataretentie (2006/24/EG) het standpunt ingenomen dat de mogelijkheid van datamining op de communicatie- en bewegingspatronen van onverdachte personen zou moeten worden uitgesloten[18]. Het CBP heeft in het kader van de begrenzing van de toegang tot bewaarde gegevens eveneens op dit standpunt gewezen in zijn advies op het Wetsontwerp implementatie Europese Richtlijn Dataretentie d.d. 22 januari 2007. Wat betreft function creep in het kader van doelbinding dient opgemerkt te worden dat met name overheidsinstanties over gegevens van burgers kunnen beschikken op grond van een wettelijke verplichting tot het uitoefenen van een specifieke overheidstaak. In het doelgebonden gebruik zijn de nodige waarborgen voor die burger gelegen, die door het gebruik van data-analyse teniet worden gedaan.

6. Waarborgen voor de burger

Uit het bovenstaande blijkt dat onvoldoende rekenschap is gegeven van de nadelen en risico's die zijn verbonden aan de voorgestelde maatregelen. Daardoor is onvoldoende inzichtelijk welke waarborgen adequaat zijn. Dit klemt des te meer nu de Wbp en aanpalende wetgeving niet van toepassing is op de verstrekkingen ten behoeve van de diensten, zodat de burger daar, waar het zijn waarborgen aangaat, geen beroep op kan doen.

Ten aanzien van de bijzondere bevoegdheden, waar de artikelen 28 Wiv 2002 e.v. onder vallen, bestaat een wettelijk verankerd toetsingskader (artikel 31 Wiv 2002), de verplichting een verslag te maken van de uitoefening van een bijzondere bevoegdheid (artikel 33 Wiv 2002) en een onafhankelijke toezichthouder, de CTIVD. Behalve het toezicht door de CTIVD, zijn de andere twee waarborgen niet van toepassing op de verruiming van de verstrekking door bestuursorganen (artikel 17a in het wetsvoorstel).

[18] Artikel 29 WP, opinie 3/2006, 25 maart 2006, p. 3

Het CBP wijst er in dit kader nogmaals op dat in het wetsvoorstel niet is voorzien in een beveiligingsbepaling, noch in een evaluatie- en/of horizonbepaling.

7. Conclusie

De noodzaak de voorgestelde maatregelen in het belang van de nationale veiligheid in te voeren is onvoldoende onderbouwd. Omdat de precieze invulling van de in het wetsvoorstel genoemde sectoren alsmede de aard van de gegevens van communicatiediensten onzeker is, kan noch de proportionaliteit noch de subsidiariteit van die invulling beoordeeld worden. Niet is aannemelijk gemaakt dat de huidige bevoegdheden onvoldoende mogelijkheden bieden de taken effectief uit te voeren. Bovendien baart het ontbreken van de proportionaliteit van de maatregelen, afgezet tegen de onduidelijkheid waar het de omvang van de reeds bestaande bevoegdheden betreft, zorgen. Dit terwijl de bij wet gestelde regels ten aanzien van de bescherming van persoonsgegevens opzij gezet worden indien sprake is van een verwerking ten behoeve van de diensten.

De mogelijkheid verantwoordelijken te verplichten op grote schaal gegevens te verstrekken, welke tevens met het oog op data-analyse kunnen worden verwerkt, heeft gevolgen voor de burger, maar ook voor de verantwoordelijken en de diensten. Deze gevolgen zijn niet, althans onvoldoende, onderkend. Bij AMvB wordt een aantal belangrijke elementen binnen dit wetsvoorstel ingevuld, waarover nu nog onduidelijkheid bestaat. De beveiliging van de gegevens is niet expliciet in het wetsvoorstel geregeld. De risico's die data-analyse met zich brengt zijn onderbelicht gebleven.
Juist omdat de risico's en nadelen onvoldoende aan bod zijn gekomen, kan niet beoordeeld worden of de waarborgen een adequaat tegengewicht bieden. Het is evenwel zeker dat het ontbreken van een beveiligingsbepaling en van een evaluatie- en/of horizonbepaling niet bijdraagt aan het benodigde evenwicht.

Het CBP beveelt dan ook aan het wetsvoorstel op bovenstaande opmerkingen nader te beschouwen, met name waar het de noodzaak van de voorgestelde maatregelen betreft. De nadelen en risico's die deze maatregelen meebrengen, zullen beter in kaart moeten worden gebracht. Alleen dan kunnen afwegingen van proportionaliteit en subsidiariteit worden gemaakt en kunnen de maatregelen op hun rechtmatigheid worden beoordeeld en worden voorzien van adequate waarborgen.