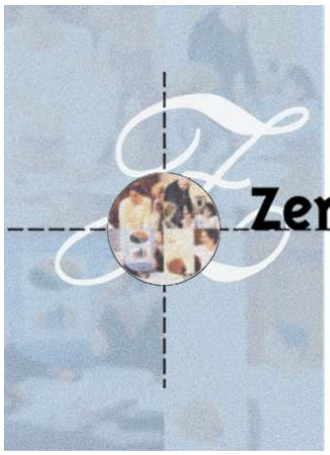


De toekomst van persoonsinformatiebeleid

Een dynamische kijk op privacy

In opdracht van:
De heer H.J.M. van Zon
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Innovatie en Informatiebeleid Openbare Sector

Auteurs:
Drs. Abdelilah Azouz
Mr. Huib Gardeniers
Drs. Pim Jörg
Drs. Femke Polman
Drs. Bettine Pluut
Dr. Arre Zuurmond

Inhoudsopgave

1. Inleiding

1.1. Synopsis

In het digitale tijdperk is sprake van veelzijdige ontwikkelingen die consequenties hebben voor het persoonsinformatiebeleid. Deze ontwikkelingen maken structureel nadenken over het persoonsinformatiebeleid noodzakelijk.
De volgende ontwikkelingen zijn relevant:

- *maatschappelijke en internationale ontwikkelingen*, bijvoorbeeld: liberalisering en globalisering van de maatschappij en economie, en het daarmee samenhangende belang van terrorisme- en fraudebestrijding;
- *bestuurlijke ontwikkelingen*: bijvoorbeeld de ontwikkeling naar meer digitale debatten en interactieve besluitvorming;
- *organisationele ontwikkelingen*: bijvoorbeeld de ontwikkelingen rond een geïntegreerde front-office, en/of rond proactieve dienstverlening;
- *technologische ontwikkelingen*: bijvoorbeeld de toename van koppelingen en het toegenomen gebruik van een steeds grotere variatie aan technologische hulpmiddelen;
- *juridische ontwikkelingen*: bijvoorbeeld veranderingen in wet- en regelgeving aangaande de bevoegdheden van inlichtingen- en veiligheidsdiensten.

Met het oog op de snelheid waarmee deze ontwikkelingen zich aftekenen, heeft de Minister voor Bestuurlijke Vernieuwing en Koninkrijkrelaties aan Zenc de opdracht gegeven de wenselijkheid tot herijking van het persoonsinformatiebeleid te onderzoeken en beleidsprioriteiten voor en ingrediënten van dit beleid te benoemen.
Het onderzoek bestaat uit een duiding van het begrip privacy in het kader van het persoonsinformatiebeleid, een oriëntatie op de relevante ontwikkelingen, uit een analyse van de huidige situatie omtrent privacy(beleving) en uit het opstellen van toekomstscenario's. Besluitvorming over een eventuele herijking van het persoonsinformatiebeleid en het daarmee verbonden proces van besluitvorming behoren niet tot deze opdracht. Dit onderzoek reikt daartoe bouwstenen aan.

Inzicht in het begrip privacy
In deze studie is als uitgangspunt gehanteerd dat privacy een samenstel is van normen, waarden en overtuigingen, waarbij vrijheid, individualiteit, (enige mate van) controle over informatie die over elke persoon beschikbaar is en de vrijwaring voor de oordelen van anderen kenmerkende elementen zijn. De precieze aard en betekenis van die normen, waarden en overtuigingen kunnen zich onder invloed van tal van factoren, zoals maatschappelijke ontwikkelingen, wijzigen. Ook de omgeving waarin een persoon zich bevindt (thuis, ziekenhuis, openbaar vervoer) is van invloed op het belang dat mensen aan privacy hechten. Privacy kan zowel worden beschouwd als een *contextafhankelijk als een dynamisch begrip*.
Hoe noodzakelijk is de herijking van het persoonsinformatiebeleid? Daarvoor is genuanceerd inzicht in het concept privacy met zijn verschillende bouwstenen en aspecten van belang. In hoofdstuk twee wordt verslag gedaan van de literatuurstudie die tot een dergelijke uiteenrafeling van het concept en het benadrukken van het contextgebonden karakter leidt. Van oudsher zijn vier aspectgebieden aan het begrip privacy onderscheiden. Deze zijn traditioneel geordend naar de mate waarin zij direct zichtbaar zijn voor de betrokkene, en wel als volgt:

- *de ruimtelijke privacy:* het recht op een eigen fysieke ruimte[1];
- *de lichamelijke privacy*: het recht op integriteit van lichaam en geest;
- *de relationele privacy*: het recht om te communiceren met personen van je eigen keuze en het recht op geheimhouding van die communicatie[2];
- *de informationele privacy*: het recht van individuen, groepen of instituties om voor zichzelf te bepalen welke informatie over hen hoe, wanneer en in welke mate wordt gecommuniceerd.

Vaak wordt daar waar het gebruik van persoonsinformatie betreft dataprotectie als uitgangspunt voor privacy genomen. De focus ligt dan op *het gereguleerd afschermen van persoonsgegevens*. Het denken over privacy in de context van het persoonsinformatiebeleid is echter geholpen bij een breder begrip, waarbij de focus ligt op *informationele privacy*. Informationele privacy kan gezien worden als een recht op *informationele zelfbeschikking.* Dit wil zeggen dat eenieder het recht heeft zelf te bepalen welke informatie over hem- of haarzelf openbaar wordt gemaakt – informationele privacy is op deze manier een *actierecht*. Daarnaast heeft iedere burger recht op bescherming in verband met de informatie die over hem bekend is of die ten aanzien van hem wordt toegepast. Informationele privacy kan daarmee ook worden gezien als een *afweerrecht*.

Naar een evenwichtige verhouding tussen privacy en andere belangen
Nu is het voor de werking van onze moderne maatschappij en economie van groot belang dat (persoons)gegevens onder bepaalde omstandigheden verwerkt worden. Deze verwerking is nooit een doel op zich. Immers, zonder het verwerken van persoonsinformatie zouden vele processen en transacties in onze maatschappij een stuk moeilijker, minder efficiënt of simpelweg onmogelijk zijn. Met andere woorden, verwerking van persoonsgegevens dient belangen als dienstverlening, veiligheid en gezondheidszorg. Daarom is er geen absoluut recht op informationele zelfbeschikking.
Deze benadering betekent een breuk met de traditionele kijk op privacy. In een meer traditionele benadering krijgt het belang van de burger om te bepalen welke informatie over hem bekend mag zijn voor anderen een bijna absoluut karakter. In deze studie onderscheiden we naast het belang van informationele privacy ook andere belangen, die om een grotere mate van verwerking van persoonsinformatie vragen dan wanneer enkel in absolute zin naar het belang van informationele privacy wordt gekeken.

Het belang van afwegingen per beleidsterrein
De vergaring, opslag en uitwisseling van persoonsinformatie dient uiteraard zorgvuldig plaats te vinden. Immers, aan de ene kant is er de wenselijkheid voor diverse instanties om toegang te hebben tot diverse persoonsgebonden gegevens en om deze uit te wisselen. Anderzijds is er het belang van informationele privacy van het individu. Een modern persoonsinformatiebeleid heeft als doel te voorkomen dat er een disproportionele inbreuk plaatsvindt op dit privacybelang van het individu. In de context van dit beleid wordt gestreefd naar een evenwichtige verhouding tussen informationele privacy en andere belangen. Een dergelijke benadering kenmerkt zich door het uitgangspunt dat er geen absolute, vaste bepaling is te doen voor de mate waarin individuele gegevens beschikbaar zijn voor anderen. Het gewicht dat verschillende belangen, omstandigheden en overwegingen krijgen, is contextgebonden en kan niet waardevrij zijn. Ter illustratie, de afweging wat betreft de mate waarin persoongebonden informatie voor instanties beschikbaar is, valt in het geval van terrorismebestrijding

[1] Hieronder valt bijvoorbeeld het recht om anderen uit je huis te weren (het huisrecht).
[2] Hieronder valt bijvoorbeeld het briefgeheim en het telefoongeheim, maar ook het recht om niet opgebeld te worden of geen ongevraagde post te krijgen.

wezenlijk anders uit dan wanneer commerciële bedrijven inzicht willen krijgen in potentiële doelgroepen voor nieuwe producten.
Het gaat daarmee om een subjectieve, vaak politieke afweging, die in essentie door de wetgever moet worden bepaald. Deze afweging is zowel gecompliceerder als urgenter geworden vanwege de opkomst van ICT en bijvoorbeeld de toenemende mogelijkheden tot koppeling van gegevensbestanden.

Op welke waarden en belangen heeft dit afwegingsproces dan precies betrekking? Aan privacy liggen in den brede belangrijke waarden ten grondslag. Burgers willen dat hun privacy gegarandeerd wordt omdat op deze manier recht wordt gedaan aan waarden als zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie. Maar aan deze waarden wordt niet door iedereen en in iedere context hetzelfde belang gehecht. De belangen van terreinen van veiligheid, gezondheidszorg, opsporing, fraudebestrijding en administratieve lastenverlichting kennen elk een andere afweging met betrekking tot de informationele privacy van de burger. Ieder beleidsterrein kent dan ook zijn eigen belangen, waarden en vereisten die in het afwegingsproces omtrent een nieuwe maatregel moeten worden meegenomen. Door procesbegeleiding van het persoonsinformatiebeleid wordt gezorgd dat geen vereisten over het hoofd worden gezien.

Kansen en uitdagingen
De hedendaagse ICT-toepassingen en inzichten bieden de mogelijkheid om verbeteringen aan te brengen op elk van bovenstaande terreinen. Zij bieden kansen voor politieke processen en processen ten aanzien van beleidsontwikkeling, dienstverlening, handhaving, bedrijfsvoering en beheer. Deze verbeteringen kunnen echter bij een onvoldoende sterk vormgegeven persoonsinformatiebeleid niet in verhouding staan tot de eventuele negatieve gevolgen voor informationele privacy. In het onderzoek is echter gebleken dat de papieren koppeling van gegevens net zo goed bedreigingen voor de informationele privacy met zich meebrengt als digitale koppelingen van persoonsgegevens. Daarbij komt dat een herijking van het persoonsinformatiebeleid mogelijk wordt doordat dezelfde technologieën die een bedreiging voor de informationele privacy kunnen zijn ook mogelijkheden bieden om informationele privacy te borgen en een nieuw, contextafhankelijk evenwicht te bereiken. Zo biedt de technologie de mogelijkheid om voor elke burger die dat wenst op zijn Persoonlijke Internet Pagina te tonen welke organisaties op welk moment welke gegevens hebben geraadpleegd.

De studie naar de eerder onderscheiden ontwikkelingen laat zien dat burgers momenteel veel waarde hechten aan correcte omgang met hun persoonsinformatie, maar dat zij tegelijkertijd weinig zicht hebben op deze omgang. Tegelijkertijd kan worden geconstateerd dat de burger in de afgelopen jaren een ander optimum met betrekking tot informationele privacy geaccepteerd lijkt te hebben, mede in het licht van de preventie en bestrijding van terrorisme en criminaliteit. Ook lijken onderzoeken erop te wijzen dat het optimum op het terrein van de zorg verschuift[3]. Het gevaar bestaat dat veranderingen in de omgang met persoonsinformatie leiden tot een aanzienlijke vermindering van het vertrouwen in overheidsinstanties. Dit staat haaks op de huidige trend van het streven naar een betere overheidsdienstverlening en verbeterde relatie tussen overheid en burger. Bovendien is een verminderd vertrouwen in de overheid vanuit innovatief en economisch oogpunt onwenselijk. Uit onderzoek blijkt immers dat voor het slagen van

[3] Voor een nadere uitwerking en onderbouwing hiervan, zie hoofdstuk vier.

technologische innovaties vertrouwen van burgers in de overheid essentieel is. En een gebrek aan vertrouwen kost geld.

Begeleiding van het afwegingsproces
Persoonsinformatiebeleid is nooit een doel op zich, maar is altijd aanpalend aan ander beleid (bijvoorbeeld veiligheidsbeleid). Dit betekent dat bij de totstandkoming van beleid expliciet het doel en het gewenste effect van een in te zetten middel (bijvoorbeeld cameratoezicht) afgewogen worden tegen de mogelijke effecten op de informationele privacy. Daarbij bewaakt het persoonsinformatiebeleid dat in te zetten middelen tegen de juiste (wettelijke of aanvullende) vereisten worden getoetst, en dat er oog is voor de cumulatieve effecten van wet- en regelgeving. Daarnaast heeft het persoonsinformatiebeleid als belangrijke taak dat dergelijke afwegingen transparant en communiceerbaar zijn.

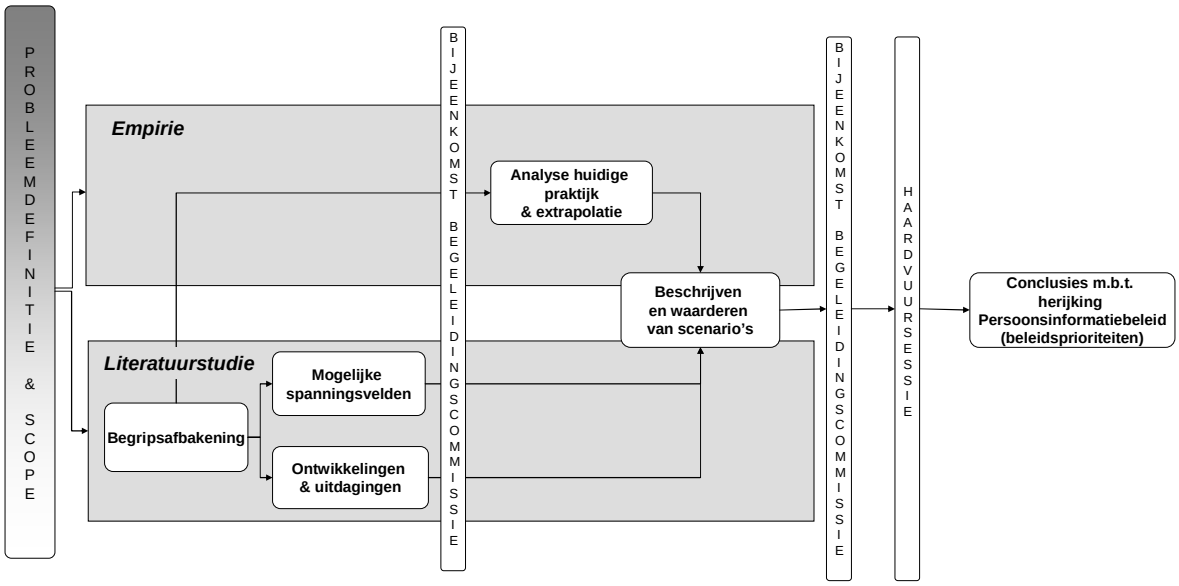
Privacy in de uitvoeringspraktijk
In de praktijk blijkt het slecht gesteld te zijn met de informationele privacy van de burger. Op papier lijken papieren koppelingen een aantrekkelijk alternatief voor digitale koppelingen, maar zij blijken dat in de praktijk niet te zijn. In gemeenten komt het bijvoorbeeld voor dat papieren dossiers die veel persoonsgegevens en daarmee privacygevoelige informatie bevatten, in officieel gesloten gangkasten liggen, soms kwijt raken en niet beveiligd vervoerd worden van de ene locatie naar de andere. Daarnaast blijkt dat de Wet bescherming persoonsgegevens, alhoewel deze wel degelijk mogelijkheden biedt om de privacy te waarborgen, in de praktijk lastig te handhaven. Het draait uiteindelijk om de uitvoeringspraktijk en daarin bestaat een gebrek aan actieve controle en toezicht op het gebruik van persoonsinformatie. Tot slot is privacy in de onderzochte praktijk nauwelijks vormgegeven als actierecht. De burger heeft zelden de mogelijkheid om over het uitwisselen van zijn eigen persoonsgegevens te beslissen. Al deze bevindingen maken een herijking van het persoonsinformatiebeleid urgent.

Prioriteiten en instrumenten voor het persoonsinformatiebeleid
Burgers moeten kunnen vertrouwen op de integriteit van instellingen die over hun persoonsinformatie beschikken. Daarom heeft het persoonsinformatiebeleid als belangrijke prioriteit de relatie tussen overheid en burger te optimaliseren. Overheden dienen openheid te verschaffen over de afwegingen die worden gemaakt omtrent het gebruik van deze informatie. Daarnaast is het essentieel dat de burger meer de regie krijgt over het gebruik van zijn persoonsinformatie. Daarbij draait het niet alleen om het gebruik van persoonsinformatie door overheidsorganisaties, maar ook door private partijen. Deze aspecten van de informationele privacy zijn de afgelopen jaren onderbelicht geweest in het maatschappelijk en politiek debat.
Voor het welslagen van het persoonsinformatiebeleid is het debat rond de afweging tussen de informationele privacy en de inhoudelijke belangen urgent. Om dit debat te stimuleren, kan op basis van het persoonsinformatiebeleid wet- en regelgeving worden geëvalueerd en kan onderzoek worden gedaan naar de huidige privacyproblematieken en privacybeleving van burgers. Op basis van dit beleid kunnen privacy-effectrapportages worden opgesteld. Voorts dient het persoonsinformatiebeleid het gebruik van ICT te stimuleren op een manier dat nieuwe optima tussen privacy en andere belangen worden gerealiseerd. Dit vanuit de visie dat de papieren omgang met persoonsinformatie geen voldoende waarborg voor de privacy biedt, daar waar de slimme inzet van ICT dat wel mogelijk maakt.

1.2. Onderzoeksopzet en opbouw van dit rapport

Om tot rapportage van onze bevindingen te komen, zijn de nodige stappen gezet. De stappen laten zich als volgt omschrijven. Bij aanvang is sprake geweest van een *intensieve literatuurstudie*. Vervolgens zijn enkele praktijksituaties en –ontwikkelingen geïnventariseerd en geanalyseerd. Als laatste is sprake geweest van een confrontatie tussen empirie en theorie, uitmondend in conclusies ten aanzien van een mogelijke herijking van het persoonsinformatiebeleid.
Als ondersteuning voor de lezer is de rode draad in het betoog geïntroduceerd in de synopsis in dit hoofdstuk. De diverse stappen die het betoog in stand houden, worden successievelijk uitgewerkt in de volgende hoofdstukken.

De verschillende onderzoeksfasen zijn in onderstaande figuur weergegeven.



Figuur 1.1: Onderzoeksfasen

De inhoud van elk van de drie delen van het onderzoeksrapport is als volgt:

- *Deel 1: theoretische verkenning*

In dit onderdeel van het onderzoek is het begrip privacy nader verkend en is de relatie gelegd met het thema persoonsinformatiebeleid. Op basis van deze literatuurstudie is de keuze voor een begripsafbakening gemaakt. Vervolgens is er in de literatuurstudie aandacht besteed aan de mogelijke spanningsvelden tussen privacy en de belangen van andere beleidsterreinen. Tevens is gekeken naar relevante ontwikkelingen, hun betekenis voor de informationele privacy en de uitdagingen die deze ontwikkelingen stellen aan het persoonsinformatiebeleid.

- *Deel 2: privacy in de praktijk*

Het is niet mogelijk mogelijke beleidsprioriteiten en bijpassende instrumenten van, en voor, het persoonsinformatiebeleid te formuleren als geen inzicht bestaat in de huidige situatie omtrent privacy en persoonsinformatie. Op basis van de begripsafbakening en de onderscheiden ontwikkelingen, uitdagingen en spanningsvelden is aan de hand van een

drietal casussen de huidige situatie onderzocht. Het streven is geweest om de casussen zodanig te kiezen dat de mogelijke spanningsvelden tussen privacy en ander belangen terugkomen in de te onderzoeken praktijk.

Met de personen die betrokken zijn bij de praktijkcasus is niet alleen de huidige situatie besproken, maar is eveneens van gedachten gewisseld over de mogelijke scenario's. Dit is gebeurd door met hen te reflecteren op kansen en bedreigingen voor de (informationele) privacy in de toekomst. Op deze manier kon een extrapolatie van de huidige situatie plaatsvinden. Ook is zo maatschappelijke inbreng gerealiseerd.

- *Deel 3: de toekomst van persoonsinformatiebeleid*

Als afsluiting van de studie zijn enkele toekomstscenario's opgesteld. Het beeld van het functioneren van de toekomstige overheid is gebaseerd op scenario's zoals beschreven in "De Overheid als Infrastructuur"[1]. In de scenario's worden de onderzochte casussen geplaatst in een denkbeeldige, toekomstige situatie.
Uiteindelijk worden in deze studie de mogelijke beleidsprioriteiten en -instrumenten voor het persoonsinformatiebeleid benoemd. Deze zijn besproken, aangevuld en op deze manier gevalideerd tijdens een bijeenkomst met de begeleidingscommissie.

1.3. Begeleidingscommissie en haardvuursessie

Interactie over de huidige en toekomstige situatie van het persoonsinformatiebeleid is van wezenlijk belang. In dit onderzoek zijn daarom de stakeholders en/of experts bij het onderzoeksproces betrokken. Zij zijn gevraagd mee te denken over:

- de te ontwikkelen definitie van privacy;
- de schets van de onderscheiden ontwikkelingen;
- de keuze voor de empirische casussen;
- de interpretatie van de scenario's;
- de betekenis van dit geheel voor de mogelijke herijking van het persoonsinformatiebeleid.

De stakeholders en/of experts is drie keer gevraagd om hun mening te geven. Allereerst is een begeleidingscommissie samengesteld, waarin de opdrachtgever, opdrachtnemer en experts van gedachten hebben gewisseld over de inhoudelijke en procesmatige vormgeving van het onderzoek. De eerste bijlage bevat de samenstelling van deze begeleidingscommissie.
De begeleidingscommissie is tweemaal bijeengekomen. De eerste keer is geweest na de conceptrapportage over het theoretische gedeelte, wanneer de commissie de invulling van de definitie, de afbakening, de beschrijving van het persoonsinformatiebeleid en de keuze voor en invulling van concrete casus heeft besproken. Na afsluiting van het empirische gedeelte en het opstellen van de conceptscenario's heeft een tweede ontmoeting van de begeleidingscommissie plaatsgevonden. Daarin is de conceptanalyse besproken en is in gezamenlijkheid gediscussieerd over de conceptscenario's en mogelijke beleidsprioriteiten en - instrumenten.
Nadat de scenario's zijn opgesteld en de beleidsprioriteiten en –instrumenten zijn vastgesteld in de eindrapportage, worden tijdens een haardvuursessie met een bredere groep stakeholders de onderzoeksresultaten besproken.

Deel één:
Een theoretische verkenning van privacy

2. Privacy: definities en invalshoeken[4]

In dit hoofdstuk wordt een theoretisch kader geschetst rondom de begrippen privacy en persoonsinformatiebeleid. Dit gebeurt op basis van een bestudering van de literatuur. De literatuur betreft natuurlijk de privacy zelf en tevens een analyse van de privacywetgeving alsmede een analyse van geschiedenis, doel, verantwoordelijkheid en bereik van het persoonsinformatiebeleid. De literatuurverkenning dient ertoe om de verschillende onderdelen van privacy te doorgronden en om te begrijpen dat het concept geen statisch maar juist een contextgebonden en dynamisch karakter heeft. In de eerste paragraaf wordt de complexiteit van het begrip privacy geschetst. Vervolgens vindt een verenging plaats en wordt het begrip privacy bezien in relatie tot wet- en regelgeving. In aansluiting daarop wordt privacy beschouwd in relatie tot beginselen van gegevensbescherming. Vervolgens wordt het bredere perspectief van de informationele privacy geanalyseerd.
Om in het licht van persoonsinformatiebeleid een keuze te maken voor een afbakening van het begrip privacy, is het van belang dat het doel en bereik van persoonsinformatiebeleid in ogenschouw worden genomen. Hier zal in paragraaf 2.3 bij worden stilgestaan. Dit hoofdstuk mondt vervolgens uit in een keuze voor een begripsafbakening met betrekking tot privacy en persoonsinformatiebeleid.

2.1. Privacy vanuit verschillende invalshoeken: definiëring van een complex begrip

2.1.1. Uitwerking van het begrip privacy

Bij de omschrijving van het begrip privacy wordt vaak verwezen naar noties als *het recht om met rust gelaten te worden*. Deze benadering plaatst privacy in de categorie van de afweerrechten. Het waren Warren en Brandeis[2] die privacy ruim een eeuw geleden op deze wijze op de kaart hebben gezet. Het is een benadering die verwantschap vertoont met de klassieke grondrechten: vrijheidsrechten van de burger ten opzichte van de overheid.
Een van recenter datum afkomstige benadering om privacy te duiden is meer actief. Hier wordt privacy gezien als *het recht om zelf te bepalen wat er met de toegang tot, en met zijn of haar persoonsinformatie gebeurt*. Het is meer een actierecht. De persoon zelf is degene die zijn eigen vrije ruimte bewaakt en behoudt. Deze benadering, ontstaan in de jaren ’60 en waarvan Westin[3] de grondlegger genoemd kan worden, roept de gedachte op van de sociale grondrechten: de aanspraken op een maatschappelijk en cultureel volwaardig leven.[4]

De visies vanuit het individu bezien richten zich op de (afzonderlijke) positie van actoren. In de privacyvisie van Johnson[5] ligt de nadruk meer op de relatie tussen de betrokken actoren. De rol of functie die privacy speelt in het maatschappelijk verkeer ligt in deze relatiegerichte visie in *de bescherming van bepaalde aspecten van individuen tegen de (positieve of negatieve) evaluatieve oordelen van anderen*. Een precieze afbakening wordt daarbij keer op keer bepaald door uiteenlopende factoren zoals bijvoorbeeld maatschappelijke omstandigheden of ontwikkelingen in techniek en technologie.[6]

[4] Dit hoofdstuk is mede tot stand gekomen op basis van de inbreng van Eric Schreuders, tevens lid van de begeleidingscommissie.

De relatiegerichte benadering stelt voorop dat de betekenis en inhoud van privacy dynamisch en afhankelijk is van de omstandigheden. Volledig vaststaande kaders, begrippen of definities passen daar niet bij. Wat vandaag nog onaanvaardbaar is, kan morgen bij een weliswaar gelijkblijvend juridisch toetsingskader maar gewijzigde maatschappelijke omstandigheden wel degelijk tot de mogelijkheden behoren, of andersom. Het relatiegerichte perspectief op privacy plaatst door zijn nadruk op de context de relatie van het individu met anderen meer centraal dan de visies die in het bijzonder het perspectief van het individu hanteren.

Een relatiegericht perspectief op privacy maakt de vraag naar de opvattingen van individuen over privacy relevant. Immers, indien de betekenis en inhoud van privacy afhankelijk zijn van omstandigheden, dan is het interessant wat de (huidige) dominante opvattingen van burgers zijn.
Er is de afgelopen decennia in Nederland[7] een aantal onderzoeken uitgevoerd naar privacy, de praktische uitvoering en uitvoerbaarheid van privacywetgeving en de opvattingen van individuen over privacy en privacybedreigingen[8]. Maar het onderzoek *Privacybeleving van burgers in de informatiemaatschappij*[9] is in feite het enige Nederlandse onderzoek dat de vraag naar de waarden, normen en opvattingen achter privacy centraal stelt. De waarden die volgens dit onderzoek achter opvattingen over privacy schuilgaan zijn:

- zelfstandigheid;
- bewegingsvrijheid;
- gelijkheid;
- vrij blijven van stigmatisering;
- ongestoord leven;
- eigenwaarde;
- vrij blijven van manipulatie;
- integriteit en autonomie.[10]

De bevindingen[11] over de onderliggende waarden en opvattingen over privacy zijn enerzijds dat verschillende personen verschillende waardestelsels hanteren en verschillende waarden meer of minder belangrijk vinden. Anderzijds is het zo dat dezelfde personen in verschillende situaties andere waarden belangrijk vinden. Privacy en de waarden die daarbij een rol spelen zijn derhalve in algemene zin wel in kaart te brengen, maar de waarde of waarden die als het meest belangrijk of vormend voor privacy worden beschouwd, verschillen van persoon tot persoon en van situatie tot situatie.[12]

Samenvattend
Samenvattend kan privacy gezien worden als een samenstel van normen, waarden en overtuigingen, waarbij vrijheid, individualiteit, (enige mate van) controle over informatie over iemand zelf en de vrijwaring voor de oordelen van anderen kenmerkende elementen zijn. Daarbij kan privacy worden gezien als een afweer- en een actierecht. Een doel van privacy is dat de individualiteit en de individuele eigenschappen en verdiensten van individuen gerespecteerd worden. Daarbij is het wel zo dat de precieze aard en betekenis van die normen, waarden en overtuigingen onder invloed van tal van factoren, zoals maatschappelijke en economische ontwikkelingen, kunnen wijzigen. Hierdoor kan gesteld worden dat privacy een contextafhankelijk begrip is.

2.1.2. Vier vormen van privacy

Het begrip privacy kan worden onderverdeeld naar aspectgebieden. Deze zijn traditioneel geordend naar de mate waarin zij direct zichtbaar zijn voor de betrokkene, en wel als volgt:

- *de ruimtelijke privacy:* het recht op een eigen fysieke ruimte[13];
- *de lichamelijke privacy*: het recht op integriteit van lichaam en geest;
- *de relationele privacy*: het recht om te communiceren met personen van je eigen keuze en het recht op geheimhouding van die communicatie[14];
- *de informationele privacy*: het recht van individuen, groepen of instituties om voor zichzelf te bepalen welke informatie over hen hoe, wanneer en in welke mate wordt gecommuniceerd.

De scheidslijnen tussen deze vier vormen van privacy zijn in het digitale tijdperk minder duidelijk. Vele, soms zeer ingrijpende, inbreuken op de privacy vinden niet tot nauwelijks voor de betrokkenen zichtbaar plaats. Te denken is aan het inkijken van internetverkeer, filmen in de openbare ruimte of, zoals op vliegvelden wel gebeurt, het gebruik van infrarode camera's om op basis van waargenomen lichaamstemperatuur te beoordelen of iemand een mogelijk drager van het SARS-virus is. Een opsplitsing van het begrip privacy is echter nuttig voor een analyse in de context van het persoonsinformatiebeleid, doordat de verschillende vormen met elkaar kunnen worden vergeleken en de verhoudingen tussen de verschillende vormen kunnen worden benoemd.

2.1.3. Privacy in relatie tot wet- en regelgeving

Privacy als grondrecht wordt (voor Nederland) in juridische zin beschermd in artikel 10, eerste lid, en de artikelen 11 tot en met 13 van de Grondwet, in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)[15] en in artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR).[16] Daarnaast heeft informationele privacy juridische erkenning en uitwerking gekregen in de beginselen ter bescherming van persoonsinformatie. In zowel de OESO[17] privacyrichtlijnen,[18] het Databeschermingsverdrag van 1981 van de Raad van Europa (RvE),[19] in de EG-Privacyrichtlijnen,[20] en in artikel 10, tweede en derde lid, van de Grondwet gaat het om de bescherming van persoonsinformatie.[21] Het gaat hierbij om dataprotectieregels. Dat de bescherming van privacy (privé-leven) en de bescherming van persoonsinformatie twee zelfstandige onderdelen zijn, komt ook naar voren in het Ontwerp Handvest van de Grondrechten van de Europese Unie, waar beide een eigen vermelding hebben.[22]

Bij aandacht voor juridische normen over en ter bescherming van privacy verkleint het blikveld zich, vaak nogal impliciet, van het brede concept van privacy tot regels die de omgang met persoonsinformatie tot onderwerp hebben. Zoals uit bovenstaande blijkt, zijn privacyregels over het verwerken van persoonsinformatie maar een onderdeel van de regulering van privacy en privacybescherming. Privacyregels zijn ook de regels ten aanzien van bijvoorbeeld het huisrecht (ruimtelijke privacy),[23] over de lichamelijke en geestelijke integriteit (lichamelijke privacy),[24] en regels ten aanzien van communicatie (relationele privacy)[25].

Gemeenschappelijk in de beschrijvingen en opvattingen over privacy is het niet-absolute karakter daarvan en de afweging van belangen. De positie van de betrokkene, van de 'aantaster' en het meer overkoepelende belang van de maatschappelijke ordening spelen daarbij een rol. Een eenduidige definitie van privacy is dus niet realiseerbaar en is

overigens voor een juridische vormgeving van privacy en de bescherming daarvan ook niet nodig. Het hanteren van privacy als een ‘concept’ levert geen onoverkomelijke problemen op voor een juridische bescherming.

Samenvattend
Ook een juridisch perspectief op privacy geeft geen duidelijke definitie van privacy of privacybescherming. Wel wordt in specifieke regels duidelijk *welke aantasting geoorloofd is of kan zijn* en dus wat in ieder geval binnen de bescherming van privacy ligt. Dit aspect lijkt typisch of kenmerkend voor juridische bescherming van privacy: het zijn de regels die bepaalde inbreuken mogelijk maken en die als gevolg daarvan aangeven en juridisch vaststellen wat ‘dus’ tot het domein van privacy behoort. Een optelsom van deze verschillende inbreukveroorlovende regels en waarden geeft een beeld van het begrip privacy.
In de wet- en regelgeving is privacy echter grotendeels ontdaan van haar dynamische kenmerken. Daarmee kan gesteld worden dat de juridische interpretatie van privacy zich impliciet verengt naar het fenomeen dataprotectie. Privacy is echter een breder en alomvattender concept, dat verder reikt dan de bescherming van persoonsinformatie.

