Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2006–2007

30 312 Algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het burgerservicenummer (Wet algemene bepalingen burgerservicenummer)

F

NADERE MEMORIE VAN ANTWOORD

Ontvangen 8 juni 2007

De leden van de commissie hebben, na lezing van de memorie van antwoord, nog nadere vragen en opmerkingen die voortborduren op de bezwaren die in het voorlopig verslag zijn geformuleerd.

De regering waardeert de grondige discussie over het voorliggende wetsvoorstel. Er is een verschil in perspectief merkbaar. De commissie meent dat het wetsvoorstel een fundamentele verschuiving van het beleid inzake de persoonsinformatiehuishouding inhoudt. De regering beoogt met het wetsvoorstel slechts een vernieuwing van het stelsel van persoonsnummers (van sofi-nummer naar burgerservicenummer) tot stand te brengen. Deze vernieuwing is ook belangrijk, maar veel minder omvattend.
In deze nadere memorie van antwoord poogt de regering ook antwoorden te geven op de vragen die gesteld zijn in het bredere kader van de persoonsinformatiehuishouding en die niet direct voortvloeien uit het wetsvoorstel maar die natuurlijk wel van belang zijn.

Op 17 april 2007 werd door ambtenaren van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een technische presentatie gegeven aan leden van de Eerste Kamer over de «Landkaart», waarop algemene informatie over het gebruik van het BSN zal worden zichtbaar gemaakt. Tijdens deze presentatie bleek behoefte aan een actuele beschrijving van de gegevensuitwisseling in de sector werk en inkomen in Nederland en aan een vergelijking met de Belgische situatie, in het bijzonder de Kruispuntbank. De bedoelde beschrijving, die ik u mede namens de minister van Sociale Zaken en Werkgelegenheid aanbiedt, treft u aan in de bijlage bij deze nadere memorie van antwoord.

De invoering van het burgerservicenummer (BSN) is van groot belang voor de informatiehuishouding van de overheid, maar is daarnaast ook onontbeerlijk voor de totstandkoming van elektronische gegevensuitwisseling in de zorgsector. De regering hoopt daarom dat de beantwoording van de vragen, de mondelinge toelichting op de «Landkaart» en de in de bijlage opgenomen informatie bijdragen aan de voorspoedige voortzetting van de behandeling van het onderhavige wetsvoorstel.

KST107717
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2007

2. Het karakter van het wetsvoorstel

De commissie sprak in het voorlopig verslag haar zorg uit over het kaderstellende karakter van het wetsvoorstel, waarbij het materialiseren van de wet in formele zin wordt overgelaten aan lagere wetgeving. Die zorg is niet weggenomen door de memorie van antwoord, terwijl het toch gaat om in grondwettelijke opdracht te beschermen grondrechten. De commissie meent dat de systematiek van een kaderwet zekere praktische voordelen biedt, maar dat voorbij gegaan wordt aan de vaststelling dat het om de bescherming van een grondrecht gaat.

Wellicht kan het karakter van het wetsvoorstel verduidelijkt worden door aan te geven wat het niet is. Het wetsvoorstel biedt géén algemene grondslag voor het verwerken van persoonsgegevens. Het voorstel is géén «kaderwet» in die zin. De materiële regels over de verwerking van persoonsgegevens zijn op dit moment neergelegd in de Wet bescherming persoonsgegevens (Wbp) en in sectorale wetgeving[1]. Dat verandert niet met de invoering van het BSN. Het onderhavige wetsvoorstel voegt daar enkele materiële regels aan toe, als bij de verwerking het BSN wordt gebruikt. Zie met name de artikelen 10 (de bevoegdheid voor overheidsorganen om het BSN te gebruiken), 11 (de verplichting om onder omstandigheden het BSN te vermelden), 12 (de vergewisplicht voor gebruikers) en 13 (het recht van de burger om geen ander nummer te verstrekken). Bij al deze artikelen is géén delegatiegrondslag voor lagere regelgevers opgenomen.
Het wetsvoorstel kent buiten de overheid alleen gebruikers van het BSN voor zover dit gebruik bij of krachtens de wet (in formele zin) is voorgeschreven. De Aanpassingswet BSN zal bestaande gevallen waarin het gebruik van het sofi-nummer is voorgeschreven, omzetten in gebruik van het BSN. Voor verdere uitbreiding moet een grondslag in een wet in formele zin worden gecreëerd. Het voorstel voor een Wet gebruik burgerservicenummer in de zorg is daarvan een voorbeeld[2]. Het parlement is bij een dergelijke uitbreiding als medewetgever volledig betrokken.

Het wetsvoorstel bevat verder regels over het stelsel als zodanig. Meer in het bijzonder zijn dat regels over het aanmaken, ter beschikking stellen en toekennen van het BSN, over het bieden van faciliteiten om de vergewisplicht uit te voeren, over sectorale berichtenvoorzieningen en over de informatievoorziening aan de burger[3]. Bij deze regels is wel delegatie toegepast. De delegatie betreft de vaststelling van nadere (technische) regels, zoals regels over het uitwisselingsformat. Het vaststellen van deze regels op een lager niveau biedt inderdaad praktische voordelen. Er is vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer geen bezwaar tegen om deze nadere, veelal technische, regels bij of krachtens algemene maatregel van bestuur vast te stellen.
De kern van de bescherming van de persoonlijke levenssfeer ligt immers in materiële bepalingen. Zoals gezegd zijn deze regels vastgelegd in de Wbp en in sectorwetgeving. Daarin wordt (onder meer) geregeld of en in welke gevallen persoonsgegevens vastgelegd en uitgewisseld mogen worden, dat de gegevens beveiligd moeten worden rekening houdend met de stand van de techniek en dat de gegevens niet verder verwerkt mogen worden op een wijze die onverenigbaar is met het doel waarvoor ze zijn verkregen. In de Wbp worden bovendien de rechten van de burger inzake de verwerking geregeld, zoals het recht op informatie over de gegevensverwerking, op correctie en op verzet[4]. Het voorliggende wetsvoorstel doet geen afbreuk aan het – reeds in bestaande wetgeving neergelegde – niveau van bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens.

[1] Er zijn vele sectorwetten die regels bevatten over gegevensverwerking. In de memorie van antwoord is al gewezen op de Zorgverzekeringswet (hoofdstuk 8, gegevensverstrekking) en de Wet structuur uitvoeringsorganisatie werk en inkomen (hoofdstuk 9, informatiebepalingen). Zie Kamerstukken I 2006/07, 30 312, D, blz. 3.
[2] Voorstel van Wet gebruik burgerservicenummer in de zorg (Kamerstukken I, 30 380).
[3] De memorie van antwoord beschrijft het onderscheid in de twee typen regels en geeft van beide typen een uitgebreide beschrijving. Zie het antwoord op de vraag van de leden van de CDA-fractie inzake het kaderstellende karakter van het wetsvoorstel (Kamerstukken I 2006/07, 30 312, D, blz. 2 e.v.).
[4] De Wbp dekt niet het gehele veld van persoonsregistraties. Zo zijn de rechten van de burger inzake de bevolkingsboekhouding vastgelegd in de Wet gemeentelijke basisadministratie persoonsgegevens.

3. De regie over de informatie

De commissie meent dat het wetsvoorstel een fundamentele ontwerpkeuze behelst, waarbij de overheid optreedt als regisseur van persoonsgegevens in plaats van de burger in kwestie. De commissie stelt in dat verband de volgende vragen. Klopt het dat het technisch zeer wel mogelijk is de burger de autonomie en het toezicht te laten behouden over diens eigen gegevens? Is boven de gekozen optie, het zogenaamde opt-in scenario niet verreweg te prefereren? Daarbij krijgt immers een burger, die bijvoorbeeld een uitkering wil aanvragen vooraf inzicht in welke informatie door welke partijen hoe lang gebruikt gaat worden in de aanvraagprocedure.

De commissie ziet in het wetsvoorstel een fundamentele keuze voor de overheid als «regisseur van persoonsgegevens». De commissie doelt met de «regisseur» wellicht op degene die bepaalt of persoonsgegevens worden verzameld, of en hoe ze worden vastgelegd, of en tussen wie ze worden uitgewisseld, wie recht heeft op inzage en correctie en zo meer. Over deze belangrijke aspecten van het beleid van de overheid inzake de persoonsinformatiehuishouding kan, los van het wetsvoorstel, het volgende worden opgemerkt.
De overheid heeft in verband met de persoonsinformatiehuishouding vele gedaanten. Er liggen zowel bij de overheid als bij de burger elementen van «regie». Enkele voorbeelden kunnen dit verhelderen.
De overheid stelt als wetgever normen over het verwerken van persoonsgegevens. Voor vrijwel alle verwerking van persoonsgegevens geldt de Wet bescherming persoonsgegevens (Wbp). De Wbp regelt in welke gevallen gegevens verwerkt mogen worden en stelt (onder meer) regels over verdere verwerking en beveiliging. De Wbp geeft de burger «regie» in die zin dat de burger recht heeft op inzage en correctie van gegevens. In geval van bijzondere persoonlijke omstandigheden is de «regie» sterker en kan de burger verzet aantekenen tegen (bepaalde) gegevensverwerkingen.
De overheid regelt ook als wetgever de bevolkingsboekhouding (Wet GBA). In termen van «regie» bepaalt de wetgever welke gegevens worden opgenomen en welke gegevens wanneer aan wie worden verstrekt. De burger heeft «regie» in die zin dat hij de over hem verzamelde gegevens kan inzien en kan laten corrigeren. Onder bijzondere omstandigheden is het voor de burger mogelijk om in plaats van zijn woonadres een briefadres op te geven. Deze mogelijkheid is er voor mensen die wonen in een instelling waarvan de aard meebrengt dat door opneming van het adres daarvan, de persoonlijke levenssfeer ernstig kan worden geschaad. In andere bijzondere omstandigheden worden op verzoek van de burger bepaalde gegevens verwijderd uit de GBA (bijvoorbeeld bij geslachtswijziging). Verstrekkingen uit de GBA aan andere overheidsorganen kan de burger over het algemeen niet blokkeren. De Wet GBA geeft hem onder omstandigheden wel «regie» door het bieden van de mogelijkheid om gegevensverstrekkingen aan niet-overheidsorganen tegen te houden.
De overheid die in de gedaante van het UWV vaststelt of een persoon recht heeft op een uitkering krachtens de Wet werk en inkomen naar arbeidsvermogen (WIA) doet dit met inachtneming van tal van regels op grond van de WIA. Die wet kent een bijzondere regeling in verband met het toezenden van medische gegevens aan de werkgever. De wetgever heeft daar de «regie» van de burger vergroot door te bepalen dat de gegevens slechts worden toegezonden als de werknemer daarvoor toestemming heeft gegeven (een «opt-in» constructie).
De overheid, nu als college van burgemeester en wethouders dat beslist op de aanvraag van een uitkering op grond van de Wet werk en bijstand (Wwb), zamelt gegevens in overeenkomstig de regels in en op grond van de Wwb. Bovendien moet het college de nieuwe regelgeving in verband

met de GBA als basisregistratie in acht nemen. Die regelgeving verplicht het college om – behoudens uitzonderingen – gegevens niet aan de burger te vragen, maar deze indien mogelijk uit de GBA te halen. Er is dan géén «regie» van de burger in die zin dat hij kan bepalen of hij de gegevens wil verstrekken.