2.1.4. Beginselen voor de verwerking van persoonsgegevens

In voorgaande paragraaf is geconstateerd dat de privacydiscussie zich vaak verengt tot een discussie over dataprotectie en bijbehorende wetgeving. In deze paragraaf zal worden gekeken naar de beginselen die ten grondslag (zouden moeten) liggen aan wet- en regelgeving of aan beleid dat het verwerken regelt van persoonsinformatie.

De beginselen voor de verwerking van persoonsgegevens en de hiermee verbonden bescherming van de persoonlijke levenssfeer zijn terug te vinden in internationaal aanvaarde beginselen, zoals neergelegd in de OESO-privacyrichtlijnen (zie bijlage 2) en het Europese Databeschermingsverdrag. Het doel van de beginselen is te waarborgen dat enerzijds de negatieve aspecten van de technologie tot een minimum worden beperkt en anderzijds voldoende ruimte over wordt gelaten om van de voordelen van deze vormen van technologie te kunnen blijven profiteren. Al deze beginselen hebben met de tijd bewezen waardevolle aanknopingspunten te zijn voor een flexibele benadering van de bescherming van informationele privacy in het licht van de vele technologische ontwikkelingen.

De gedachte achter de beginselen is, dat indien men volledige informationele privacy wil bereiken, aan alle beginselen voldaan moet zijn. Met andere woorden, de beginselen geven een minimumstandaard voor bescherming. Zij zijn juridisch niet bindend, maar vormen wel wereldwijd de basis voor diverse dataprotectie wet- en regelgeving. De Europese wet- en regelgeving heeft vergelijkbare beginselen als uitgangspunt.

2.1.5. Een vergelijking van dataprotectie en informationele privacy

Een belangrijk onderscheid dat in dit hoofdstuk naar voren is gekomen, is het verschil tussen informationele privacy en dataprotectie. In het laatste gedeelte van dit hoofdstuk zullen de begrippen informationele privacy[26], dataprotectie en persoonsinformatiebeleid nader verkend worden om zo te komen tot een beargumenteerde begripsafbakening.

Onderstaande tabel geeft de verschillen tussen dataprotectie en informationele privacy weer. Deze verschillen worden in deze paragraaf uitgewerkt

Dataprotectie	Informationale privacy
Juridisch begrip	Contextafhankelijk en dynamisch begrip
Afweerrecht	Afweerrecht én actierecht
Recht op bescherming van persoonsgegevens	Recht op informationele zelfbeschikking
Het draait om het beperken van risico's van gegevensuitwisseling	Het draait om afwegingen tussen verschillende belangen

Tabel 2.1: Verschillen tussen dataprotectie en informationele privacy

Dataprotectie is een juridisch begrip. In wet- en regelgeving met betrekking tot dataprotectie wordt bepaald welke aantasting van de informationele privacy geoorloofd is. Daarbij blijft de *afscherming van gegevens* centraal staan. Het feitelijke gebruik van gegevens, waardoor een eventuele inbreuk op de persoonlijke levenssfeer kan plaatsvinden, wordt daardoor vooral indirect geregeld. De gedachte hierachter is dat als je alle mogelijke vormen van gebruik reguleert, je uiteindelijk ook het concrete gebruik reguleert. Informationele privacy is veel meer een dynamisch, contextafhankelijk begrip. Het heeft betrekking op de eerder genoemde waarden die achter het begrip privacy schuilgaan, zoals bewegingsvrijheid, gelijkheid en eigenwaarde.

Dataprotectiewetgeving, zoals de 'wet bescherming persoonsgegevens' regelt voornamelijk de bescherming van gegevens. Privacy is daarin met name een afweerrecht. Dit is een wezenlijk verschil met de invalshoek van de informationele privacy, waarbij het, naast een recht op bescherming ook draait om een recht op informationele zelfbeschikking. Privacy is dan zowel een afweer- als een actierecht.

Wanneer er geen afdoende aanpalend beleid –lees persoonsinformatiebeleid- is dat de informationele privacy regelt, zal diezelfde privacy enkel vorm krijgen vanuit een dataprotectie-invalshoek. Concreet betekent dit dat ontwikkelingen die door nieuwe informatietechnologie mogelijk gemaakt worden (bijvoorbeeld basisregistraties) het gevaar lopen door deze dataprotectiewetgeving afgeremd te worden. Immers, de techniek biedt vele vormen van mogelijk gebruik van gegevens die vanuit een dataprotectie-invalshoek alle op voorhand strak geregeld dienen te worden. Dataprotectie focust daarmee op het mogelijk misbruik van persoonsgegevens. Informationele privacy, daarentegen, kijkt meer naar de voor- en nadelen van het gebruik van persoonsgegevens en de daarmee verbonden belangenafwegingen.

Er zijn aanzienlijke verschillen tussen de invalshoek van informationele privacy en die van dataprotectie. Waar vanuit de dataprotectie-invalshoek veelal op voorhand alle mogelijke verwerkingen van persoonsinformatie geregeld worden, worden vanuit de informationele privacyinvalshoek veel meer de kaders gesteld waaraan mogelijk gebruik/verwerking van persoonsinformatie moet voldoen. Zolang informationele privacy, zoals nu het geval is, met name geregeld wordt vanuit dataprotectiewetgeving als de 'Wet bescherming persoonsgegevens' is het lastig een optimum te bereiken ten aanzien van informationele privacy en andere beleidsthema's waaraan nieuwe technologieën een

bijdrage willen leveren. Het is hierbij goed op te merken dat informationele privacy niet betekent dat geen dataprotectiewetgeving dient te worden gemaakt. Informationele privacy betekent dat je naast (een minimale vorm van) dataprotectiewetgeving ernaar streeft een optimum te bereiken tussen privacy en andere belangen en dat je naast het afweerrecht ook actierechten creëert.

2.2. Privacy in relatie tot het persoonsinformatiebeleid

De discussie heeft zich tot op heden rondom de drie begrippen privacy, dataprotectie en informationele privacy afgespeeld. Geconcludeerd kan worden dat privacy een breed begrip is. Het begrip heeft immers ook betrekking op zaken als de integriteit van lichaam en geest.
Om nu in het licht van persoonsinformatiebeleid een beargumenteerde keuze te maken tussen het enge begrip dataprotectie en het bredere begrip informationele privacy, is het van belang dat het doel en bereik van persoonsinformatiebeleid in ogenschouw genomen wordt. Hiervoor zal eerst kort worden stilgestaan bij de geschiedenis van het persoonsinformatiebeleid. Vervolgens zal ingegaan worden op de definiëring van het persoonsinformatiebeleid en het verantwoordelijkheidsvraagstuk. Tot slot volgt een begripsafbakening omtrent privacy in relatie tot het persoonsinformatiebeleid.

2.2.1. Geschiedenis van het persoonsinformatiebeleid

De geschiedenis van het persoonsinformatiebeleid is terug te voeren tot 1967, het jaar waarin vanuit de automatiseringsbeweging het voorstel wordt gedaan om een persoonsnummer aan te maken. Omdat in toenemende mate behoefte ontstond aan wettelijke maatregelen omtrent de bescherming van de privacy bij persoonsregistraties, wordt in 1972 de staatscommissie Koopmans ingesteld. Een algemeen informatiebeleid is door het kabinet vastgesteld in 1989[27]. Daarom heen is een veelheid aan beleidsnota's en adviezen verschenen rond het gebruik van administratienummers. Kenmerkend voor het beleid in die tijd is het blauwdrukdenken bij de vormgeving van het persoonsinformatiebeleid. Tijdens de periode 1990-2000 wordt het blauwdrukdenken vanwege de complexiteit en snelheid van ontwikkelingen losgelaten. De nadruk komt dan meer en meer te liggen op de stapsgewijze, projectmatige invoering van bouwstenen, waarmee het persoonsinformatiebeleid op praktische wijze wordt ingevuld.

2.2.2. Doel van het persoonsinformatiebeleid

Wanneer gesproken wordt over het doel van het persoonsinformatiebeleid, kan voorop gesteld worden dat het verwerken van gegevens nooit een doel op zich mag en kan zijn. Het verwerken van en omgaan met gegevens is altijd een middel om een ander beleidsdoel te bereiken. Van het Burger Service Nummer (BSN) kan bijvoorbeeld gesteld worden dat de invoering hiervan geen doel op zich is. Het BSN is –zoals zoveel e-overheidsvoorzieningen- een middel om meerdere beleidsdoelen, zoals verbetering van dienstverlening en vermindering van administratieve lasten te bereiken. Anders gezegd, de inzet van dit middel sorteert een bepaald effect, zoals een reductie van administratieve lasten. Het doel van het persoonsinformatiebeleid zou moeten zijn om een evenwichtige belangenverhouding te realiseren (bijvoorbeeld tussen administratieve lastenverlichting en informationele privacy). Hiertoe dient te worden beoordeeld of het beoogde effect van het middel zich verhoudt tot de gevolgen voor de informationele

privacy. Gevolgen die zowel negatief als positief kunnen zijn. Door minder foutieve gegevensuitwisseling kan het BSN de privacy bijvoorbeeld ook verhogen.

Wanneer dus vanuit het perspectief van de informationele privacy naar het persoonsinformatiebeleid wordt gekeken, wordt bij de totstandkoming van beleid expliciet het doel en het gewenste effect van een in te zetten middel afgewogen tegen de mogelijke effecten op de informationele privacy. Als de invoering van het BSN daarentegen louter vanuit een dataprotectie-invalshoek wordt bezien, beperkt de discussie zich tot het middel op zich. Dan wordt immers gekeken naar alle mogelijke verwerkingen van persoonsinformatie en de gevaren hiervan, zonder daarbij het te bereiken beleidsdoel en het mogelijk effect mee te wegen.

In meer juridische termen wordt bij de afweging over het doel en het middel gesproken over de vereisten van proportionaliteit en subsidiariteit. Het vereiste van proportionaliteit ziet toe op de verhouding tussen doel en middel. Het gebruikte middel (verwerken van persoonsgegevens) dient dan in een redelijke verhouding te staan tot het te bereiken doel (de te bereiken beleidsdoeleinden). Het vereiste van subsidiariteit heeft betrekking op het middel zelf. Uitgangspunt is dat een middel gekozen dient te worden (een vorm van verwerken van persoonsgegevens) dat de informationele privacy het minst aantast. Bij met name dit vereiste van subsidiariteit kan echter wel een kanttekening geplaatst worden. Uiteraard kan het minst aantastende middel als uitgangspunt genomen worden, maar een dergelijk uitgangspunt veronderstelt wel (impliciet) dat er tenminste twee (of meer) alternatieve middelen zijn die een vergelijkbare effectiviteit hebben. Anders gezegd: een subsidiariteitstoets kan pas worden toegepast als er meerdere vergelijkbare middelen zijn en is daarmee niet altijd zinvol. Later in dit onderzoek zullen ook andere vereisten en afwegingscriteria worden beschreven en geanalyseerd.

2.2.3. Bereik en verantwoordelijkheid persoonsinformatiebeleid

In dit onderzoek wordt een onderscheid gemaakt tussen informatiebeleid en *persoons*informatiebeleid. Dit onderscheid is gebaseerd op het al dan niet bestaan van een koppeling van informatie aan personen. Indien informatie gekoppeld *is* aan personen, dan valt deze informatie onder het persoonsinformatiebeleid. Als het gekoppeld *kan* worden, is dit niet het geval. Voorts betreft persoonsinformatiebeleid het gebruik van persoonsinformatie, niet het mogelijk of daadwerkelijk misbruik van gegevens over personen. Hierbij moet wel worden opgemerkt dat dergelijke inschattingen van wat wel of niet het persoonsinformatiebeleid betreft, functie- en contextgevoelig zijn.

De stelselverantwoordelijkheid voor het persoonsinformatiebeleid ligt bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De feitelijke uitvoering ervan is verspreid onder diverse departementen en uitvoeringsorganisaties. Zo is de WBP ondertekend door de minister van Justitie, mede-ondertekend door de minister van BZK, en valt het College Bescherming Persoonsgegevens tevens onder het ministerie van Justitie. De technische uitvoering voor een aantal elementen van het persoonsinformatiebeleid ligt echter bij de Belastingdienst. Informatieketens lopen door verschillende publieke en private sectoren. Persoonsinformatiebeleid is hiermee een diffuus terrein waarbij de aanspreekbaarheid niet altijd duidelijk is.

2.3. Keuze voor een focus op informationele privacy

Zoals eerder beschreven is de verwerking van en omgang met persoonsinformatie geen doel op zich. Vanuit deze gedachte kan geconcludeerd worden dat de dataprotectie-invalshoek te eng is voor het daadwerkelijk kunnen vormgeven van persoonsinformatiebeleid. Voor het komen tot een mogelijke herijking van het persoonsinformatiebeleid is daarom gekozen om in het vervolg van dit onderzoek de invalshoek van informationele privacy te hanteren. Binnen deze invalshoek wordt privacy gezien als een afweerrecht (een recht op dataprotectie) en een actierecht (een recht op informationele zelfbeschikking). Deze invalshoek lijkt de consequentie van een herijking van het persoonsinformatiebeleid met zich mee te brengen. Een eerste implicatie van deze invalshoek is immers dat het persoonsinformatiebeleid als belangrijk doel krijgt het proces van afwegingen rondom de totstandkoming van beleid te begeleiden, waarbij de beoogde effecten van een bepaald middel worden afgewogen tegen de gevolgen de informationele privacy[28]. Op deze manier streeft het persoonsinformatiebeleid naar *een evenwichtige verhouding* tussen informationele privacy en andere belangen[29].
Om nu dit idee van een evenwichtige belangenverhouding nader in te vullen, worden in het volgende hoofdstuk verschillende maatschappelijke contexten en daarmee samenhangende belangen of beleidsthema's onderscheiden, waarbinnen het afwegingsproces anders dient te worden ingevuld.

3. Informationele privacy en andere belangen

In dit hoofdstuk wordt eerst het belang van informationele privacy nader uitgewerkt. Vervolgens wordt ingegaan op de verschillende afwegingen wat betreft het belang van informationele privacy binnen verschillende maatschappelijke contexten. Dit betreft de context van veiligheid, gezondheidszorg, opsporing, fraudebestrijding, en administratieve lastenverlichting. In dit hoofdstuk worden situaties geschetst waar bij de totstandkoming van beleid op een bepaald terrein een inschatting dient te worden gemaakt van de voordelen van dit beleid (het middel) en de gevolgen op de informationele privacy. Dit vormt vervolgens de basis voor een verkenning in het volgende hoofdstuk van de recente voor privacy relevante ontwikkelingen, die het persoonsinformatiebeleid voor nieuwe kansen en uitdagingen plaatsen.

3.1. Het belang van informationele privacy

In het voorgaande hoofdstuk werd duidelijk dat een achttal waarden schuil gaan achter opvattingen van burgers omtrent informationele privacy. Resumerend zijn dit de volgende:

- zelfstandigheid;
- bewegingsvrijheid;
- gelijkheid;
- vrij blijven van stigmatisering;
- ongestoord leven;
- eigenwaarde;
- vrij blijven van manipulatie;
- integriteit en autonomie.

Deze waarden geven een eerste inzicht in het belang van informationele privacy. Wanneer de informationele privacy van personen wordt geschaad, betekent dit tegelijkertijd dat geen recht wordt gedaan aan één of enkele van bovenstaande waarden. Deze waarden geven daarmee op zichzelf het belang van informationele privacy aan. Anders gezegd, informationele privacy heeft als belangrijk doel dat de individualiteit en de individuele eigenschappen en verdiensten van individuen gerespecteerd worden. Voor een door de burgers als betrouwbaar, als legitiem ervaren overheid is het van belang dat de burgers erop kunnen *vertrouwen* dat deze waarden een onderdeel vormen van belangenafwegingen die door de overheid worden gemaakt. Hierover gaat deze paragraaf.

3.1.1. Vertrouwen in informationele privacy

Een in academische kringen geaccepteerde definitie van vertrouwen is: “de overtuiging dat een andere partij zich zal gedragen zoals verwacht”. Vertrouwen geeft daarbij de bereidheid aan van iemand om je kwetsbaar naar een ander op te stellen[30]. In relatie tot informationele privacy kan vertrouwen gezien worden als de overtuiging dat ‘correct’ met persoonsinformatie wordt omgegaan of dat deze ‘correct’ worden verwerkt.

Over het algemeen leidt het waarborgen van iedere vorm van privacy tot vertrouwen. Het wekt daarom geen verbazing dat het College Bescherming Persoonsgegevens (CBP) in haar jaarverslag 2005 stelt dat privacy het vertrouwen van de burger in de samenleving

dient[31]. Informationele privacy in het algemeen en Privacy Enhancing Technologies[32] in het bijzonder, zijn een voorwaarde voor het creëren van vertrouwen bij burgers in de omgang met zijn of haar persoonsinformatie[33]. Dit betekent dat het niet zozeer van belang is wat een organisatie weet van een burger, of over welke gegevens de organisatie beschikt, maar dat het draait om wat de organisatie vervolgens met de gegevens doet[34].

3.1.2. Informationele privacy en vertrouwen in de rechtstaat

Op 5 mei 1998 stelde de toenmalige minister van Binnenlandse Zaken, Dijkstal, ter gelegenheid van het 150-jarig bestaan van de Nederlandse Grondwet dat in hoofdstuk één van de Grondwet het morele acquis van de samenleving is vervat.[35] Via de Grondwet heeft de overheid als het ware een commitment afgegeven ten aanzien van een aantal minimumvoorwaarden die zij garandeert in haar relatie tot burgers. Eén daarvan ziet toe op het respect voor de privacy van burgers[36]. In de literatuur is vele malen op de grote – ook symbolische - betekenis van de Grondwet als grondregel en referentiekader voor onze democratie en rechtsstaat gewezen.[37]
Het recht op bescherming van de persoonlijke levenssfeer behoort expliciet tot de in de grondwet verankerde belangen. Dit betekent dat vraagstukken, toekomstambities en keuzes op het terrein van de informationele privacy ook duidelijk een constitutionele uitdaging vormen. En daarmee ook een uitdaging voor de toekomst van onze rechtsstaat.

3.1.3. Informationele privacy als voorwaarde voor succesvolle ICT-innovaties

Het door het Kabinet Balkenende II geïnitieerde Programma Andere Overheid[38] kent een viertal doelstellingen: betere dienstverlening, minder bureaucratie, een slagvaardige organisatie en een andere werkwijze. In de notitie ‘Op weg naar de Elektronische Overheid’ is dit programma geconcretiseerd en wordt duidelijk dat Informatie- en Communicatietechnologie (ICT) een centrale rol vervult bij het realiseren van deze vier doelstellingen. Dit is een van de redenen waarom overheden te maken hebben gekregen met een grote hoeveelheid aan innovaties op het gebied van E-government. In de beleving van velen staan deze innovaties echter op gespannen voet met de informationele privacy van personen. Velen beschouwen nieuwe vormen en toepassingen van ICT als bedreigend voor de informationele privacy van burgers. Dit vormt vervolgens een gevaar voor het slagen van deze innovaties. Zonder vertrouwen zal de weerstand tegen een efficiënte en persoonsgerichte dienstverlening immers toenemen en zal die dienstverlening met achterdocht worden bekeken[39].
Scherper gezegd, informationele privacy en vertrouwen zijn een voorwaarde voor het slagen van e-overheids-innovaties. De overheid, en andere organisaties die (elektronisch) persoonsinformatie uitwisselen, doen er goed aan aandacht te besteden aan de aspecten die het vertrouwen van burgers in deze elektronische uitwisseling beïnvloeden[40].

3.1.4. Het economisch belang van informationele privacy

Ook vanuit economisch oogpunt bezien, zijn informationele privacy en vertrouwen belangrijk. Vertrouwen in de correcte verwerking van persoonsinformatie leidt namelijk tot lagere transactiekosten. Indien een persoon een organisatie vertrouwt in haar omgang met persoonsinformatie, is er minder behoefte aan dure technologieën om deze privacy te garanderen. Aan de andere kant is het zo dat organisaties die investeren in Privacy Enhancing Technologies (PETs) sneller worden vertrouwd.

Indien vertrouwen eenmaal is opgebouwd, wordt de kans dat zich problemen voordoen op het gebied van de informationele privacy steeds kleiner. Burgers zullen wanneer zij een organisatie vertrouwen in haar omgang met persoonsinformatie minder snel bezwaar maken tegen de invoering van een nieuwe technologie die als doel heeft de dienstverlening te verbeteren.

3.2. Spanningsvelden tussen informationele privacy en andere belangen

Zoals uit hoofdstuk twee is gebleken, verschilt de manier waarop (informationele) privacy wordt beleefd van persoon tot persoon en van situatie tot situatie. Er is echter een belangrijke en veelvoorkomende overeenkomst tussen burgers in hun beschrijvingen van privacy en de opvattingen daarover. Deze overeenkomst is dat zij in een aantal situaties een afweging maken tussen privacy en andere belangen.
In het laatste deel van dit hoofdstuk zal vanuit burgerperspectief nader worden ingegaan op het spanningsveld tussen informationele privacy enerzijds en anderzijds het terrein van veiligheid, gezondheid, opsporing, fraude bestrijding en dienstverlening en administratieve lastenverlichting; terreinen waarop het denken over privacy bij uitstek in beweging is. In het vorig hoofdstuk is immers geconcludeerd dat de gekozen invalshoek betekent dat het persoonsinformatiebeleid procesbegeleiding dient te bieden met betrekking tot het afwegen van het belang van informationele privacy en de belangen van deze terreinen.

3.2.1. Informationele privacy en het belang van veiligheid[41]

De overheid beschikt over diverse preventieve instrumenten voor het verhogen van de veiligheid. Door diverse controlemechanismen, zoals surveillancetechnieken en de identificatieplicht, verhoogt de overheid de kans dat bijvoorbeeld terrorisme en andere bedreigingen voor de veiligheid van de burger in een vroeg stadium worden ontdekt, opgespoord en wellicht zelfs voorkomen. Ook hoopt de overheid, bijvoorbeeld door cameratoezicht, het gevoel van veiligheid op straat te vergroten en de criminaliteit tegen te gaan. Middels diverse opsporingsmethoden kan een veiliger Nederland gerealiseerd worden voor de burgers, zo redeneren de pleitbezorgers van strengere controle.

Burgers zijn, vanwege de angst voor met name terrorisme en misdaad, bereid gebleken een deel van hun informationele privacy in te leveren, maar hier zijn grenzen aan[42]. Opnieuw geldt dat er geen absoluut recht is op informationele zelfbeschikking. Het is eerder zaak te zoeken naar een optimum tussen informationele privacy en veiligheid. Hoe ver mag de overheid gaan in haar streven naar (een gevoel) van collectieve veiligheid en vooral, wat gebeurt er met alle vergaarde informatie? Een toename in het controleren van de burger heeft als risico dat de gegevens veel makkelijker en sneller kunnen worden uitgewisseld met anderen, met als gevolg dat er misbruik van kan worden gemaakt.
Daarbij moet ook kritisch worden gekeken naar geïnitieerde maatregelen die ter voorkoming van terrorisme worden ingezet en de daadwerkelijke dreiging van terrorisme en andere criminaliteit. Bieden zij inderdaad de noodzakelijke bescherming voor de burger? Met andere woorden, het is niet altijd zeker of het ‘offer’ van de informationele privacy daadwerkelijk leidt tot het bewerkstelligen van dat andere belang, het belang van veiligheid. Dergelijk inzicht vraagt om evaluatie van de uitvoering van wet- en regelgeving en de (cumulatieve) gevolgen hiervan voor de informationele privacy van de burger[43].

Opnieuw speelt vertrouwen hier een belangrijke rol. De burger is sneller geneigd het belang van terrorismebestrijding te laten prevaleren boven dat van de informationele privacy, indien zij de overheid en andere organisaties vertrouwt in hun correcte omgang met de informatie die door strengere controle vrijkomt.

3.2.2. Informationele privacy en het belang van gezondheidszorg

Om goede zorg te kunnen bieden, hebben gezondheidsinstellingen een volledig beeld nodig van de patiënt. Een zo volledig mogelijk beeld ontstaat op het moment dat gegevens uitgewisseld worden tussen de verschillende gezondheidsinstellingen.
Het is daarmee in het voordeel van een efficiënte en degelijke gezondheidszorg en dus in het voordeel van de patiënt wanneer zijn of haar medisch dossier zo volledig mogelijk en voor zoveel mogelijk zorgverleners toegankelijk is. Echter, des te meer mensen en organisaties toegang hebben tot patiëntgegevens, des te kwetsbaarder de patiënt en des te groter het gevaar van schending van de informationele privacy van de patiënt[44]. Loopt de patiënt (de burger) niet het risico dat er misbruik gemaakt wordt van zijn persoonsinformatie en dat onbevoegden toegang krijgen tot de deze gegevens en deze vervolgens voor niet medische doeleinden gaan gebruiken? Zo liet Spaink[45] een aantal experts (hackers) de beveiliging van twee ziekenhuizen testen. De resultaten waren niet positief. De genoemde experts hebben twee weken lang toegang gehad tot 1,2 miljoen patiëntgegevens, zonder dat iemand dit heeft opgemerkt[46]. Zo konden medische gegevens ingezien, gekopieerd, verwijderd of veranderd worden.
Ook binnen dit terrein gaat het erom een evenwichtige verhouding te vinden tussen het belang van informationele privacy en dat van een goede gezondheidszorg. En om maatregelen te nemen zodat situaties zoals aangetoond door Spaink in de toekomst kunnen worden voorkomen.

3.2.3. Informationele privacy en het belang van opsporing[47]

Aangezien wetsovertreders niet vrijwillig meewerken aan de handhaving van het strafrecht heeft de overheid opsporingsbevoegdheden nodig om verborgen criminele activiteiten aan het licht te brengen[48]. Door van deze bevoegdheden gebruik te maken, kan de overheid zware criminaliteit in een vroeg stadium ontdekken en opsporen, waardoor de samenleving in Nederland veiliger wordt en de criminaliteit aangepakt wordt. Immers, een veilige samenleving is een algemeen aanvaarde norm.

Neem als voorbeeld de situatie waarin niet verdachte burgers worden gescreend op potentieel verdacht gedrag. Lopen burgers dan niet het risico dat ze bijvoorbeeld vanwege deelname aan verdachte groepen worden gescreend en afgeluisterd, terwijl ze met geen enkele vorm van criminaliteit te maken hebben? Door de opsporingsmethoden kunnen behalve de verdachte ook bijvoorbeeld de relaties, kennissen en familieleden van de verdachte worden getapt. Aan de andere kant, criminaliteit kan in een vroeg stadium opgespoord en wellicht voorkomen worden.

Het is goed voor te stellen dat de burger bereid is meer van zijn informationele privacy op te geven met als doel bestrijding van zware criminaliteit. Maar we weten inmiddels dat de opvattingen over privacy in het algemeen, en informationele privacy in het bijzonder, van burger tot burger en situatie tot situatie verschillen. Het is daarom aannemelijk dat een deel van de bevolking de huidige toepassing van opsporingstechnieken te ver vindt gaan en de privacy te sterk schaadt. Bovendien vindt een persoon de toepassing van bepaalde opsporingstechnieken wellicht acceptabel wanneer het een massamoordenaar betreft, terwijl dezelfde persoon deze technieken onacceptabel vindt indien iemand

verdacht wordt van fraude. Dergelijke voorbeelden geven aan dat afwegingen moeten worden gedifferentieerd naar verschillende vormen en bevoegdheden van opsporing en naar verschillende opsporingsterreinen.

3.2.4. Informationele privacy en het belang van fraudebestrijding

In het kader van fraudebestrijding vindt veel vergaring, opslag en uitwisseling van persoonsinformatie plaats. Het is hierbij met het oog op de informationele privacy met name belangrijk dat organisaties trouw zijn aan het principe dat gegevens alleen worden gebruikt voor het doel waarvoor ze verzameld zijn[49]. Maar gegeven het belang van fraudebestrijding is het vaak verleidelijk het OESO-beginsel van "Purpose Specification" (zie bijlage 2) uit het oog te verliezen.
Niet alleen de overheid krijgt de beschikking over de gegevens van de burgers, maar ook andere instanties. Wordt de burger die bijvoorbeeld een uitkering aanvraagt niet als een potentiële fraudeur gezien die onbeperkt gecontroleerd mag worden? Nutsbedrijven verstrekken gegevens van burgers aan sociale diensten om na te gaan of er wellicht uitkeringsgerechtigden staan ingeschreven op adressen waar geen water of energie wordt gebruikt, om zo aan de partnertoets te ontsnappen[50]. Een ander voorbeeld is dat de gemeente Amsterdam voor wooncontroles gebruik maakt van commerciële bureaus[51]. Komen hierdoor geen bestaande of toekomstige gegevens vrij voor politie en justitie die gegenereerd zijn door de private sector? En: vinden burgers fraudebestrijding belangrijk genoeg om het risico van privacyschending te lopen? Met andere woorden, wanneer is er sprake van een disproportionele inbreuk op de persoonlijke levenssfeer van burgers[52] en daarmee hun informationele privacy?

3.2.5. Informationele privacy en het belang van administratieve lastenverlichting

Administratieve lastenverlichting is één van de doelstellingen van het eerder genoemde Programma Andere Overheid. De gedachte hierachter is dat overheden hun taken beter kunnen uitvoeren wanneer gegevensuitwisseling sneller, efficiënter en betrouwbaarder plaatsvindt. Dit maakt vervolgens een andere doelstellingen van het PAO mogelijk: het verbeteren van overheidsdienstverlening.
Het algemene beleid omtrent informatievoorziening binnen de publieke sector is gericht op het tegengaan van onderlinge verrekening tussen de verschillende overheden[53].
Verschillende ministeries, gemeenten, provincies, waterschappen en nog enkele honderden bestuursorganen vormen de publieke sector, waarbinnen zich informatierelaties afspelen[54]. De publieke sector onderhoudt daarnaast informatierelaties met bijna zeventien miljoen burgers, en honderdduizenden bedrijven en maatschappelijke organisaties[55].
Burgers en bedrijven zijn vanuit het oogpunt van dienstverlening gebaat bij de koppeling van persoonsinformatie, omdat ook voor hen een significante afname van administratieve lasten het gevolg kan zijn. Zo hoeven zij door een koppeling van gegevensbestanden niet langer een papieren uitdraai (uittreksel) uit de computer van de ene overheidsorganisatie op te vragen om deze vervolgens bij een andere overheidsorganisatie aan te tonen. Door koppeling van gegegevensbestanden kan tevens het niet gebruik van subsidies en uitkeringen worden tegengegaan, doordat deze proactief aan personen kunnen worden verstrekt, op basis van de informatie die reeds bekend is over deze personen.
Maar kan de burger erop vertrouwen dat er niet meer informatie voor een bepaalde organisatie beschikbaar is dan hij zelf vrijwillig verstrekt heeft? Met andere woorden, kan hij aanspraak maken op informationele privacy als actierecht? Hoe kan worden

bewerkstelligd dat de burger zelf regie heeft over het gebruik van zijn persoonsgegevens? Door koppeling van de gegevens loopt de burger het risico dat (overheids)organisaties de gegevens voor andere doeleinden gebruiken dan strikt noodzakelijk en/of dat bepaalde gegevens ongewenst aan anderen worden verstrekt.

3.3. Het belang van gedifferentieerde afwegingen

In dit hoofdstuk is op drie manieren het belang van privacy aangegeven. Allereerst liggen aan privacy in den brede belangrijke waarden ten grondslag. Burgers willen dat hun privacy gegarandeerd wordt omdat op deze manier recht wordt gedaan aan waarden als zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie. Ten tweede is informationele privacy belangrijk omdat vertrouwen in het feit dat (overheids-) organisaties deze vorm van privacy garanderen een voorwaarde is voor het slagen van innovaties. Innovaties die nieuwe kansen bieden op diverse terreinen, zoals terrorismebestrijding, dienstverlening en zorg. Tot slot is informationele privacy interessant vanuit economisch perspectief: het verlaagt de transactiekosten en werkt daarmee kostenbesparend.
In dit hoofdstuk zijn naast het belang van (informationele) privacy, ook andere belangen onderscheiden. Zo is het belang van vergaring, opslag en uitwisseling van persoonsinformatie geschetst ten behoeve van de veiligheid, gezondheidszorg, opsporing, fraudebestrijding en dienstverlening en administratieve lastenverlichting. Binnen deze terreinen kan het persoonsinformatiebeleid in de toekomst een contextafhankelijke en evenwichtige belangenverhouding realiseren.