Deze voorbeelden laten zien dat de persoonsinformatiehuishouding en daarmee de «regie» over de persoonsgegevens, is vastgelegd in vele wetten en andere regels en steeds is toegesneden op de omstandigheden van het geval. De gegeven beschrijvingen zijn van toepassing ongeacht of wel of niet een persoonsnummer als het sofi-nummer of het BSN wordt gebruikt.

Er is niet één wet die de gehele persoonsinformatiehuishouding omspant – en zeker niet de Wet algemene bepalingen burgerservicenummer. Het wetsvoorstel beoogt niet om een fundamentele wijziging in die huishouding aan te brengen – dat zou met het wetsvoorstel ook niet kunnen. Het wetsvoorstel regelt een stelsel van persoonsnummers. Dat lijkt bescheiden, maar het is een belangrijk hulpmiddel voor een goede persoonsinformatiehuishouding.

Het beleid inzake de persoonsinformatiehuishouding is overigens in beweging. Hiervoor werd reeds de ontwikkeling van basisregistraties genoemd[1]. Door het inrichten van basisregistraties kan een overheidsorgaan de gegevens die het nodig heeft voor zijn taak uit dergelijke registraties halen en hoeft het orgaan niet (nogmaals) de gegevens aan de burger te vragen. Het BSN heeft daarbij ook een rol: als hulpmiddel voor een foutloze uitwisseling van persoonsgegevens tussen overheidsorgaan en basisregistratie.

Een andere ontwikkeling die genoemd kan worden is de persoonlijke internetpagina (PIP). Met behulp van zijn PIP kan een burger bijvoorbeeld inzage krijgen in de gegevens die over hem zijn opgenomen in verschillende gegevensverzamelingen van de overheid, zoals in de GBA. Een dergelijke PIP biedt de burger een handzaam hulpmiddel bij het voeren van de «regie» over zijn gegevens.

De commissie vraagt waarom gekozen is voor een systeem van vrijelijk communicerende vaten en is gebroken met de lange traditie van doelbinding en zelfbeschikking bij actualisering en selectie. Is het niet zuiverder om schotten te zetten tussen de gegevens voor de verschillende rollen van de overheid?

Een overheidsorgaan dient niet méér persoonsgegevens te verzamelen dan hij nodig heeft voor de uitvoering van zijn taak. Als gegevens voor bepaalde doeleinden zijn verkregen mogen ze niet worden verwerkt op een wijze die met die doelen onverenigbaar is. De gegevens moeten worden beveiligd tegen onrechtmatige verwerking, zoals ongeoorloofde inzage. Deze uitgangspunten verdienen een wettelijke verankering – en die hebben ze ook gekregen in (onder meer) de Wbp (zie de artikelen 6 tot en met 13 Wbp).

Het is goed dat er schotten staan in het veld van overheidsinformatie, die belemmeren dat gegevens die de overheid in de ene rol verzameld heeft, in een andere rol worden gebruikt. Dat volgt ook uit het beginsel van doelbinding zoals neergelegd in de Wbp. Om bij het voorbeeld te blijven dat de commissie voorlegt: als een burger medische gegevens aan het UWV verstrekt inzake zijn aanvraag voor een uitkering op grond van de WIA, dienen die gegevens niet gebruikt te worden door het UWV als werkgever van de betrokkene.

[1] Zie bijvoorbeeld de wet tot wijziging van de Wet gemeentelijke basisadministratie persoonsgegevens in verband met de aanpassing aan de eisen die gelden voor basisregistraties (kamerstukken 30 514). Het wetsvoorstel is op 28 september 2006 zonder beraadslaging en zonder stemming aangenomen door de Tweede Kamer. De Eerste Kamer heeft het voorstel op 31 oktober 2006 als hamerstuk afgedaan. Zie ook het voorstel van wet houdende regels omtrent een basisregister van ondernemingen en rechtspersonen (Kamerstukken 30 656).

Het wetsvoorstel laat al deze uitgangspunten en de wettelijke verankering daarvan onverlet. De veronderstelling van de commissie dat het wetsvoorstel er toe strekt dat het gebruik van persoonsgegevens vrij is gegeven en dat het beginsel van doelbinding is verlaten, is onjuist.
Het beginsel van zelfbeschikking heeft zijn uitdrukking gevonden in het recht van de burger op (onder meer) inzage en correctie. In bijzondere gevallen heeft de wetgever de betrokkene het recht toegekend om bepaalde gegevensverwerking te doen beëindigen. Het wetsvoorstel brengt hier geen verandering in aan.

De commissie vraagt of de regering op de hoogte is van onderzoek zoals het recente proefschrift van dr. Wouter Teepe, «Reconciling Information Exchange and Confidentiality», dat een methode omschrijft om privacy en informatie-uitwisseling te harmoniseren.

Dr. Teepe beschrijft in zijn proefschrift een methode om informatie uit te wisselen, waarbij alleen de nodige gegevens worden uitgewisseld en niet méér dan die gegevens. Een voorbeeld kan zijn de uitwisseling van gegevens in het kader van terrorismebestrijding[1]. Stel, de Verenigde Staten beschikken over een lijst met gegevens van (mogelijke) «terroristen». Een luchtvaartmaatschappij beschikt over een lijst met gegevens over de passagiers van een vliegtuig. Om te bezien of er terroristen aan boord van het vliegtuig zijn kan de luchtvaartmaatschappij haar lijst met passagiersgegevens aan de (personen belast met de grensbewaking van de) Verenigde Staten geven, of kan de Verenigde Staten de lijst met gegevens over de terroristen aan de luchtvaartmaatschappij geven. Dr. Teepe werkt een andere mogelijkheid uit, waarbij noch de Verenigde Staten de kennis krijgen over de gegevens van alle passagiers, noch de luchtvaartmaatschappij de gegevens over alle terroristen te weten komt.

Deze methode kan bij bepaalde soorten van gegevensuitwisseling van nut zijn. Maar het proefschrift staat geheel los van het antwoord op de vraag of de betrokkenen met hun BSN op de passagierslijst (of op de lijst met «terroristen») zijn vermeld. De relatie met het voorliggende wetsvoorstel is minder duidelijk.

4. Fouten, controle, correctie

De commissie vraagt aandacht voor de situatie waarin een overheidsorgaan een dienst verleent aan een burger, daarbij gegevens gebruikt die afkomstig zijn van een ander overheidsorgaan en dit andere overheidsorgaan foute gegevens heeft verstrekt.

In het geval dat de commissie voor ogen heeft, zal de betrokken burger zich in eerste instantie richten tot het orgaan waarvan hij de dienst verlangt.

Een voorbeeld kan dit wellicht verduidelijken. Laten we aannemen dat een burger het oneens is met het voornemen van de Sociale Verzekeringsbank (SVB) om een uitkering te weigeren. De burger meent dat de SVB zijn voornemen baseert op onjuiste gegevens, en meldt dat de SVB. De SVB deelt mee dat het de gegevens van een ander bestuursorgaan heeft gekregen, bijvoorbeeld uit de gemeentelijke basisadministratie persoonsgegevens (GBA).

Artikel 3.2 van de Algemene wet bestuursrecht draagt de SVB op om bij de voorbereiding van het besluit tot weigering, de nodige kennis over de relevante (dus de juiste) feiten te vergaren[2]. Afhankelijk van de omstandigheden van het geval kan van de burger verwacht worden dat hij aannemelijk maakt dat de gegevens onjuist zijn. Als de burger heeft aangegeven

[1] Dit voorbeeld is door dr. Teepe genoemd bij de verdediging van zijn proefschrift.
[2] In dit voorbeeld wordt er van uit gegaan dat er geen bijzondere wettelijke regels zijn gesteld over de in aanmerking te nemen feiten. Soms zijn er wel dergelijke regels, zie bijvoorbeeld artikel 19b, eerste lid, van de Algemene ouderdomswet.

dat naar zijn mening de gebruikte gegevens onjuist zijn, kan de SVB niet volstaan met het antwoord dat die gegevens afkomstig zijn van een ander overheidsorgaan. De SVB zal nader dienen te onderzoeken wat de feiten zijn. Het is daarbij niet de burger die de bron van de fout moet opsporen (als een dergelijke bron al te vinden is). Indien de gegevens onjuist blijken, moet het bestuursorgaan zijn voornemen heroverwegen en vervolgens het besluit nemen op basis van de juiste gegevens.

Als nu, zoals in dit voorbeeld, de gegevens afkomstig zijn uit de GBA, dan is het mogelijk dat hetzelfde probleem terugkeert. Immers, de GBA is een (basis)registratie waar overheidsorganen algemene gegevens uit putten. Bij het nemen van een besluit over een volgend uitkeringstijdvak zal de SVB in eerste instantie wederom gebruik maken van de gegevens uit de GBA. Als deze (nog steeds) onjuist zijn, dreigt een herhaling van zetten. Het is daarom wenselijk dat de SVB de fout meldt aan de GBA. Zodra de wijziging van de Wet GBA in verband met de aanpassing aan de eisen voor basisregistraties[1] voor de SVB van kracht wordt, is de SVB zelfs verplicht om de onjuistheid van een authentiek gegeven aan de GBA te melden[2]. Bovendien kan de betrokkene zelf (ook nu al) vragen om correctie van zijn GBA-gegevens.

De vraag van de commissie noch het bovenstaande antwoord spreekt over het BSN van de betrokkene. Dat is ook terecht. De beschouwing heeft zowel betrekking op het geval dat géén gebruik wordt gemaakt van een persoonsnummer, als op het geval dat gebruik gemaakt wordt van het sofi-nummer of, in de beoogde toekomstige situatie, van het BSN.
Het BSN-stelsel biedt wel voorzieningen die het gebruikers van het BSN makkelijker maken om bepaalde fouten op te sporen. Met behulp van de beheervoorziening BSN kan snel een antwoord worden gevonden op de vraag of aan een bepaalde persoon reeds een burgerservicenummer is toegekend en zo ja, welk burgerservicenummer, op de vraag aan welk persoon een bepaald burgerservicenummer is toegekend en of het Nederlandse identiteitsdocument met behulp waarvan een persoon zich identificeert, geldig is.

De leden van de commissie vragen of de automatische uitwisseling zonder verdere verificatie en het facultatieve controlemechanisme van het huidige BSN stelsel niet tot grote risico's van fouten leidt, die vooral voor minder technisch vaardige burgers zo zeer problematisch te corrigeren zijn, dat zij feitelijk in een achtergestelde positie geraken. Heeft de regering een schatting gemaakt van de extra kosten, die het weghalen van de huidige controleslag door de burger zelf zal veroorzaken?