4. Ontwikkelingen en hun uitdagingen

In het vorige hoofdstuk zijn spanningsvelden geschetst die bestaan tussen informationele privacy en andere belangen. Deze dilemma's verschaffen de basis voor de herijking van het persoonsinformatiebeleid. Zij krijgen extra betekenis en diepgang in het licht van technologische, organisationele, bestuurlijke, maatschappelijke, juridische en internationale ontwikkelingen. Pas dan wordt in de volle breedte duidelijk wat het belang is van, en de mogelijkheden zijn voor, een herijking van het beleid.
Het persoonsinformatiebeleid staat met de komst van deze ontwikkelingen ook voor een aantal (nieuwe) uitdagingen. Het persoonsinformatiebeleid heeft als doel om door benutting van de kansen van deze (in elk terrein anders tot uiting komende) ontwikkelingen een contextafhankelijk optimum tussen privacy en andere belangen te bewerkstelligen.

Het doordenken van informationele privacy is gezien recente technologische ontwikkelingen opnieuw aan de orde. In de eerste paragraaf is er daarom aandacht voor technologische ontwikkelingen. Vervolgens komen de bestuurlijke reactie van overheidsinstellingen hierop en de implicaties op het organisationele vlak aan de orde.
Hieropvolgend zal worden ingegaan op de maatschappelijke ontwikkelingen en hoe deze tot uitdrukking komen in wet- en regelgeving. Deze ontwikkelingen worden behandeld door de in hoofdstuk drie geschetste dilemma's door te vertalen naar de hedendaagse samenleving. Anders gezegd, gekeken wordt welke trends er kunnen worden onderscheiden als het gaat om de maatschappelijke waardering voor privacy in relatie tot andere belangen als veiligheid, kwaliteit van zorg en administratieve lastenverlichting.
Tot slot is er in dit hoofdstuk aandacht voor relevante internationale ontwikkelingen. Gekeken wordt welke (mogelijke) gevolgen de veranderende internationale verhoudingen hebben voor de informationele privacy.
Het spreekt voor zich dat in dit hoofdstuk de verschillende ontwikkelingen niet in hun volle omvang worden beschreven. Doel is die ontwikkelingen te selecteren die relevant zijn voor de informationele privacy en de rol die het persoonsinformatiebeleid, met het oog op deze ontwikkelingen, kan spelen in het creëren van een nieuw optimum.

4.1. Technologische ontwikkelingen[56]

Een eerste voor het persoonsinformatiebeleid relevante technologische ontwikkeling is dat mogelijkheden tot transparantie zijn toegenomen door bijvoorbeeld de grotere toegankelijkheid van internet[57]. Actuele voorbeelden van transparantieprojecten die gebruik maken van de toegenomen toegankelijkheid van het internet zijn Samenwerkende Catalogi, Bekendmakingen, en de Persoonlijke Internet Pagina (PIP). Toch is het simpelweg online publiceren of bij elkaar brengen van persoonsinformatie en overheidsinformatie niet altijd verstandig. De provinciale risicokaarten leken potentiële terroristen bijvoorbeeld wel erg veel inzicht te geven in de kwetsbare plekken van ons land. Bovendien mag het niet zo zijn dat de burger met een overload aan informatie wordt geconfronteerd. Met andere woorden, optimale en niet maximale transparantie is het streven.

Een tweede ontwikkeling en uitdaging, is de ontwikkeling van 'ambient intelligence'. Computers worden steeds kleiner en op manieren toegepast die wij niet verwachten. Computers raken verweven in allerlei apparaten en daarmee, vrijwel onbewust, in ons

dagelijks leven. Van een ‘standaard personal computer’ zijn we ons inmiddels steeds vaker bewust dat deze gegevens bevat of wanneer er sprake is van een verbinding met het internet. Van computers zonder toetsenbord en muis is dit minder duidelijk. Wat betekent het voor de privacy als de koelkast gegevens verstuurt naar de online winkel? En wat wordt er nu precies allemaal opgeslagen op een RFID-tag[58], waarmee efficiënt kan worden afgerekend. Wie kan deze gegevens uitlezen? Is hiermee consumentengedrag voor iedereen te volgen? Een uitdaging is om inzicht te verschaffen in de privacy-aspecten van deze ‘ambient intelligence’.
Als derde is er een ontwikkeling naar steeds krachtigere computers. Encryptiesleutels die vroeger onkraakbaar leken, blijken dat niet langer te zijn. De uitdaging is om een niveau van beveiliging te hanteren dat niet achterhaald wordt door de kracht van de computer en dat burgers vertrouwen geeft in de veiligheid van hun transacties. De krachtige computers stellen ons ook in staat om patronen en personen beter te herkennen. Eerder in dit stuk kwamen de SARS-camera’s reeds naar voren. De biometrische irisscan stelt mensen bovendien in staat om zich met hun oog te identificeren. Voor burgers versnelt dit de incheckprocedure op vliegvelden en bovendien komt het de veiligheid ten goede. Automatische nummerbordherkenning in grote steden zorgt ervoor dat mensen zonder parkeervergunning te vinden zijn. Het herkennen van patronen en personen biedt daarmee duidelijke kansen voor dienstverlening en handhaving. Toch zijn de nieuwe systemen nog niet feilloos, wat bijvoorbeeld kan leiden tot identiteitsdiefstal. Betrouwbaarheid blijft dan ook een belangrijk punt van aandacht, dat bij afwegingen over het wel of niet inzetten van deze middelen moet worden meegenomen. Ook is onduidelijk hoe de burger tegenover zaken als biometrie, spraakherkenning, elektronisch stemmen staat. Dit vraagt om een persoonsinformatiebeleid dat kennis heeft van de voor- en nadelen van dergelijke technologische ontwikkelingen, verschillende toepassingen en burgeropvattingen. Zonder dat is iedere afweging onvolledig. Een tweede uitdaging is het in kaart brengen en het nemen van maatregelen tegen identiteitdiefstal, die door digitalisering minder zichtbaar wordt.

De opkomst van camera’s, het gebruik van satellietbeelden en de koppeling daarvan met het internet zijn tevens technologische ontwikkelingen die gevolgen hebben voor de informationele privacy van de burger. Vrijwel iedere burger beschikt over een telefoon met camera en/of een webcam. Google Earth stelt ons in staat om te zien op welk hagelwit strand de komende vakantie doorgebracht gaat worden. De uitdaging is de voordelen van dergelijke technologie te benutten en tegelijkertijd te voorkomen dat er een gevoel ontstaat van ‘Big Brother is watching you’.

Gerelateerd aan het kleiner worden van computers, is de toenemende traceerbaarheid (tracking en tracing) van mensen en goederen. Diefstalgevoelige auto’s worden uitgerust met GPS en in de VS wordt met het bellen naar het alarmnummer direct de locatie van de GSM meegestuurd, waardoor de politie en brandweer kan uitrukken ondanks dat het slachtoffer zijn eigen locatie niet kent. In Noord-Brabant wordt een file automatisch opgemerkt wanneer de mobiele telefoons van automobilisten op de snelweg minder snel bewegen tussen de netwerkmasten. Een uitdaging is het verschaffen van inzicht in het gebruik van tracking and tracing door bijvoorbeeld mobiele en draadloze technieken.

Dan is er nog de trend om allerlei persoonlijke informatie online te zetten en te delen met het (sociale) netwerk. Door Hyves, weblogs, podcasts, Second Life wordt het internet persoonlijker. Politici doen aan deze zogenaamde “web 2.0 trend” mee, maar ook gemeenten zijn te vinden in de virtuele wereld van Second Life. Het is niet alleen leuk, maar stelt ook mensen die minder mobiel zijn, in staat om een druk virtueel sociaal leven

te hebben. Een keerzijde is dat alle informatie die men verstrekt, in principe altijd blijft bestaan en min of meer ongrijpbaar wordt. De informatie is vrijwel onuitwisbaar geworden. Een uitdaging is te onderzoeken wat het betekent dat (sociale) informatie beschikbaar blijft door onder andere de mogelijkheden te verkennen om hierin meer inzicht bij gebruikers te verschaffen.
Een laatste, aan het bovenstaande gerelateerde ontwikkeling is dat burgers, door het publiceren van informatie, de rol van journalist op zich nemen. In tegenstelling tot journalisten hebben burgers echter geen ethische vakcodes ontwikkeld, waardoor informatie 'ongefilterd' op het internet verschijnt. Een voorbeeld is de discussie over het al dan niet publiceren van de achternaam van een verdachte. Een maatschappelijk debat waarbij bewustzijn over de gevolgen van dergelijke besluiten wordt gecreëerd, zou in dit kader een mogelijke oplossingsrichting zijn.
Concluderend kunnen we stellen dat technologische ontwikkelingen veel nieuwe kansen bieden, maar dat er tegelijkertijd aandacht dient te zijn voor de valkuilen van technologische toepassingen. Het creëren van bewustzijn van zowel deze kansen als deze valkuilen is een andere belangrijke uitdaging voor het persoonsinformatiebeleid. Scholing en voorlichting zijn hierbij mogelijke instrumenten.

Onderstaande geeft de technologische ontwikkelingen en hun uitdagingen weer.

Type Ontwikkeling	**Ontwikkelingen**	**Uitdagingen voor de informationele privacy**
Technologische ontwikkelingen	▪ Het internet wordt steeds toegankelijker o Breedband internet o Mobiele en draadloze technieken[59] ▪ Onderdelen worden kleiner o PDA's/MDA's/Laptops o Ambient Intelligence / Embedded software ▪ Computers worden krachtiger ▪ Betere patroonherkenning en identificatie van personen o Slimme camera's (bijv. SARS-camera's) o Biometrie o Spraakherkenning ▪ Camera's registreren steeds meer: o Satelliettoepassingen (Google Earth e.d.) o Webcams ▪ Traceerbaarheid neemt toe: o RFID (Radio Frequency Identification) o GSM o GPS ▪ Het Internet wordt een "Social Internet" (web 2.0)	▪ Bewustzijn creëren ten aanzien van de kansen en valkuilen van technologie. ▪ Mogelijkheid tot transparantie wordt groter. De vraag is welk niveau van transparantie in welk geval gewenst is ▪ Inzicht (verschaffen) in de gevolgen van ambient intelligence. ▪ Bepalen wat een zinvol beveiligingsniveau is voor overheidsdiensten ▪ Inzicht (verschaffen) in de betrouwbaarheid en burgeropvattingen ten aanzien van biometrie, spraakherkenning, elektronisch stemmen etc. ▪ Risico's en maatregelen ten aanzien van identiteitsdiefstal ▪ Voorkomen (gevoel van) "Big Brother is watching you" ▪ Inzicht (verschaffen) in het gebruik van tracking and tracing (▪ Inzicht (verschaffen) in implicaties van web 2.0-technieken ▪ Burgers nemen deel werkzaamheden professionals over, maar hebben geen ethische vakcodes

Tabel 4.1: Technologische ontwikkelingen en hun uitdagingen

4.2. Bestuurlijke en organisationele ontwikkelingen

Om de bestuurlijke en organisationele ontwikkelingen in kaart te brengen, wordt gebruik gemaakt van de procesindeling zoals opgesteld door Hiemstra[60]. Na het schetsen van de ontwikkelingen per proces, zullen de meest relevante uitdaging(en) op het terrein van informationele privacy gepresenteerd worden.
Hiemstra onderscheidt de volgende processen, waar iedere overheidsinstelling mee te maken heeft: politiek, ontwikkeling van beleid (beleidsvorming), dienstverlening, handhaving, bedrijfsvoering en beheer. Deze worden hieronder één voor één behandeld, hetgeen betekent dat de volgende tabel zal worden ingevuld:

Type ontwikkeling	Proces	Ontwikkelingen	Uitdagingen voor het persoonsinformatie-beleid
Bestuurlijke ontwikkelingen	**Politieke processen**		
	Beleidsontwikkeling		
Organisationele ontwikkelingen	**Dienstverlening**		
	Handhaving		
	Bedrijfsvoering		
	Beheer		

Tabel 4.2: Ordening van bestuurlijke en organisationele ontwikkelingen

4.2.1. Ontwikkelingen in politieke processen

Een eerste ontwikkeling hier kan worden onderscheiden, is het toenemend gebruik van Polls en peilingen op het internet: burgers wordt gevraagd hun mening te geven op bepaalde onderwerpen, via websites van de overheid. Burgers waarderen een anonieme bijdrage aan dergelijke debatten omdat zij niet bang hoeven te zijn voor afkeuring van overheidsinstanties, werkgevers, buren of bekenden. In een fysiek debat in bijvoorbeeld een buurtgemeenschap is het veel moeilijk anoniem deel te nemen en voelen burgers zich dus sneller geneigd een sociaal wenselijke standpunt in te nemen. Kritische geluiden zouden wellicht niet gehoord worden als burgers hun mening niet anoniem via het internet kunnen geven. Hierdoor heeft deze bestuurlijke ontwikkeling een onmiskenbaar maatschappelijk nut[61].
Daarnaast is te zien dat politici steeds vaker weblogs bijhouden. In een aantal gevallen zijn dat weblogs die gefaciliteerd worden door de ICT-afdelingen van overheidsinstanties. Voorts zijn overheidsinstanties steeds transparanter wat betreft het politieke proces. Hierbij wordt het principe “openbaar, tenzij” gehanteerd.
Een laatste door ons onderscheiden bestuurlijke ontwikkeling is dat de databases die de politiek kan gebruiken bij haar sturing steeds omvangrijker en verfijnder worden.

Uitdagingen politieke processen
Onlangs bleek door controle van het IP-adres dat een negatieve uitlating over een gemeentebestuur afkomstig was van de computer van de burgemeester thuis. Is het vanuit de informationele privacy geredeneerd wel redelijk dat de anonimiteit van deze bijdrage werd opgeheven? Hier is te zien dat misbruik wordt gemaakt van het middel "internetforum", aangezien het technisch middel ingezet wordt voor een doel anders dan het verkrijgen van een burgerstandpunt. In deze context is het anoniem houden van bijdragen op overheids(sites) belangrijk. Eveneens is belangrijk dat mensen die politieke stukken raadplegen op de websites van overheidsinstanties dat kunnen doen zonder dat gelogd wordt dat zij deze stukken lezen.
Het bovenstaande toont dat de waarde democratie in het digitale tijdperk anders kan worden vormgegeven. Het is daarbij zaak technologische innovaties weloverwogen in te zetten. Dit vraagt van het persoonsinformatiebeleid dat zij zicht heeft op de bestuurlijke ontwikkelingen, en middelen en mechanismen die de informationele privacy kunnen borgen. Hierdoor kunnen de kansen van deze politieke ontwikkelingen worden benut en een hoger niveau van informationele privacy worden bereikt dan voorheen tijdens fysieke debatten mogelijk was.

4.2.2. Ontwikkelingen in beleidsontwikkelingsprocessen

Het ontwikkelen van beleid is in feite een politiek proces, zij het dat veel ambtelijke ondersteuning wordt ingezet. Steeds vaker betrekken overheidsinstanties burgers en relevante ketenpartners bij de ontwikkeling van hun beleid. Er kan dan gesproken worden van interactieve beleidsvorming. Ook wordt burgers gevraagd hun mening te geven, terwijl talrijke intermediaire partijen benaderd worden een bijdrage te leveren. Ook hier zien we veel internettoepassingen ontstaan, met digitale debatten en het op internet plaatsen van concept-besluitvorming, zodanig dat er nog inspraak mogelijk is.

Uitdagingen beleidsontwikkeling
Ook hier kan worden gesproken van uitdagingen voor de informationele privacy. De eerste vraag is of er sprake is van vrije toegang: kan iedere burger zich toegang verschaffen tot het digitale debat? In de gemeente Delft bijvoorbeeld, wordt over bepaalde bouwprojecten inspraak georganiseerd per wijk. Deelnemers aan het debat moeten zich dan met DigiD digitaal identificeren. Dat zorgt ervoor dat alleen inwoners uit die wijk deelnemen aan het digitale debat. Maar er is ook een keerzijde: de identiteit, of in ieder geval het adres, van eenieder die deelneemt is bekend. Wat doet een overheidsinstelling, in dit geval de gemeente, daarmee? De basisvraag is of een aan een digitaal debat geleverde bijdrage niet herleidbaar is tot een persoon, als hij of zij dat niet wil.

4.2.3. Ontwikkelingen in dienstverleningsprocessen

Dienstverlening, met name de inrichting van dienstverleningsprocessen, wordt sterk beïnvloed door ICT. Veel overheidsinstellingen gaan over op klantcontactcentra, waar burgers direct naar kunnen bellen voor al hun vragen. Het streven van veel van deze call centra is zoveel mogelijk vragen ook direct af te handelen. Daartoe wordt steeds meer informatie vanuit verschillende delen van de organisatie samengebracht, zodat de medewerkers van de call centra 'met een druk op de knop' de relevante informatie kunnen inzien en overzien.
Parallel daaraan is te zien dat steeds meer formulieren en andere diensten on-line komen. Burgers kunnen diensten aanvragen via het internet en vullen elektronische formulieren in, die ze dan opsturen. Om ervoor te zorgen dat de dienstverlening via het loket en via internet synchroon loopt, wordt aan multi-channeling gedaan: het wederzijds

afstemmen van de verschillende ter beschikking staande kanalen: internet, telefoon, post en fysiek loket. Inmiddels gaan sms en msn ook tot de mogelijkheden behoren, terwijl de fax aan het verdwijnen is.
Het klantcontactcentrum, multi-channeling en de elektronische dienstverlening veranderen de dienstverlening al sterk, maar zodra de informatie-infrastructuur op orde is, ontstaan ook mogelijkheden tot de 'geen-loket-benadering': het proactief leveren van diensten, nog voordat de burger erom gevraagd heeft. Bekend voorbeeld is het op voorhand kwijtschelden van lokale heffingen, door op basis van het koppelen van verschillende bestanden geen aanslagen te sturen aan die mensen waarvan je eigenlijk al weet dat ze in aanmerking komen voor kwijtschelding.
Tot slot is te zien dat ook steeds vaker de life-event-benadering toegepast worden. Dit komt erop neer dat je alle overheidshandelingen die samenhangen met één gebeurtenis van een burger in zijn/haar leven, ook in één keer afhandelt. Voorbeelden daarvan zijn het bij het aanbieden van een nieuwe woning door een woningcorporatie ook direct wijzigen van de GBA-gegevens[62] van de betreffende burger. Voorwaarde is natuurlijk dat de relevante informatie dan beschikbaar is op de plek waar de burger zijn/haar life-event start.

Uitdagingen dienstverlening
Hoe hoogwaardiger de dienstverlening, des te meer de dienstverlenende overheid moet weten van de betrokken burger. Daarmee is de uitdaging voor de informationele privacy geschetst. Voor elk afgesproken niveau van dienstverlening moet op voorhand bepaald worden wat de betrokken dienstverlenende organisatie nu wel en wat zij nu niet mag weten, zodanig dat er sprake is van proportionele kennisdeling. Ook de mogelijkheden tot regie van de burger op het gebruik van zijn persoonsgegevens is een belangrijke uitdaging.
Als de burger via internet formulieren invult, moet hij zeker weten dat niemand meekijkt. In hoeverre zijn de formulieren afgeschermd van pottenkijkers en hoe zeker is het dat formulieren, onderweg via internet, niet door anderen gelezen worden? Bij de gewone post is er het briefgeheim en heeft de burger er vertrouwen in dat door het dichtplakken van de envelop niemand meeleest.
Hierbij kan gebruik worden gemaakt van ontkoppeld koppelen, eventueel in combinatie met een tussenorganisatie, zoals de Kruispuntbank Sociale Zekerheid dat in België. Als daar bijvoorbeeld een sociale dienst een korting wil geven, dan vraagt deze dienst aan de kruispuntbank of de beoogde cliënt in de doelgroep valt. De kruispuntbank verzamelt dan de ruwe gegevens uit de verschillende bronnen, interpreteert deze en geeft vervolgens alleen een gezaghebbend ja of nee door aan de sociale dienst. De gezaghebbendheid is juridisch gereguleerd: het elektronisch verstrekte 'ja' is voldoende voor de rechtmatigheidsbepaling. Meer informatie over hoe binnen de Kruispuntbank Sociale Zekerheid met informationele privacy wordt omgegaan, bevindt zich in de derde bijlage.
De ontwikkelingen in dienstverlening zijn van dien aard, dat de ICT van een veel hoogwaardiger niveau zal moeten zijn, met name op het terrein van autorisatie en authenticatie en beveiliging. Autorisaties betreffen de vraag wie wel of niet toegang heeft tot bepaalde informatie. Nu kan men vaak slechts toegang geven tot een applicatie en daarmee automatisch tot alle gegevens in die applicatie, in de toekomst zal per te onderscheiden rol steeds een specifieke, daarop toegesneden subset van gegevens uit een applicatie ter beschikking gesteld moeten kunnen worden.
De authenticatie betreft enerzijds de burger, die middels een goede elektronische identificatie toegang tot de systemen wordt verstrekt. Maar ook de overheidsdienstverlener zal zich steeds beter moeten authenticeren. Bovendien zal

middels logging van zijn raadplegingen, altijd achteraf reconstrueerbaar moeten zijn welke gegevens door de dienstverlenend ambtenaar zijn geraadpleegd. Om dit veilig te laten gebeuren zullen, afhankelijk van het belang van de betrokken gegevens, steeds strengere kwaliteitseisen gesteld moeten worden[63].
Een persoonsinformatiebeleid staat voor de uitdaging om bij iedere afweging dergelijke oplossingsrichtingen en hun voors en tegens moeten communiceren, zodat de mogelijkheden voor en de weg naar een nieuw optimum tussen informationele privacy en dienstverlening duidelijk worden.

4.2.4. Ontwikkelingen in handhavingsprocessen

Voor handhaving geldt in zekere zin hetzelfde als voor dienstverlening. Door de sterke informatisering van de overheid, is te zien dat de overheid over een steeds betere informatiepositie beschikt. Dat biedt de overheid de mogelijkheid om haar handhavingstaken te bundelen, en aan integrale handhaving te gaan doen: inspecteurs van de leerplicht, van de sociale dienst, van burgerzaken treden dan gezamenlijk op en beschikken over gedeelde gegevens.
Daarnaast kunnen ze betere risicoprofielen opstellen, zodat hun handhavingcapaciteit beter ingezet wordt (hogere 'hit-rate'). In het verlengde hiervan ligt de benadering van het 'meervoudig kijken': daarvan is sprake als er niet meer drie inspecteurs gezamenlijk optreden, maar als elk van die drie inspecteurs ook namens de andere mag optreden. In dat geval treedt een soort vermenigvuldiging van de handhavingcapaciteit op, zeker in combinatie met risicoprofielen. Efficiency en effectiviteit stijgen beide, hetgeen sterke invloed heeft op productiviteit van de handhaving. Gevolg daarvan is dat de burger met een overmacht aan handhaving kan worden geconfronteerd.
Parallel daaraan worden de in de vorige paragraaf beschreven technologieën geïntroduceerd, zoals tracking, tracing en monitoring.

Uitdagingen handhaving
De afgelopen jaren is een verruiming opgetreden van de mogelijkheden om informatie te gebruiken voor de handhavingscapaciteit[64]. Het lijkt erop dat de balans zoek kan raken. Er is echter nauwelijks een weg terug. Om de risico's op dit terrein te beheersen, kunnen tegenmaatregelen overwogen worden, die de mogelijkheid scheppen om op een hoger niveau tot een nieuw evenwicht te komen.
Zo kan per handhavingstaak en handhavingsmedewerker zeer nauwgezet specificeren wat hij wel/niet mag opvragen aan informatie en welke consequenties daar wel/niet aan verbonden mogen worden. De keuzen die daarin gemaakt worden, moeten niet door de professionele handhavers zelf genomen worden, maar voorgelegd worden aan het politieke bestuur, zodat de keuzen democratisch gelegitimeerd kunnen worden. De begeleiding van dit keuze- of afwegingsproces kan opnieuw door het persoonsinformatiebeleid worden geboden.
Daarnaast kan de opslag van allerhande tracking en tracing informatie beperkt worden in tijd en plaats. Met andere woorden, de ontsluitbaarheid kan worden beperkt.
Een belangrijke uitdaging is het risico van stigmatisering: als in risicoprofielen te veel wordt gestuurd op etnische of andere persoonlijke kenmerken, dan leidt het risicogestuurde handhaven tot mogelijke stigmatisering en aldus tot een disproportionele inbreuk op de informationele privacy. De keuzen die professionals op het terrein van handhaving maken, tenslotte, kunnen genormeerd worden.

4.2.5. Ontwikkelingen in bedrijfsvoeringsprocessen

De digitalisering van de informatie in overheidsorganisaties, het toenemend aantal koppelingen tussen bestanden en applicaties, en de toenemende interoperabiliteit van ICT-infrastructuren, zorgen ervoor dat overheidsorganisaties hun werkwijzen sterk kunnen rationaliseren. Onnodige papieren tussenstappen kunnen worden weggesaneerd en bundeling van activiteiten is op de schaal van de overheid als één geheel mogelijk. Het is niet ondenkbaar dat het CJIB voor alle overheidsorganisaties de incasso's gaat doen, terwijl bijvoorbeeld de belastingdienst alle inkomensgerelateerde betalingen voor haar rekening zal nemen -inclusief de maandelijkse uitkering van de sociale dienst. De sociale dienst kan zich dan ontwikkelen tot zorg-contact-kantoor, dat zich bedient van het betalingscentrum van de Belastingdienst om toegekende uitkeringen over te maken. Gesprekken over zorgtoeslagen en huursubsidie kunnen door de sociale dienst namens het Rijk gevoerd worden. Hiertoe ontstaan steeds grotere shared service centres, waarvan de call centra eigenlijk ook al een voorbeeld zijn. Deze ontwikkeling ontstaat doordat overheidsorganisaties, nadat zij hun systemen gekoppeld hebben, steeds meer gaan kantelen, meer in netwerken van organisaties gaan samenwerken en daarmee (persoons)informatie uitwisselen.

Uitdagingen bedrijfsvoering

Met name de uitbesteding en het verplaatsen van taken en daarmee van informatie in de keten zorgt ervoor dat informatie op heel andere plaatsen in de keten beschikbaar komt, dan waar zij oorspronkelijk vandaan komt. Informatie stroomt en tijdens dat stromen moet de informatie zodanig afgeschermd worden, dat alleen daartoe geautoriseerden de informatie kunnen aftappen. Elke gebruiker van de informatie moet daartoe specifiek geautoriseerd zijn, en waar mogelijk kunnen PET-middelen ingezet worden, om onnodige informatieverspreiding tegen te gaan. Gezien de omvang van de risico's is het te overwegen om het toezicht op het feitelijk gebruik van gegevens te versterken.
Tot slot is het mogelijk, zoals men van plan is bij de Kruispuntbank Sociale Zekerheid in België, om de burger toegang te geven tot alle informatie en daarbij te zien welke informatie door welke overheidsorganisatie op welk moment gebruikt is. Dan kan de burger meer tegenmacht ontwikkelen. Op deze manier kan informationele privacy als actierecht worden geborgd.

4.2.6. Ontwikkelingen in beheerprocessen

Beheer betreft hier vooral het leveren van diensten in de buitenruimte, zoals parkeerbeheer, maar ook groenbeheer. Deze, op het oog onschuldige, collectieve producten ondergaan interessante veranderingen. Het proces van rationaliseren zorgt ervoor dat meer informatie over allerlei vormen van beheer beschikbaar komen. Sms'ende vuilniscontainers melden wanneer zij vol zitten en bieden daarmee informatie over waar veel en waar weinig vuil aangeleverd wordt. Elektronische formulieren voor het aanmelden van grofvuil lenen zich gemakkelijker voor hergebruik van informatie dan hun papieren voorgangers. Een parkeervergunning kan geweigerd worden als bekend is dat betrokkene zijn belastingschulden en/of boetes niet betaalt. Machine Leesbare identificatiemiddelen maken het tenslotte beter mogelijk om na te gaan wie welke collectieve voorziening intensief, dan wel extensief gebruikt. De druk om te verantwoorden waaraan deze collectieve goederen worden besteed, leidt ertoe dat ook hier steeds meer informatie verwerkt en opgeslagen wordt. Zo zijn er gemeenten die de mogelijkheid bieden aan buurtbewoners om het niveau van groenbeheer te beïnvloeden (inspraak op beheer), terwijl het gedifferentieerd tariferen van afvalverwerking (Diftar) sterk toeneemt.

Deze ontwikkelingen vinden vaak plaats als onderdeel van de trend van vraagsturing, die op gespannen voet met de informationele privacy kan staan. Diensten worden niet geleverd op het moment dat de leverende dienst dat uitkomt, maar op het moment dat de klant erom vraagt. Dat kan alleen maar als er meer informatie over die klant beschikbaar komt.

Uitdagingen beheerprocessen
Ook binnen de beheerprocessen stijgt de informatierijkheid. Ook hier zal daarom overwogen moeten worden welke maatregelen genomen kunnen worden en waar het optimum ligt tussen verbetering van beheerprocessen en het (tot op zekere hoogte) garanderen van de informationele privacy. Mogelijke maatregelen zijn het proportioneel en gelokaliseerd gebruik van informatie introduceren. Bijvoorbeeld door een afdeling groenbeheer toegang te geven tot een beperkt aantal data, binnen een bepaald district.

Hieronder zijn de bestuurlijke en organisationele ontwikkelingen in tabelvorm weergegeven.

Type ontwikkeling	Proces	Ontwikkelingen	Uitdagingen voor het persoonsinformatiebeleid
Bestuurlijke ontwikkelingen	**Politieke processen**	▪ Polls/digitale debatten/peilingen ▪ Weblogs ▪ Toenemende transparantie ▪ Omvangrijkere en verfijndere databases	▪ Kennis van middelen en mechanismen om privacy te borgen ▪ Misbruik fora en databases voorkomen ▪ Garanderen anonimiteit deelnemers aan digitale debatten
	Beleidsontwik-keling	▪ Interactieve beleidsvorming ▪ Digitale debatten ▪ Openbare concept-besluitvorming	▪ Vrije toegang ▪ Onnaspeurbare bijdragen
Organisationele ontwikkelingen	**Dienstverlening**	▪ Klantcontactcentra ▪ Elektronische dienstverlening ▪ Multichanneling ▪ Life Events ▪ 'Geen-loket-benadering'	▪ Proportionele kennisdeling ▪ Regie van de burger invullen ▪ Afgeschermd invullen ▪ Geconditioneerde ter beschikking stelling ▪ Gedifferentieerde autorisatie mechanismen ▪ Hoogwaardige authenticatie/beveiliging ▪ Logging van gebruik ▪ Democratisch gelegitimeerd hergebruik
	Handhaving	▪ Integrale handhaving ▪ Risicogestuurd handhaven ▪ Meervoudig kijken ▪ Tracking, tracing, monitoring	▪ Gespecificeerd gebruik ▪ Democratisch gelegitimeerd gebruik ▪ Gelimiteerde opslag in tijd en plaats ▪ Vrijwaring stigmatisering ▪ Normering professionals
	Bedrijfsvoering	▪ Shared service centres ▪ Koppelen, kantelen, ketenen ▪ Uitbesteden	▪ Deugdelijke afscherming ▪ Autorisatie gebruik ▪ PET ▪ Toezicht ▪ Burger meer tegenmacht geven (actierecht)
	Beheer	▪ Rationaliseren ▪ Verantwoorden ▪ Massaal maatwerk ▪ Gedifferentieerd tariferen (Diftar) ▪ Vraagsturing	Proportioneel en gelokaliseerd gebruik van persoonsinformatie

Tabel 4.3: Bestuurlijke en organisationele ontwikkelingen

4.3. Maatschappelijke en juridische ontwikkelingen

In het tweede deel van dit hoofdstuk staan maatschappelijke en juridische ontwikkelingen centraal. Hierbij wordt gekeken hoe in onze huidige maatschappij wordt omgegaan met de in het vorig hoofdstuk onderscheiden spanningsvelden tussen informationele privacy en andere belangen en welke veranderingen in wet- en regelgeving zich binnen deze

terreinen hebben voltrokken. Wat dit laatste betreft is niet gekeken naar alle regelgeving over het verwerken van persoonsgegevens, maar naar die regelgeving die in belangrijke mate van invloed is op de informationele privacy[65].

4.3.1. Maatschappelijke waardering van privacy, veiligheid en opsporing

Na de aanslagen van 11 september 2001 in de Verenigde Staten, de moord op filmmaker en kritische cineast Theo van Gogh eind 2004 en, meer algemeen, de toenemende dreiging van het terrorisme in Amerika en Europa, is de waarborging van de veiligheid van burgers en de rol die (informationele) privacy daarin moet nemen een veelbesproken onderwerp. Uitbreidingen van de bevoegdheden van opsporingsdiensten zijn echter al voor de aanslagen van 11 september 2001 gestart[66]. Zo is het al sinds september 1994 toegestaan dat de rechter-commissaris het bevel geeft tot het verrichten van DNA-onderzoek wanneer er sprake is van verdenking van zware misdrijven of 'dringende noodzakelijkheid'. Ook de Telecommunicatiewet en het Besluit Verstrekking Gegevens Telecommunicatie stammen van voor 2001.
De toegenomen terrorismedreiging sinds 2001 heeft echter wel een extra impuls gegeven aan de toepassing en verruiming van dergelijke opsporingsbevoegdheden. De Nederlandse overheid heeft haar inspanningen op het gebied van bewaking en controle duidelijk verhoogd, met als rechtvaardiging de strijd tegen terrorisme en criminaliteit. Het CBP spreekt in deze context zelfs van een 'controlesamenleving'[67], hetgeen zich bijvoorbeeld uit in diverse vormen van cameratoezicht[68]. Camera's vormen sinds eind jaren negentig steeds vaker een vanzelfsprekend onderdeel van het straatbeeld in Nederland. Deze toename in het gebruik van camera's heeft ook gevolgen gehad voor de wetgeving op dit terrein. Sinds 2004 is de wet die heimelijk en ongecontroleerd cameratoezicht strafbaar stelt, uitgebreid. En de Wet Cameratoezicht uit 2006 reguleert de plaatsing van camera's in de openbare ruimte en het gebruik van camerabeelden.
Andere voorbeelden van wet- en regelgeving ten aanzien van opsporingsbevoegdheden zijn de Wet Bijzondere Opsporingsbevoegdheden (2000)[69], de Wet op de Inlichtingen- en Veiligheidsdiensten (2002)[70], de Wet Identificatieplicht (2005), de Wet Computercriminaliteit (2006) en de Wet Vorderen Gegevens (2006).

Eén van de gevolgen van bovenstaande wetten is dat zij het onder andere mogelijk hebben gemaakt dat het afluisteren van telefoongesprekken en het traceren van zoek- en surfgedrag van personen op het internet steeds vaker voorkomt, waarbij sinds de invoering van de Telecommunicatiewet van telefonie- en internet aanbieders wordt verlangd dat ze informatie over het telefoon- en internetverkeer dienen te bewaren[71].
Een ander voorbeeld van een opsporingsbevoegdheid waarvan het gebruik de afgelopen jaren fors is toegenomen,[72] is gegevenskoppeling. Tevens is het verzamelen van informatie uit publieke en private bronnen en het delen hiervan met een groeiend aantal opsporingsinstanties en nationale veiligheidsdiensten een belangrijke ontwikkeling.

Kortom, in de Nederlandse samenleving is een trend te zien naar het laten prevaleren van het belang van veiligheid en opsporing, ook als hiervoor op het gebied van informationele privacy concessies gedaan moeten worden (zie ook het onderstaand kader). Wat hierbij opvalt is dat veel van deze aanpassingen in de wet- en regelgeving tot weinig maatschappelijke discussies hebben geleid. Privacy voert duidelijk niet de boventoon in het debat over de toenemende veiligheidsmaatregelen[73]en als privacy al een onderwerp van discussie is, dan wordt de discussie van de privacy enkel in relatie tot één beperkte maatregel gevoerd. Een algehele discussie over de bedreiging van informationele privacy in onze samenleving wordt maar door weinigen gevoerd. Inzicht in het cumulatief effect van bovenstaande ontwikkelingen op de informationele privacy ontbreekt.

Privacy en veiligheid: de beleving van burgers

Enkele uitkomsten uit het Nationaal Vrijheidsonderzoek 2007 (Comité 4 en 5 mei, april 2007):

- Het recht op privacy wordt door 39% van de ondervraagden genoemd als één van de drie belangrijkste grondrechten. Hiermee staat het op de vierde plaats, na *vrijheid van meningsuiting* (60%), *sociale rechten* (44%) en *gelijke behandeling in gelijke gevallen* (42%). Sinds 2002 is het belang van het recht op privacy redelijk constant gebleven;
- Op de vraag of er in Nederland groepen actief zijn die de rechtstaat bedreigen, antwoordde 78% van de ondervraagden bevestigend;
- Geconfronteerd met het dilemma “individuele recht op privacy” versus “nationale veiligheid” neigt 25% van de ondervraagden naar “individuele recht op privacy”, 71% naar “nationale veiligheid” en 4% “weet niet”. Hierbij kiezen ouderen (> 35 jaar) en lager opgeleiden vaker voor nationale veiligheid en jongeren (< 35 jaar) en hoger opgeleiden vaker voor het individuele recht op privacy;
- Onderstaande tabel geeft de antwoorden weer op de vraag of de ondervraagden een maatregel tegen terrorisme al dan niet aanvaardbaar vinden:

	Aanvaardbaar (%)	Onaanvaardbaar (%)
cameratoezicht op openbare plekken	94	6
bij verdenking huiszoeking doen	87	13
preventief fouilleren	84	16
identificatieplicht vanaf 12 jaar	84	16
gegevensverstrekking vliegtuigmaatschappijen	82	18
bij verdenking iemand in hechtenis nemen	81	19
ieders dna-profiel afnemen	76	24
plaatsbepaling door scannen autokentekens	72	28
plaatsbepaling door mobiele telefoons	63	37
alle e-mail en internetverkeer bekijken	55	45
alle telefoonverkeer afluisteren	50	50

- 34% van de ondervraagden vindt dat de overheid altijd openheid van zaken moet geven en 49% vindt dat de overheid in het belang van de veiligheid zaken mag achterhouden. 16% is hier neutraal in;
- 50% van de ondervraagden vindt dat als de overheid meer over burgers weet, de veiligheid toeneemt. 26% vindt dat de veiligheid dan afneemt en 25% is neutraal.

Tabel 4.4: Enkele uitkomsten van het Nationaal Vrijheidsonderzoek 2007

Uitdagingen voor het persoonsinformatiebeleid

Voor welke uitdagingen staat het persoonsinformatiebeleid, gegeven bovenstaande ontwikkelingen?

Allereerst is het van belang dat de burger en (commerciële) organisaties vertrouwen krijgen en/of behouden in een overheid die steeds meer opsporingsbevoegdheden heeft. Eén van de middelen die zij daarvoor tot haar beschikking heeft is transparante

communicatie over afwegingen en evaluatie van de uitgebreide wet- en regelgeving. Daarbij staat zij voor de taak om per terrein evenwichtige belangenverhoudingen te realiseren. Hierbij is zicht op burgeropvattingen essentieel. Wanneer vinden burgers dat er sprake is van disproportionele inbreuken op hun privacy? Om hier inzicht in te krijgen, kan de overheid een maatschappelijk debat creëren over de wenselijke verhouding tussen informationele privacy, veiligheid en opsporing. Daarnaast is voor het maken van afwegingen tussen verschillende belangen inzicht nodig in het cumulatief effect van de maatregelen die de afgelopen jaren op dit terrein zijn genomen. Alleen dan kunnen immers de (relatieve) effecten van een nieuwe maatregel goed worden ingeschat. Tot slot zijn er duidelijke en transparante afspraken nodig over, en controle op, de koppeling van gegevensbestanden.

4.3.2. Maatschappelijke waardering van privacy en kwaliteit van zorg[74]

In de Nederlandse gezondheidszorg zijn veranderingen aanstaande die vergaande gevolgen kunnen hebben voor de wijze waarop zorg wordt verleend, besteed en gefinancierd[75]. Uit onderzoek van TNS NIPO blijkt dat veel (medische) fouten worden veroorzaakt door gebrekkige communicatie[76]. Onderzoek van het WinAP laat bovendien zien dat er jaarlijks 90.000 ziekenhuisopnames zijn als gevolg van vermijdbare medicatiefouten[77]. Deze cijfers geven de urgentie aan van innovaties in de zorgsector, gericht op een verbetering van de toegang die artsen hebben tot patiëntgegevens. De cijfers verklaren tevens de toenemende roep om kwalitatief hoogwaardiger zorg in onze samenleving.
Het EPD, EMD en het wetsvoorstel ‘gebruik burgerservicenummer in de zorg’ zijn middelen die een verbetering van de kwaliteit van zorg in het algemeen, en van de integrale opslag en uitwisseling van patiëntgegevens in het bijzonder mogelijk maken. Dergelijke innovaties kunnen gevolgen hebben voor de informationele privacy. Juridisch is in deze context de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) uit 1995 relevant. Deze wet legt hulpverleners de verplichting op vertrouwelijk met patiëntengegevens om te gaan. Een hulpverlener is op grond van de WGBO verplicht bij het verschaffen van toegang tot patiëntgegevens aan andere hulpverleners, zich te houden aan het aantal randvoorwaarden. Zo dient de patiënt toestemming te verlenen, al is hierop een aantal uitzonderingssituaties[78].

Recent opinieonderzoek van EPN laat zien dat 97% van de Nederlanders bereid is toestemming te geven aan huisarts, specialist en apotheek voor het inzien van zijn medische gegevens. Dit percentage ligt aanzienlijk hoger dan voor het toestemming geven van inzage in medische gegevens aan familie en vrienden die voor de patiënt zorgen. De meerderheid zou deze toestemming niet geven. Een andere opvallende bevinding uit het opinieonderzoek is dat 33% van de Nederlanders het goed vindt als zijn zorgverzekeraar inzage heeft in zijn medische gegevens[79]. Burgers lijken zich dus zich meer zorgen te maken over de huidige kwaliteit van zorg dan over de gevaren die innovaties in deze sector betekenen voor de informationele privacy. Met andere woorden, het optimum tussen gezondheidszorg en privacy lijkt te verschuiven.

Uitdagingen voor het persoonsinformatiebeleid

Net als voor het terrein van de veiligheid en opsporing geldt hier dat er behoefte is aan dialoog over de belangen van informationele privacy en gezondheidszorg en hoe deze zich tot elkaar verhouden. Er is behoefte aan een persoonsinformatiebeleid dat de aandacht verlegt van dataprotectie en ad hoc discussies over de gevaren van bijvoorbeeld het EPD naar een meer integraal debat over waar het optimum op dit terrein

ligt en hoe dit optimum kan worden bewerkstelligd. Opnieuw is daarvoor inzicht in burgeropvattingen nodig. Onderzoek wijst erop dat de burger veel belang hecht aan betere uitwisseling van persoonsgegevens, zodat de kwaliteit van de gezondheidszorg kan toenemen. Het in stand houden van de huidige situatie, waarbij door onvoldoende gegevensuitwisseling vermijdbare medicatiefouten worden gemaakt, lijkt daarmee geen optie.

4.3.3. Maatschappelijke waardering van privacy, fraudebestrijding en administratieve lastenverlichting

Zoals reeds aangegeven, groeien door de komst en snelle ontwikkeling van ICT ook de mogelijkheden om gegevens te koppelen en uit te wisselen. Bij overheidsinstanties groeit de afgelopen jaren het bewustzijn van de mogelijke voordelen van gegevenskoppeling en –uitwisseling. Enerzijds maakt dit een betere dienstverlening richting burger en bedrijfsleven mogelijk, anderzijds kan door gegevenskoppeling en -uitwisseling fraudebestrijding worden verbeterd. Voorbeelden hiervan zijn woonfraude en fraude bij sociale verzekeringen[80]. Tot slot komt gegevensuitwisseling de bedrijfsvoering ten goede en dient het de administratieve lastenverlichting voor burger en bedrijfsleven.

Fraudebestrijding is onder de noemer handhaving reeds aan de orde geweest in het eerste deel van dit hoofdstuk. Geconstateerd kan worden dat een efficiënte en doeltreffende bestrijding van misbruik van sociale voorzieningen en uitkeringen hoog op de politieke en maatschappelijke agenda staat[81]. Gemeenten willen bijvoorbeeld ter bestrijding van fraude met uitkeringen steeds meer gegevensbestanden ontsluiten en koppelen[82]. Eén van de belangrijkste bestanden is uiteraard de Gemeentelijke Basisadministratie (GBA). De gegevens uit de GBA worden door diverse (semi-) overheidsinstanties gebruikt bij de uitvoering van publiekrechtelijke taken. De wet WGBA (Wet Gemeentelijke Basisadministratie persoonsinformatie) uit 1994 geeft hierbij aan hoe de gemeente dient te handelen bij het opnemen van persoonsinformatie in de GBA, bij wijzigingen in persoonsinformatie, bij het verstrekken deze gegevens aan anderen en bij het verlenen van inzage. Het CBP ziet toe op de uitvoering van de WGBA.

Niet alleen gemeenten, maar ook het Ministerie van Sociale Zaken heeft fraudebestrijding tot een van haar prioriteiten gemaakt[83]. Zo blijkt uit het fraude onderzoeksrapport ‘Integrale Rapportage Handhaving 2005’ van dit ministerie dat er voor € 200 miljoen is gefraudeerd (werkgevers- en uitkeringsfraude). Ook in de private sector is fraudebestrijding een belangrijk thema. Hierbij kan gedacht worden aan hypotheekfraude, maar ook aan identiteitsfraude, waarbij de fraudeur gebruik maakt van de identiteit van een ander[84]. De op komst zijnde invoering van het BSN dient onder andere ter bestrijding van de identiteitsfraude.

Uitdagingen voor het persoonsinformatiebeleid

De steeds groter wordende aandacht voor fraudebestrijding zal naar verwachting leiden tot een nieuwe verhouding tussen informationele privacy en fraudebestrijding. Het is zoeken naar een nieuw optimum. De opstellers van “het PET witboek voor beslissers[85]” stellen dat met behulp van Privacy Enhancing Technologies, zowel de informationele privacy tot op zekere hoogte kan worden gegarandeerd als fraude kan worden bestreden. Gegevensverwerking vindt dan niet volledig anoniem plaats, maar wanneer gegevens worden gescheiden ontstaan wel nieuwe mogelijkheden. De identiteit kan dan worden losgekoppeld van overige gegevens. Wanneer er vervolgens een vermoeden van fraude bestaat, kan ervoor worden gekozen iemands ware identiteit te achterhalen.

Uiteraard moeten hieraan strikte voorwaarden worden gesteld, maar dit voorbeeld geeft wel aan dat er verschillende oplossingsrichtingen zijn bij de omgang met de spanningsvelden tussen informationele privacy en in dit geval fraudebestrijding. Het persoonsinformatiebeleid staat voor de uitdaging een instrumentarium te bieden voor inventarisatie van en besluitvorming over deze oplossingsrichtingen.

4.4. Internationale ontwikkelingen

De dreiging van en aandacht voor terrorisme heeft ook gevolgen op internationaal niveau. De druk van buitenlandse overheden op Nederland ten aanzien van de uitwisseling van persoonsinformatie neemt toe. Zo is er in Nederland de doorgifte van passagiersgegevens op vluchten naar de Verenigde Staten een belangrijke maatregel[86]. Sinds maart 2003 eist de Amerikaanse overheid dat Europese vliegtuigmaatschappijen haar toegang verschaft tot de 'Passenger Name Records' en het Advanced Passenger Information System. De twee gegevensbronnen tezamen bieden de Verenigde Staten onder andere inzicht in namen, geboortedata, paspoortnummers en nationaliteit. Dat vliegtuigmaatschappijen hieraan meewerken kan worden verklaard door angst voor het verlies van landingsrechten. Het vereiste echter wel een aanpassing van de Europese privacyregels, waarover in 2006 een akkoord is bereikt.
Uit dit laatste blijkt een andere belangrijke ontwikkeling: de invloed van de Europese Unie. Enige tijd geleden zou het nog noodzakelijk zijn geweest om de opsporingsbevoegdheden via Nederlandse wet- en regelgeving aan te passen. Steeds meer komt dergelijke wetgeving direct van Europa. Zinsconstructie Dit vraagt om de ontwikkeling van een Europees persoonsinformatiebeleid.
Voorts moet er voor de toekomst rekening mee gehouden worden dat door de economische groei van landen als China en India de buitenlandse druk niet alleen vanuit de Verenigde Staten zal komen. Met andere woorden, de internationale verhoudingen zullen veranderingen met zich meebrengen en deze verhoudingen kunnen een mogelijke bedreiging van de informationele privacy in de toekomst betekenen.
Tot slot werken nationale inlichten- en veiligheidsdiensten in toenemende mate samen bij de bestrijding van criminaliteit en veiligheid. Ook hier worden in toenemende mate gegevensbestanden gekoppeld en persoonsinformatie uitgewisseld. Dit laatste vraagt om duidelijke afspraken over en controle op de gegevensuitwisseling tussen landen. En ook hier is er behoefte aan een kwalitatief hoogwaardig afwegingsproces op basis waarvan deze afspraken kunnen worden gemaakt.

4.5. Een ordening van maatschappelijke, juridische & internationale ontwikkelingen

In onderstaande tabel staan de maatschappelijke, juridische en internationale ontwikkelingen en hun uitdagingen in tabelvorm samengevat.

Type Ontwikkeling	Ontwikkelingen	Uitdagingen voor het persoonsinformatiebeleid
Internationale ontwikkelingen	▪ Toenemende druk vanuit het buitenland ▪ Toenemende invloed van Europa op wet- en regelgeving inzake privacygerelateerde thema's ▪ Toenemende samenwerking tussen nationale inlichtingen- en veiligheidsdiensten	▪ Duidelijke afspraken en controle op gegevensuitwisseling tussen landen en inlichtingen- en veiligheidsdiensten ▪ Ontwikkeling van begeleiding van het afwegingsproces, zodanig dat informationele privacy adequaat kan worden afgewogen tegenover andere belangen ▪ Ontwikkeling van Europees persoonsinformatiebeleid
Maatschap-pelijke ontwikkelingen	▪ Hoge maatschappelijke waardering voor veiligheid, opsporing, fraudebestrijding en zorg ▪ Verschuivingen in de verhouding tussen informationele privacy enerzijds en veiligheid, opsporing, fraudebestrijding en zorg anderzijds ▪ Weinig aandacht voor privacy in het maatschappelijk debat over opsporingsbevoegdheden en fraudebestrijding ▪ Weinig aandacht voor het cumulatief effect van privacybedreigende maatregelen	▪ Vertrouwen creëren en borgen ▪ Optimale transparantie over afwegingen en evaluatie van wet- en regelgeving ▪ Aandacht hebben en/of creëren voor informationele privacy in het maatschappelijk debat ▪ Inzicht verschaffen in het cumulatief effect van maatregelen binnen verschillende beleidsterreinen op de informationele privacy ▪ Duidelijke afspraken over en controle op de koppeling van gegevensbestanden
Juridische ontwikkelingen	▪ Uitbreiding van de wettelijke bevoegdheden van politie, inlichtingen- en veiligheidsdiensten binnen het veiligheidsdomein ▪ Wettelijke rechten en plichten van zorgverleners en patiënten bepaald ten aanzien van patiëntgegevens in de zorgsector ▪ Wettelijke regelgeving ten aanzien van de omgang met persoonsgegevens door gemeentelijke diensten	▪ Evaluatie van en debat over de (cumulatieve) effecten van wet- en regelgeving op de informationele privacy en op het beoogd beleidsterrein ▪ Totstandkoming van nieuwe wet- en regelgeving onderdeel maken van het persoonsinformatiebeleid door begeleiding van het afwegingsproces ▪ Duidelijk onderscheid maken tussen doel en middel van wet- en regelgeving.

Tabel 4.5: Internationale, maatschappelijke en juridische ontwikkelingen

4.6. Naar een passend instrumentarium

In dit hoofdstuk zijn de belangrijkste ontwikkelingen van de afgelopen jaren geschetst die de zoektocht naar een nieuw optimum tussen informationele privacy en andere belangen mogelijk maken. Nieuwe ICT-toepassingen en inzichten bieden de mogelijkheid om verbeteringen aan te brengen in politieke processen en processen ten aanzien van beleidsontwikkeling, dienstverlening, handhaving, bedrijfsvoering en beheer. Deze kansen voor verbetering stellen het persoonsinformatiebeleid voor nieuwe uitdagingen

en vragen om een instrumentarium dat erin slaagt een nieuw optimum te bewerkstelligen.

De maatschappelijke, juridische en internationale ontwikkelingen laten zien dat informationele privacy de afgelopen jaren onder druk is komen te staan. Dit komt doordat de kansen die technologische ontwikkelingen bieden voor belangen als veiligheid, opsporing, zorg en administratieve lastenverlichting belangrijker lijken te worden geacht dan informationele privacy. Zowel terrorisme- als fraudebestrijding hebben aan maatschappelijke aandacht gewonnen. De wettelijke bevoegdheden van politie, inlichtingen- en veiligheden zijn bijvoorbeeld uitgebreid. Er is hierbij nauwelijks aandacht voor het cumulatieve effect van dergelijke maatregelen op de informationele privacy. De roep om het gebruik van ICT voor het verbeteren van de Nederlandse gezondheidszorg wordt bovendien luider. Dit hoeft niet noodzakelijkerwijs te leiden tot een verminderde informationele privacy, maar het gevaar bestaat dat veranderingen in de omgang met persoonsinformatie leiden tot een aanzienlijke vermindering van het vertrouwen in overheidsinstanties. Dit staat haaks op het streven naar een betere overheidsdienstverlening en een verbeterde relatie tussen overheid en burger. Bovendien is dit vanuit innovatief en economisch oogpunt onwenselijk. Uit onderzoek blijkt immers dat voor het slagen van technologische innovaties vertrouwen van burgers in de overheid essentieel is.

Bij het zoeken naar oplossingen voor bovenstaande uitdagingen zal elke keer weer moeten worden afgewogen wat informationele privacy in een bepaalde context en op een bepaald tijdstip inhoudt en welke waarde het heeft. Belangrijke vraag die daarbij gesteld moet worden is: welke andere waarde dan privacy komt bij een bepaalde ontwikkeling op de tocht te staan? Welk belang hechten burgers aan deze waarde?
En hoe stellen we burgers zo veel mogelijk in staat hun eigen keuzen te maken ten aanzien van het gebruik van hun persoonsgegevens?

Burgers moeten kunnen vertrouwen op de integriteit van instellingen die over hun persoonsinformatie beschikken. Overheden dienen daarom openheid te verschaffen over de afwegingen die worden gemaakt wat betreft het gebruik van deze informatie. Dit aspect van de informationele privacy is de afgelopen jaren onderbelicht geweest in het maatschappelijk debat[87]. Voor het welslagen van het persoonsinformatiebeleid is het debat rond de afweging tussen de informationele privacy en de inhoudelijke belangen urgent.
Het voorgaande laat zien dat het in een veranderende context noodzakelijk is dat het instrumentarium voor het persoonsinformatiebeleid verandert. In het volgende hoofdstuk wordt verslag gedaan van de praktijkstudies, waarin de mogelijkheden voor en verdere invulling van dit passende instrumentarium van het persoonsinformatiebeleid nader worden verkend.

Deel twee:
Privacy in de praktijk

5. Praktijkstudies

In dit hoofdstuk wordt verslag gedaan van drie praktijkstudies, die het empirisch gedeelte van het onderzoek vormen.
Deze praktijkstudies hebben tot doel inzicht te krijgen in de huidige situatie omtrent de omgang met persoonsinformatie. Binnen verschillende beleidsterreinen wordt onder andere bekeken welke persoonsgegevens tussen wie en op welke manier worden uitgewisseld. Ook wordt geanalyseerd wat de dominante invalshoeken ten aanzien van privacy zijn.

De volgende casussen komen aan bod:
- Het toezicht op de AIVD op het terrein van de collectieve veiligheid;
- Het proces van het aanvragen van een bijstandsuitkering;
- De problematiek omtrent slachtoffers van eergerelateerd geweld die in een blijf-van-mijn-lijf-huis verblijven.

Binnen elk van de casussen is er sprake van spanningsvelden tussen informationele privacy en de belangen van andere beleidsterreinen. Zo komt in de AIVD-casus het spanningsveld tussen informationele privacy en veiligheid aan de orde. In de casus over de bijstandsuitkering is er aandacht voor de spanningsvelden tussen informationele privacy, fraudebestrijding en administratieve lastenverlichting. En in de casus over de problematiek omtrent slachtoffers van eergerelateerd geweld staan privacy, gezondheidszorg en veiligheid op gespannen voet met elkaar. De manier waarop momenteel in de praktijk afwegingen tussen deze belangen worden gemaakt, is een belangrijk onderwerp van het praktijkonderzoek. Met mensen uit het veld is bovendien gereflecteerd op de betekenis van relevante ontwikkelingen voor de drie casussen en de (mogelijke) rol van het persoonsinformatiebeleid.

Als voorbereiding op de interviews met mensen in de praktijk is bij iedere casus een literatuurstudie verricht naar relevante ontwikkelingen en huidige kaders (waaronder wet- en regelgeving). Na bijeenkomsten en gesprekken met mensen uit het veld is het verzamelde materiaal geanalyseerd. Deze analyses zijn vervolgens via het principe van hoor en wederhoor getoetst bij de geïnterviewden. Hieronder volgen de belangrijkste bevindingen van de praktijkstudies. Een overzicht van de geïnterviewde personen bevindt zich in de vierde bijlage.

5.1. Het toezicht op de AIVD binnen het veiligheidsterrein

Zoals eerder in deze rapportage al werd geconstateerd, hebben zich op het veiligheidsterrein tal van ontwikkelingen voltrokken die een bedreiging vormen voor de informationele privacy. Met name de bevoegdheden van de inlichtingen- en veiligheidsdiensten, waaronder die van de Algemene Inlichtingen en Veiligheidsdienst (AIVD), zijn de afgelopen jaren sterk uitgebreid. Om zicht te krijgen op de wijze waarop door de AIVD met persoonsinformatie wordt omgegaan, zou het interessant zijn een concrete casus te onderzoeken. Hierbij valt te denken aan het reconstrueren van de gang van zaken omtrent een persoon tegen wie het ernstige vermoeden bestaat dat hij zich bezighoudt met aan terrorismegerelateerde activiteiten. De geheimhouding rondom de handelingen van de AIVD laat een dergelijke reconstructie van informatiestromen en van de concrete afwegingen die in de praktijk worden gemaakt echter niet toe. Om deze

reden wordt gefocust op het *toezicht* op de afweging tussen collectieve veiligheid en informationele privacy.

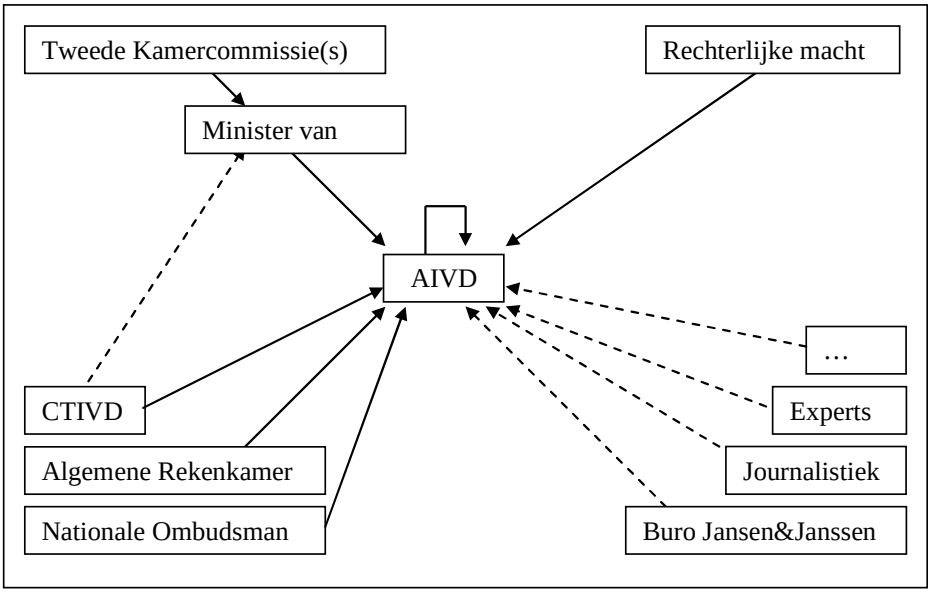
Dit leidt tot de volgende onderzoeksvraag:
Op welke wijze wordt in Nederland de afweging tussen collectieve veiligheid en informationele privacy gemaakt, op welke wijze vindt er toezicht plaats ten aanzien van deze afweging en wat is de (mogelijke) rol van persoonsinformatiebeleid hierbij?

5.1.1. Toezicht en het toezichtsproces

In deze casus wordt de volgende indeling gehanteerd met betrekking tot toezicht op de afweging tussen collectieve veiligheid en informationele privacy:

- Intern toezicht: toezicht door de AIVD zelf;
- Extern toezicht: toezicht door organisaties die expliciet als taak hebben om toezicht te houden, zoals de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de Nationale Ombudsman;
- Extern rechterlijk toezicht: toezicht door de rechterlijke macht;
- Extern democratisch toezicht: toezicht door de politiek ;
- Extern maatschappelijk toezicht: toezicht door maatschappelijke actoren als journalisten, actiegroepen en individuele burgers.

Persoonsinformatiebeleid en informationele privacy zijn onderwerpen die op elk toezichtstype van toepassing zijn. Intern, extern en rechterlijk toezicht focussen hierbij voornamelijk op de juridische kaders rondom de afweging tussen collectieve veiligheid en informationele privacy. Democratisch en maatschappelijk toezicht focussen voornamelijk op de politieke, maatschappelijke en legitimiteitsvraagstukken van de afweging tussen collectieve veiligheid en informationele privacy.
In onderstaand figuur zijn de vijf vormen van toezicht op de AIVD grafisch weergegeven. De figuur wordt op de volgende pagina toegelicht.



Figuur 5.1: Vormen van toezicht op de AIVD

In de figuur geven de ononderbroken pijlen het directe toezicht weer: toezicht waarbij de AIVD zelf direct betrokken is. De stippellijnen geven indirect toezicht weer. De pijl tussen het CTIVD en de Minister van Binnenlandse Zaken en Koninkrijksrelaties toon het proces van gevraagd en ongevraagd adviseren aan deze minister.
Een beschrijving van de in de figuur vermelde actoren bevindt zich in de vijfde bijlage.

5.1.2. Huidige kaders voor het toezicht

Ten aanzien van het toezicht op de AIVD zijn meerdere kaders van toepassing. We noemen hier de belangrijkste:

Interne richtlijnen AIVD
De AIVD heeft interne richtlijnen opgesteld voor haar handelswijze. Het is onbekend hoe deze er precies uitzien. Deze richtlijnen worden telkenmale aangescherpt en aangevuld. De CTIVD toetst de rechtmatigheid van deze richtlijnen. In het toezichtsrapport van de CTIVD betreffende de Contra Terrorisme Infobox[88] wordt meer inzicht gegeven in de criteria en de procedures die de AIVD hanteert ten aanzien van het gebruik van de Contra Terrorisme Infobox.

Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
Het CTIVD toetst de werkwijze en de taakuitvoering van de AIVD aan de grondbeginselen die zijn geformuleerd in dit verdrag.

Wet op de Inlichtingen- en Veiligheidsdiensten 2002
Het belangrijkste kader dat de CTIVD gebruikt voor haar toezicht is de Wet op de Inlichtingen- en Veiligheidsdiensten 2002. In deze wet staan beginselen beschreven rondom rechtmatigheid en doelbinding (artikel 12) en subsidiariteit en proportionaliteit (artikel 31 en 32). Daarnaast wordt er in de wet nadrukkelijk aandacht geschonken aan persoonsgegevens (artikelen 13, 40-42, 47-50). In 2006 is een wetsvoorstel ingediend voor een aantal wijzigingen ten aanzien van de WIV2002. Eén van de voorgestelde wijzigingen betreft de invoering van de *verplichting* om (persoons)gegevens te verstrekken door enkele, daartoe aangewezen, bestuursorganen aan de veiligheidsdiensten. Op grond van de huidige wet kunnen bestuursorganen worden *verzocht* om gegevens aan te leveren, wat een extra afwegingsmoment meebrengt tussen verschillende belangen. Dit afwegingsmoment vervalt als de wetswijziging wordt aangenomen.

Behoorlijkheidswijzer Nationale Ombudsman
De Nationale Ombudsman heeft als kerntaak om, naar aanleiding van een klacht van een burger, te toetsen of de overheid zich al dan niet behoorlijk heeft gedragen. Hiervoor heeft hij een *behoorlijkheidswijzer* opgesteld, waarin 23 behoorlijkheidsvereisten staan beschreven die de Nationale Ombudsman hanteert. De onderzoeken waarin klachten aan de hand van deze vereisten worden beoordeeld, kunnen gezien worden als ‘ombudsprudentie’. Dit betreft nadrukkelijk géén wet- en regelgeving. In de zesde bijlage staan de 23 behoorlijkheidsvereisten.

5.1.3. Dominante invalshoek ten aanzien van privacy

Binnen het toezicht op de afweging tussen veiligheid en privacy, wordt niet alleen aandacht besteed aan informationele privacy. Het werk van de AIVD raakt naast de informationele privacy ook de ruimtelijke privacy (denk aan doorzoekingen van

bijvoorbeeld huizen) en de relationele privacy (te denken valt aan telefoontaps). Wat desondanks opvalt is de expliciete aandacht voor persoonsgegevens in de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (artikelen 13, 40-42, 47-50). Dit is te verklaren door het feit dat de Wet Bescherming Persoonsgegevens niet van toepassing is op de verwerking van persoonsgegevens door de Inlichtingen- en Veiligheidsdiensten.

Het huidige toezicht is hoofdzakelijk juridisch bepaald. Het bestaat uit de eerder beschreven kaders en bijbehorende jurisprudentie. Wanneer er bijvoorbeeld maatschappelijke onrust is omtrent het onderzoek van de AIVD naar journalisten van de Telegraaf, onderzoekt de CTIVD op basis van bestaande wet- en regelgeving of de AIVD juist heeft gehandeld[89]. In haar uiteindelijk rapport geeft zij vervolgens een algemene beschouwing over hoe in de toekomst in dergelijke situaties dient te worden gehandeld door de verschillende actoren.