De vraag van de leden lijkt te zijn ingegeven door de vrees dat de invoering en het gebruik van het BSN autonoom leidt tot een welhaast ongebreidelde uitwisseling van ongeverifieerde persoonsgegevens. Dat is echter niet wat het onderhavige wetsvoorstel bewerkstelligt. Het wetsvoorstel behelst de invoering van een persoonsnummer, een hulpmiddel bij gegevensverwerking, ter vervanging van het huidige sociaal-fiscaalnummer. Het sociaal-fiscaalnummer wordt thans door vele (overheids-) sectoren gebruikt bij het registreren en uitwisselen van gegevens. De verantwoordelijkheden met betrekking tot die gegevensverwerkingen wijzigen door het onderhavige wetsvoorstel niet. Ook de correctiemogelijkheden voor de burger blijven volledig in stand. En van een «automatische uitwisseling zonder verdere verificatie» is na de invoering van het BSN evenmin als thans sprake. Met de invoering van het BSN wordt de kans op fouten naar verwachting juist kleiner, mede doordat de toekenning van burgerservicenummers met extra waarborgen wordt omkleed en er (technische) voorzieningen in werking worden gesteld om verificatie te ondersteunen. In het licht van het voorgaande is er naar de overtuiging

[1] Staatsblad 2007, 76.
[2] Zie artikel 62, eerste lid, van de Wet GBA.

van de regering met dit wetsvoorstel dan ook geen sprake van «het weghalen van de huidige controleslag door de burger».

In de memorie van antwoord is in antwoord op vragen van de leden van de PvdA-fractie en de VVD-fractie beschreven dat de burger in geval van een fout in het BSN zelf, beroep kan doen op zijn correctierecht op grond van de Wet GBA. De leden van de commissie wijzen in dat verband op een rapportage van de Amsterdamse gemeentelijke ombudsman van december 2006, waarin staat dat burgers soms flink worden gedupeerd omdat zij verkeerd geregistreerd staan bij de GBA. De leden van de commissie vragen of de beschreven situatie uniek is voor Amsterdam en of burgers na invoering van het BSN eenvoudig fouten kunnen herstellen.

In december 2006 heeft de gemeentelijke ombudsman van Amsterdam twee rapporten gepubliceerd met betrekking tot onjuiste inschrijvingen in de GBA[1]. Het betrof totaal zes gevallen waarin de betrokken burgers belastingen of heffingen kregen opgelegd die ten onrechte te hoog waren vastgesteld, vanwege een onjuiste vermelding in een gemeentelijke registratie.

In vier gevallen was er sprake van een enigszins ingewikkelde adressituatie (zoals na een splitsing in appartementen), die onjuist in de GBA was vermeld. In één geval was een woning als bedrijfsruimte geregistreerd bij de Dienst Belastingen Gemeente Amsterdam. Het laatste geval had betrekking op een ten onrechte doorgevoerde adreswijziging in de GBA.

Uit de rapporten komt naar voren dat meldingen van de burger onvoldoende werden verwerkt binnen de gemeentelijke organisatie, zodat bijvoorbeeld de belastingaanslag wel werd gecorrigeerd, maar de vermelding in de GBA fout bleef. Dat had tot gevolg dat in een volgende periode wéér een verkeerde aanslag werd opgelegd. De ombudsman oordeelde in de genoemde gevallen dat de gemeentelijke organisatie niet behoorlijk heeft gehandeld. Vervolgens heeft hij enkele concrete aanbevelingen gedaan.

De conclusie van de ombudsman strekt niet tot het oordeel dat de regelgeving (bijvoorbeeld de regelingen om op te komen tegen een onjuiste belastingaanslag of een foute vermelding in de GBA) onjuist of onvolledig is. Het ging in die gevallen niet goed in de uitvoering. Dat naast passende regelgeving een goede uitvoering van groot belang is, zal een conclusie zijn die niet uniek is voor Amsterdam.

In al deze gevallen was overigens het persoonsnummer van de betrokkene (zijn sofi-nummer of A-nummer) niet de veroorzaker van de fout. Dit nummer was evenmin een hindernis bij het herstel. Het is niet te verwachten dat dit na de invoering van het BSN anders zal zijn.

5. Privacy en rechtsbescherming

De leden van de commissie vragen een reactie van de regering op de bijzonder lage plaats van Nederland op de National Privacy Ranking 2006 van Privacy International.

In het bedoelde onderzoek wordt van een aantal landen nagegaan hoe zij scoren op het gebied van privacy en het houden van toezicht op mensen («surveillance»)[2]. Hierbij worden algemene criteria gehanteerd zoals de (grond)wettelijke bescherming van burgers, de invulling van de rol van toezichthouder op de privacy en de waarborgen die democratische procedures bieden. Ook worden criteria gehanteerd specifiek gericht op het

[1] Rapporten van de gemeentelijke ombudsman van de gemeenten Amsterdam, Almere, Landsmeer, Oostzaan, Waterland, Weesp en Zaanstad van 13 december 2006 (RA0612384) en van 18 december 2006 (RA12546).

[2] Het rapport meldt de doelstelling: «This study and the accompanying ranking chart measure the extent of surveillance and privacy».

houden van toezicht op mensen, zoals de mate waarin sprake is van visueel observeren met camera's, afluisteren van communicatieverbindingen en monitoren van werkplekken.

De regering heeft in antwoord op vragen van de Tweede Kamer over dit onderzoek laten weten dat zij de opvattingen in het onderhavige onderzoek niet deelt en dan ook geen aanleiding ziet om maatregelen te nemen. Met de in het onderzoek genoemde (Nederlandse) bevoegdheden wordt immers beoogd een bijdrage te leveren aan de nationale veiligheid. De bescherming van de nationale veiligheid is een van de in artikel 8, tweede lid, van het EVRM opgesomde legitieme doelstellingen op basis waarvan het recht op de persoonlijke levenssfeer kan worden beperkt[1].

De antwoorden van de regering op vragen in het voorlopig verslag met betrekking tot de (rechts-)bescherming van de individuele burger tegen de mogelijkheid van onjuist of zelfs crimineel gebruik van het BSN stellen de leden van de commissie niet gerust. Het is volgens hen van een zeker abstractieniveau, laat vrijwel alles over aan de verantwoordelijke voor de gegevensverwerking die in de back offices plaatsvindt, maar steunt hem of haar alleen in de verstrekking van een in begrijpelijke taal geschreven leeswijzer inzake de verplichtingen die voortvloeien uit relevante wettelijke bepalingen. Tegen wie overigens kan de gedupeerde burger een claim indienen ingeval hij wordt geconfronteerd met het hier geschetste mogelijke misbruik?

In de memorie van antwoord, maar ook in eerdere parlementaire stukken betreffende het onderhavige wetsvoorstel[2], is op verschillende plaatsen uiteengezet wat de (individuele) burger kan doen indien hij wordt geconfronteerd met onjuist gebruik (waaronder mede begrepen crimineel gebruik) van zijn BSN door anderen. Zulke uiteenzettingen hebben per definitie een zeker abstractieniveau, omdat onjuist (c.q. crimineel) gebruik van persoonsgegevens zeer uiteenlopende gedaanten kan hebben en zo ook de remedie (van burger, verantwoordelijke of overheid) tegen dat onjuist gebruik. Algemeen geldt echter: onjuist gebruik van gegevens mag niet en dat is des te meer het geval indien dat gebruik een crimineel karakter heeft. Wetten alleen zijn in de geschiedenis echter niet toereikend gebleken om ongewenst of crimineel gedrag uit te bannen. De burger die in het kader van gegevensverwerkingen met zulk gedrag wordt geconfronteerd, heeft daarom een aantal mogelijkheden (die trouwens voor hem openstaan ongeacht of het BSN erbij betrokken is). In de eerdere stukken is uiteengezet dat voor de burger de volgende mogelijkheden open staan, al naar gelang de omstandigheden van het geval: (1) bezwaar, (2) correctie, (3) klachten, (4) beroep, (5) hoger beroep, (6) klachten bij de (Nationale) ombudsman en (7) bemiddeling en advies door het College bescherming persoonsgegevens. Bovendien kan bij criminele activiteiten het openbaar ministerie optreden. De burger kan aangifte doen van strafbare feiten. De burger staat in ieder geval niet met lege handen.

De «verantwoordelijke» voor de gegevensverwerking (zo duidt de Wbp hem aan) draagt hierbij inderdaad een grote verantwoordelijkheid. Zo legt de Wbp de verantwoordelijke de verplichting op, onjuist gebruik van persoonsgegevens (waaronder het BSN) waar mogelijk te voorkomen en maatregelen te treffen indien onjuist gebruik is opgetreden. In verband hiermee voorziet de Wbp tevens in toezicht en sancties. Om de personen en organisaties die met het BSN werken bij dit alles te ondersteunen, zal ook nog eens in heldere taal worden uiteengezet onder welke voorwaarden het BSN gebruikt kan worden, welke regels daarop van toepassing zijn en welke tips en «good practices» daarbij te melden zijn (de handleiding die ook wel is aangeduid als «toetsingskader»).

[1] Aanhangsel Handelingen II 2006/07, nr. 538.
[2] Zie onder meer Kamerstukken II 2005/06, 30 312, nr. 7, blz. 14, 21 en 24.

Op de vraag van de commissieleden, tegen wie de burger een claim kan indienen in het geval dat hij wordt geconfronteerd met misbruik van persoonsgegevens (c.q. zijn BSN), kan helaas opnieuw slechts een enigszins abstract antwoord worden gegeven. De algemene regel is dat iemand die schade leidt door de onrechtmatige gedraging van een ander die ander kan aanspreken tot vergoeding van die schade[1]. De Wbp bevat een uitbreiding op dit beginsel in die zin dat ook nadeel dat niet bestaat uit vermogensschade voor schadevergoeding in aanmerking komt (vergoeding voor immateriële schade)[2]. Bovendien bevat de Wbp voor de burger een extra mogelijkheid om de rechter te verzoeken gedragingen te verbieden die schade toebrengen of dreigen toe te brengen[3].

De commissie vraagt vervolgens welke verantwoordelijkheid de centrale overheid draagt voor een afdoende beveiliging van het BSN-systeem.

Het BSN-systeem bestaat uit de beheervoorziening BSN zoals omschreven in artikel 3 van het wetsvoorstel. Op grond van het tweede lid van artikel 3 is de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk voor de afdoende beveiliging hiervan.

6. Veiligheid

De leden van de vaste commissie vragen of de conclusie correct is dat er geen protocollen en standaards zijn ontwikkeld voor de veiligheid en beveiliging van de verschillende typen BSN-gegevens.

Door overheidsorganisaties worden meerdere soorten van persoonsgegevens verwerkt. Het kan gaan om algemene gegevens zoals die in de bevolkingsboekhouding, om financiële gegevens bijvoorbeeld bij het heffen van belastingen maar ook om gegevens over het ziekteverzuim van werknemers in het kader van de collectieve verzekeringen. Bij deze verwerkingen van persoonsgegevens worden steeds identificerende gegevens van de betrokken burger vastgelegd. Het moet immers duidelijk zijn welke burger ergens recht op heeft, welke burger aan een bepaalde plicht moet voldoen en welke burger waar gevonden kan worden. De identificerende gegevens van de burger die worden vastgelegd bestaan uit zijn naam en aanvullende gegevens zoals geboortedatum, geslacht en dergelijke.
Daarnaast wordt vaak een persoonsnummer, bijvoorbeeld het sociaalfiscaalnummer, van de burger vastgelegd. Een persoonsnummer maakt het mogelijk om de gegevens die op een bepaalde persoon betrekking hebben op te zoeken zonder daarvoor gebruik te hoeven maken van de naam van de persoon in kwestie aangevuld[4] met informatie zoals geboortedatum en/of -plaats die samen met de naam meestal een unieke combinatie vormt.
Het is de bedoeling dat in de toekomst het BSN bij deze gegevensverwerkingen gebruikt gaat worden door overheidsorganen. De gegevensverwerkingen zelf bestaan veelal reeds geruime tijd, met inbegrip van de maatregelen zoals protocollen en standaards die de veiligheid en beveiliging van de gebruikte systemen verzorgen. Zo bezien worden geen nieuwe protocollen en standaards gebruikt indien het BSN aan de persoonsgegevens wordt toegevoegd of het reeds toegevoegde sociaalfiscaalnummer wordt hernoemd tot BSN.

De invoering van het BSN bij een bepaalde gegevensverwerking kan wel tot enige aanscherpingen in de (bestaande) maatregelen en protocollen voor beveiliging leiden. Een eerste voorbeeld betreft het gebruik van de verbindingen die worden gebruikt wanneer gebruikers van het BSN de beheervoorziening BSN raadplegen. Deze verbindingen zijn extra beveiligd door het gebruik van de zogeheten PKI-technologie. Hiermee wordt

[1] Artikel 162 Boek 6 BW.
[2] Artikel 49 Wbp.
[3] Artikel 50 Wbp.
[4] Wanneer iedereen een eenvoudig te spellen en unieke naam zou hebben, dan bestond er geen noodzaak voor persoonsnummers en dus ook niet voor het burgerservicenummer.

bereikt dat alleen geautoriseerden de beheervoorziening kunnen raadplegen en dat de informatie die wordt uitgewisseld niet door derden kan worden onderschept. Een ander voorbeeld betreft de plicht die op een gebruiker van het BSN rust om zich ervan te vergewissen dat een BSN inderdaad hoort bij een bepaalde persoon. Deze plicht moet geoperationaliseerd worden in een concrete maatregel/protocol die per sector een andere vorm kan aannemen, afhankelijk van de aard van de gegevens die worden verwerkt en de overige omstandigheden van het geval.

De leden stellen verschillende vragen over de keuze om één enkel nummer toe te kennen en niet meerdere nummers afhankelijk van de verschillende rollen en identiteiten van een persoon.

Het onderhavige wetsvoorstel bestrijkt slechts een deel van alle mogelijke rollen die een persoon in het maatschappelijk verkeer kan hebben. Buiten beschouwing blijven rollen zoals lid zijn van een vrijwilligersorganisatie, van een vereniging, van een vakbond of van een politieke partij. De vraag of en zo ja op welke wijze deze en andere maatschappelijke organisaties hun leden van een nummer voorzien, wordt door dit wetsvoorstel dan ook niet beïnvloed. Evenmin bestrijkt het onderhavige wetsvoorstel het toekennen van nummers aan bedrijven en instellingen (dat komt aan de orde in het wetsvoorstel voor het handelsregister)[1]. Het is dus bepaald niet zo dat voor alle rollen van een persoon, een en hetzelfde nummer wordt ingevoerd.

De vraag spitst zich daarom toe op de redenen die ten grondslag liggen aan de keuze om de burger een enkel persoonsnummer toe te kennen voor de rollen die hij heeft in relatie tot de overheid, zoals daar zijn: belastingbetaler, ingezetene van Nederland, stemgerechtigde, aanvrager van een paspoort, aanvrager van huurtoeslag, studiefinanciering of bijstand, ontvanger van een uitkering op grond van de AOW, aanvrager van een vergunning, betaler van een boete, rechthebbende op thuiszorg en/of vergoeding voor een traplift. Waarom, zo vragen de leden van de vaste commissie, heeft de regering gekozen voor een en hetzelfde persoonsnummer voor deze gevallen?

Een persoonsnummer is een hulpmiddel waarmee de gegevens die op een bepaalde persoon betrekking hebben, op een goede en betrouwbare manier kunnen worden opgezocht. Het gebruik van meerdere persoonsnummers maakt de dienstverlening aan de burger onnodig complex. De verschillende rollen die een burger heeft in relatie tot de overheid zijn immers nauw met elkaar verweven. Een voorbeeld kan dit verduidelijken. Het gebruik van het ene persoonsnummer voor de belastingaanslag en een ander persoonsnummer voor de huurtoeslag, betekent in de praktijk dat het ene nummer omgezet moet kunnen worden in het andere nummer. Voor het vaststellen van het recht op en de hoogte van de huurtoeslag moeten immers de inkomensgegevens worden bepaald die ontleend worden aan de belastingaanslag. Het gebruik van twee persoonsnummers leidt ertoe dat een koppeltabel moet worden opgezet en in stand gehouden en dat het raadplegen van de gegevens van de belastingaanslag mede inhoudt dat deze koppeltabel wordt geraadpleegd. Dat is een substantiële verhoging van de complexiteit in de dienstverlening aan de burger, waardoor niet alleen fouten geïntroduceerd kunnen worden maar ook extra kwetsbaarheden ontstaan omdat dit soort van koppeltabellen door allerlei partijen geraadpleegd moet worden bij hun dienstverlening. Ze moeten dus voortdurend beschikbaar zijn voor meerdere partijen maar mogen uiteraard alleen door geautoriseerde organisaties worden gebruikt. Voorts ontstaat door het gebruik van meerdere nummers en koppeltabellen de noodzaak om te verifiëren of de aan de nummers gekoppelde persoonsgegevens overeen komen. Daartoe moet

[1] Kamerstukken II 2006/07, 30 656, nr. 2.

meer uitwisseling van persoonsgegevens plaatsvinden, hetgeen ook uit een oogpunt van privacy ongewenst kan worden geacht.

De leden vragen of het mogelijk wordt dat met één toegang alle informatie wordt ontsloten omdat er met een moedersleutel wordt gewerkt in plaats van met verschillende sleutels voor verschillende ingangen.

Persoonsnummers zijn niet te vergelijken met sleutels waarmee men zich toegang kan verschaffen tot systemen en computers waarin persoonsgegevens worden opgeslagen. Die toegang wordt per systeem verzorgd door maatregelen voor toegangsbeveiliging en autorisatie die zijn toegesneden op de risico's die de verwerking en de aard van de gegevens met zich meebrengen. Voorbeelden van sleutels die daarbij horen zijn wachtwoorden en smartcards met of zonder pincode. En om dezelfde redenen dat persoonsnummers niet vergeleken kunnen worden met sleutels, kan het BSN niet vergeleken worden met een moedersleutel. Het BSN biedt geen toegang tot alle informatie over een persoon.

De commissie vraagt wat de noodzaak is van de keuze van één nummer in één enkele nummerreeks; ze vraagt tevens in hoeverre er gebruik wordt gemaakt van beveiligingen zoals checksums, waardoor gevalideerd kan worden of een geldig nummer is ingevoerd in plaats van een typefout.

De burgerservicenummers worden gegenereerd door een nummergenerator. Hiermee is het mogelijk om ervoor te zorgen dat de achtereenvolgend gegenereerde nummers, geen opeenvolgende nummers zijn. Er wordt dus niet gebruik gemaakt van slechts één enkele nummerreeks.

Het BSN is een nummer dat is opgebouwd uit negen cijfers. Niet alle combinaties van negen cijfers vormen een geldig BSN. De cijfers moeten voldoen aan de zogeheten elfproef. Hiermee kunnen typefouten, zoals het verwisselen van twee cijfers, worden gedetecteerd.

De leden vragen of er voor gezorgd is dat geen informatie beschikbaar komt over anderen en dat fuzzy zoekopdrachten worden voorkomen als dekmantel voor het opsporen (skimming) van specifieke gegevens.

De verwerking van persoonsgegevens dient op een rechtmatige wijze plaats te vinden. De maatregelen die de verantwoordelijke neemt tegen onrechtmatige verwerking dienen een passend beveiligingsniveau te realiseren gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Het gebruik van het BSN biedt de verantwoordelijken voor gegevensverwerkingen nieuwe mogelijkheden om onrechtmatige kennisname van persoonsgegevens te voorkomen. Het BSN maakt het raadplegen van gegevens in databases effectiever in vergelijking met de situatie waarin op naam en aanvullende identificerende informatie moet worden gezocht. Burgerservicenummers zijn immers uniek voor de persoon waarop ze betrekking hebben en ze leiden nauwelijks tot spelfouten of andere onnauwkeurigheden die bij het invoeren van namen niet ongebruikelijk zijn. Dat zorgt er voor dat het uit een oogpunt van privacy ongewenste verschijnsel waarbij de gegevens van een andere persoon dan de beoogde op het scherm van de ambtenaar komt, minder vaak zal voorkomen.

«Fuzzy» zoekopdrachten worden in de regel gebruikt wanneer de gezochte informatieset niet eenduidig geïdentificeerd kan worden. Een voorbeeld is de situatie waarin wel bekend is dat de naam van iemand de letters «Pieter» bevat maar waarin niet bekend is of de naam «Pieters» of

«Pietersen» is. De zoekopdracht bestaat eruit dat naar alle namen wordt gezocht met daarin de letterreeks «Pieter». Het antwoord op deze opdracht omvat dan de gegevens van meerdere personen. Wanneer nu het BSN consequent wordt gebruikt, zijn alle informatiesets eenduidig van een nummer voorzien. Er bestaat dan geen noodzaak om met behulp van gedeeltelijke informatie van een naam een «fuzzy» zoekopdracht te maken. Daardoor kan het door de commissie genoemde opsporen van specifieke gegevens, «skimming», worden teruggedrongen.

Wordt de wisselwerking tussen PIP, DigiD en BSN niet onbeheersbaar?