Alhoewel het toezicht, en daarmee de gemaakte afwegingen, sterk juridisch zijn ingestoken, draait het bij het toezicht duidelijk niet alleen om dataprotectie, maar zeker ook om belangenafwegingen. Er kan echter nauwelijks gesproken worden van een recht van burgers op informationele privacy, omdat door het veiligheidsbelang van geheimhouding burgers geen zicht hebben op de informatie die over hen bekend is of die ten aanzien van hen wordt toegepast. Als burgers al rechten hebben om zelf toe te zien op bescherming van hun privacy, dan is dit nadat hun persoonsinformatie is verzameld en/of uitgewisseld. Op die manier wordt informationele privacy binnen het veiligheidsterrein meer als afweerrecht dan als actierecht vormgegeven.

5.1.4. Het functioneren van het toezicht

De afweging tussen collectieve veiligheid en informationele privacy en het toezicht daarop lijken behoorlijk tot goed te functioneren volgens verschillende onderzoeken[90] en de geïnterviewden. Het afwegingskader zoals dat in de WIV2002 is geschetst lijkt voldoende te zijn om de afwegingen op een juiste wijze te kunnen maken. Daar waar de wettelijke kaders hiaten geven, wordt dit opgevuld door de behoorlijkheidswijzer van de Nationale Ombudsman en de jurisprudentie die de CTIVD opbouwt door de wettelijke kaders in concrete casussen te duiden.
De CTIVD gaat onder andere over tot onderzoek wanneer er sprake is van maatschappelijke onrust (bijvoorbeeld wanneer media gegronde twijfels uiten bij het handelen van de AIVD in bepaalde gevallen) of wanneer er expliciet door de politiek wordt gevraagd om onderzoek. We kunnen hierbij stellen dat het toezicht casusgericht is: toezicht wordt ingestoken op casusniveau en op basis van onderzoek naar specifieke casussen. Op basis hiervan worden eventueel algemene beschouwingen gegeven. Een integrale evaluatiefunctie van wet- en regelgeving is binnen het toezicht niet ingevuld. Er ontstaan door deze vorm van toezicht houden wel beleidsregels, waaraan de AIVD zich in het vervolg ook gehouden acht. Beleidsmatig toezicht waarbij een specifiek aspect (zoals bijvoorbeeld de omgang met persoonsgegevens) breed wordt onderzocht (over meerdere casussen heen) is een andere taak van de CTIVD. (Evaluatie)onderzoek van de WIV2002 is geen taak van de CTIVD.
Zowel de CTIVD als de Nationale Ombudsman krijgen bij hun onderzoeken inzage in dossiers van de AIVD. Hiervoor zijn betrokken medewerkers volgens de WIV2002 gescreend en geautoriseerd. De informatie die voor deze onderzoeken wordt verkregen wordt in papieren vorm opgeslagen in kluizen of op locatie ingezien. De CTIVD kan eveneens zelfstandig de digitale systemen en documenten doorzoeken. De CTIVD en de Nationale Ombudsman hebben aangegeven dat de AIVD zich coöperatief opstelt bij onderzoeken.

Tot slot lijkt over het algemeen van een ongenuanceerdheid bij de toezichtsactoren geen sprake. Tijdens de gesprekken is de indruk ontstaan dat door de actoren zowel het belang van collectieve veiligheid als dat van privacy wordt onderschreven.

5.1.5. Mogelijkheden tot tegenmacht voor de burger

De burger heeft verschillende middelen tot zijn beschikking om bezwaar te maken tegen het handelen van de AIVD of om achteraf zicht te krijgen op het gebruik van zijn persoonsgegevens. Deze middelen kunnen gezien worden als mogelijkheden om privacy, weliswaar nadat persoonsgegevens zijn verzameld, opgeslagen en/of uitgewisseld, als actierecht vorm te geven. Zij geven de burger tegenmacht ten opzichte van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Wij behandelen drie van deze middelen.

Allereerst is er de notificatieplicht. In de WIV2002 is een zogeheten notificatieplicht opgenomen. Dit houdt in dat vijf jaar na uitoefening van bijzondere bevoegdheden door onder andere de AIVD wordt onderzocht of hiervan verslag kan worden uitgebracht aan de persoon op wie deze bevoegdheden van toepassing zijn geweest. In de loop van 2007 zullen de eerste beoordelingen in dit kader plaatsvinden. Het is onduidelijk hoe dit zal uitpakken in termen van aantallen verslagen en de impact van deze verslagen. Het is mogelijk dat het verschijnen van meerdere verslagen een vliegwieleffect heeft ten aanzien van de publieke belangstelling voor de handelswijze van AIVD.

Ten tweede het indienen van klachten door burgers bij de CTIVD en de Nationale Ombudsman. Sinds 2003 heeft de CTIVD zeven klachten behandeld die betrekking hadden op de AIVD. De Nationale Ombudsman heeft sinds 2002 drie klachten behandeld die direct betrekking hadden op de AIVD. Dit is ronduit laag te noemen. Een door geïnterviewden geopperde verklaring is dat personen die door de AIVD worden onderzocht over het algemeen geen personen zijn die contact zoeken met de overheid omdat zij zo ongewenst de aandacht op zich vestigen.

Tot slot is er de rechterlijke macht. De rechterlijke macht is in veel gevallen een laatste stap voor burgers als zij een actie (in dit geval een belangenafweging) van de overheid onrechtmatig vinden. In het geval van de belangenafweging bij de AIVD is dat lastiger. In eerste instantie is deze belangenafweging ‘onzichtbaar’ voor de burger en als je iets niet weet kun je dat ook niet voor de rechter brengen. In tweede instantie is de rechtspraak in Nederland gebaseerd op *openheid* en de werkwijze van de AIVD is gebaseerd op *geheimhouding*. Er zijn wel regelingen voor dit dilemma, maar het gaat te ver om deze hier uiteen te zetten. Kort gezegd kan een (van de) rechter(s) of een rechter-commissaris in bepaalde gevallen AIVD-stukken inzien, maar deze kunnen inhoudelijk niet behandeld worden tijdens een rechtszaak. Hierbij speelt ook het feit dat de AIVD geen enkele mededeling doet over of iemand onderwerp van onderzoek is. Bij een rechtszaak wordt dit echter soms (impliciet) bevestigd.

5.1.6. Rol van persoonsinformatiebeleid binnen het veiligheidsterrein

Deze casus biedt een aantal interessante aanknopingspunten voor de invulling van het toekomstige persoonsinformatiebeleid in het algemeen en binnen het terrein van de veiligheid in het bijzonder.

Afwegingen op basis van wet- en regelgeving én andere criteria

Als het gaat om de afweging tussen (informationele) privacy en collectieve veiligheid dan wordt door de CTIVD aangegeven dat deze is gebaseerd op wet- en regelgeving (de WIV2002 en andere relevante regelgeving als het Europees Verdrag van de Rechten van de Mens). De CTIVD geeft daarbij aan dat de duiding van wet- en regelgeving altijd een subjectieve component kent. Zij heeft hiervoor haar eigen instrumentarium ontwikkeld, waaronder de analyse van gelijksoortige casussen, het analyseren van de (verhouding tussen) verschillende wetten en regelingen en het opbouwen van jurisprudentie.
De behoorlijkheidswijzer van de Nationale Ombudsman reikt verder dan wet- en regelgeving. Dit omdat het beoordelen van zaken als subsidiariteit en proportionaliteit vraagt om het in acht nemen van een aantal waarden die niet bij wet geregeld zijn: iets kan wel rechtmatig zijn, maar niet behoorlijk. Dit laatste laat zien dat procesbegeleiding van het afwegingsproces door het persoonsinformatiebeleid vraagt om een instrumentarium voor het duiden van wet- en regelgeving en het onderscheiden van andere waarden en criteria (behoorlijkheidscriteria). Deze waarden en criteria kunnen per terrein verschillen.

Niet in elke sector is behoefte aan een extra speler omtrent het afwegingsproces
Het 'gereguleerde' toezicht op de AIVD bestaat uit meerdere vormen die worden uitgevoerd door meerdere instanties. Deze vorm van checks-and-balances werkt volgens verschillende onderzoeken en de geïnterviewden behoorlijk. Persoonsinformatiebeleid wordt door de verschillende actoren gezien als het totaal aan bestaande wet- en regelgeving en het CBP. Dit functioneert volgens de actoren naar behoren en er bestaat dan ook geen behoefte aan een extra speler rondom het afwegingsproces. Dit neemt niet weg dat de communicatie omtrent het afwegingsproces wel kan worden verbeterd. Dit wordt hieronder nader beschreven.

Het verschaffen van inzicht in cumulatieve effecten door evaluatie
Volgens het Rathenau-instituut is er momenteel geen zicht op het cumulatief effect van de wijzigingen in wet- en regelgeving op het veiligheidsterrein. Binnen het toezicht is er momenteel geen partij die zich hiermee bezighoudt: het huidig toezicht heeft betrekking op de uitvoering van afzonderlijke wetten en de vertaling van wet- en regelgeving naar afzonderlijke casussen. Evaluatie van wet- en regelgeving wordt gezien als een politieke aangelegenheid. Hier lijkt een duidelijke hiaat te liggen welke door het persoonsinformatiebeleid kan worden ingevuld. Zij kan hierbij zowel bij de totstandkoming van wet- en regelgeving stimuleren dat evaluatie hiervan in de wet wordt opgenomen, als zelf deze evaluatie van (cumulatieve effecten) van wet- en regelgeving initiëren. Op deze manier wordt de transparantie binnen het veiligheidsterrein vergroot en het maatschappelijk debat gestimuleerd.

Optimaliseren van de relatie burger-overheid
Zoals in dit rapport al meerdere keren is gesteld: privacy is context- en doelgroepafhankelijk. De maatschappelijk tendens is een belangrijke bepalende factor van het belang dat door individuele burgers aan privacy wordt gehecht. Momenteel blijkt privacy voor burgers grotendeels ondergeschikt te zijn aan het belang van veiligheid. Het is de vraag op welke wijze het persoonsinformatiebeleid met deze maatschappelijke tendens(en) omgaat. Zo kan het zodanig worden ingestoken dat zij probeert deze tendensen te keren en dus probeert de maatschappelijke waardering voor privacy te verhogen. Een andere insteek is dat het persoonsinformatiebeleid zich met name focust op de afweer- en actierechten voor burgers die wel waarde hechten aan hun privacy, zodat het burgers zelf de keuze laat.

In beide gevallen heeft het persoonsinformatiebeleid de belangrijke rol om de relatie tussen overheid en burger te optimaliseren en te zorgen dat de burger door transparantie vertrouwen heeft in de over zijn persoonsgegevens beschikkende overheid. Op deze manier wordt voorkomen dat vanwege het onvermijdelijke gebrek aan transparantie van informatiestromen op het veiligheidsterrein, en door het toenemend gebruik van techniek, de burger vervreemdt van de overheid.

5.2. De aanvraag van een bijstandsuitkering

Het doel van deze casus is het verkrijgen van inzicht in de wijze waarop er binnen het klantproces van het aanvragen van een bijstandsuitkering wordt omgegaan met de uitwisseling van vertrouwelijke persoonsinformatie van de aanvrager. Tevens is getracht concreet inzicht te verkrijgen in de informatie-uitwisseling tussen de verschillende verantwoordelijke instanties en de aanvrager.

Dit leidt tot de volgende onderzoeksvraag:
Hoe ziet het klantproces van het aanvragen van een bijstandsuitkering eruit, welke partijen zijn hierbij betrokken en hoe gaat men in dit proces specifiek om met de uitwisseling van privacygevoelige persoonsinformatie van de betrokken burger?

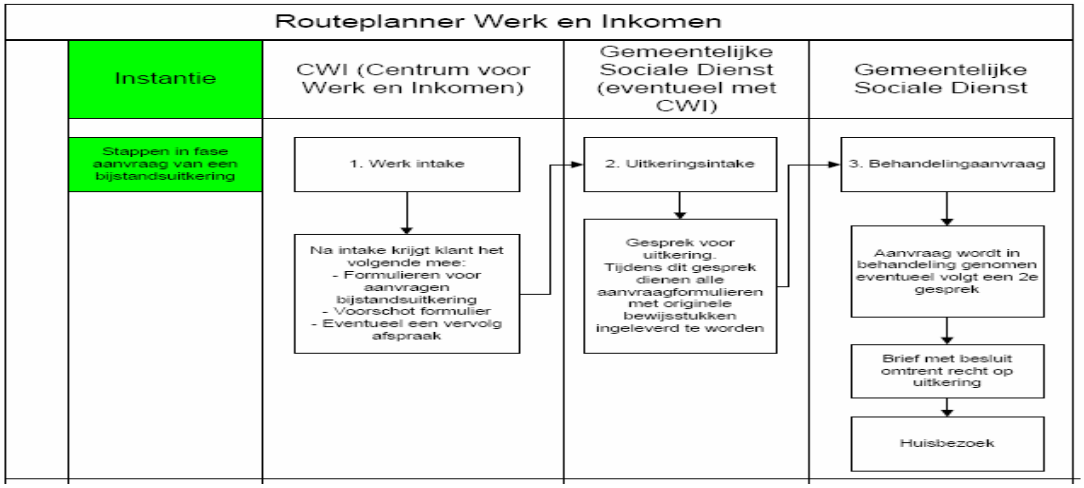
5.2.1. Bijstand en bijbehorende belangen

Een bijstandsuitkering is een uitkering in het kader van de Wet Werk en Bijstand (WWB), waarvoor een burger in aanmerking komt als deze in Nederland woont en over de Nederlandse nationaliteit of een geldige verblijfsvergunning beschikt, niet genoeg geld heeft om in zijn/ haar levensonderhoud te voorzien en ook niet in aanmerking komt voor een andere uitkering. De bijstandsuitkering is bedoeld om de periode te overbruggen van het moment dat iemand werkloos geraakt tot het moment waarop de burger weer een baan heeft gevonden. De hoogte van de uitkering is afhankelijk van de persoonlijke omstandigheden, mogelijkheden en middelen van de burger.

In deze casus ligt de focus op drie belangen: informationele privacy, dienstverlening en fraudebestrijding. De Gemeentelijke Sociale Dienst (GSD) is verantwoordelijk voor de uitvoering van de bijstandsuitkering oftewel de Wet Werk en Bijstand (WWB). Dit betekent dat de gemeente haar dienstverlening dusdanig dient in te richten dat ze garant kan staan voor de rechtmatige verdeling van uitkeringen. Rechtmatige verdeling betekent enerzijds dat zij die recht hebben op een uitkering deze ook ontvangen (minimaliseren van niet-gebruik) en anderzijds dat zij die hier geen recht op hebben deze ook niet ontvangen (fraudebestrijding[91]). Teneinde aan deze dienstverlenings- en handhavingverplichting te kunnen voldoen heeft de gemeente vanaf een vroeg stadium diverse persoonsgegevens nodig van de uitkeringsaanvrager. Om met het oog op de fraudebestrijding de juistheid van deze persoongegevens te achterhalen, heeft de GSD een aantal middelen tot haar beschikking die mogelijkerwijs op gespannen voet staan met de informationele privacy van de aanvrager. Dergelijke afwegingen tussen de drie onderscheiden belangen staan in deze casus centraal.

5.2.2. Het klantproces en betrokken actoren

Het aanvragen van een bijstandsuitkering en de samenwerking van de bij dit proces betrokken actoren is uiteen te zetten in een aantal stappen, zoals in onderstaand figuur is weergegeven.



Figuur 5.2: Routeplanner van de aanvraag van een bijstandsuitkering

In bovenstaand figuur is te zien dat de burger die een bijstandsuitkering wil aanvragen zich eerst aanmeldt bij het CWI. Deze gaat vervolgens samen met de burger na of er eventueel direct werk beschikbaar is. Is dit er niet dan zal de medewerker van het CWI een afspraak maken voor een intakegesprek voor een uitkering en zal de burger enkele formulieren meekrijgen om thuis in te vullen, ter voorbereiding van het volgende intakegesprek. Tijdens deze uitkeringsintake worden de ingevulde formulieren doorgenomen en de nodige bewijsstukken gecontroleerd. In de achtste bijlage bevindt zich een overzicht van de bewijsstukken die moeten worden aangeleverd.

De formulieren en bewijsstukken worden eerst in de computer overgenomen en opgeslagen, waarna er een papieren dossier door de Gemeentelijke Sociale Dienst (GSD) wordt gevormd, welke de aanvraag tevens in behandeling neemt. De GSD is verantwoordelijk voor het beoordelen van de aanvraag en het uiteindelijk uitkeren van de bijstand.
Wanneer de GSD de aanvraag in behandeling neemt, wordt de cliënt door haar uitgenodigd voor een gesprek. Tevens gaat de GSD in een aantal gemeenten zoals bijvoorbeeld de gemeente Amsterdam en Rotterdam, maar ook in de onderzochte gemeente onaangekondigd bij de cliënt langs voor een huisbezoek, ter controle en verificatie van de opgegeven informatie en bewijsstukken.

In de onderzochte casus vindt 100% controle plaats. Dit houdt in dat er bij iedereen die een bijstandsuitkering aanvraagt een huisbezoek wordt afgelegd, ook wanneer er geen verdenking van mogelijke fraude is. Tijdens deze huisbezoeken wordt gezocht naar aanwijzingen die erop kunnen duiden dat de cliënt onrechtmatig een uitkering ontvangt, ondermeer door - met goedkeuring van de cliënt - in kasten en laden te kijken. Werkt de cliënt echter niet mee aan het huisbezoek dan krijgt deze een kleine 15 minuten bedenktijd. Gaat de cliënt hier niet op in dan loopt deze het reële risico dat zijn of haar uitkering wordt stopgezet. Ook wordt tijdens het huisbezoek bijvoorbeeld gekeken naar

het merk parfum dat een cliënt in zijn of haar bezit heeft, omdat dit indicaties van het uitgavenpatroon van de aanvrager geeft. De zevende bijlage bevat meer informatie over het klantproces.

5.2.3. Huidige wettelijke kaders voor het uitwisselen van gegevens

In artikel 64 van de Wet Werk en Bijstand zijn de instanties benoemd die gerechtigd zijn persoonsgegevens van aanvragers uit te wisselen (zie hiervoor bijlage negen).
Naast het uitwisselen van gegevens beschikt de GSD over de mogelijkheid om haar bestanden te vergelijken met bijvoorbeeld bestanden van het CWI en het UWV. Hieraan is wel een aantal voorwaarden verbonden. Zo moet de bestandsvergelijking ten eerste noodzakelijk zijn voor een goede uitvoering van de WWB en worden het proportionaliteit- en subsidiariteitsbeginsel gehanteerd. Daarnaast heeft de GSD een informatieplicht welke voorschrijft dat een cliënt geïnformeerd dient te worden zodra er over hem gegevens zijn verkregen via andere partijen of instanties.

5.2.4. Problemen door uitwisseling van papieren dossiers

Het vergaren, opslaan en uitwisselen van persoonsgegevens gebeurt verre van optimaal. In de onderzochte praktijk wordt voornamelijk met papieren dossiers gewerkt, die naast diverse door de cliënt ingevulde formulieren kopieën van bewijsstukken bevatten. Hierbij is gebleken dat de professionals zonder de aanwezigheid van het fysieke dossier hun werk niet goed kunnen verrichten, omdat de digitale dossiers niet compleet zijn. Daarnaast worden papieren dossiers in gangkasten opgeslagen die voor veel mensen toegankelijk zijn. Een ander probleem is het verplaatsen van papieren dossiers per post en/ of koerier zonder dat het dossier verzegeld of afgeschermd is. Hierdoor is de kans aanwezig dat privacygevoelige cliëntgegevens op straat komen te liggen. Zo blijkt in de praktijk dat het dossier zoek kan raken, waardoor het in handen van onbevoegden kan komen, met alle mogelijke gevolgen van dien.

Veel persoonsgegevens worden nog steeds bij de cliënt zelf opgevraagd, terwijl tal van deze gegevens tevens via andere partijen opgevraagd kunnen worden, bijvoorbeeld bij de RDW of de Belastingdienst. Ketenpartners hebben vanuit het oogpunt van dataprotectie geen toegang tot elkaars systemen. Wel is het voor de afdeling ‘bijzonder onderzoek’ van de Gemeentelijke Sociale Dienst mogelijk om informatie bij andere instanties zoals de RDW op te vragen. Resultaat is dat controles achteraf plaatsvinden, waardoor er door de Gemeentelijke Sociale Dienst bij geconstateerde fraude een terugvorderingproces opgezet moet worden.

5.2.5. Privacy in de praktijk

Met het oog op fraudebestrijding worden door de Gemeentelijke Sociale Dienst veel privacygevoelige gegevens opgevraagd en verwerkt. Zo vraagt zij bijvoorbeeld informatie bij de cliënt omtrent diens tijdsbesteding, dagritme, het gebruik van alcohol en verdovende middelen, maar ook naar zijn woninginrichting. Tevens worden er vragen gesteld over medische aangelegenheden, zoals over het gebruik van geneesmiddelen, over lichamelijke beperkingen en over eventuele sociale of psychische problemen. De gemeentelijk medewerkers die deze informatie verzamelen wonen vaak in hetzelfde dorp of stad als de aanvrager van de bijstandsuitkering, hetgeen als een extra inbreuk op de informationele privacy kan worden ervaren.
We constateren dat het werk van GSD zowel de informationele privacy alsook de lichamelijke privacy raakt. Met de huiszoekingen wordt tevens een inbreuk gemaakt op

de ruimtelijke privacy van de burger. De verzamelde informatie wordt vervolgens ook in dossiers vastgelegd, zodat uiteindelijk ook de informationele privacy wordt beïnvloed.

Zoals uit de beschrijving van de wettelijke kaders blijkt, zijn er voorwaarden gesteld aan het vergaren en opslaan van persoonsgegevens. De aanvrager heeft echter geen middelen tot zijn beschikking om zelf de regie te voeren over het vergaren en gebruik van zijn persoonsgegevens. Wanneer een uitkeringaanvrager bijvoorbeeld weigert mee te werken aan een huiszoeking wordt zijn uitkering geweigerd of onmiddellijk stop gezet.

Hiermee kan geconcludeerd dat de focus in deze casus meer ligt op fraudebestrijding dan op privacy. Gemeenten achten het noodzakelijk dat fraudebestrijding ten koste gaat van de privacy van de aanvrager. De Gemeentelijke Sociale Dienst lijkt van mening te zijn dat het belang van het rechtmatig verdelen van gemeenschapsgeld zwaarder weegt dan de privacy van de 'burger in nood'. Aangezien de uitkeringsaanvrager moet kunnen voorzien in zijn levensonderhoud zal hij daarvoor 'enige concessies' moeten doen. De wettelijke kaders moeten ervoor zorgen dat de privacyinbreuk niet disproportioneel wordt.

Administratieve lastenverlichting als vorm van dienstverlening naar de burger lijkt daarentegen minder belangrijk te worden gevonden dan de bescherming van persoonsgegevens. Met het oog op dataprotectie wordt ervoor gekozen geen koppelingen tussen digitale bestanden aan te brengen. Echter, de praktijk laat zien dat de privacy van aanvragers met de huidige papieren organisatie van het proces niet gegarandeerd kan worden. Ook de papieren koppeling van gegevens brengt namelijk problemen op het gebied van de privacy met zich mee. In de onderzochte praktijk blijkt bijvoorbeeld dat het UWV geen toegang heeft tot digitale gegevens van de Gemeentelijke Sociale Dienst, waardoor papieren dossieruitwisseling van afdeling naar afdeling nodig is. Hierdoor gaat het dossier door vele, niet te controleren en bij de burger niet bekende, handen.

5.2.6. Rol van het persoonsinformatiebeleid in het klantproces

Wat betekenen bovenstaande bevindingen voor het persoonsinformatiebeleid? Gegeven de huidige focus op fraudebestrijding en de papieren koppeling van persoonsgegevens lijkt er op dit terrein een duidelijke rol weggelegd voor het persoonsinformatiebeleid. Voor de burger die veel waarde hecht aan zijn privacy zijn er momenteel weinig mogelijkheden. Het niet verstrekken van persoonsgegevens staat gelijk aan het niet ontvangen van een bijstandsuitkering. Er is een duidelijk gebrek aan middelen die de burger tegenmacht bieden en regie op zijn persoonsgegevens geven. Het persoonsinformatiebeleid kan op een dusdanige manier worden ingestoken dat de burger meer ruimte krijgt om zelf te bepalen wat er met persoonsgegevens gebeurt, waardoor privacy meer als actierecht en recht op informationele zelfbeschikking wordt vormgegeven. Het op komst zijnde Digitale Klant Dossier kan hiervoor onder andere worden aangegrepen.
De papieren situatie laat ook zien dat er behoefte is aan een duidelijker en vollediger afwegingsproces en aan een transparante communicatie over gemaakte afwegingen. Waarom bijvoorbeeld wel wordt gekozen voor huisbezoeken, ook al betekenen deze een sterke inbreuk op de privacy en niet wordt gekozen voor digitale koppelingen van gegevensbestanden is niet geheel duidelijk.

Tot slot toont de huidige casus dat hoewel er in de digitalisering van het klantproces wellicht gevaren voor de privacy schuilen, de huidige papieren situatie verre van optimaal

is. Vanwege het belang van dataprotectie wordt de digitale koppeling van gegevens vermeden, maar de gevolgen van papieren koppeling blijken voor de privacy net zo nadelig uit te pakken. In de praktijk pakken keuzen die worden gemaakt vanwege het belang van dataprotectie dus anders uit dan aanvankelijk de bedoeling was.

5.3. Hulpverlening in blijf van mijn lijf huizen

Doel van deze derde case is het verschaffen van inzicht in hoe er in het hulpverleningsproces aan vrouwen die in blijf van mijn lijf huizen verblijven, wordt omgegaan wordt met de uitwisseling van persoonsgegevens. Meer specifiek wordt ingegaan op het fenomeen eergerelateerd geweld, vanwege de complexiteit van deze opkomende problematiek.

De volgende vraag staat centraal in deze case:
Hoe wordt in de hulpverlening aan vrouwen in blijf van mijn lijf huizen omgegaan met de uitwisseling van vertrouwelijke persoonsgegevens?

5.3.1. Over blijf van mijn lijf huizen

Blijf van mijn lijfhuizen zijn opvanghuizen voor vrouwen en kinderen die slachtoffer zijn van, of bedreigd worden met, huiselijk geweld. Huiselijk geweld is geweld dat wordt gepleegd in de privé-sfeer, waarin de relatie tussen slachtoffers en plegers centraal staat. De huiselijke kring bestaat daarbij uit (ex)partners, gezinsleden, familieleden en huisvrienden. Huiselijk geweld kan de vorm aannemen van kindermishandeling en seksueel misbruik (incest), partnerrelatiegeweld en mishandeling en verwaarlozing van ouderen (Vink, 2006[92]). Vrouwen en kinderen die in aanraking komen met huiselijk geweld kunnen opvang aangeboden krijgen in een blijf van mijn lijf huis. Tevens kunnen de slachtoffers hulp krijgen bij het vinden van juridische of gerechtelijke bijstand, en eventueel bij het vinden van woonruimte na de opvang.

5.3.2. Het hulpverleningsproces en betrokken actoren

Wanneer een vrouw zich meldt bij de politie of een andere instantie omdat zij mishandeld en/of bedreigd wordt, kan zij doorverwezen worden naar een blijf van mijn lijf huis. De vrouw krijgt het telefoonnummer van het blijf van mijn lijf huis, waarna er een telefonische intake plaats vindt. Bij opname van de vrouw in een blijf van mijn lijf huis vindt een risicoscreening plaats om de ernst van de situatie te bepalen.

Sinds enkele jaren verdient het fenomeen eergerelateerd geweld bijzondere aandacht. Onder eergerelateerd geweld wordt verstaan: elke vorm van geestelijk of lichamelijk geweld, gepleegd in reactie op een (dreiging van) schending van de eer van een man of vrouw en daarmee van zijn of haar familie, waarvan de buitenwereld op de hoogte is of dreigt te raken. Vrouwen die (in de ogen van familieleden) de familie-eer geschonden hebben, worden vaak niet alleen gezocht door een geweldadige ex-partner, maar door een hele gemeenschap. Dit maakt dat het waarborgen van de privacy van deze vrouwen extra complex. Het zorgvuldig omgaan met de persoonsgegevens van deze vrouwen is een middel om de privacy van de doelgroep te waarborgen.

In de vrouwenopvang staat het belang van de vrouw altijd voorop. In de praktijk betekent dit dat gegevens zo veel mogelijk vastgelegd worden in papieren dossiers. Er is geen uitwisseling van gegevens tussen de verschillende opvanghuizen om de veiligheid van

de vrouwen zo veel mogelijk te waarborgen. De vraag die gesteld kan worden is of de vrouw op deze manier wel de kwaliteit van gezondheidszorg ontvangt die zij verdient. Het uitwisselen van gegevens tussen verschillende partijen in de gezondheidszorgketen kan immers de kwaliteit van zorg vergroten. Hieruit blijkt het in deze casus ervaren spanningsveld tussen informationele privacy en de veiligheid van de vrouwen enerzijds en de kwaliteit van hulpverlening anderzijds.
De vrouwenopvang heeft zich in de loop der jaren ontwikkeld van een op zich zelf staande opvangvoorziening voor vrouwen en kinderen naar een brede opvang en ondersteuningsvoorziening. Om deze reden neemt het aantal betrokken actoren toe. Het blijf van mijn lijf huis werkt steeds vaker samen met andere partijen in de regio zoals politie, openbaar ministerie en hulpverlenende instanties zoals de huisarts, het maatschappelijk werk of de geestelijke gezondheidszorg. In het geval van kinderen is het gezin soms bekend bij Bureau Jeugdzorg of de Raad voor de kinderbescherming (als de kinderen onder toezicht staan).

5.3.3. Huidige kaders

De Wet GBA stelt dat iedere burger verplicht is zijn of haar woonadres binnen vijf dagen na verhuizing kenbaar te maken aan de overheid. Het adres wordt dan opgenomen in de persoonsadministratie van de overheid, de Gemeentelijke Basisadministratie. Op het GBA-adres dient de betrokkene voor de overheid bereikbaar te zijn. Indien geen sprake is van een vaste woon- of verblijfplaats, of wanneer het om zwaarwegende redenen niet wenselijk is het verblijfadres op te nemen in de GBA, biedt artikel 1 van diezelfde wet de mogelijkheid een briefadres te kiezen. Een dergelijk adres kan geen postbus zijn; een vereiste die de overheid stelt is dat de voor de burger bestemde geschriften door de briefadresgever in ontvangst kunnen worden genomen en worden doorgezonden. Voor vrouwen in de opvang betekent dit dat zij bij een persoon die zij vertrouwen, desnoods in een andere gemeente, een briefadres kunnen kiezen.

Het College van Burgemeester en Wethouders kan daarnaast conform artikel 67 van de wet GBA in de gemeente gevestigde opvanghuizen aanwijzen als instelling waar de bewoners op grond van privacyoverwegingen een briefadres kunnen kiezen. Op grond van artikel 102 van de wet GBA kan de burger verzoeken om geheimhouding van zijn of haar gegevens, of de betrokkene nu op een briefadres staat ingeschreven of niet. De persoonsgegevens van een persoon die om geheimhouding verzocht heeft worden dan alleen nog verstrekt aan instellingen die een publiekrechtelijke taak vervullen. Bij levering van de persoonsgegevens wordt een signaal “indicatie geheim” meegeleverd aan de afnemer. In een circulaire d.d. 17 mei 2005 benadrukt het Agentschap BPR (verantwoordelijk voor de GBA) aan alle Colleges van burgemeester en wethouders nogmaals het belang van het zorgvuldig omgaan met persoonsgegevens van vrouwen in de opvang. BPR legt daarbij de nadruk op het zorgvuldig uitvoeren van de wettelijke bepalingen die het al mogelijk maken de veiligheid van bedreigde vrouwen te vergroten.

Op 1 april 2007 is de Wet Basisregistratie GBA van kracht geworden. De overheid zet hiermee een belangrijke stap in de richting van het eenmalig vastleggen en meervoudig gebruiken van persoonsgegevens. Als de wet op het Burger Service Nummer aangenomen wordt, kunnen zij de gegevens uitwisselen op basis van dit persoonsnummer. Overheden gaan hun gegevens dus beter delen. Voor bedreigde vrouwen betekent dit dat het extra belangrijk wordt dat toegezien wordt op de naleving van bepalingen die hun veiligheid helpen waarborgen.

Vanwege de opkomende problematiek rondom eergerelateerd geweld is door het ministerie van Justitie in samenwerking met het Ministerie van Sociale Zaken en werkgelegenheid een programmabureau eergerelateerd geweld opgericht. Het programmabureau behartigt de belangen van vrouwen die het slachtoffer van eerwraak dreigen te worden.