De wisselwerking tussen PIP, DigiD en BSN wordt bepaald door drie relaties: de relatie tussen PIP en DigiD, tussen PIP en BSN en tussen DigiD en BSN.
De persoonlijke internet pagina of PIP beoogt de burger toegang te geven tot gegevens die de overheid over hem of haar heeft. Voor de meeste gegevens en voor de meeste vormen van toegang zal een vorm van authenticatie van de burger nodig blijken te zijn. Voordat immers persoonsgegevens van een burger toegankelijk worden gemaakt voor hem of haarzelf, moet duidelijk zijn dat de burger in kwestie zelf daarmee heeft ingestemd. De algemene authenticatievoorziening DigiD zal hierbij als middel worden ingezet. DigiD is dus noodzakelijk voor de toegangsbeveiliging van de PIP.
Het vinden van de gegevens die de overheid over een burger heeft, vereist dat van de burger identificerende gegevens zijn vastgelegd. Bij de dienstverlening door de overheid wordt daarvoor veelal het sociaal-fiscaalnummer als persoonsnummer gebruikt. Overheidsdienstverlening waarbij geen persoonsnummers wordt gebruikt, komt niet voor ontsluiting via de PIP in aanmerking. Beoogd wordt om de rol van het sociaal-fiscaalnummer over te laten nemen door het BSN. Het BSN is dus noodzakelijk om de PIP te realiseren.
Voor de inzet van het authenticatiesysteem DigiD bij een bepaalde vorm van dienstverlening, is het nodig dat bij deze dienstverlening door de betrokken overheidsinstantie gebruik wordt gemaakt van een persoonsnummer zoals het sociaal-fiscaalnummer. De relatie met het BSN is dat beoogd wordt dat dit nummer de plaats van het sociaal-fiscaalnummer in gaat nemen. DigiD zal dus gebruik gaan maken van het BSN wanneer dit de plaats van het sociaal-fiscaalnummer in gaat nemen. DigiD bouwt daarmee voort op het BSN. Het omgekeerde is overigens niet het geval. Het BSN vormt dus de meest elementaire bouwsteen van de elektronische overheid die zowel voor DigiD als voor PIP gebruikt kan worden. De invoering van het BSN kan er toe bijdragen dat DigiD en PIP gebruikt kunnen worden bij alle vormen van overheidsdienstverlening. Dat vloeit voort uit het feit dat het BSN door alle overheidsorganisaties gebruikt kan worden, in tegenstelling tot het sociaal-fiscaalnummer. Het BSN wordt niet beïnvloed door DigiD of door PIP.

Van belang is dat de PIP een hulpmiddel is dat specifiek voor de burger wordt gemaakt. De PIP maakt het mogelijk dat de burger de gegevens die de overheid over hem heeft, eenvoudig en in hun samenhang kan inzien. Organisaties kunnen de PIP dus niet gebruiken en krijgen dus langs deze weg geen inzage in de gegevens over de burger die de verschillende overheidsorganisaties vastliggen.

De commissie vraagt naar de mening van de regering over de stelling van experts als de Nijmeegse professor Bart Jacobs, dat de beschikbare technologie nog niet voldoende geavanceerd is om de veiligheid van het BSN te waarborgen. Ze vraagt ook naar de wijze waarop oneigenlijke toegang wordt voorkomen en daarmee de risico's van diefstal van identiteit met alle gevolgend van dien, ook op de toegang tot de gegevens van de over-

heid zelf. Creditcardmaatschappijen vragen standaard een aantal gegevens die straks allemaal zijn op te vragen via de PIP.

De kern is dat geen enkele verzameling van persoonsgegevens adequaat beveiligd is als voor het verschaffen van toegang tot de verzameling het kennen van het BSN van betrokkene zou volstaan. De verzameling zou net zomin goed beveiligd zijn als de toegang afhankelijk zou zijn van het kennen van de naam van de betrokkene.
In termen van beveiliging moet dus bijvoorbeeld de naam of het BSN geen geheime toegangssleutel zijn. De verantwoordelijke voor de (beveiliging van) de gegevensverwerking moet er van uitgaan dat iemands naam of BSN bij willekeurige derden bekend is.
Beveiliging van de toegang tot een verzameling persoonsgegevens wordt vormgegeven door deze afhankelijk te stellen van bijvoorbeeld een geheim zoals een wachtwoord dat bij een gebruikersnaam hoort of door geavanceerde technieken zoals smartcards.

Professor Jacobs staat een systeem van meerdere nummers voor die corresponderen met de verschillende rollen die burgers kunnen hebben[1]. Op de overwegingen om niet voor zo'n systeem te kiezen, is hiervoor in gegaan. Daarbij is ook ingegaan op de misvatting dat het BSN toegang zou kunnen verschaffen tot gegevens.

Het begrip identiteitsdiefstal is geen eenduidig omschreven begrip. Het wordt vaak gebruikt om de situatie aan te duiden waarin iemand gebruik maakt van gegevens en/of objecten die aan een andere persoon toehoren om zo voor die ander door te gaan. Objecten die daarbij gebruikt kunnen worden zijn bijvoorbeeld paspoorten of rijbewijzen. De kwestie spitst zich toe op de vraag of het BSN een gegeven is dat – meer dan het sociaal-fiscaalnummer – aangewend kan worden om zich voor te doen als een ander persoon. Die vraag moet ontkennend worden beantwoord. Gebruikers van het BSN moeten zich er immers van vergewissen dat een bepaald BSN betrekking heeft op de persoon die aangeeft dat het op hem of haar betrekking heeft. Wanneer gebruikers dat niet doen, handelen zij derhalve in strijd met de wet. De positie van de burger is in dit opzicht dus verbeterd wanneer de situatie met het BSN wordt vergeleken met de huidige situatie met het sociaal-fiscaalnummer.

De leden merken op dat creditcardmaatschappijen aan hun toekomstige klanten standaard een aantal gegevens vragen die straks allemaal op te vragen zouden zijn via de PIP. Het bestaan van de PIP in de toekomst impliceert echter niet dat deze creditcardmaatschappijen hun gegevens kunnen ontlenen aan de PIP. Het gebruik van de gegevens die met de PIP toegankelijk worden gemaakt, is en blijft voorbehouden aan degene waarop deze gegevens betrekking hebben.

De commissie vraagt naar de reactie van de regering op signalen als van de internetuitvinder Vint Cerf, dat een kwart van alle PC's van buitenaf bestuurd wordt, zodat het afvangen van inloggegevens of de inhoud van communicatie bijna zeker is, waardoor het uitbreiden van BSN mogelijkheden tot ernstig misbruik en kwetsbaarheid voor identiteitsdiefstal kan leiden.

Het citaat van Vint Cerf is de regering bekend[2]. Voor de aanpak van cybercrime wordt kortheidshalve verwezen naar de brief van 18 mei 2006 van de staatssecretaris van Economische Zaken[3]. Voor de goede orde zij vermeld dat het citaat van de heer Cerf de uitdrukking «computers on the net» hanteert. Het citaat impliceert dus niet dat een kwart van de computers waarop de gegevensverwerking van de Nederlandse overheid plaats vindt, door botnets is overgenomen.

[1] Zie bijvoorbeeld de internetpublicatie «De Menselijke Maat in ICT», Versie 1.0, Januari 2007, pagina 44.
[2] De BBC News website citeert Vint Cerf als volgt: «Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets, said Vint Cerf, one of the fathers of the internet». De website vermeldt tevens: «The panel of leading experts was discussing the future of the internet at the World Economic Forum in Davos». De bijeenkomst vond plaats in januari 2007.
[3] Kamerstukken II 2005/06, 26 671, nr. 24.

Op de relatie tussen het BSN en identiteitsdiefstal is hiervoor reeds ingegaan.

De leden van de commissie vragen of de regering de opvatting deelt dat het gebruik van het BSN door de overheid als werkgever uitgesloten dient te zijn, omdat de gegevens zijn vergaard vanuit de rol van de overheid als maatschappelijk regisseur.

Het is niet geheel duidelijk welke gegevens de leden van de commissie bedoelen, indien zij aangeven dat deze gegevens zijn vergaard vanuit de rol van de overheid als maatschappelijk regisseur. In ieder geval kan niet worden gesteld dat de overheid als werkgever het BSN van haar werknemers niet zou mogen gebruiken. Zoals iedere werkgever dient de overheid in bepaalde gevallen thans het sociaal-fiscaalnummer van haar werknemers te registreren ter uitvoering van wettelijke verplichtingen op het gebied van belastingen en sociale verzekeringen. Na de invoering van het BSN zal zij in die gevallen het BSN dienen te hanteren. In zoverre neemt de overheid als werkgever in ieder geval geen bijzondere positie in ten opzichte van andere werkgevers. Wellicht heeft de vraag van de commissieleden mede betrekking op de bevoegdheid die artikel 10 van het wetsvoorstel beoogt te verlenen aan overheidsorganen. Op grond van artikel 10 mag een overheidsorgaan het BSN gebruiken, indien het persoonsgegevens verwerkt in het kader van de uitvoering van zijn taak. Dit artikel is bedoeld om een breed gebruik van het BSN binnen de overheid mogelijk te maken, maar stelt aan dat gebruik wel de nodige voorwaarden. In de eerste plaats heeft de bepaling slechts betrekking op overheidsorganen, hetgeen impliceert dat de hoedanigheid van het orgaan in bepaalde gevallen dient te worden vastgesteld («is het orgaan in dit kader overheidsorgaan of niet?»). Voorts betreft het de verwerking van persoonsgegevens. Die gegevensverwerking is gereguleerd, in het algemeen op grond van de Wbp. Uiteraard dient te worden vastgesteld of de gegevensverwerking als zodanig rechtmatig plaatsvindt, alvorens kan worden vastgesteld of daarbij het BSN van degene waarop de gegevens betrekking hebben, kan worden gebruikt. Ook geldt ten aanzien van het gebruik van het BSN de algemene regel dat het verwerken ervan toereikend, ter zake dienend en niet bovenmatig is (artikel 11 Wbp). Ten slotte dient te worden vastgesteld of de desbetreffende gegevensverwerking geschiedt in het kader van het uitvoeren van de taak van het desbetreffende overheidsorgaan. Het is aannemelijk dat die taak veelal niet zal kunnen worden uitgevoerd zonder inzet van personeel, c.q. zonder dat het overheidsorgaan een deugdelijke personeelsadministratie voert. Bij dat laatste zal een persoonsnummer dienstig zijn. Voor de overheid is dat nummer het BSN, buiten de overheid een ander nummer tenzij het BSN wettelijk is voorgeschreven.

7. Gewetensbezwaarden

De commissie vraagt of de regering bereid is alsnog een uitzonderingsmogelijkheid voor gewetensbezwaarden te creëren, aangezien het gaat om de koppeling van het BSN aan een groot aantal persoonsgebonden gegevens en gesteld zou kunnen worden dat het bijzonder naïef dan wel misleidend is om te stellen dat het BSN een puur technisch, inhoudsloos middel is.

Zoals de leden van de commissie terecht opmerken is in de memorie van antwoord ingegaan op gewetensbezwaren die zich richten tegen het nummer zelf. De regering heeft daarbij aangegeven geen reden te zien om een uitzonderingsmogelijkheid te creëren voor mensen die geen nummer willen zijn omdat het BSN mensen niet tot een nummer degradeert. Het is

immers (slechts) een hulpmiddel om er voor te zorgen dat gegevens over personen niet met elkaar verwisseld worden.
Het is op voorhand niet geheel uit te sluiten dat er daarnaast gewetensbezwaren bestaan tegen het gebruik van het BSN in combinatie met andere persoonsgegevens. Het gaat dan klaarblijkelijk niet om het BSN op zichzelf maar om de combinatie van BSN met die andere gegevens. Ook bij een combinatie van BSN met andere gegevens geldt dat het BSN zelf een puur technisch en inhoudsloos middel is. Dat geldt uiteraard niet voor de persoonsgegevens die voor de uitvoering van een bepaalde taak of dienst nodig zijn. Voor zover er uitzonderingsmogelijkheden nodig worden geacht voor de verwerking van deze gegevens, kan daarin worden voorzien door de desbetreffende wet- en regelgeving. De regering overweegt daarom nog steeds niet om in dit wetsvoorstel een uitzonderingsmogelijkheid voor gewetensbezwaarden op te nemen.

8. Positie Eerste Kamer

De commissie vraagt hoe het kan zijn dat in een passage over het burgerservicenummer in de aangiftebrief inkomstenbelasting wordt gedaan alsof het burgerservicenummer al is ingevoerd. Ze vraagt tevens wat de opvatting van de regering is over het feit dat talrijke (overheids-) instanties het doen voorkomen alsof het BSN per 1 januari 2007 is ingevoerd. De regering wordt gevraagd mee te delen waarom het voor de zoveelste keer voorkomt dat het bestaan van de Eerste Kamer genegeerd wordt en of de regering zich kan voorstellen dat de vaste commissie dit langzamerhand als een belediging van de Eerste Kamer ervaart.

Het is geenszins de bedoeling om het bestaan van de Eerste Kamer te negeren. Alle voorbereidingen voor het BSN kunnen teruggedraaid worden. Er zijn geen onomkeerbare stappen gezet. Mocht het wetsvoorstel niet de kracht van wet krijgen, dan blijft de toestand zoals deze nu bestaat met het sociaal-fiscaalnummer van kracht.

Het gegeven dat sommige organisaties ten onrechte de term burgerservicenummer gebruiken, betekent niet dat het BSN reeds zou zijn ingevoerd. Deze organisaties hebben voorbarig de aanduiding sociaal-fiscaalnummer ingeruild voor de aanduiding burgerservicenummer. De verplichtingen en de mogelijkheden die het wetsvoorstel schept, zijn niet van kracht. Er wordt nog gewerkt met het sofi-stelsel.
De fout van een aantal organisaties om op sommige formulieren in plaats van de term «sociaal-fiscaalnummer» de term «burgerservicenummer» te zetten, hangt samen met de relatief lange doorlooptijd bij het produceren van grote hoeveelheden formulieren, gekoppeld aan een verkeerde inschatting van de datum waarop de wet in werking zou zijn getreden. In de communicatie over het burgerservicenummer, wordt vanaf eind 2006 gemeld dat invoering niet eerder dan ruim vier weken na instemming van het parlement plaats kan vinden. Ik betreur dat op meerdere formulieren al de term BSN is verschenen.

De Eerste Kamer heeft haar eigen belangrijke rol in het wetgevingsproces. Zonder aanvaarding van het wetsvoorstel kan het burgerservicenummer niet worden ingevoerd. Ik zie onze mondelinge discussie vol vertrouwen tegemoet.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A. Th. B. Bijleveld-Schouten

De uitwisseling van persoonsgegevens in de sector werk en inkomen in Nederland en België

1. Inleiding

Op 17 april 2007 werd een technische presentatie gegeven aan leden van de Eerste Kamer van de landkaart van het burgerservicenummer[1]. Tijdens deze presentatie bleek behoefte aan een actuele beschrijving van de gegevensuitwisseling in de sector werk en inkomen in Nederland en een vergelijking met de Belgische situatie, in het bijzonder de Kruispuntbank. Deze notitie bevat die beschrijving en vergelijking.

De gegevensuitwisseling in de sociale sector is in ontwikkeling. Het kabinet heeft in zijn brief van 13 mei 2005 aan het parlement zijn voornemens op dit gebied uiteengezet[2]. Daarin speelt het in ontwikkeling zijnde digitaal klantendossier (DKD) een belangrijke rol. Inmiddels zijn ook wetgevingsvoorstellen aan het parlement aangeboden waarin het leidend principe wordt vastgelegd dat elk gegeven dat in de keten van werk en inkomen aan de burger wordt gevraagd, slechts eenmaal gevraagd mag worden[3]. Gelet op de vragen van de Eerste Kamer handelt deze notitie niet over deze ontwikkelingen maar concentreert zij zich op de gegevensuitwisselingen zoals die nu bestaan tussen de uitvoeringsorganisaties.

2. De situatie in Nederland

2.1. Gegevensuitwisseling in de Suwi-keten

De uitwisseling van persoonsgegevens in de sector werk en inkomen is in hoge mate gereguleerd in wettelijke voorschriften. De regels voor de gegevensuitwisseling zijn enerzijds neergelegd in de algemene wetgeving – met name de Wet bescherming persoonsgegevens (Wbp) – en anderzijds in de Suwi-sectorwetgeving. Verder in deze notitie wordt vooral aandacht besteed aan deze sectorwetgeving en blijft de algemene wetgeving op de achtergrond.

De Suwi-sectorwetgeving omvat de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi), het Besluit Suwi, de Regeling Suwi en het Besluit Inlichtingenbureau gemeenten. De Wet Suwi stelt uitvoeringsorganen in als de Centrale organisatie werk en inkomen (CWI)[4], het Uitvoeringsinstituut werknemersverzekeringen (UWV) en de Sociale verzekeringsbank (SVB)[5]. Deze uitvoeringsorganen en de gemeenten dragen zorg voor de uitvoering van de wetgeving inzake werk en bijstand (Wet werk en bijstand), volksverzekeringen (zoals de Algemene Ouderdomswet en de Algemene Kinderbijslagwet) en werknemersverzekeringen (zoals de Werkloosheidswet en de Wet werk en inkomen naar arbeidsvermogen).
De wet draagt het UWV op om een polisadministratie in stand te houden, waarin (onder meer) gegevens zijn vastgelegd die nodig zijn om een (eventueel) recht op uitkering te bepalen[6]. De wet draagt de SVB op om een verzekerdenadministratie in stand te houden, die een vergelijkbaar doel kent. Bij de uitvoering van de sociale zekerheid zijn meerdere uitvoeringsorganen betrokken die elk een deel van de dienstverlening uitvoeren. De wet maakt het mogelijk dat gegevens uit polis- en verzekerdenadministratie worden gebruikt om te vermijden dat de uitvoeringsorganisaties de relevante gegevens telkens bij de burger zelf op moeten vragen[7].

De Wet Suwi kent vele bepalingen waarin de gegevensuitwisseling tussen de verschillende organisaties in de Suwi-keten zijn geregeld[8]. Om enkele voorbeelden te noemen:

[1] Deze landkaart beoogt in beeld te brengen welke gegevensverwerkingen plaatsvinden waarbij het BSN wordt gebruikt. Momenteel brengt de landkaart in beeld welke gegevensverwerkingen plaatsvinden waarbij het sociaal-fiscaalnummer is betrokken. De landkaart bevat niet alleen informatie over de gegevensverwerkingen zelf maar ook over hun wettelijke grondslag.
[2] Kamerstukken II 2004/05, 26 448, nr. 206.
[3] Kamerstukken II 2006/07, 30 970, nr. 2.
[4] De Centrale organisatie werk en inkomen draagt zorg voor de instandhouding van vestigingen in het land, genaamd Centra voor werk en inkomen. Deze centra zijn gedeconcentreerde onderdelen van de Centrale organisatie werk en inkomen.
[5] De Wet Suwi noemt ook de Raad voor werk en inkomen. Deze raad is een overlegorgaan en geen uitvoeringsorgaan (artikel 17 Wet Suwi). Bovendien verwijst de Wet Suwi naar de Stichting Inlichtingenbureau (IB) als intermediair voor gegevensuitwisseling met de gemeenten.
[6] In de bijlage bij het Besluit Suwi wordt uitgebreid beschreven welke gegevens worden vastgelegd, wat de bron is van die gegevens en met welk doel de gegevens zijn opgenomen.
[7] Zie de artikelen 33a, tweede lid, en 35, vijfde lid, Wet Suwi.
[8] Zie met name hoofdstuk 9, informatiebepalingen.

- verstrekking van gegevens aan de CWI, het UWV en de SVB door de gemeenten, de Belastingdienst, het College voor zorgverzekeringen, pensioenfondsen, Kamers van Koophandel, rechtbanken, de Informatie Beheer Groep (artikel 54 Wet Suwi);
- uitwisseling tussen de CWI, het UWV, de SVB en de gemeenten (artikel 62 Wet Suwi);
- verstrekking door de CWI, het UWV en de SVB aan pensioenuitvoerders, werkgevers of ziektekostenverzekeraars (artikel 73 Wet Suwi).

De Wet Suwi draagt de minister van SZW op om ten behoeve van (bepaalde) Suwi-taken een elektronische infrastructuur voor gegevensuitwisseling in stand te houden. Deze infrastructuur is het Suwinet.

2.2. Gegevensuitwisseling over het Suwinet

In het kort komen de volgende vraagpunten aan de orde:
- welke gegevens worden tussen wie uitgewisseld en wie beslist daarover;
- hoe wordt geregeld dat de gegevens ter beschikking komen van degene die de gegevens mag verwerken (autorisatie);
- hoe wordt ongeoorloofde toegang tot of wijziging van gegevens voorkomen (beveiliging).

Welke gegevens worden tussen wie uitgewisseld?
De Suwi-partijen CWI, UWV en gemeenten zijn verplicht om elkaar alle gegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun Suwi-taken (artikel 62, eerste lid, Wet Suwi)[1]. Zij moeten bij hun onderlinge uitwisseling gebruik maken van het Suwinet (artikel 64, Wet Suwi). De gemeenten zijn aangesloten op het Suwinet door tussenkomst van het Inlichtingenbureau (IB). Het Suwinet biedt aan de Suwi-partijen de mogelijkheid om bij elkaar gegevens te raadplegen (inkijken) en om elkaar gegevens te verstrekken (meldingen versturen).

De algemene wettelijke opdracht aan de Suwi-partijen om gegevens uit te wisselen wordt nader gepreciseerd in het Gegevensregister Suwi. Daarin is vermeld welke gegevens in welke gevallen tussen welke partijen worden uitgewisseld. De status van het Gegevensregister Suwi is een ministeriële regeling op basis van de Wet Suwi (artikel 64, tweede lid, Wet Suwi). Daarmee is ook de vraag beantwoord wie er beslist over de gegevensuitwisseling: de (gedelegeerde) regelgever, meer in het bijzonder de minister van SZW.

De inkijkmogelijkheden van Suwinet omvatten op dit moment klantgegevens die afkomstig zijn van CWI, de GSD's, UWV en GBA. CWI levert gegevens over inschrijvingen bij CWI en gegevens over beroepservaring en opleidingen die een persoon gevolgd heeft. De gegevens van GSD's hebben betrekking op uitkeringen en uitkeringsaanvragen in het kader van de WWB. De gegevens van UWV hebben betrekking op arbeidsrelaties en uitkeringsverhoudingen. Naast de genoemde persoonsgegevens levert Suwinet-inkijk aanvullende informatie aan de ketenpartners. Via een aansluiting op het Verificatie Identificatie Systeem (VIS), zijn gegevens over de status van identiteitsbewijzen beschikbaar. Van identiteitsbewijzen uit verschillende landen kan op die manier worden vastgesteld of zij als vermist of vervalst staan geregistreerd.