5.3.4. Dominante invalshoek ten aanzien van privacy

Om de privacy van de vrouw te waarborgen, worden gegevens in de praktijk zo min mogelijk uitgewisseld. Dat houdt in dat gegevens die kunnen bijdragen aan de hulpverlening van de vrouw niet optimaal uitgewisseld worden, om te voorkomen dat de verblijfplaats van de vrouw bekend wordt. Vanuit een dataprotectie-oogpunt is dit een logische stap.

Het bekend worden van de persoonsgegevens vergroot zoals we gezien hebben het risico voor de vrouw. Andere vormen van privacy (huiselijke, lichamelijke en relationale privacy) kunnen gewaarborgd worden door middel van het borgen van de informationele privacy. Immers, als een man moeilijker aan de persoonsgegevens van een vrouw kan komen, wordt het lastiger haar te vinden, haar te mishandelen of ongewenst met haar in contact te treden. Het automatisme om door te schieten in dataprotectie is te begrijpen, ware het niet dat bij een goede en bewuste belangenafweging tussen kwaliteit van hulpverlening aan de vrouw en het uitwisselen van persoonsgegevens de balans anders uit zou kunnen slaan. Voorwaarde daarbij is wel dat de juiste waarborgen ingebouwd zijn om de informationele privacy te kunnen garanderen.

5.3.5. Bronnen van dreiging

Er kunnen vier bronnen van dreiging worden onderscheiden voor de veiligheid van de vrouw die slachtoffer is van (eergerelateerd) huiselijk geweld.
Allereerst kan de vrouw zelf als bron van dreiging worden gezien. Hoewel de vrouwen in de opvang zich terdege bewust zijn van de dreiging die hen boven het hoofd hangt, is de vrouw tegelijkertijd zelf vaak een bron van dreiging. Het achterlaten van de vertrouwde omgeving –hoe bedreigend die ook geworden is- valt een aantal vrouwen zo zwaar dat zij toch weer contact opnemen met hun oude omgeving. Dit kan opnieuw leiden tot bedreigende situaties. Als de vrouw zelf het contact niet zoekt, wordt zij toch vaak gevonden door het zogenaamde “informele circuit”. Via de moskee of de nieuwe school van de kinderen worden de vrouwen toch weer gevonden door de gemeenschap.

Ten tweede is de overheid een bron van dreiging. Als de vrouw zelf geen contact zoekt met haar bedreigende omgeving is het voor de omgeving soms mogelijk via de overheid de verblijfplaats van de vrouw te achterhalen. De verblijfplaats van de vrouw kan in de GBA (gemeentelijke basisadministratie) aangemerkt worden als geheim. Vrouwen kiezen vaak een briefadres; dit briefadres is vaak gelegen in de plaats waar de opvang daadwerkelijk plaatsvindt. Dit maakt het zoeken een stuk makkelijker; je weet immers al in welke gemeente je moet zoeken. Het briefadres en de indicatie ‘geheim’ worden vanuit de GBA doorgeleverd aan derden (bijv. IB-groep), die de indicatie geheim niet altijd in hun systeem over kunnen nemen. Medewerkers bij de afnemende partij hebben zodoende toegang tot de NAW-gegevens van de vrouw, zonder daarbij de vermelding te krijgen dat de gegevens geheim zijn.
Soms is het via familieleden of kennissen die bij Burgerzaken of een van de afnemende partijen werken mogelijk de verblijfplaats van een vrouw te achterhalen; gegevens met de indicatie “geheim” uit de GBA zijn immers niet afgeschermd voor medewerkers. Alle

medewerkers die toegang hebben tot de GBA kunnen dus ook de persoonsgegevens van vrouwen met indicatie “geheim” zien. Daarnaast blijkt in de praktijk dat het mogelijk is telefonisch de verblijfplaats te achterhalen wanneer familieleden/ kennissen zich voordoen als medewerkers van Burgerzaken uit een andere gemeente. Hoewel het bij wet verboden is telefonisch dit soort informatie te verstrekken, wijst de praktijk uit dat dit wel degelijk mogelijk is en gebeurt. Ook via de formele weg is het mogelijk de verblijfplaats van de vrouw te achterhalen. Vaders kunnen bij burgerzaken hun persoonslijst opvragen. Op die persoonslijst staan ook de kinderen, met hun huidige adres, vermeld. Uit het voorgaande blijkt dat *regels op papier niet altijd naleving in de praktijk betekenen.*

Als derde zijn private partijen een bron. Het vastleggen van persoonsgegevens beperkt zich niet tot overheidsinstanties. Banken en zorgverzekeraars zijn belangrijke bronnen van informatie. Banken sturen bijvoorbeeld bij verhuizingen vaak een servicebericht naar het oude adres, met de bevestiging van de verhuizing naar het nieuwe adres. Voor een ex-partner is de verblijfplaats van de vrouw zo gemakkelijk te achterhalen.
In 2004 werd bijvoorbeeld slachtoffer van huiselijk geweld Gül B. voor de deur van een Zaans blijf-van-mijn-lijfhuis doodgeschoten. Telkens wist de ex-echtgenoot van Gül B., haar verblijfplaats te achterhalen, waardoor zij van het ene naar het andere opvanghuis moest verhuizen. Haar ex-echtgenoot kwam achter haar adresgegevens via de website van haar zorgverzekeraar.
Hieruit blijken de uitdagingen van publiek-private samenwerking. Het afschermen van de gegevens in de publieke sector laat onverlet dat de persoonsgegevens via de private sector bekend kunnen worden. Soms hebben private instanties (banken, zorgverzekeraars, ziekenhuizen) geen weet van de situatie waarin de vrouw verkeert en geen besef van de gevolgen van de bedreigende situatie voor hun eigen werkprocessen. Vele medewerkers van deze instanties hebben toegang tot de persoonsgegevens van de vrouw, waardoor de mogelijkheid tot “lekken”, bewust of onbewust, groter wordt.

Tot slot internet als bron. Het toenemend gebruik van internet draagt ook bij aan de vindbaarheid van bedreigde vrouwen. Via www.google.nl of sites als www.hyves.nl wordt het makkelijker mensen te vinden.

Tot op heden hebben we ons vooral gericht op de problematiek van vrouwen in de opvang. De dreiging houdt echter niet op nadat de opvang stopt. In veel gevallen blijft de dreiging nog jaren nadat de vrouw uit de opvang vertrokken is bestaan. Vrouwen worden gemotiveerd na de periode van opvang een nieuw leven te beginnen met een nieuw huis, een nieuwe omgeving en wellicht een bijstandsuitkering. Om gebruik te maken van voorzieningen als huurtoeslag en een bijstandsuitkering is een inschrijving in de GBA vereist. Zoals we eerder zagen kan een dergelijke inschrijving bijdragen aan een bedreigende situatie voor de vrouw

5.3.6. Rol van het persoonsinformatiebeleid binnen het hulpverleningsproces

In deze casus is gebleken dat er een grote spanning bestaat tussen de informationele privacy van een vrouw die verblijft in een blijf van mijn lijf huis en het belang van een goede hulpverlening. Het privacybelang (en daarmee het veiligheidsbelang) van de vrouw wordt centraal gesteld, hetgeen in de praktijk automatisch betekent dat gegevens niet uitgewisseld worden. Dit gebeurt vanuit een diepgewortelde angst voor het schenden van onder andere de lichamelijke privacy van de vrouw. Hoewel dit automatisme begrijpelijk is, kan het persoonsinformatiebeleid een belangrijke bijdrage leveren aan het bereiken van een nieuw optimum, waarbij de hulpverlening aan de vrouw

een hoger niveau kan bereiken. In de –mondelinge- overdacht van gegevens kan immers gemakkelijk informatie vergeten worden en blijven bepaalde verbanden onzichtbaar. Op het gebied van gezondheidszorg -lichamelijk of psychisch- aan de vrouw zouden derhalve grote sprongen gemaakt kunnen worden als meer gegevens uitgewisseld worden, mits uiteraard de informationele privacy afdoende geborgd blijft.
Daarnaast kan het goed vormgeven van het persoonsinformatiebeleid bijdragen aan het voorkomen van het niet-gebruik van overheidsvoorzieningen waar deze vrouwen wel degelijk recht op hebben.

Om dit te bereiken dient het toezicht op de naleving van de regels rondom het uitwisselen van persoonsgegevens verbeterd te worden. De partijen die gegevens afnemen uit de GBA zijn niet altijd voldoende op de hoogte van de mogelijke gevolgen van het bekend worden van de persoonsgegevens van vrouwen die een indicatie “geheim” hebben. Voorafgaand aan het beter vormgeven van het toezicht op de omgang met persoonsgegevens is het creëren van bewustzijn dus een vereiste. In de casus zagen we dat er geen natuurlijke scheidslijn ligt tussen publieke en private partijen waar het gaat om het uitwisselen van persoonsgegevens van bedreigde vrouwen. Als het gaat om het creëren van bewustwording in de betrokken sectoren via de vakverenigingen (bijvoorbeeld NVVB, maar ook het Collectief van Zorgverzekeraars), dan ligt daar een belangrijke rol weggelegd voor het persoonsinformatiebeleid, in haar streven naar een nieuw optimum voor bedreigde vrouwen.
Vanuit dit bewustzijn kan ook het gebruik van middelen en mechanismen ter beveiliging van persoonsgegevens gestimuleerd worden. Zo kan het overnemen van de indicatie “geheim” in systemen van afnemers een grote bijdrage leveren aan het beschermen van de informationele privacy van de vrouw. Daarnaast zou het technisch afschermen van de persoonsgegevens van bedreigde vrouwen voor onbevoegden hieraan kunnen bijdragen.

5.4. Algemene conclusies van de praktijkstudies

Wanneer we de casussen nader analyseren en vergelijken, valt een aantal zaken op[93]. Enkel in de casus van het toezicht op de AIVD zien we dat in de praktijk een bewuste belangenafweging wordt gemaakt. Met behulp van wettelijke en niet-wettelijke kaders, in het bijzonder de WIV2002 en de behoorlijkheidswijzer, worden concrete vraagstukken uit de praktijk geanalyseerd, waarbij de verhouding tussen informationele privacy en veiligheid centraal staat. Het toezicht is dusdanig georganiseerd dat de partijen zich bewust zijn van de spanningsvelden die bestaan tussen veiligheid en privacy en de partijen proberen hier met behulp van de aanwezige kaders een oplossing voor te vinden. In deze casus is geen behoefte aan een extra kader, of aan een persoonsinformatiebeleid als extra speler binnen het afwegingsproces. Waar wel behoefte aan is aan de evaluatie van de cumulatieve effecten van wet- en regelgeving en aan een bewuster communicatiebeleid, zodat het huidige vertrouwen van de burger in de overheid blijft bestaan of zelfs wordt vergroot.
In de andere twee casussen ontbreekt het duidelijk aan dergelijk toezicht en actieve controle op de naleving van wet- en regelgeving. Een mooi voorbeeld wordt gevormd door de papieren koppelingen in de casus van de bijstandsuitkering, die op papier een aantrekkelijk alternatief voor digitale koppelingen lijken, maar dat in de praktijk niet blijken te zijn. De dossiers blijken in officieel gesloten gangkasten te liggen, soms kwijt te kunnen raken en niet beveiligd vervoerd te worden van de ene locatie naar de andere. Een voorbeeld uit de derde casus zijn de protocollen omtrent de indicatie ‘geheim’ in de

GBA, die in de praktijk blijken niet te kunnen voorkomen dat de privacy van vrouwen die verblijven in blijf van mijn lijf huizen wordt geschonden, soms met dodelijke gevolgen. Het aan de voorkant regelen van privacy is dus duidelijk niet voldoende. Waar de WBP wel degelijk mogelijkheden biedt om de privacy te waarborgen, blijkt deze in de praktijk lastig te handhaven. Het draait uiteindelijk om de uitvoeringspraktijk. Om die te kunnen optimaliseren is actievere controle en toezicht nodig. Diezelfde uitvoeringspraktijk zou dus verantwoording af moeten leggen over de uitvoering van beleid, waarbij de conclusies van deze verantwoording –ongeacht in welke vorm die plaatsvindt- de basis kunnen vormen voor diepgravender onderzoek. Bovendien vraagt dit om evaluatie van wet- en regelgeving en hoe deze in de praktijk uitpakken.

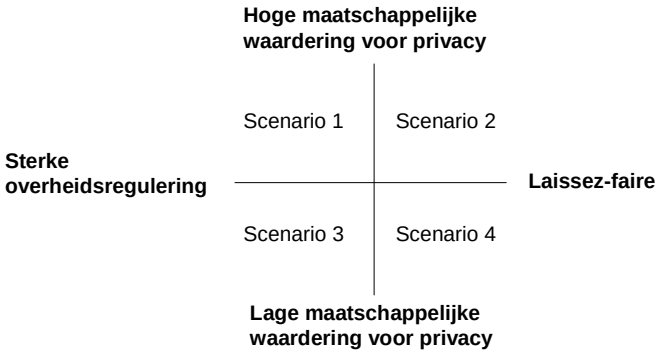
Daarnaast valt op dat onvoldoende wordt geredeneerd vanuit netwerken van organisaties. De problemen met de indicatie geheim zijn hiervan opnieuw een voorbeeld. Veel van de problemen met privacy ontstaan *tussen* organisaties, niet binnen organisaties. Het persoonsinformatiebeleid dient dan ook over informatieketens heen te kijken. Bovendien zien we dat burgers vaak nog hinder (kunnen) ondervinden van het feit dat gegevens niet uitgewisseld worden tussen ketenpartijen. Zoals blijkt uit de bijstandscasus is de bewijslast enorm en moeten verhalen bij verschillende instanties opnieuw verteld worden. Door het koppelen van bestanden kan de (pro-actieve) dienstverlening aan de burger vergroot worden, mits daarbij de juiste waarborgen in acht genomen worden. Een goede informatiehuishouding aan de achterkant maakt het tevens mogelijk de burger via meerdere kanalen met behoud van dezelfde kwaliteit van dienstverlening te bedienen.
Communicatie over de gevaren van gegevensuitwisseling voor de informationele privacy van de burger blijft essentieel. Zeker in de casus omtrent de blijf van mijn lijf huizen is dit evident. Een manier om de aandacht van de afnemers op de thematiek te vestigen is via de zogenaamde vakverenigingen. We zagen in de casussen dat het onderscheid tussen publieke en private partijen daarbij moeilijk te handhaven is.

Tot slot is privacy in alledrie de casussen nauwelijks vormgegeven als actierecht. De burger heeft zelden de mogelijkheid om over het uitwisselen van zijn eigen persoonsgegevens te beslissen. Zeker nu blijkt dat de papieren opslag en papieren uitwisseling van persoonsgegevens verre van een garantie voor geborgde privacy blijkt, is het van groot belang dat het persoonsinformatiebeleid met behulp van technologische middelen het recht van de burger op informationele privacy actiever vormgeeft.

Deel drie:
De toekomst van persoonsinformatiebeleid

6. Toekomstscenario's

Tot aan dit hoofdstuk is in dit rapport met name stilgestaan bij het heden en ontwikkelingen die zich momenteel voltrekken. Nu is het moment aangebroken om naar de toekomst te kijken. Als input voor het proces van het bepalen van beleidsprioriteiten en een bijpassend instrumentarium, worden in dit hoofdstuk vier toekomstscenario's beschreven. De scenario's vormen een (zo nu en dan extreme) schets van de Nederlandse samenleving in 2020 en de waarde die dan aan informationele privacy en de andere belangen wordt gehecht. Bij het opstellen van de scenario's zijn twee 'assen' onderscheiden. Door deze twee assen te kruisen ontstaan vier vlakken en dus vier mogelijke toekomstscenario's. Dit is in onderstaande figuur schematisch weergegeven.



Figuur 6.1: Scenario's

Met laissez-faire wordt verwezen naar een overheid die wet- en regelgeving tot een minimum beperkt. Dit is het tegenovergestelde van een situatie waarin sprake is van een sterke overheidsregulering. In geval van een hoge maatschappelijke waardering voor privacy zijn burgers geneigd veel aandacht te vragen voor privacy en inbreuken op de privacy, hetgeen in een scenario met een lage maatschappelijke waardering voor privacy zelden tot nooit zal voorkomen.

Aangenomen wordt dat het persoonsinformatiebeleid geen invloed op de assen kan uitoefenen: scenario's komen van buiten, strategieën komen van binnen: de assen bepalen de ruimte waarbinnen het persoonsinformatiebeleid robuuste strategieën dient te bepalen. Dit is tegelijkertijd het doel van de scenario's: door huidige ontwikkelingen door te vertalen naar de toekomst zijn zij een instrument voor strategiebepaling en vergroten zij het anticiperend vermogen van het persoonsinformatiebeleid. Dit door gedachtevorming over de rol van het persoonsinformatiebeleid in de verschillende scenario's te stimuleren. De scenario's liggen ten grondslag aan de uiteindelijke suggesties voor beleidsprioriteiten en –instrumenten.
De scenario's zijn beschrijvingen van een mogelijke toekomst, niet van een wenselijke. Daar waar waardeoordelen in de scenario's worden geuit, betreft het inschattingen van mogelijke burgeropvattingen in het jaar 2020.

Hieronder volgen de vier scenario's.

6.1. Scenario 1: Hoge privacywaardering & sterke regulering

Het is het jaar 2020. Burgers hebben groot geloof in de maakbaarheid van de samenleving. De overheid spaart mensen noch middelen om een hoge kwaliteit van dienstverlening en gezondheidszorg te realiseren. Ook doet de overheid er alles aan om een veilige samenleving te creëren.
Burgers doen er op hun beurt alles aan om de overheid aan te zetten tot acties die hun wensen inwilligen. Zij maken daarom veel gebruik van diverse vormen van inspraak: digitale debatten, referenda. De jonge generatie voert deze debatten op Third Life, een opvolger van Second Life, dat bij haar introductie in 2006 nog zo veel te weeg had gebracht. De wat oudere generaties, de laatste die niet met computers zijn opgegroeid, komen samen in door de overheid georganiseerde debatmiddagen en inspraakavonden. Als zij anoniem hun stem willen laten horen, dan kunnen zij daarvoor gebruik maken van 'inspraakformulieren' die per post kunnen worden verstuurd aan de afdeling 'inspraak' van hun gemeente.

Privacyonderzoek binnen de blijf van mijn lijf keten
Bernard, privacyonderzoeker bij de gemeente Den Haag, heeft vandaag zijn vaste 'veldwerkdag'. Op zo'n dag probeert hij een proces van a tot z door te lichten, om zo te kijken hoe in dat proces met persoonsinformatie wordt omgegaan. Vandaag is het hulpverleningsproces aan vrouwen in blijf van mijn lijf huizen aan de beurt. Dat is een complex proces en hij verwacht dat hij ook volgende week nog nodig heeft om de informatieketen te doorgronden. Wat het zo moeilijk maakt is dat hij hier te maken heeft met zowel private als publieke partijen. Al geruime tijd is geconstateerd dat het essentieel is dat de systemen van alle ketenpartners in staat moeten zijn om de indicatie 'geheime gegevens' over te nemen. Maar in de praktijk is dat lastig: ketenpartners, zeker bedrijven, wisselen voortdurend. Vandaar dat hij ieder jaar een controle uitvoert. Dat komt overigens mooi uit, want op de digitale debateringssite van de gemeente is zojuist weer eens deze problematiek aangesneden. Mensen hebben vraagtekens bij de betrouwbaarheid van een psychologenpraktijk en een zorgverzekeraar. Ze zijn gelukkig wel zo netjes geweest om geen namen te noemen.
Bernard kijkt op zijn pocket-pc. Half negen. De hoogste tijd om aan de slag te gaan.

Of burgers nu jong of oud zijn, zij vragen in debatten altijd uitgebreid aandacht voor privacy en de afwegingen die in die context moeten worden gemaakt. Met name op het terrein van de veiligheid is de schreeuw van de burger om openheid en meer tegenmacht steeds luider gaan klinken. Dat was aan het begin van de 21e eeuw wel anders geweest. Toen was er nog gesproken van Nederland als controlestaat. Het merendeel van de burgers had, mede vanwege toenemende terrorismedreiging, weinig weerstand geboden tegen uitbreidingen van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Maar een reeks incidenten heeft voor veel maatschappelijke onrust gezorgd. Zo was het binnen een half jaar meerdere malen voorgekomen dat een vliegtuig niet mocht landen in de Verenigde Staten omdat er 'verdachte' personen in het vliegtuig zaten. En asielzoekers met een bepaald 'risicoprofiel' bleken te worden gediscrimineerd bij het toekennen van een verblijfsvergunning. Het maatschappelijk debat werd aangewakkerd, burgers dienden meer en meer klachten in bij de daarvoor bestemde instanties en uiteindelijk werd besloten tot meer openheid van zaken. Dat is de rechtse fracties in de Tweede Kamer een doorn in het oog geweest, maar het is nu eenmaal geven en nemen in een tijd van grote politieke tegenstellingen.
Door voorlichtingscampagnes maakt de overheid aan burgers duidelijk op welke manier de inlichtingen- en veiligheidsdiensten op hoofdlijnen handelen en door welke

overwegingen zij zich laten leiden. Zo weten burgers om welke redenen de inlichtingendiensten kunnen besluiten tot telefoontaps of het onderscheppen van e-mailverkeer. Dat kan in individuele gevallen natuurlijk niet bekend worden gemaakt, maar doordat de algemene afwegingen rondom de werkwijze van bijvoorbeeld de AIVD en de EIVD (de Europese Inlichtingen- en Veiligheidsdienst) duidelijker worden, accepteert het merendeel van de burgers dat. Bovendien verstevigt de overheid de functie van het toezicht. Ook de uitwerking van wet- en regelgeving wordt in de praktijk geëvalueerd, zodat daar vervolgens sterker op kan worden gestuurd.

Als het gaat om de dienstverlening, dan stelt de overheid een uitgebreide infrastructuur aan de samenleving ter beschikking. De burger kan met al zijn vragen terecht bij talrijke klantcontactcentra, die zowel via internet, telefoon als fysiek te benaderen zijn. Er is weinig 'niet gebruik' van overheidsdiensten omdat de overheid haar dienstverlening pro-actief organiseerd, waarbij door handige organisatievormen en technische oplossingen de privacy minimaal wordt aangetast.

De moeiteloze bijstandsuitkering

Nadat haar man haar heeft verlaten, dreigt Karin Zondervan als alleenstaande moeder van twee kinderen in een benarde financiële situatie terecht te komen. Maar vanaf het moment dat de scheiding rond is, wordt er iedere maand een vast bedrag op haar rekening bijgeschreven. Het enige wat ze daarvoor hoeft te doen, is op een formulier aangeven dat zij het sociale zekerheidsinstituut toestemming geeft om de veranderingen in haar persoonlijke situatie door te geven aan de gemeente. Dat had ze natuurlijk ook via haar persoonlijke internetpagina kunnen doen, maar ze heeft aan de gemeente laten weten dit soort zaken liever via het ouderwetse papier af te handelen.

Die uitkering is niet het enige mechanisme dat automatisch in werking is getreden nadat de echtscheidingspapieren zijn ondertekend. Zij ontving direct een brief van de gemeente waarin haar werd medegedeeld dat de vereiste ouderschapsbijdrage voor schoolgaande kinderen automatisch wordt verlaagd en dat de kindertoeslag met maar liefst 50% wordt verhoogd. Zij maakte zich wel zorgen over hoe het toch kan dat de overheid wist van haar scheiding, haar inkomen en haar thuissituatie. Deze vraag had ze dan ook gesteld aan de "Stichting ter bevordering van de privacy," maar die stelden haar volledig gerust. Het sociale zekerheidsinstituut is de enige instantie die over alle persoonsinformatie die voor het bovenstaande nodig is beschikt. Ze hadden alleen de broodnodige informatie aan de gemeente doorgegeven, namelijk dat haar inkomen onder de bijstandsgrens ligt en in dat instituut is haar persoonsinformatie net zo veilig als het goud in Fort Knox; als medewerkers daar ook maar een keer persoonsinformatie raadplegen of uitwisselen zonder dat dat duidelijk nodig is voor hun werkzaamheden, worden ze op staande voet ontslagen.

"Wat hebben we het toch mooi voor elkaar in dit land," dacht Karin.

6.2. Scenario 2: Hoge privacywaardering & laissez-faire

We leven in het jaar 2020. In het afgelopen decennium heeft zich een trend tot privatisering voltrokken. De overheid laat onderwijs en gezondheidszorg grotendeels over aan het bedrijfsleven. Burgers organiseren zich in groten getale in belangenorganisaties, die strijden voor een transparante overheid die de burger regie geeft op het gebruik van persoonsgegevens. Via een gegevenskluisje en een persoonlijke internetpagina kan de burger zelf bepalen welke gegevens voor welke organisatie toegankelijk zijn. De overheid biedt de burger een infrastructuur aan, die hem in staat stelt zijn eigen afwegingen en keuzen te maken. Ook kan de burger in iedere sector terecht bij een particulier privacycollectief indien hij van mening is dat gegevens over hem onrechtmatig zijn verkregen of wanneer van deze gegevens misbruik is gemaakt. Onderzoek in 2019 heeft aangetoond dat burgers die ontevreden zijn ook snel geneigd zijn van deze mogelijkheid gebruik maken. Maar vaak is protest van burgers al genoeg om organisaties (hetzij publiek, hetzij privaat) uit angst voor imagoschade zo ver te krijgen dat zij persoonsgerelateerde informatie uit de publiciteit halen. Dat is een trend die eigenlijk in 2007 al ingezet is. De beheerders van Hyves hadden destijds een mechanisme ingebouwd waardoor je kon zien wie jouw site had bezocht. Woedend waren de gebruikers geweest, waardoor Hyves de statistieken binnen no time weer van de sites had afgehaald.

De gezondheidschip

Mathilde loopt het Alexia-ziekenhuis binnen. Ze meldt zich aan de balie met behulp van haar gezondheidspas. Hieraan kan de receptioniste aflezen met wie ze de afspraak heeft. “Het is allemaal wat uitgelopen bij dokter Huisman, zie ik. Het zal naar schatting nog ongeveer een uur duren. Als u wilt kunt u nog even een wandeling maken of wat winkelen”. Mathilde geeft aan dat ze zich dat uur wel vermaakt. Ze heeft haar laptop meegenomen en daar kan ze via het netwerk van het ziekenhuis mee op internet. Dat komt mooi uit, dan kan ze op de gezondheidswiki nog wat informatie over haar ziektebeeld opzoeken.

Als de dokter haar roept, heeft ze door alle informatie nog een aantal belangrijke vragen bedacht voor de arts. Dokter Huisman leest haar kaartje met zijn kaartlezer – dezelfde als die van de receptioniste, maar met andere toegangsrechten. Hiermee ontsluit hij niet alleen Mathilde’s NAW-gegevens, maar ook haar medische gegevens uit haar patiëntdossier. Op haar patiëntpagina heeft ze aangegeven dat dokter Huisman alle gegevens mag inzien, zodat hij een volledig beeld van haar medische status krijgt. Deze hele infrastructuur is door de overheid georganiseerd maar het ziekenhuis, dat geprivatiseerd is, mag hier natuurlijk ook gebruik van maken. Een belangengroepering heeft pas geprobeerd het ziekenhuissysteem te kraken, maar dat is gelukkig niet gelukt. Vorig jaar is dat nog wel anders geweest. Voorpaginanieuws op elke krant. Het ziekenhuis kon zich deze negatieve publiciteit niet veroorloven en nam daarom de nodige maatregelen. Een deel daarvan was technisch, maar het personeel heeft ook een opleidingsprogramma gevolgd zodat ze zich meer bewust worden van de werking van technologie en het belang van de bescherming van persoonsgegevens.

Mathilde neemt plaats op de stoel, tegenover het bureau van dokter Huisman.

“Zo, zegt dokter Huisman, eens even zien …..”

Beveiligde vrouwen
Fátima loopt terug naar huis na het doen van boodschappen bij de supermarkt op het Albert Plesmanplein in Zaandam. Nou ja, naar huis. Zo voelt het nog steeds niet. Sinds drie maanden woont ze in een blijf van mijn lijf huis. De situatie thuis is onhoudbaar geworden. Nadat haar man erachter is gekomen dat ze een relatie heeft met één van haar collega's is de gehele familie furieus. Haar man slaat haar aan de lopende band en ze heeft gegronde vermoedens dat zij het slachtoffer van eerwraak dreigt te worden. Om die reden heeft ze onderdak gezocht in een blijf van mijn lijf huis, speciaal bedoeld voor Islamitische vrouwen. Omdat de problematiek van deze groep vrouwen zo lastig is (een hele gemeenschap is naar hen op zoek) regelen ze daar extra zaken om haar veiligheid te garanderen. Daarom loopt Johan nu naast haar. Johan werkt bij een beveiligingsbedrijf en is één van de bewakers die je kunt vragen met je mee te gaan als je genoeg krijgt van het binnen zitten. Sinds drie jaar is er deze mogelijkheid, die wordt gefinancierd vanuit 50% overheidssubsidies en 50% donaties van burgers. Het vergroot het gevoel van veiligheid van de vrouwen enorm.

Inlichtingen- en veiligheidsdiensten, opsporingsambtenaren, politie en medewerkers van de sociale dienst werken nauw samen met private partijen. Zo laten gemeenten "fraudebestrijdingsbedrijven" huiszoekingen doen bij mensen met een bijstandsuitkering bij wie een sterk en gegrond vermoeden tot uitkeringsfraude is. Maar die private partijen houden zich amper bezig met de privacy van die burgers en dit heeft al tot een aantal schandalen geleid. Een medewerker van het bedrijf "afraudeskia" is uit de school geklapt en heeft zijn verhaal over een bezoek aan een man die met drie vrouwen blijkt samen te leven aan de media verkocht. De politiek is nu in nauwe samenspraak met burgers en de fraudebestrijdingbedrijven aan het zoeken naar een oplossing. Maar uiteindelijk komen ze hier altijd wel weer uit…

6.3. Scenario 3: Lage privacywaardering & sterke regulering

In het kader van 30 jaar Nationaal Vrijheidsonderzoek onderzoekt het Comité 4 en 5 mei in 2020 wat er in de afgelopen 30 jaar is veranderd. Hierbij stuiten de onderzoekers op een onderzoeksrapport uit 2007, met daarin de volgende tekst onder het kopje "maatregelen ter bevordering van de nationale veiligheid":

"Men schat de effectiviteit van de voorgelegde maatregelen in het algemeen positief in, maar de inbreuk op de privacy wordt groot gevonden. Opvallend echter is dat ondanks deze inbreuk op de privacy, geen van de maatregelen door een meerderheid onaanvaardbaar wordt gevonden. Dit impliceert een groot vertrouwen in de wijze waarop de overheid met persoonsgegevens omgaat. Dit blijkt ook uit de bevinding dat de groep die denkt dat de veiligheid toeneemt wanneer de overheid meer over burgers weet, veel groter is dan de groep die denkt dat de veiligheid dan afneemt (bijvoorbeeld door misbruik van informatie)."

De onderzoekers moeten glimlachen bij de zin "de inbreuk op de privacy wordt groot gevonden". Ze lezen het een aantal maal, totdat ze het snappen. In 2020 is privacy namelijk geen issue meer, laat staan dat het een onderzoeksvraag waard is. Er zijn nog een handvol personen die vragen om aandacht voor privacy, maar de meerderheid van de mensen verwacht simpelweg dat de overheid gewoon effectieve maatregelen ter bevordering van de veiligheid neemt. En daar is nu eenmaal informatie over personen voor nodig. De onderzoekers concluderen dat andere beleidsthema's het gewonnen hebben van de privacy.
Na de enorme debacles met geprivatiseerde overheidstaken als de NS, de energiebedrijven (massale stroomstoringen in 2010), de Belastingdienst en de gemeenten Dordrecht en Enschede is in 2020 de tucht van de overheid weer helemaal terug. Burgers merken dat zij in de zogenaamde 'markten' veel meer geld kwijt zijn aan

zorgverzekeringen en dergelijke. Door de ervaringen geven burgers aan dat zij het belangrijk vinden dat de overheid meer taken op zich neemt, maar deze tegelijkertijd ook efficiënt en kwalitatief goed uitvoert. Om dit laatste te realiseren is het noodzakelijk dat de overheid heldere regels neerzet en deze regels streng handhaaft.

De roep om een sterkere overheid heeft ook geleid tot een verdriedubbeling van de ledenaantallen van politieke partijen. De Socialistische Partij en de Groep Wilders zijn de grootste partijen geworden en regeren samen. Zij hebben als gemeenschappelijk thema dat de overheid meer regels moet stellen en deze veel duidelijker en strenger bewaakt.

Tegelijk met het "30 jaar Nationaal Vrijheidsonderzoek" vindt het slotsymposium plaats van het College ter Bescherming Persoonsgegevens (CBP). De Tweede Kamer heeft in ruime meerderheid besloten dat het CBP niet langer nodig is. Als er al burgers zijn die klagen over privacy, dan kunnen zij zich wenden tot het Nederlandse rechtssysteem. Als laatste stuiptrekking organiseert het CBP een slotsymposium om terug te kijken op 22 jaar bescherming persoonsgegevens. Een vijftal topsprekers is uitgenodigd om diverse thema's te belichten:

Veiligheid
De eerste spreker gaat in op de veiligheid. De strijd tegen terrorisme is heftiger geworden en de overheid treedt hier veel krachtiger tegen op door zo veel mogelijk informatie te verzamelen, te koppelen en te onderzoeken met behulp van data mining technieken. Onder het mom "alle informatie kan relevant zijn", wordt zo veel mogelijk informatie verzameld, zoals boodschappengegevens, reisgedrag (kentekenscanning, OV-chipkaart, loopgedrag door middel van camera's), onderwerpen van werkstukken van kinderen en ga zo maar door. De data mining- en opslagtechnieken zijn zodanig verbeterd dat de hoeveelheid informatie die hiervoor dient te worden opgeslagen geen probleem meer is.

Dienstverlening
De dienstverlening van de overheid is volgens de tweede spreker enorm verbeterd. Zoals de slogan van de Belastingdienst al aangeeft: "leuker kunnen we het wel maken, en dat zullen we doen ook!". Er is, waar mogelijk, sprake van geautomatiseerde dienstverlening 'voorbij het loket': burgers ontvangen diensten automatisch, omdat de overheid op basis van het koppelen van informatie weet dat zij er recht op hebben. Hierdoor is er ook nauwelijks 'niet-gebruik' van overheidsdiensten, waardoor met name de onderklasse er de laatste jaren sterk op vooruitgaat. Daar is met name de SP uiterst trots op. Door middel van 'profiling' en doelgroepbenaderingen wordt de overheid ook meer en meer een adviseur van en voor haar burgers. Zo kan de overheid

Automatisch aan het werk?
Karin Zondervan krijgt moeiteloos een uitkering, direct de dag nadat ze is gescheiden. Zonder dat ze iets hoeft te doen, wordt er geld op haar rekening gestort. Daarnaast worden haar gegevens en CV op de landelijke vacaturebank geplaatst. Karin zag dat er direct drie afspraken zijn ingepland. Deze afspraken met mogelijke nieuwe werkgevers, zijn geautomatiseerd aangemaakt op basis van haar profiel. De agenda van Karin is ook zichtbaar op de vacaturebank, zodat anderen daar afspraken in kunnen plannen en kunnen zien waar Karin allemaal solliciteert. De eerste drie banen vind Karin niets en ze gaat niet in op het aanbod wat ze daar krijgt, wat direct wordt vermeld op de vacaturesite. Dat is wel een risico wat ze daar neemt. Na het afzeggen van vijf banen zal ze automatisch gekort gaan worden op haar uitkering.

bijvoorbeeld, op basis van informatie uit werkstukken van leerlingen, aangeven wat de beste beroepskeuze voor hen is.

Handhaving
De derde spreker is de landelijke Handhavingsman. Hij spreekt vol trots over de resultaten die de nationale Handhavingsdienst heeft bereikt. Door het combineren van alle overheidstaken rondom handhaving (politie, milieu, bouw, economisch, sociaal etc.) wordt de handhaving fors goedkoper. Er worden letterlijk miljarden bespaard. Daarnaast wordt er dankzij het slim koppelen van informatie veel effectiever gewerkt, waardoor risico-sturing, profiling, op afstand handhaven en tracking-and-tracing (Live Google Earth) mogelijk zijn. Burgers ervaren hun leefomgeving als veel prettiger en geven dat ook aan in het Nationale Geluksonderzoek.

Ahmed Handhaver
Ahmed werkt voor de nationale Handhavingsdienst en is Handhaver voor drie wijken in Emmen. Zijn taak is om daar 'alles in de gaten te houden wat in de gaten gehouden moet worden.' Hij moet letten op criminele en illegale activiteiten op allerlei terreinen, zoals diefstal, inbraak, illegale bouw, illegale milieustortingen, overbewoning, huiselijk geweld, fraude, noem maar op.
's Ochtends na het ontbijt pakt hij zijn "Mobile Agent' die continu in verbinding staat met de hoofdcentrale van de nationale Handhavingsdienst. Daar worden, op basis van informatie uit allerlei bronnen, risicoplekken vastgesteld. Ahmed ziet op zijn 'Mobile Agent' een digitaal kaartje waarop risicoplekken staan vermeld en met kleur is aangegeven om welke risico's het gaat. Als hij klikt op een risicoplek dan krijgt hij alle gegevens van de betrokken bewoners (inclusief foto's, relaties met mogelijke overtreders en bijvoorbeeld lidmaatschappen of abonnementen). Daarnaast krijgt hij een voorstel voor een route, zodat hij de belangrijkste risicoplekken als eerste bezoekt.
Als Ahmed de deur uitloopt begint zijn dag. Dankzij tracking-and-tracing kunnen zijn bazen ook zien dat Ahmed begonnen is. Als Ahmed in gevaar is, dan pikt zijn "Mobile Agent" dit op door de veranderingen in zijn bewegingen en zijn stem. Automatisch worden dan zijn collega's die het dichtste bij zijn opgeroepen.

Beleidsvorming
De vierde spreker is aan de beurt. "Beleidsvorming heeft een totaal andere betekenis gekregen dan 20 jaar geleden," zo stelt hij. Beleidsvorming kent veel kortere lijnen, is zo laag mogelijk belegd en kent over het algemeen veel kortere doorlooptijden. Zo worden veel beleidskeuzes over een wijk gemaakt door de bewoners van die wijk via interactieve en digitale beleidsvorming. Ook kan de overheid, op basis van profielen, heel direct doelgroepen betrekken bij haar beleidsvorming. Dankzij de snelheid en betrouwbaarheid van de digitale technieken is het mogelijk om beleid en regels rechtstreeks te formuleren op basis van interactieve peilingen. Ook de vertaling van beleid naar uitvoering kan tegenwoordig veel sneller gemaakt worden, in een groot aantal gevallen zelfs al real-time.

ICT
De laatste spreker laat een toetsenbord zien. "Kennen jullie dit nog?," vraagt hij aan de aanwezigen. In 2020 zijn de toetsenborden verdwenen en werken mensen vrijwel alleen nog maar met geïntegreerde ('embedded') technologie. Hierbij wordt veelal gecommuniceerd door middel van stem- of draadloze technieken als RFID-3. Daarnaast zijn de analysetechnieken sterk verbeterd, waardoor het mogelijk is beleid en regelgeving automatisch te vertalen naar de relevante systemen.

De dagvoorzitter concludeert tenslotte dat burgers weinig waarde hechten aan hun privacy, omdat ze in een land wonen dat zij als veiliger, prettiger en leuker beleven dan 22 jaar geleden. Hij komt tot de conclusie dat het CBP nuttig werk heeft verricht in de afgelopen jaren, maar dat ze nu als apart controlerend orgaan overbodig is. Daarna nodigt hij iedereen uit voor de borrel.

6.4. Scenario 4: Lage privacywaardering & laissez-faire

We schrijven het jaar 2020. Privacy lijkt een woord uit het verleden: schoolkinderen weten niet meer hoe ze het moeten schrijven. Afhankelijk van de school waar kinderen heen gaan weten ze nog net wat het begrip inhoudt; vanuit de laissez faire gedachte van de overheid wordt het bepalen van de lesstof immers overgelaten aan de schoolbedrijven (learning factories). Heb je veel Linden dollars op je bankrekening, dan kun je naar een school met een hoge kwaliteitsrating.

De tijd dat de overheid nog burgerpanels opricht vanuit een bezorgdheid over de steeds groter wordende kloof tussen overheid en burger, lijkt een eeuwigheid geleden. In 2007 is er nog een onderzoek verschenen naar het persoonsinformatiebeleid van de overheid. Het idee was toen dat de overheid mogelijk een rol zou moeten spelen in het waarborgen van de privacy van burgers. De enorme kloof tussen overheid en burger in 2020 maakt dat burgers hierom lachen. De overheid interesseert ze niet en burgerbewegingen komen op voor de belangen van burgers op terreinen als veiligheid en gezondheidszorg. Zij eisen een maximale uitwisseling van gegevens tussen overheid en private partijen om de belangen waarvoor zij strijden zo goed mogelijk te behartigen.

De overheid besteedt veel van wat vroeger nog tot haar takenpakket gerekend werd uit aan private partijen. Zij wordt gekenmerkt door haar reactieve opstelling. Het niet-gebruik van de weinige overheidsvoorzieningen die er zijn is hoog. Bevolkingsgroepen die wel een helpende hand kunnen gebruiken vinden deze bijvoorbeeld bij de private voedselbanken.

Onverwacht bezoek
Karin Zondervan zit op de bank als de bel gaat. Voor zover ze weet heeft ze geen afspraak, dus ze vraagt zich af wie er voor de deur staat. Even twijfelt ze om open te doen. Wat nu als het een deurwaarder is? Sinds ze haar baan verloren is, vreest ze het moment dat de deurwaarder op de stoep staat om haar meubels in beslag te nemen. Ze logt in op Google Earth Live en zoomt in op haar voordeur. Daar staat iemand met een groot pakket in zijn handen. Nieuwsgierig doet ze haar deur open. Voor de deur staat een voor haar onbekende man. Onzeker vraagt Karin hem wat hij komt doen. De man vertelt haar dat zijn naam Klaas Michielsen is en dat hij haar een voedselpakket komt brengen vanuit K-Mart. Ietwat achterdochtig vraagt Karin hem om zijn identiteit. De man geeft haar zijn identiteitspasje en Karin checkt met behulp van haar PDA zijn persoonsnummer in de GBA-online. Nu ze weet dat de man is wie hij zegt te zijn, ebt haar onzekerheid weg. Karin opent de deur verder en laat de man binnen. Fijn toch, dat K-Mart had kunnen zien dat ze geen melk meer in haar koelkast heeft en dat nu aan komt vullen. Zelf was ze niet meer in staat geweest melk te kopen omdat haar inkomsten opgedroogd zijn. Karin knoopt een gesprek aan met de man in de hoop dat hij haar wellicht een baan kan bezorgen bij K-Mart. Met weemoed denkt ze ondertussen terug aan de verhalen van haar moeder over de tijd dat er nog een bijstandsuitkering was als je je baan verloor….

In de samenleving van 2020 is het concept web 3.0 volledig verankerd; het verschil tussen online identiteit en fysieke identiteit is hiermee welhaast verdwenen. Op Life (vroeger bekend als second life) is een fors aantal actiegroepen actief. Deze actiegroepen zetten zich in voor de bestrijding van malaria in Nederland, vergroting van

de binnenlandse veiligheid door het bestrijden van terrorisme en voor verbetering van de kwaliteit van onderwijs. Het succes van de actiegroepen is niet te stuiten; alleen al de afgelopen maand heeft de actiegroep tegen bestrijding van malaria, 'Malaria Uitgebannen' (m.u.g.) 3.000.000.000 Linden Dollars opgehaald om onderzoek te doen naar deze opkomende ziekte. De grote onderzoeksbedrijven kunnen het werk bijna niet aan. De online beschikbare database met medische dossiers kent een ongekend aantal hits en de slimste queries worden geschreven om de rode draad in de ontwikkeling van de ziekte boven tafel te krijgen.

Een zonnebril in de winter
Fatima belt aan bij haar vriendin Femke. Ze wipt van het ene been op het andere in de hoop dat Femke de deur snel opendoet. Fatima slaakt een zucht van verlichting als de deur opengaat. Verbaasd kijkt Femke haar aan. Hartje winter staat Fatima duidelijk nerveus voor haar deur met een zonnebril op. Snel laat ze haar binnen. Met horten en stoten komt het verhaal van Fatima eruit. Ze heeft een buitenechtelijke relatie met een collega en is daarom door haar man geslagen. In een onbewaakt ogenblik is ze aan zijn aandacht ontsnapt en naar het huis van Femke gegaan. Ze wist niet waar anders heen te gaan. De politie is een optie, maar wat voor hulp zouden die haar verder kunnen bieden? Na het doen van aangifte moet ze immers ook ergens heen. Bovendien is Fatima bang gevonden te worden op basis van de gegevens die ze aan de politie verstrekt. Samen zoeken Fatima en Femke op Life naar de actiegroep voor vrouwen die het slachtoffer zijn van eergerelateerd geweld. Ze maken een afspraak met een vertegenwoordiger van de actiegroep, die die avond nog langs kan komen. Huilend vallen ze elkaar in de armen, wetend dat ze elkaar waarschijnlijk een lange tijd niet zullen gaan zien, nu Fatima naar een veiligere plaats buiten Nederland gebracht zal worden…

De talrijke actiegroepen eisen van de overheid dat ze haar gegevens deelt om sprongen te kunnen maken op het gebied van voornamelijk veiligheid en gezondheidszorg. Deze eisen worden vrij gemakkelijk ingewilligd; slechts een klein groepje van privacyridders ligt even dwars. Het collectief van actiegroepen maakt de gegevens van deze privacy-ridders echter openbaar en geven daarnaast een negatieve rating aan hun web 3.0 identiteit. Door deze negatieve rating wordt het voor de privacyridders wel erg moeilijk nieuwe vrienden te maken en de vrijgezelle ridders ondervinden hierdoor dubbele hinder, aangezien ook het daten een stuk moeilijker wordt. Maar gelukkig kunnen zij de hulp inroepen van een privacyombudsman, die zal kijken of de 'openbaarheidsridders' wel het recht hadden de persoonsgegevens op het web te plaatsen.

Dit is niet het enige dat de privacyridders steekt aan het handelen van de overheid. Het is heel goed dat de overheid zich beperkt tot het optreden in gevallen van maatschappelijke commotie, maar het is wel vaak die meerderheid die haar zin krijgt. Als het aan de privacyridders lag, had K-Mart echt geen toegang gekregen tot hun persoonsgegevens uit de basisregistratie GBA. Met een overheid die haar infrastructuur ter beschikking stelt aan private partijen is een dergelijke beweging echter niet tegen te houden.

7. Conclusies: beleidsprioriteiten en een bijpassend instrumentarium

In dit onderzoek heeft de wenselijkheid van herijking van het persoonsinformatiebeleid centraal gestaan. Indien dit inderdaad wenselijk is, zouden beleidsprioriteiten en een bijpassend instrumentarium worden benoemd. Om dit doel te bereiken is het onderzoek gestart met een theoretische gedeelte. Tijdens dit theoretische gedeelte is het begrip privacy afgebakend, zijn mogelijke spanningsvelden tussen privacy en andere belangen onderscheiden en zijn relevante ontwikkelingen benoemd. Vervolgens zijn tijdens het empirisch gedeelte van het onderzoek met behulp van praktijkstudies privacy-problematieken in het veld geanalyseerd. Vervolgens zijn theorie en praktijk samengekomen in hoofdstuk 6, waarin toekomstscenario's zijn geschreven. Deze scenario's vormen de basis voor dit hoofdstuk. Wat vragen de scenario's nu voor strategieën van het persoonsinformatiebeleid? Waar zouden de prioriteiten van het persoonsinformatiebeleid de komende jaren moeten liggen? En welk instrumentarium is nodig om deze prioriteiten vorm te geven? In de hoofdstuk wordt op deze vragen een antwoord geformuleerd.

7.1. Beleidsprioriteiten

Op basis van de conclusies uit het theoretisch en empirisch gedeelte, wordt hieronder voor de periode tot 2020 een viertal prioriteiten voor het persoonsinformatiebeleid voorgesteld. Hierbij is het goed het bereik van het persoonsinformatiebeleid in het achterhoofd te houden. Alhoewel het onderscheid tussen persoonsinformatie en informatie niet volgens een objectieve standaard te bepalen is, blijkt het onderscheid in de praktijk werkbaar en nuttig. Onderstaande beleidsprioriteiten hebben dan ook betrekking op beleid ten aanzien van het *gebruik* van gegevens die gekoppeld zijn aan personen. Voorts kan gesteld worden dat door de trend naar globalisering het gebruik van deze persoonsgegevens zich niet enkel binnen de landsgrenzen voltrekt. Onderstaande prioriteiten hebben betrekking op het gebruik van persoonsgegevens van inwoners van Nederland. De eventuele samenwerking met andere overheden op dit gebied is een belangrijk aandachtspunt, maar valt buiten dit onderzoek. Nadat het persoonsinformatiebeleid binnen Nederland haar koers heeft bepaald, kan zij een internationale beleidsagenda ontwikkelen[94].

7.1.1. Beleidsprioriteit 1: netwerkgericht werken stimuleren

De talrijke ontwikkelingen die tijdens dit onderzoek zijn onderscheiden, tonen aan dat het persoonsinformatiebeleid dient mee te bewegen met veranderingen in maatschappij, wet- en regelgeving, bestuur, organisaties, technologie en internationale verhoudingen. Momenteel zien we een samenleving waarin publieke en private partijen zich vanwege de toenemende complexiteit, interdependentie en individualisering genoodzaakt zien (samen) te werken in netwerken van organisaties. Dit betekent dat het persoonsinformatiebeleid zich niet kan beperken tot afzonderlijke organisaties. Persoonsgegevens stromen binnen en tussen publieke én private organisaties. Dit betekent dat het persoonsinformatiebeleid betrekking heeft op het vergaren, opslaan en uitwisselen van persoonsgegevens binnen *en* tussen publieke *en* private partijen. Daarbij dient nog wel goed te worden nagedacht over wanneer, welke persoonsinformatie met

welke private partijen wordt gedeeld. Het persoonsinformatiebeleid kan door de correcte omgang met persoonsinformatie binnen netwerken van organisaties te stimuleren, een bijdrage leveren aan een vraaggerichte, effectieve en efficiënte overheid.

7.1.2. Beleidsprioriteit 2: het optimaliseren van de relatie burger-overheid

In dit onderzoek is meerdere malen geconstateerd dat het vertrouwen van burgers (en bedrijfsleven) in de overheid en haar omgang met persoonsgegevens essentieel is. Vertrouwen in de omgang met persoonsgegevens is een voorwaarde voor het slagen van ICT-innovaties en is vanuit economisch oogpunt interessant. Een belangrijke prioriteit van het persoonsinformatiebeleid is daarmee het optimaliseren van het vertrouwen in de relatie tussen overheid en burger, bijvoorbeeld door transparantie van processen. De instrumenten die later in de hoofdstuk worden beschreven bieden handvatten voor de concrete invulling van deze beleidsprioriteit.

Het persoonsinformatiebeleid dient te worden verankerd in een opvatting over de wijze waarop de relatie tussen overheid en burger op het gebied van informatieverwerking dient te zijn. Gegeven de ontwikkeling naar netwerkgericht werken en daarmee de toenemende publiek-private samenwerking, is het essentieel dat het persoonsinformatiebeleid niet alleen toeziet op het gebruik van persoonsinformatie door overheidsinstanties, maar ook door private partijen. Direct of indirect raakt alle gebruik van persoonsinformatie de relatie burger-overheid.

7.1.3. Beleidsprioriteit 3: een evenwichtige belangenverhouding realiseren

Het vergaren, opslaan en uitwisselen van persoongegevens is nooit een doel op zich. Daarmee is ook persoonsinformatiebeleid geen doel op zich. Persoonsinformatiebeleid is altijd aanpalend aan ander beleid en streeft naar een evenwichtige verhouding tussen privacybelangen en de belangen van terreinen zoals dienstverlening, veiligheid, gezondheidszorg, fraudebestrijding en administratieve lastenverlichting.. Bij privacybelangen kan hierbij gedacht worden aan waarden als zelfstandigheid, bewegingsvrijheid, gelijkheid, vrij blijven van stigmatisering, ongestoord leven, eigenwaarde, vrij blijven van manipulatie, integriteit en autonomie.

Het persoonsinformatiebeleid heeft als prioriteit het proces van belangenafwegingen te faciliteren om zo tot een evenwichtige belangenverhouding te komen.

7.1.4. Beleidsprioriteit 4: privacy als afweerrecht en actierecht vormgeven

Het persoonsinformatiebeleid ziet erop toe dat privacy zowel als afweerrecht wordt vormgegeven als actierecht. Allereerst stimuleert en controleert het persoonsinformatiebeleid de totstandkoming en uitvoering van wet- en regelgeving die de burger een minimale vorm van bescherming geeft tegen het incorrect gebruik van zijn persoonsgegevens. Daar waar mogelijk geeft zij de burger tevens zijn recht op informationele privacy: het recht om zelf te bepalen wanneer, door wie en hoe informatie over hem wordt gebruikt.

Wanneer binnen het persoonsinformatiebeleid privacy als actierecht wordt vormgegeven, is het nuttig om een onderscheid te maken tussen informationele privacy en andere vormen van privacy (lichamelijke, ruimtelijke en relationele). Op deze manier kan bij belangenafwegingen worden gekeken hoe de verschillende vormen van privacy zich tot elkaar verhouden. De vormen kunnen in sommige gevallen als het ware tegen elkaar worden geruild. Een aanvrager van een bijstandsuitkering zou in de huidige uitvoeringspraktijk bijvoorbeeld de keuze kunnen worden geboden: of een huisbezoek

waarbij zijn persoonsgegevens worden gecontroleerd (inbreuk op ruimtelijke privacy), of een uitvoerig onderzoek naar zijn financiële gedrag (inbreuk op informationele privacy).

7.2. Een passend instrumentarium

Hieronder volgt een overzicht van een aantal instrumenten, op basis waarvan binnen het persoonsinformatiebeleid de beleidsprioriteiten kunnen worden ingevuld. Deze instrumenten kunnen gezien worden als robuuste strategieën: zij kunnen worden ingezet ongeacht de maatschappelijke waardering van privacy en de mate van overheidsregulering. De precieze invulling en implementatie van de instrumenten kan wel wisselen al naar gelang de mate van waardering voor privacy en overheidsregulering toe- of afnemen. Indien dit het geval is, zal hiervoor bij de uitwerking van de instrumenten aandacht zijn.
Leden van de begeleidingscommissie hebben zich gebogen over het belang, de haalbaarheid, praktische invulling en verantwoordelijkheid voor de hieronder beschreven instrumenten. De resultaten hiervan bevinden zich in bijlage 10.

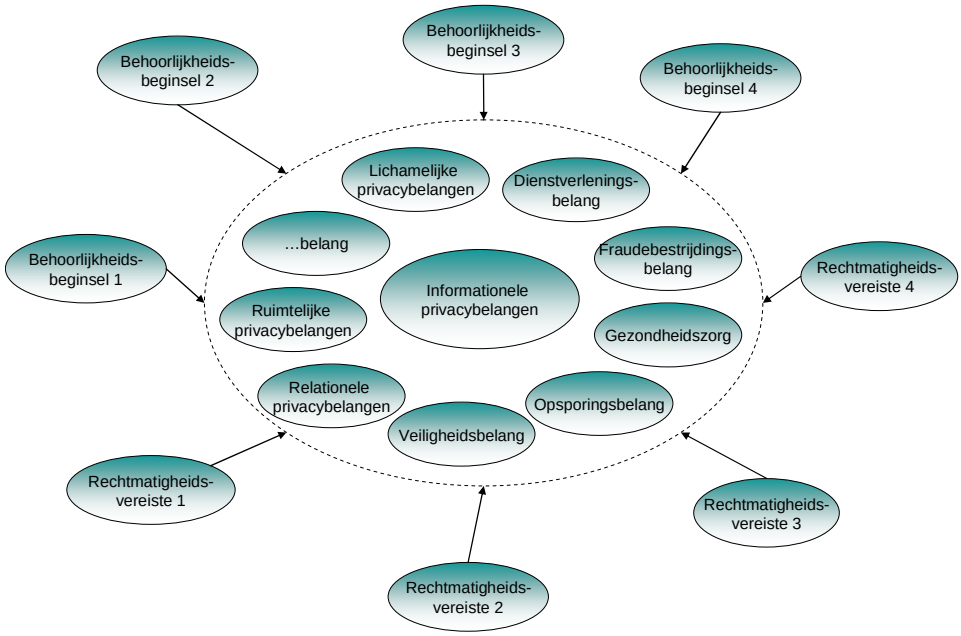
7.2.1. Instrument 1: procesbegeleiding

Om een evenwicht tussen privacybelangen en de belangen van andere beleidsterreinen te bewerkstelligen, vraagt ieder terrein om een eigen afwegingsproces, met eigen waarden, belangen en vereisten. Dezelfde burger hecht nu eenmaal een andere waarde aan zijn privacy wanneer hij in het ziekenhuis ligt, dan wanneer hij zich bij de balie van het gemeentehuis meldt voor een paspoort. Het persoonsinformatiebeleid begeleidt dit proces, waarbij zij bewaakt dat belangen en vereisten over het hoofd worden gezien en er aandacht is voor de cumulatieve effecten van wet- en regelgeving. Daarnaast zorgt zij dat afwegingen communiceerbaar en transparant zijn.
De afwegingen per terrein zijn gebaseerd op een onderscheid tussen beleidsdoel, beleidsmiddel en beleidseffecten. De keuze voor een bepaald middel (bijvoorbeeld cameratoezicht) wordt gemaakt door een afweging van de effecten op de privacy en een ander beleidsthema (bijvoorbeeld de veiligheid).

Bepalen van de relevante belangen en vereisten
Per beleidsterrein worden andere belangen en vereisten meegenomen in de afweging. Het bepalen van deze belangen en vereisten vormt geen onderdeel van deze studie. Wel kan op hoofdlijnen worden aangegeven wat in het afwegingsproces wordt meegenomen:

- de relevante belangen en hun spanningsvelden;
- rechtmatigheidsvereisten;
- behoorlijkheidsvereisten.

Dit betekent dat binnen ieder terrein rechtmatigheidsvereisten worden bepaald en behoorlijkheidsbeginselen worden geselecteerd. Voorbeelden van rechtmatigsheidsvereisten zijn de beginselen van proportionaliteit en subsidiariteit. Voorbeelden van behoorlijkheidsbeginselen zijn materiële behoorlijkheid (bijvoorbeeld gelijkheid en redelijkheid), formele behoorlijkheid (bijvoorbeeld hoor en wederhoor en motivering) en zorgvuldigheid (te denken valt aan administratieve nauwkeurigheid en correcte bejegening). Deze kunnen per terrein bovendien anders worden gedefinieerd. In de zesde bijlage bevinden zich de behoorlijkheidsvereisten van de Nationale Ombudsman. Schematisch weergegeven ziet dit er als volgt uit:



Figuur 7.1: Ingrediënten van het afwegingsproces

Op basis van de geselecteerde belangen, beginselen en vereisten kunnen criteria en vragen worden bepaald, met behulp waarvan afwegingen worden gemaakt. Ook een toets van de uitvoerbaarheid van beleid kan deel uitmaken van het afwegingsproces.

Inzet van procesbegeleiding

Wanneer er sprake van sterke overheidsregulering is, werkt het persoonsinformatiebeleid samen met beleidsdepartementen aan het vormgeven en uitvoeren van het afwegingsproces. In geval van een laissez-faire beleid, stelt de overheid haar procesbegeleiding ter beschikking aan diverse organisaties, waaronder lokale overheden en private partijen.

Daarnaast kan de procesbegeleiding proactief en reactief worden ingezet. In geval van een lage waardering van privacy, kan enkel van de begeleiding gebruik worden gemaakt wanneer er maatschappelijke onrust ontstaat, of wanneer burgers zich beklagen over het gebruik van hun persoonsgegevens. Wanneer er sprake is van een hoge privacywaardering, kan de procesbegeleiding proactief worden ingezet bij de totstandkoming van beleid: bij het opstellen van, en besluiten over, wetsvoorstellen.

7.2.2. Instrument 2: het stimuleren van optimale transparantie

Een belangrijk tweede instrument voor het persoonsinformatiebeleid is dat zij optimaal transparant is naar burgers, politiek en publieke en private organisaties over (gemaakte afwegingen omtrent) het gebruik van persoonsgegevens.

Hierbij kunnen twee gebieden van optimale transparantie worden onderscheiden:

- Transparantie over het vergaren, opslaan en uitwisselen van de persoonsgegevens van individuele burgers
- Transparantie van processen en de afwegingen die hierbinnen worden gemaakt

Beide vormen van transparantie zijn met name belangrijk voor het optimaliseren van de relatie overheid-burger en daarmee voor het borgen van het vertrouwen in de overheid. Wanneer de wijze waarop gegevens worden verwerkt transparant is, krijgt de burger meer mogelijkheden om zijn actieve privacyrecht in te zetten.
Hierbij is het van belang dat gestreefd wordt naar *optimale* transparantie. Transparantie betekent namelijk niet dat koste wat het kost alle mogelijke informatie naar de buitenwereld wordt gecommuniceerd. Het gaat erom afhankelijk van de doelgroep, díe informatie te selecteren en dusdanig te communiceren dat deze aansluit bij de belevingswereld en belangen van de ontvanger. Dit bepalen van communicatievorm en inhoud is onder andere afhankelijk van de waardering voor privacy en de mate van overheidsregulering.

Transparantie over gebruik persoonsgegevens van individuele burgers
Ongeacht de waardering voor privacy is het belangrijk privacy zoveel mogelijk als actierecht vorm te geven. Idealiter krijgt de burger de kans om voordat zijn persoonsgegevens worden gebruikt zijn eigen afwegingen te maken. Denk aan scenario 1, waarin een onlangs gescheiden vrouw aan een speciaal orgaan toestemming geeft tot uitwisseling van haar persoonsgegevens. Maar ook transparantie achteraf heeft een belangrijke functie. Hierbij valt te denken aan scenario 2, waarin een patiënte op haar persoonlijke patiëntpagina kan regelen dat een arts haar patiëntgegevens kan inzien. Wanneer burgers bovendien achteraf horen welke afwegingen ten grondslag lagen aan het gebruik van hun persoonsgegevens dient dit het vertrouwen en creëert het mogelijkheden voor debat en eventuele klachtenprocedures.

Transparantie van processen
Wij zien een zevental onderwerpen van transparante communicatie over processen en de afwegingen die hierbinnen worden gemaakt:
- Omtrent wetsvoorstellen;
- Omtrent politieke besluitvorming;
- Omtrent evaluatie van wet- en regelgeving (zie ook instrument 3);
- Omtrent technologische innovaties;
- Omtrent klachtenprocedures;
- Omtrent berichtgeving in de media;
- Omtrent burgeropvattingen (zie ook instrument 5).

Het persoonsinformatiebeleid zal in vele gevallen niet de partij zijn die de communicatie zelf verzorgt; zij stimuleert transparantie bij verschillende actoren. Bij een regulerende overheid zullen het vaak de overheden zelf zijn die transparant communiceren over processen en afwegingen. Maar ongeacht het niveau van regulering zullen ook altijd private partijen gebaat zijn bij hulp met de communicatie over afwegingen naar burgers.
In een privacywaarderende maatschappij is het bovendien belangrijk dat dit *proactief* gebeurt, omdat de kans op maatschappelijke onrust omtrent gevaren voor de privacy groot is. Het is dan zaak vooraf het debat te sturen door afwegingen helder te maken, in plaats van achteraf het debat te repareren door afwegingen te verdedigen. Ook zal er binnen een terrein met een hoge waardering voor privacy behoefte zijn aan een grotere hoeveelheid informatie over processen en afwegingen, dan binnen terreinen waar weinig waardering voor privacy bestaat. Binnen die terreinen zal een meer beperkte en reactieve vorm van communicatie volstaan.

Technologie is voor veel mensen een ‘black box’ die veel onzekerheid veroorzaakt. Op deze manier vormen (ICT) innovaties een gevaar voor de relatie tussen overheid en

burger. Transparante communicatie over de voor-, nadelen en afwegingen omtrent ICT-toepassingen verdient daarom bijzondere aandacht, zodat duidelijkheid wordt verschaft over de betekenis en werking van technologie.
Transparantie omtrent klachtenprocedures kan worden vormgegeven door allereerst een meldpunt misbruik en oneigenlijk gebruik van persoonsinformatie, gekoppeld aan een meldpunt identiteitsfraude, op te richten. Vervolgens kunnen de afwegingen die zijn gemaakt omtrent het gebruik van persoonsinformatie worden geanalyseerd en geëvalueerd. De resultaten hiervan kunnen vervolgens worden gecommuniceerd naar de burger. Wij zien voor het persoonsinformatiebeleid in elk van de scenario's een belangrijke taak weggelegd als het gaat om het evalueren van wet- en regelgeving. Hierover communiceert het persoonsinformatiebeleid in alle scenario's zelf. Daarom werken we dit instrument hieronder nader uit.

7.2.3. Instrument 3: evaluatieonderzoeken en privacy-effectrapportages

Het is niet alleen belangrijk dat bij de totstandkoming van beleid bewust wordt nagedacht en gecommuniceerd over de diverse afwegingen, maar dat tevens de daadwerkelijke effecten van beleid in kaart worden gebracht. Wij onderscheiden hierbij drie vormen van evaluatieonderzoek:

- Evaluatie van de effecten van afzonderlijke wetten op de privacy;
- Evaluatie van de beoogde effecten van afzonderlijke wetten;
- Evaluatie van de cumulatieve effecten van wet- en regelgeving op de privacy.