Een voorbeeld van meldingen die met behulp van Suwinet verstuurd kunnen worden, heeft betrekking op het re-integratieproces. Van een werkloze burger vindt een «werkintake» plaats bij de CWI. Bij deze werkintake wordt een analyse gemaakt van de mogelijkheden tot re-integratie van de cliënt hetgeen resulteert in een re-integratieadvies. De CWI

[1] In artikel 70 van de Wet Suwi is bepaald dat de minister van SZW bepalingen omtrent de uitwisseling over het Suwinet van overeenkomstige toepassing kan verklaren op de SVB.

verstuurt dit re-integratieadvies naar de organisatie waarvan de burger zijn uitkering ontvangt (UWV of GSD). De uitkerende instantie beoordeelt het ontvangen re-integratieadvies en doet daarvan een terugmelding aan de CWI. Deze berichten zorgen ervoor dat de uitkeringsorganisaties en de CWI over en weer geïnformeerd zijn over de mogelijkheden om de cliënt weer aan het werk te helpen.

Autorisatie
Het centrale beheer van het Suwinet is opgedragen aan de CWI (artikel 6.3, eerste lid, Regeling Suwi). In dat kader heeft de CWI een gemeenschappelijke faciliteit voor toegangsbeveiliging ingericht. Alle Suwinetpartijen moeten beschikken over een eigen toegangsmachtigingadministratie. Dit autorisatiesysteem, dat strekt tot het verlenen van toegang aan de juiste personen of instellingen, wordt nader uitgewerkt in het Stelselontwerp Suwinet (artikel 66, tweede lid, Wet Suwi).

Om de autorisaties af te dwingen, worden verschillende beveiligingsmaatregelen getroffen. Bij het versturen van *meldingen* wordt door vercijfering en digitale ondertekening van berichten bewerkstelligd dat onbevoegden de gegevens tijdens het transport niet kunnen inzien en dat zeker wordt gesteld dat de gegevens tijdens het transport niet gewijzigd kunnen worden. Berichten kunnen voorts alleen verstuurd worden naar netwerkadressen van aangesloten partijen. Er is dus geen verkeer met het «open» Internet.

De logische toegang tot gegevens via de *inkijk* voorzieningen van Suwinet, wordt beschermd door programmatuur voor toegangsbeveiliging. Voordat een gebruiker gegevens kan benutten, dient hij aan te loggen. Op grond van de gegevens in de toegangsmachtigingadministratie, kan worden vastgesteld of de gebruiker voldoende toegangsrechten heeft voor de gegevens. Hierbij wordt gebruik gemaakt van rollen voor gebruikers. Per rol is vastgelegd welke berichten de houder ervan kan benutten.

Suwinet-inkijk is een voorbeeld van een systeem waarmee een veelheid van gebruikers kan werken zonder dat alle gebruikers dezelfde toegang krijgen tot alle gegevens. Suwinet-inkijk stelt ambtenaren van uitvoeringsorganisaties in staat om gegevens te bekijken van cliënten in de sociale zekerheid zoals die zijn opgenomen in de bestanden van de CWI, het UWV, de GSD's, de GBA en andere organisaties. Een ambtenaar wordt voor het gebruik van Suwinet-inkijk gemachtigd op basis van een bepaalde rol die op hem van toepassing is. Zo'n rol kan omvatten dat de ambtenaar gerechtigd is om naast de gegevens van zijn eigen organisatie[1] ook de gegevens van de GBA te raadplegen of om het Verificatie Identificatie Systeem (VIS) te raadplegen. De beheerorganisatie van Suwinet (BKWI) zorgt ervoor dat deze rollen beschikbaar zijn voor de deelnemers in Suwinet. De deelnemende organisaties zijn zelf verantwoordelijk voor het op een correcte wijze toedelen van de rollen aan hun medewerkers zodat onder meer voldaan wordt aan de eisen betreffende proportionaliteit en doelbinding zoals vastgelegd in de Wbp. Het Digitaal Klant Dossier (DKD) waaraan nu wordt gewerkt, is te beschouwen als een doorontwikkeling van Suwinet-inkijk. Het ligt in de bedoeling dat met het DKD ook burgers inzage kunnen krijgen in de gegevens die over hen zijn verzameld. Wanneer er sprake is van incorrecte gegevens, kan de burger dat door het DKD eenvoudiger dan voorheen constateren en correctieve actie initiëren.

Beveiliging
In algemene zin geldt voor eenieder die werkzaam is in het Suwi-kader een geheimhoudingsplicht (artikel 74 Wet Suwi). De wet legt de CWI, het

[1] Voor CWI gaat het om gegevens over beroepservaring en opleidingen die een persoon gevolgd heeft. De gegevens van GSD's hebben betrekking op uitkeringen en uitkeringsaanvragen in het kader van de WWB. De gegevens van UWV hebben betrekking op arbeidsrelaties en uitkeringsverhoudingen.

UWV en het IB op om zorg te dragen voor de nodige technische en organisatorische voorzieningen ter beveiliging van de gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van de gegevens (artikel 76 Wet Suwi). Die zorgplicht wordt nader uitgewerkt in de bijlage Beveiliging Suwinet (artikel 6.4 Regeling Suwi).

Ieder van de Suwinet-partijen stelt een beveiligingsplan op dat invulling geeft aan de normen die zijn vastgelegd in de bijlage Beveiliging Suwinet. Een van de aandachtspunten in het geheel van normen betreft de administratieve organisatie. Voorgeschreven wordt onder meer dat functiescheiding wordt toegepast en dat er een beveiligingsfunctionaris is binnen elke organisatie. Deze functionarissen komen regelmatig bijeen. Ze houden zich bezig met de controle op de beveiligingsmaatregelen en verzorgen rapportages over de status van de beveiliging van Suwinet. Andere voorgeschreven maatregelen betreffen het opstellen van calamiteitenplannen, het screenen van personeel, het bevorderen van het beveiligingsbewustzijn, logging en het voorkomen van de aanwezigheid van kwaadwillende software zoals virussen. De beveiligingsnormen waaraan voldaan moet worden, omvatten alle aandachtsgebieden van informatiebeveiliging zoals die beschreven worden in de internationale standaard Code voor Informatiebeveiliging en in de relevante publicaties van het Cbp op dit gebied.

2.3. Gegevensuitwisseling met behulp van het RINIS-netwerk

Niet alle (geautomatiseerde) gegevensuitwisseling in de Suwi-keten verloopt via het Suwinet. Andere belangrijke stromen verlopen via het RINIS-netwerk. RINIS staat voor Routerings Instituut Nationale Informatiestromen. RINIS is een systeem voor uitwisseling van elektronische berichten, dat voortkomt uit de sociale zekerheid. Ook andere sectoren als zorg, justitie, onderwijs en belastingen maken gebruik van RINIS. Het RINIS-netwerk is gericht op het uitwisselen van grote aantallen berichten; het wordt niet gebruikt om gegevens bij een andere partij te raadplegen (inkijk).

Welke gegevens worden tussen wie uitgewisseld?
Alle uitwisseling van gegevens in de Suwi-keten over het RINIS-netwerk is gebaseerd op een wettelijke grondslag. De regelgever bepaalt welke partijen welke gegevens met elkaar uit kunnen of moeten wisselen. De partijen geven daar uitvoering aan door de uitwisseling in een uitwisselingsovereenkomst te concretiseren. Gegevensuitwisseling over het RINIS-netwerk is alleen mogelijk als deze concretisering ook is neergeslagen in het Gegevenswoordenboek RINIS, waarbij in detail is beschreven welke gegevens in welke gevallen worden uitgewisseld.

Het gegevenswoordenboek onderkent circa twintig verschillende berichten. Daarbij zijn uiteenlopende organisaties betrokken met verschillende doelstellingen. De Sociale Verzekeringsbank wisselt bijvoorbeeld berichten uit met de Belastingdienst met als doel het achterhalen en verifiëren van sofinummers. Met het oog op het verlenen van gesubsidieerde rechtsbijstand vragen de Raden voor Rechtsbijstand bij de Belastingdienst inkomensgegevens op. Het Inlichtingenbureau vraagt gegevens aan de Informatiebeheergroep over studie-inschrijvingen en studiefinanciering om het recht op bijstandsuitkeringen vast te stellen. De informatie in de berichten is op een vergelijkbare wijze nauwkeurig beschreven als de berichten van Suwinet zodat over de betekenis van de gegevens geen misverstanden kunnen ontstaan.

Autorisatie
Bij iedere berichtuitwisseling over het RINIS-netwerk wordt aan de hand

van het Gegevenswoordenboek RINIS gecontroleerd of de verzender van het bericht gerechtigd is tot het verzenden van dit type bericht en of de ontvanger gerechtigd is dit type bericht te ontvangen. Deze controle vindt plaats met behulp van een Public Key Infrastructure (PKI). Met behulp van deze infrastructuur kan een hoge mate van zekerheid worden verkregen over de identiteit van de verzender en de ontvanger en over de rechtmatigheid van de gegevensuitwisseling.

Beveiliging
Hiervoor in paragraaf 2.2 is al gewezen op de algemene geheimhoudingsplicht en op de zorgplicht voor Suwi-partijen ten aanzien van de beveiliging van hun gegevens.

Meer in het bijzonder kan over de beveiliging van het RINIS-netwerk nog het volgende worden gezegd.
De beveiliging van het netwerk start op lijnniveau: eerst wordt gecontroleerd of een verbinding is opgebouwd door bevoegde gebruikers. Daarnaast wordt gebruik gemaakt van lijn-encryptie, vervolgens wordt ook het bericht nog eens versleuteld. Mocht een onbevoegde onverhoopt doordringen tot een RINIS-server, dan is er extra bewaking via een uitgebreid stelsel van wachtwoorden, gekoppeld aan bevoegdheden. Na enkele vergeefse pogingen wordt de verbinding verbroken en alarmeert het systeem automatisch de netwerkbeheerder bij RINIS.

Elk bericht wordt bij verzending en bij ontvangst door de RINIS-programmatuur stringent gecontroleerd op validiteit. Zo mogen sommige elementen alleen uit cijfers bestaan, mogen bepaalde karakters niet voorkomen en moeten sommige gegevens altijd aanwezig zijn. Het is dus onmogelijk om zo maar een e-mail of een ander onbekend bericht naar een andere sector te sturen.

Alle gegevens binnen het RINIS-systeem worden versleuteld met grondige encryptietechnieken (DES/RSA). Via een elektronische handtekening wordt de bron van elk bericht eenduidig vastgesteld (authenticatie). Ook wordt voorkomen dat gegevens op welke wijze dan ook worden gewijzigd of beschadigd. Alle sleutels worden uitgegeven door een onafhankelijke Trusted Third Party.

RINIS kent tot slot een samenhangend beveiligingsbeleid en een beveiligingsplan, opgesteld aan de hand van de Code voor Informatie Beveiliging van het Nederlands Normalisatie Instituut en van aanbevelingen van het College bescherming persoonsgegevens (CBP).

2.4. Toezicht

Het toezicht op de uitvoering van de taken van de Suwi-partijen is door de wetgever opgedragen aan de Inspectie Werk en Inkomen (artikel 36 Wet Suwi). Dit toezicht omvat ook de naleving van de regels omtrent gegevensverwerking. De inspectie kan daarbij gebruik maken van de rapportages van de Suwi-partijen over hun stelsel van maatregelen en procedures gericht op het waarborgen van een goede gegevensverwerking (artikel 5.22, eerste lid, Regeling Suwi). De rapportages strekken zich ook uit tot de beveiliging van het Suwinet (artikel 6.4 Regeling Suwi). De inspectie heeft daarbij tevens de beschikking over een oordeel en een rapport van bevindingen van een (onafhankelijke) EDP-auditor (artikel 5.22, tweede lid, Regeling Suwi).

Naast het hiervoor omschreven sectorspecifieke toezicht is het de taak van het College bescherming persoonsgegevens om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet

bepaalde (artikel 51 Wbp). De taak van het college omvat ook de gegevensverwerking in de Suwi-keten. Het college kan daartoe ambtshalve of op verzoek een onderzoek instellen (artikel 60 Wbp). Het college kan zo nodig sancties hanteren als het toepassen van bestuursdwang, het opleggen van een last onder dwangsom en (onder omstandigheden) het opleggen van een bestuurlijke boete (hoofdstuk 10 Wbp).

3. De situatie in België

3.1. De Kruispuntbank

De uitwisseling van persoonsgegevens in de sector sociale zekerheid wordt in belangrijke mate geregeld in de Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (Kruispuntbankwet). Deze wet heeft geleid tot een voortgaande informatisering van de gegevensverwerking in de sociale zekerheid.

De instellingen van de sociale zekerheid zijn zelf verantwoordelijk voor het opslaan en bijhouden van de eigen gegevens. Tussen deze instellingen ligt een netwerk voor elektronische gegevensuitwisseling. De Kruispuntbank heeft een centrale plaats in dit netwerk. De bank beschikt over een verwijsindex (repertorium) waarin geen inhoudelijke informatie is opgeslagen, maar waarin per persoon wordt aangegeven welke gegevens bij welke instelling(en) worden bijgehouden (artikel 6 Kruispuntbankwet). Als nu een instelling van sociale zekerheid een inlichting over een bepaalde persoon nodig heeft, dient ze zich met de gegevensvraag tot de Kruispuntbank te wenden. De Kruispuntbank haalt vervolgens met behulp van de verwijsindex het gegeven op bij de instelling waar het gegeven wordt bijgehouden en stelt het ter beschikking aan de vragende instelling. Met deze manier van werken wordt voorkomen dat de gegevens telkens bij de burger zelf opgevraagd moeten worden (artikel 11 Kruispuntbankwet).

Het begrip «instellingen van de sociale zekerheid» is een veelomvattend begrip. Alle diensten en instellingen die met toepassing van de sociale zekerheid zijn belast vallen eronder, maar ook alle privaatrechtelijke instellingen die erkend zijn voor de medewerking aan de toepassing van de sociale zekerheid en de fondsen voor bestaanszekerheid (artikel 2 Kruispuntbankwet). Naar schatting zijn ongeveer twintig instellingen aangesloten op het primaire netwerk van de Kruispuntbank en een veelvoud van dat aantal is aangesloten op het secundaire netwerk en heeft zodoende indirect toegang.

3.2. Gegevensuitwisseling over het netwerk

Elke mededeling van persoonsgegevens nodig voor de toepassing van de sociale zekerheid door of aan een instelling van sociale zekerheid gebeurt in beginsel door tussenkomst van de Kruispuntbank (artikel 14 Kruispuntbankwet). Daarbij spelen eveneens de eerder genoemde vraagpunten omtrent de uitwisseling van gegevens, autorisatie en beveiliging.

Welke gegevens worden tussen wie uitgewisseld?
In de Belgische situatie wordt niet op het niveau van wet in formele zin nader bepaald welke gegevens tussen wie worden uitgewisseld maar volstaat een machtiging van de afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en de gezondheid (artikel 15 Kruispuntbankwet). Dit sectoraal comité is een onderdeel van de Commissie voor de bescherming van de persoonlijke levenssfeer, de Belgische tegenhanger van het College bescherming persoonsgegevens.
De verleende machtigingen, waarin is vastgelegd welke gegevens tussen wie kunnen worden uitgewisseld, worden door het sectoraal comité bijge-

houden op een lijst, die iedere belanghebbende bij de Kruispuntbank kan raadplegen (artikel 46 Kruispuntbankwet). Jaarlijks worden tussen de vijftig en honderd aanvragen tot machtigingen gedaan waarvan het overgrote merendeel positief wordt beoordeeld.

Autorisatie
De hiervoor beschreven machtigingen van het sectoraal comité worden door de Kruispuntbank geïmplementeerd in een toegangsmachtigingstabel. Ieder bericht dat voor uitwisseling in aanmerking komt en dat de Kruispuntbank bereikt, wordt geautomatiseerd getoetst aan de hand van deze tabel.

Beveiliging
Op eenieder die uit hoofde van zijn functie betrokken is bij de inzameling, de verwerking of de mededeling van persoonsgegevens die nodig zijn voor de toepassing van de sociale zekerheid rust de plicht om het vertrouwelijke karakter van de gegevens te eerbiedigen (artikel 28 Kruispuntbankwet). De Kruispuntbankwet verplicht de bank en de instellingen van sociale zekerheid om maatregelen te treffen om een perfecte bewaring van de persoonsgegevens te verzekeren (artikel 22 Kruispuntbankwet). De instellingen van sociale zekerheid en de Kruispuntbank zijn verplicht om een veiligheidsconsulent aan te wijzen (artikel 24 Kruispuntbankwet). De veiligheidsconsulent is een deskundige adviseur voor de desbetreffende instelling (artikel 25 Kruispuntbankwet)[1].
Wat betreft de modaliteiten van het netwerk, waaronder de beveiliging, kunnen bij koninklijk besluit regels worden gesteld (artikel 17 Kruispuntbankwet).

De Kruispuntbank heeft binnen het hiervoor geschetste kader op verschillende niveaus concrete maatregelen genomen om de integriteit, de vertrouwelijkheid en de beschikbaarheid van de door haar verwerkte persoonsgegevens op een efficiënte manier te verzekeren. Dit gebeurde meer bepaald op het vlak van de fysieke beveiliging, de logische toegangscontrole tot de gegevens, de logging van de uitgevoerde transacties, de continuïteit van de gegevensverwerking en de uitwisseling van magnetische informatiedragers tussen de instellingen van sociale zekerheid.

3.3. Toezicht

Het eerder genoemde sectoraal comité van de sociale zekerheid en van de gezondheid is met het oog op de bescherming van de persoonlijke levenssfeer (onder meer) belast met het toezicht op de naleving van de Kruispuntbankwet en haar uitvoeringsmaatregelen (artikel 46 Kruispuntbankwet).

Naast het sectoraal comité kent de wet «sociale inspecteurs», die belast zijn met het strafrechtelijke toezicht op de naleving van de Kruispuntbankwet en haar uitvoeringsmaatregelen (artikel 54 Kruispuntbankwet).

4. Overeenkomsten en verschillen

De gegevensuitwisseling in de sector werk en inkomen is in België en in Nederland wettelijk geregeld. In beide landen wordt in de wetgeving de technische en organisatorische infrastructuur aan de orde gesteld waarmee de gegevensuitwisseling plaatsvindt.

De Belgische en Nederlandse infrastructuur vertonen een aantal overeenkomsten maar ook verschillen. In Nederland is er sprake van twee concrete netwerken, Suwinet en Rinis. In België is er sprake van een primair netwerk en daarnaast van secundaire netwerken die door middel

[1] In het Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid wordt voorts voorzien in een werkgroep van (een selectie van) deze functionarissen. Deze groep heeft tot taak (a) de voorbereiding van minimumnormen m.b.t. de fysieke en logische informatieveiligheid, (b) de voorbereiding van een controlelijst voor de evaluatie van de naleving van de minimumnormen inzake fysieke en logische informatieveiligheid en (c) adviesverstrekking aan het Toezichtscomité inzake informatieveiligheid.

van een toegangspunt toegang hebben tot het primaire netwerk. De Belgische constructie vloeit voort uit de organisatie van de sociale zekerheid. Er zijn veel meer afzonderlijke organisaties dan in Nederland.

Er zijn verschillen tussen België en Nederland in de wijze waarop wordt bepaald welke gegevens in welke gevallen tussen wie mogen worden uitgewisseld. In Nederland wordt de uitwisseling van gegevens op wetsniveau preciezer vastgesteld. Op lager niveau vindt nog meer detaillering plaats. De Belgische regelgeving bevat minder precisering van de gegevensuitwisseling. De wet regelt daar dat voor elke uitwisseling een machtigingsbesluit nodig is van (een onderdeel van) de Commissie voor de bescherming van de persoonlijke levenssfeer. Het is in die situatie de toezichthouder die met zijn besluiten de gegevensuitwisseling bepaalt. In Nederland zijn het vaststellen van de regels enerzijds en het toezicht op die regels anderzijds meer uit elkaar getrokken.

In Nederland worden enige tientallen gegevensstromen onderscheiden. In de Belgische situatie gaat het om honderden gegevensstromen die in machtigingsbesluiten zijn gevat. Het grotere aantal gegevensstromen in België wordt overigens niet alleen door de wijze van beschrijven verklaard. De Kruispuntbank handelt meer (soorten van) gegevensverkeer af dan Suwinet en Rinis in Nederland[1].

De autorisatievoorzieningen zijn in beide landen gelijksoortig. Voor een gegevensuitwisseling van een leverende organisatie naar een ontvangende organisatie, moet de laatste zijn geautoriseerd. Deze autorisaties op het niveau van de organisatie zijn vastgelegd in landelijke systemen en worden landelijk afgedwongen. De autorisaties *binnen* organisaties zijn in beide landen een decentrale verantwoordelijkheid.

De informatiebeveiliging van de (inter-organisatorische) netwerken wordt in beide landen geregeld.
Beide landen kennen – naast algemene wetgeving – sectorspecifieke regels over de beveiliging van (interorganisatorische) netwerken en over de beveiliging van de informatie binnen de organisaties in de sociale zekerheid.
Inhoudelijk zijn er geen grote verschillen. In beide landen wordt voorzien in beveiligingsfunctionarissen en daaruit geformeerde werkgroepen om de informatiebeveiliging van de netwerken mede te bewaken.

Het toezicht is in beide landen wettelijk geregeld. In Nederland is de Inspectie Werk en Inkomen van belang; in België de sociale inspecteurs. Daarnaast is er de toezichthoudende rol voor het Nederlandse College bescherming persoonsgegevens en zijn Belgische tegenhanger.

Samenvattend kan gesteld worden dat zowel in Nederland als in België grote aantallen persoonsgegevens worden uitgewisseld tussen organisaties ten behoeve van uitvoeringstaken op het gebied van werk en inkomen. In beide landen zijn duidelijke structuren om deze gegevensuitwisselingen te beheersen.
De verschillen hebben betrekking op de ingezette technische netwerken en op de wijze waarop beslist wordt over de toelaatbaarheid van een bepaalde gegevensuitwisseling.
Op het gebied van autorisatie en informatiebeveiliging zijn geen essentiële verschillen te bespeuren.

[1] Over de Kruispuntbank lopen bijvoorbeeld ook gegevensstromen betreffende «Attest voor de automatische toekenning van aanvullende rechten voor openbaar vervoer en verwarmingstoelage».