De eerste twee vormen dienen gelijktijdig plaats te vinden. Op deze manier kunnen afwegingen worden gemaakt over de verhouding tussen privacy en het beleidsthema waaraan een wet een bijdrage wilde leveren. In deze context is het interessant dat uit het nationaal vrijheidsonderzoek 2007 bleek dat 75% van de Nederlanders vindt dat nieuwe veiligheidsmaatregelen die een inbreuk maken op de privacy automatisch na een jaar moeten komen te vervallen als niet kan worden aangetoond dat zij de veiligheid ten goede komen. Om dit te kunnen realiseren, is echter wel inzicht in de uiteindelijke effecten van maatregelen nodig. De bevinding van het vrijheidsonderzoek is opvallend, omdat uit hetzelfde onderzoek blijkt dat de waardering voor privacy binnen het terrein erg laag uitvalt. Dat betekent dat (het stimuleren van) de evaluatie van beoogde effecten een belangrijk instrument van het persoonsinformatiebeleid kan zijn, ongeacht de maatschappelijke waardering voor privacy.

Het collectieve veiligheidsterrein is bovendien een voorbeeld van een terrein waarbinnen zich de afgelopen jaren veel wijzigingen in wet- en regelgeving hebben voltrokken (zie hoofdstuk 4 en 5). Inzicht in het cumulatief effect van al deze wijzingen op de privacy ontbreekt echter. Ook hier is een belangrijke taak voor het persoonsinformatiebeleid weggelegd. Om inzichtelijk te maken hoe het met de privacy in ons land gesteld is, kan het persoonsinformatiebeleid, eventueel opnieuw per terrein, privacy-effectrapportages (PERs) opstellen. Hierin kan jaarlijks worden gerapporteerd over veranderingen in de omgang met persoonsgegevens en in de privacybeleving van burgers en bedrijfsleven. Een interessante invalshoek hierbij is om het cumulatief effect van wet- en regelgeving te onderzoeken vanuit het perspectief van de burger, de professional en het bedrijfsleven. Daar komen immers wet- en regelgevingen samen.

7.2.4. Instrument 4: actieve controle en toezicht organiseren

De voor de afweging geselecteerde vereisten kunnen worden gebruikt als handvat bij actieve controle en toezicht op de uitvoering van beleid. Op deze manier worden de

uitvoering en effecten van wet- en regelgeving getoetst aan deze vereisten (criteria of beginselen).
In het geval van een sterke overheidsregulering stelt het persoonsinformatiebeleid deze controle- en toezichtsorganen zelf in. Afhankelijk van de maatschappelijke waardering, worden deze organen pro-actief of reactief ingezet. Bij een hoge waardering valt te denken aan privacyonderzoekers en privacy-handhavers, die zoals in de scenario's geschetst, pro-actief op zoek gaan naar privacyproblematieken en die op deze manier aan de kaart kunnen stellen. In geval van een lage maatschappelijke waardering van privacy kan een privacyvangnet worden gecreëerd, waarbij er voor mensen die van mening zijn dat een disproportionele en/of onwettelijke inbreuk op hun privacy heeft plaatsgevonden bijvoorbeeld aanspraak kunnen maken op een privaatrechtelijke regeling. Uiteraard kunnen dergelijke constructies worden gedifferentieerd per terrein, omdat de waardering van privacy per terrein kan verschillen.

7.2.5. Instrument 5: inzicht in relevante ontwikkelingen

Om de strategie van controle en toezicht te kunnen differentiëren op basis van de maatschappelijke waardering voor privacy, is inzicht in burgeropvattingen noodzakelijk. Een vijfde belangrijk instrument is daarmee onderzoek naar de maatschappelijke (trends in de) waardering voor privacy en andere beleidsthema's. Hiertoe kan het persoonsinformatiebeleid periodieke enquêtes per beleidsterrein houden.
Daarnaast dient het persoonsinformatiebeleid op de hoogte te zijn van bestuurlijke, organisationele en internationale ontwikkelingen. Hiertoe is geen periodiek onderzoek, maar een voortdurende monitorfunctie nodig. Tot slot is het van belang dat het persoonsinformatiebeleid kennis heeft van de kansen en uitdagingen van ICT, zodat zij hier een visie op kan ontwikkelingen.
De resultaten van elk van deze onderzoeken kunnen worden verwerkt in de privacy-effectrapportages.

7.2.6. Instrument 6: communicatiegerichtheid

De evaluatieonderzoeken, uitslagen van enquêtes naar burgeropvattingen en privacy-effectrapportages kunnen vervolgens worden gebruikt in de communicatie naar burgers. Het stimuleren van maatschappelijk en politiek debat, hetzij tussen burgers, hetzij tussen politiek en burgers, is één van de denkbare communicatiestrategieën. Interactieve besluitvorming en digitale debatten op overheidssites dragen immers bij aan een betere relatie tussen burger en overheid. Met name in geval van sterke overheidsregulering en wanneer er sprake is van laissez-faire politiek waarbij veel besluitvorming overgelaten wordt aan het veld, stellen debatten burgers en bedrijven zelf beter in staat om bewust afwegingen te maken omtrent het gebruik van persoonsgegevens. Daarnaast is voorlichting en scholing over de kansen en valkuilen van ICT-innovaties voor de omgang met persoonsinformatie een manier om invulling te geven aan een communicatiegericht persoonsinformatiebeleid.

7.2.7. Instrument 7: het benutten van de kansen van ICT

In het onderzoek is gebleken dat de papieren koppeling van gegevens net zo goed bedreigingen voor de informationele privacy met zich meebrengt als digitale koppelingen van persoonsgegevens. In het geval van digitale koppelingen biedt ICT echter verschillende kansen om privacy als actierecht vorm te geven. Te denken valt aan een persoonlijke internet pagina, ontkoppeld koppelen, gegevenskluisjes, sterk gedifferentieerde autorisatiestructuren, verregaande logging van gegevensraadpleging en hoogwaardige, homogene beveiligingsinfrastructuren. Om de kansen van ICT voor het realiseren van een evenwichtige belangenverhouding te benutten, is het belangrijk

dat het persoonsinformatiebeleid kennis heeft van technologische ontwikkelingen en het gebruik van ICT stimuleert. Voorts is het uiteraard ook van belang dat zij de gevaren van ICT kent. Vanuit deze gedachten kan zij een commissie instellen, die technologische ontwikkelingen in de gaten houdt en voorstellen doet voor het implementeren van privacymaatregelen en voor het benutten van de kansen van ICT voor de informationele privacy. Ook kan binnen het informatiebeleid onderzoek naar best practices op dit gebied worden verzameld en uitgewisseld, die vervolgens weer de basis vormen voor verschillende vormen van onderwijs over privacy en het gebruik van ICT en persoonsinformatie. De elfde bijlage verschaft inzicht in hoe de Noorse overheid het benutten van ICT op deze manieren stimuleert en tegelijkertijd een aantal maatregelen neemt om de privacy te waarborgen.

In geval van een laissez-faire scenario, kan het persoonsinformatiebeleid private partijen adviseren over het gebruik van ICT bij de verwerking van persoonsgegevens of kan de overheid zelf een infrastructuur ontwikkelen die zij vervolgens ter beschikking stelt aan private partijen. In het geval van sterke overheidsregulering, is het met name de overheid zelf die van de, door ICT mogelijk gemaakte, infrastructuur gebruik maakt. In dit geval kan ook onderzocht worden hoe minimale waarborgen van de informationele privacy bij technologische innovaties wettelijk gereguleerd kan worden. Indien bovendien sprake is van een hoge maatschappelijke waardering van privacy is het denkbaar dat ICT-leveranciers of -beheerders moeten kunnen aantonen dat nieuwe ICT-toepassingen voldoen aan een aantal nader op te stellen privacyrichtlijnen.

7.3. Laatste woorden

Deze beleidsverkenning laat zien dat persoonsinformatiebeleid de afgelopen jaren alleen maar aan belang gewonnen heeft en dat de komende jaren zal blijven doen. Tegelijkertijd laat het zien dat de precieze invulling van het persoonsinformatiebeleid afhankelijk is van de zich ontwikkelende scenario's. Herijking van het persoonsinformatiebeleid is op zijn plaats. In plaats van een reactieve, op dataprotectie gebaseerde benadering, kan gekozen worden voor een proactieve, op informationele privacy gebaseerde benadering. Ontwikkelingen in de samenleving, in bestuur en organisatie en in technologie bieden daarbij kansen, maar ook nieuwe uitdagingen.
Belangrijk is het bewerkstelligen van een transparant en volledig afwegingsproces, waarbij privacy als een dynamisch en situationeel bepaald belang wordt gewaardeerd ten opzichte van andere belangen.

Per beleidsterrein dient er actiever dan nu toezicht gehouden te worden op naleving van de gekozen privacyniveaus. Burgers kunnen actievere rechten krijgen en er kunnen technologische verbeteringen doorgevoerd worden. Door dit laatste kunnen de verontrustende tekortkomingen in de huidige praktijk van uitvoeringsorganisaties die met papier werken worden weggewerkt. De scenario's laten zien dat privacy niet in iedere context even belangrijk gevonden zal worden. Desalniettemin kunnen robuuste strategieën ontwikkeld worden: maatregelen, niet per se door de overheid uit te voeren, die ervoor zorgen dat er binnen de dan geldende maatschappelijke situatie maximaal tegemoet gekomen wordt aan het belang van privacy.

Tot slot. We hebben een aantal beleidsprioriteiten en een aantal instrumenten gesuggereerd. Het is niet aan de onderzoekers om daarin een keuze te maken. Wel kunnen zij de hoop uitspreken dat het persoonsinformatiebeleid aan inhoud en positie

wint en dat dat mede gebeurt door gebruik te maken van de in dit onderzoek naar boven gehaalde inzichten.

Bijlage 1: Samenstelling begeleidingscommissie

Namens het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties:
- Jan Moelker (afdelingshoofd Informatie Infrastructuur (II), DIIOS)
- Lotte Nijland (beleidsmedewerker DIIOS/II)
- Jan Timmermans (coördinerend beleidsmedewerker DIIOS/II).

Namens het projectteam van Zenc:
- Arre Zuurmond
- Bettine Pluut
- Femke Polman

Privacy- en e-overheidsdeskundigen:
- Kees de Bakker (privacy verantwoordelijke, gemeente Amsterdam)
- Michel Bouten (programmamanager Architectuur Elektronische Overheid en Startpakket GBA, plaatsvervangend directeur ICTU)
- Gerrit Jan van 't Eind (programmamanager Kenniscentrum E-overheid, ICTU)
- Corien Prins (Hoogleraar Recht en Informatisering bij TILT, Universiteit van Tilburg)
- Eric Schreuders (privacy expert).

Bijlage 2: OESO-beginselen

Puntsgewijs weergegeven zijn de OESO-beginselen (ook wel de Fair Information Principles (FIP):

-1- Het Collection Limitation Principle
Dit beginsel geeft aan dat er beperkingen moeten gelden ten aanzien van het verzamelen van persoonlijke gegevens en dat dergelijke gegevens op een eerlijke en rechtmatige wijze zijn verkregen, en indien van toepassing, met het in kennis stellen en de toestemming van de betrokkene.

- 2- Het Data Quality Principle
Dit beginsel bepaalt dat persoonlijke gegevens relevant moeten zijn voor het doel waarvoor ze bedoeld zijn te worden gebruikt, en dat de gegevens, voor zover nodig in relatie tot dat doel, juist, volledig en up-to-date zijn.

- 3 - Het Purpose Specification Principle
Het doel waarvoor gegevens worden verzameld moet worden aangegeven op, of voorafgaande aan het moment van, het verzamelen van de gegevens. Het gebruik van de gegevens is beperkt tot het gebruik voor deze doeleinden of daarmee in overeenstemming zijnde doeleinden.

- 4 - Het Use Limitation Principle
Persoonlijke gegevens mogen niet verstrekt worden, of op een andere wijze ter beschikking worden gesteld, voor andere dan de gespecificeerde doeleinden, behalve met toestemming van de betrokkene of op basis van een wettelijk voorschrift.

-5 - Het Security Safeguards Principle
Persoonlijke gegevens moeten worden beschermd op basis van redelijke beveiligingsnormen tegen verlies, ongeautoriseerde toegang, vernietiging, gebruik, verandering of verstrekking van deze gegevens.

- 6 - Het Openness Principle
Er dient openheid te worden gegeven over ontwikkelingen, praktijken en beleid in relatie tot persoonlijke gegevens. Er moeten voorzieningen worden getroffen zodat het bestaan en de aard van persoonlijke gegevens kunnen worden medegedeeld, evenals de belangrijkste doelstellingen voor het gebruik van deze gegevens, en de identiteit en het adres van de verantwoordelijke.

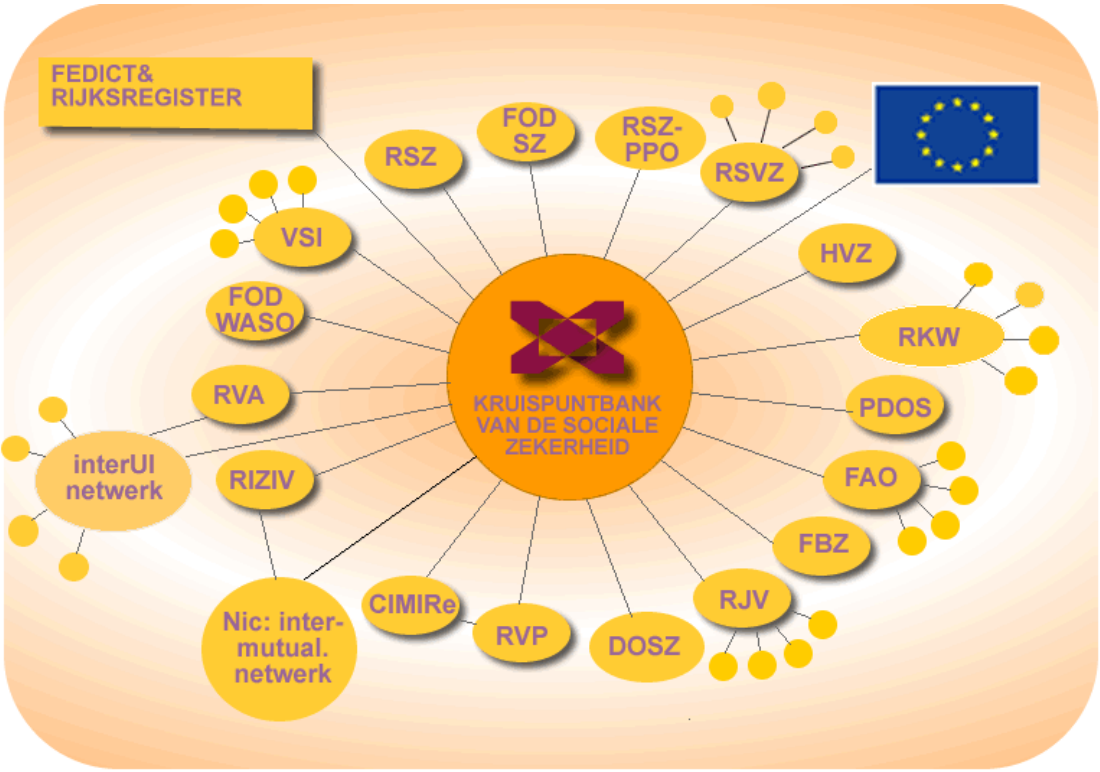
- 7- Het Individual Participation Principle
Een persoon moet het recht hebben om van een verantwoordelijke te weten te komen of gegevens over hem of haar worden verwerkt. Indien dit het geval is moet deze persoon het recht hebben, om binnen een redelijke tijd, tegen redelijke kosten, op een redelijke wijze en op een begrijpelijke wijze hierover ingelicht te worden. Indien dit wordt geweigerd, moet de persoon de reden worden gegeven waarom dit is geweigerd, en moet deze de mogelijkheid hebben hiertegen in beroep te komen. Aansluitend moet iemand de mogelijkheid hebben om bezwaar te maken tegen gegevens die over hem of haar worden verwerkt, en als dit bezwaar terecht is, om de gegevens te laten vernietigen, te verbeteren of aan te vullen.

- 8 - Het Accountability Principle

De verantwoordelijke is verantwoordelijk om zich te houden aan maatregelen voor het uitvoeren van deze beginselen.

Bijlage 3: Informationele privacy en de Kruispuntbank Sociale Zekerheid

Algemene informatie over de Kruispuntbank Sociale Zekerheid
De Kruispuntbank Sociale Zekerheid in België is in 1990 opgericht als antwoord op tekortschietende uitvoering in de sociale zekerheid. Zij heeft als centraal doel het administratief werk van alle organisaties in de Belgische Sociale Zekerheid te vereenvoudigen, terwijl tegelijkertijd de dienstverlening aan de burger moet worden verbeterd. Dit doet zij middels het opbouwen van een netwerk voor elektronische gegevensuitwisseling tussen de instellingen in de sociale zekerheid. Elke aangesloten instelling blijft verantwoordelijk voor het opslaan en bijhouden van 'eigen' gegevens. Daarnaast heeft elke instelling de verplichting informatie ter beschikking te stellen aan andere instellingen. De Kruispuntbank is geen centraal databestand, maar een netwerk-infrastructuur waaraan verschillende partijen verbonden zijn die werkzaam zijn in het Sociale Zekerheidsdomein (zie onderstaand figuur). In het centrum zit een knooppunt (het 'kruispunt'), dat al het gegevensverkeer regelt wat betrekking heeft op de Sociale Zekerheid.



De Kruispuntbank legt zelf geen gegevens vast, maar ontvangt een gegevensvraag van één van de aangesloten partijen, zoekt uit waar in het netwerk (delen van) het antwoord te vinden is (zijn), om deze gegevens vervolgens op te halen en door te sluizen naar de vrager.

Invoering is voorafgegaan aan experimenteren en wettelijke regulering. Er is daarbij sprake van een kaderwet en een wettelijk vastgelegde eenmalige gegevensuitvraag. Het is een vrij centralistisch opgezet bestel, waarbij de kruispuntbank een onbetwiste positie heeft. De kruispuntbank past binnen de bestuurlijke verhoudingen van het Belgische bestel. Het gaat om een interorganisationeel netwerk, dat ertoe geleid heeft dat de werkprocessen van de betrokken organisaties fors heringericht zijn. Daarmee zijn zowel de kwaliteit van de dienstverlening, de efficiency als de effectiviteit van het sociale zekerheidsbeleid gestegen.
De gegevens blijven eigendom van de organisatie die ze opslaat, maar zij is verplicht ze kosteloos ter beschikking te stellen aan alle partijen die gerechtigd zijn de informatie op te vragen. Aansprakelijkheid is in zoverre geregeld dat er zelfs gevangenisstraffen staan op het niet nastreven van optimale gegevenskwaliteit.

Omgang met privacyvraagstukken
Privacyvraagstukken ten aanzien van de Kruispuntbank zijn fundamenteel, maar pragmatisch opgelost. De decentrale opzet van het systeem herbergt impliciet een bescherming van privacy, doordat informatie rondom een sociaal verzekerde niet structureel bij elkaar wordt gebracht (‘één centraal bestand’). Hierdoor wordt eventueel misbruik vermeden. Naast de centrale opzet zijn er andere maatregelen genomen om het privacy-belang te waarborgen. We noemen hier de drie belangrijkste oplossingen: toezicht, ontkoppeld koppelen en logging.
Allereerst is een onafhankelijk Toezichtscomité ingesteld. Dit comité ziet toe op de zware veiligheidseisen die gelden in het netwerk. Het comité kijkt bovendien of het informatiesysteem van een organisatie aan de gestelde kwaliteitseisen voldoet om persoonsgegevens te mogen ontvangen. Tot slot moet elke gegevenslevering voorafgegaan worden door een expliciete machtiging van het comité.
In de tweede plaats maakt men in een aantal gevallen gebruik van het principe van ontkoppeld koppelen. Bij ‘ontkoppeld koppelen’ wordt alleen die informatie die van belang is voor het beantwoorden van een bepaalde vraag uitgewisseld: de interpretatie van de vraag wordt aan de Kruispuntbank als intermediair opgedragen. Zij raadpleegt de bronnen en geeft de vrager een simpel ja of nee terug, zonder de achterliggende informatie te tonen. Ter illustratie: als iemand recht heeft op kwijtscheldingen kun je aan de aanvrager natuurlijk alle gegevens verstrekken zodat hij zelf kan bepalen of er een recht bestaat. Maar je kunt ook vragen onder welke condities dat recht ontstaat, om dan als Kruispuntbank zelf de gegevens te raadplegen, deze te interpreteren en vervolgens alleen de uitkomst van de interpretatie te verstrekken.
In de derde plaats worden alle informatieverzoeken gelogd, en blijkt iemand niet gerechtigd een bepaalde vraag te stellen, dan kan daarop een ambtelijke berisping volgen. Met behulp van de logging-gegevens kan met terugwerkende kracht bepaald worden of een inbreuk op privacy heeft plaatsgevonden.
In geval van oorlog bestaat de mogelijkheid om de Kruispuntbank ‘met een druk op de knop’ op te heffen.

Bijlage 4: Geïnterviewde personen praktijkstudies

Casus "toezicht op de AIVD"
- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten: mevrouw Mr. I.P. Michiels van Kessenich-Hoogendam (voorzitter)
- De Nationale Ombudsman: de heer Mr. F.J.W.M. van Dooren (substituut ombudsman) en de heer W. van Hoogstraten.
- Overige geïnterviewden worden in verband met privacyoverwegingen niet vermeld.

Casus "aanvraag van een bijstandsuitkering"
- Teamleider Gemeentelijke Sociale Dienst;
- Senior adviseur Centrum voor Werk en Inkomen.

Casus "problematiek slachtoffers huiselijk geweld in blijf van mijn lijf huizen"
- Aanwezigen bijeenkomst 'eergerelateerd geweld'[95]

Aanvullende interviews met:
- Maartje Boots, beleidsmedewerker Programmabureau eergerelateerd geweld
- Johan Gorstworst, Beleidsmedewerker Federatie Opvang
- Mariëtte van Dorst, Directeur vrouwenopvang, Vrouwen opvang Hera Gelderland

Overkoepelende toetsing van de bevindingen
- Cees Meesters, Voorzitter Nederlandse Vereniging Voor Burgerzaken en Directeur Publiekszaken gemeente Rotterdam

Bijlage 5: Actoren die toezicht houden op de AIVD

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
De AIVD heeft interne richtlijnen opgesteld die fungeren als kaders voor de afwegingen die de AIVD maakt.

De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD)
De CTIVD toetst zowel het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) als de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) aan de juridische kaders van de Wet op de Inlichtingen- en Veiligheidsdiensten. De CTIVD is de instantie in Nederland die expliciet is belast met het toezicht op het handelen van de AIVD met de specifieke focus op rechtmatigheid. Tevens fungeert de CTIVD als klachtadviescommissie met betrekking tot klachten over de AIVD.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties
De Minister van BZK is eindverantwoordelijk voor de AIVD, legt verantwoording af aan de Tweede Kamer en stuurt de Dienst aan.

De Tweede Kamercommissie voor de Inlichtingen en Veiligheidsdiensten
De Commissie voor de Inlichtingen- en Veiligheidsdiensten bestaat uit de fractievoorzitters uit de Tweede Kamer, met uitzondering van de fractievoorzitter van de SP. Deze commissie bespreekt zaken die AIVD aangaan en kan namens de Tweede Kamer achter gesloten deuren de Minister ter verantwoording roepen. Daarnaast is er de Tweede Kamercommissie voor Binnenlandse Zaken en Koninkrijksrelaties die in bepaalde gevallen zaken bespreekt die op de AIVD betrekking hebben.

De Nationale Ombudsman
De Nationale Ombudsman heeft als kerntaak om te stimuleren dat de relatie tussen overheid en burger behoorlijk is. Burgers kunnen met een klacht over het optreden van de overheid bij hem terecht. In dit kader onderzoekt hij (gevraagd en ongevraagd) ook zaken die de AIVD betreft.

De Algemene Rekenkamer
De Algemene Rekenkamer voert zowel rechtmatigheids- als doelmatigheidsonderzoeken uit. Hierbij wordt onderzocht of beleidsdoelstellingen worden gerealiseerd door overheidsorganisaties en of publieke middelen volgens wet- en regelgeving wordt besteed.

Het rechterlijk toezicht
De rechterlijke macht toetst rechtmatigheid op basis van wet- en regelgeving in individuele gevallen. Dit toezicht is passief in de zin dat de rechterlijke macht niet zelf actief toetst, maar dit pas doet in concrete rechtszaken.

Buro Jansen&Janssen
Buro Jansen & Janssen is een onderzoeksburo dat politie- en inlichtingendiensten kritisch volgt en daar gevraagd of ongevraagd een mening over geeft.

Experts (Rathenau-instituut, UvT-TILT, Verwey-Jonker Instituut)
Onderzoeksinstituten die onderzoek verrichten naar het vraagstuk rondom veiligheid en privacy en de wijze waarop dit plaatsvindt.

Het College Bescherming Persoonsgegevens (CBP)
Het CBP heeft als kerntaak het bewaken van het belang van privacy. In de Wet Bescherming Persoonsgegevens (WBP) staat echter expliciet aangegeven (artikel 2.2b) dat de WBP niet van toepassing is op gebruik van persoonsgegevens ten behoeve van de inlichtingen- en veiligheidsdiensten. Wel voert het CBP onderzoeken uit naar de wetgeving rondom veiligheid en informationele privacy. In deze zin heeft het CBP een actieve rol in maatschappelijk toezicht.

Bijlage 6: Behoorlijkheidsvereisten van de Nationale Ombudsman

Grondrechten

1. Discriminatieverbod
2. Brief- en telefoongeheim
3. Huisrecht
4. Privacy – Recht op eerbiediging van de persoonlijke levenssfeer
5. Verbod op onrechtmatige vrijheidsontneming
6. Andere grond- en mensenrechten

Materiële behoorlijkheid

7. Verbod van misbruik van bevoegdheid
8. Redelijkheid
9. Evenredigheid
10. Coulance
11. Rechtszekerheid
12. Gelijkheid

Formele behoorlijkheid

13. Onpartijdigheid/onvooringenomenheid
14. Hoor en wederhoor
15. Motivering
16. Fair Play

Zorgvuldigheid

17. Voortvarendheid
18. Administratieve nauwkeurigheid
19. Actieve en adequate informatieverstrekking
20. Actieve en adequate informatieverwerving
21. Adequate organisatorische voorzieningen
22. Correcte bejegening
23. Professionaliteit

Bijlage 7: Aanvullende informatie klantproces

Cliëntrouting
In de onderzochte praktijk wordt gewerkt met een A, B en C cliëntenrouting, welke uitgaat van 3 cliëntenstromen:

- A: dit zijn cliënten die binnen afzienbare tijd (binnen 3 maanden) aan een baan geholpen kunnen worden;
- B: dit zijn cliënten die niet binnen 3 maanden aan een baan geholpen kunnen worden;
- C: dit zijn cliënten met bijvoorbeeld psychische problemen of (drugs)verslaafd zijn en waar het heel lang duurt voordat ze aan een baan geholpen worden.

Deze opdeling wordt gebruikt om onder andere de dienstverlening van het CWI, het UWV en de Gemeentelijke Sociale Dienst te combineren en aan de hand hiervan de dienstverlening van de ketenpartners te optimaliseren en de cliënt nog sneller aan het werk te krijgen.

Bedrijfsverzamelgebouwen (BVG)
In de onderzochte praktijk blijken naast tenminste 3 publieke partijen (Gemeentelijke Sociale Dienst, het UWV en het CWI) nog andere bedrijven zich in het gebouw te bevinden, zoals re-integratiebedrijven en uitzendbureaus. Dit om een optimale dienstverlening aan de cliënt te kunnen bieden (gemeenschappelijke cliëntenbenadering). Dit kan ook wel gezien worden als een One Stop Shop voor de cliënt die een uitkering komt aanvragen of werk zoeken.

Bijlage 8: Aan te leveren bewijsstukken voor bijstandsuitkering

Bij het opvragen van bewijsstukken wordt de volgende onderverdeling gehanteerd:

- Bewijsstukken met betrekking tot **Burgerlijke staat**, bijvoorbeeld uitschrijving bevolkingsregister (ex-)partner;
- Bewijsstukken met betrekking tot **de woonsituatie**, bijvoorbeeld een samenlevingscontract;
- Bewijsstukken met betrekking tot **huisvesting,** bijvoorbeeld een Huurcontract;
- Bewijsstukken met betrekking tot **het inkomen**, bijvoorbeeld ontslagvergunning CWI;
- Bewijsstukken met betrekking tot **zelfstandig ondernemerschap**, bijvoorbeeld uitschrijving Kamer van Koophandel;
- Bewijsstukken met betrekking tot **vermogen**, bijvoorbeeld afschrift van spaar- en betaalrekeningen;
- Bewijsstukken met betrekking tot **schulden**, bijvoorbeeld brieven;
- Bewijsstukken met betrekking tot **scholing**;
- Bewijsstukken met betrekking tot een **zorgverzekering**, bijvoorbeeld zorgverzekeraarpasje of de zorgverzekeringspolis.

Bijlage 9: Gegevensuitwisseling omtrent de aanvraag van een uitkering

In artikel 64 van de Wet Werk en Bijstand is opgenomen dat het toegestaan is om gegevens uit te wisselen met bijvoorbeeld de volgende instanties:

- ◊ Het CWI (Centraal bureau voor Werk en Inkomen);
- ◊ Het UWV (Uitvoeringsinstituut Werknemersverzekeringen);
- ◊ De SVB (Sociale Verzekeringsbank).
- ◊ De Belastingdienst;
- ◊ Het College Zorgverzekeringen in het kader van de zorgverzekeringswet of de Algemene wet Bijzondere Ziektekosten;
- ◊ De bedrijfspensioenfondsen en ondernemingspensioenfondsen;
- ◊ De Kamer van Koophandel;
- ◊ Korpschef en de bevelhebber van de Koninklijke Marechaussee in de zin van de Vreemdelingenwet 2000;
- ◊ De IBG (Informatie Beheer Groep);
- ◊ Instanties en personen die woonruimte verhuren;
- ◊ Instanties die in het kader van de openbare nutsvoorziening energie en water leveren.

Bijlage 10: Resultaten tweede bijeenkomst begeleidingscommissie

Tijdens de tweede bijeenkomst van de begeleidingscommissie op 30 mei 2007 is de commissieleden gevraagd een vragenformulier in te vullen. De vragen hadden betrekken op de in de onderzoeksrapportage beschreven instrumenten voor het persoonsinformatiebeleid. Hieronder volgen de vragen en de door de leden van de begeleidingscommissie geformuleerde antwoorden.

Vraag 1
Welke twee instrumenten zijn het meest belangrijk?

Antwoorden op vraag 1
Elk van de zeven instrumenten wordt minstens door één lid van de begeleidingscommissie als het meest belangrijk aangewezen. Optimale transparantie wordt duidelijk door de meeste leden (vier) als het belangrijkst gezien. Daarnaast worden controle en toezicht en het instrument 'evaluatieonderzoeken en privacy-effectrapportages' door drie leden als belangrijkste instrument aangemerkt.

De motivatie die voor optimale transparantie wordt gegeven is dat er bij burgers en bedrijven in de regel te weinig kennis is van informatieverwerking om een afgewogen oordeel te kunnen vormen en daarmee weloverwogen toestemming voor het gebruik van informatie te kunnen. Er is te weinig kennis om überhaupt een mening te kunnen vormen over het gebruik van persoonsgegevens.
Als motivatie voor het grote belang van privacy-effectrapportages wordt allereerst gesteld dat beleidsmakers momenteel te weinig kennis hebben van de gevolgen van wet- en regelgeving. Daarnaast hebben deze effectrapportages in potentie een belangrijke invloed op de bewustwording ten aanzien van het belang van correcte omgang met persoonsgegevens. Dat laatste is tevens een belangrijke reden voor het toepassen van het instrument procesbegeleiding. Middels deze begeleiding kunnen hoofdrolspelers op het terrein van persoonsinformatie worden gewezen op het belang van weloverwogen belangenafwegingen en een correcte omgang met persoonsgegevens.

Vraag 2
Welke twee instrumenten zijn het meest haalbaar?

Antwoorden op vraag 2
Ook hier wordt ieder instrument door minstens één lid genoemd. En ook hier wordt optimale transparantie door de meeste leden als het meest haalbare instrument gezien.

Vraag 3
Hoe zou u de belangrijkste instrumenten concretiseren? Welke ideeën heeft u bij de in- en uitvoering van de instrumenten?

Antwoorden op vraag 3

<u>Algemene ideeën bij de in- en uitvoering van de instrumenten:</u>

- Politiseren, bijvoorbeeld door directe betrokkenheid van de Tweede Kamer te organiseren (denk aan een beleidsprogramma en voortgangsrapportages).
- Beleggen bij een Ministerie/expertcentrum
- Overleg moet een hoofdrol spelen, bijvoorbeeld met instanties als de Koninklijke Nederlandse Maatschappij tot Bevordering van de Geneeskunst
- Casusgericht werken (met voorbeelden en pilots) en incident based werken (men dient zich te richten op zaken die een issue zijn). Na vijf of tien jaar op deze manier te hebben gewerkt, kan worden bezien of er algemene lijnen zijn te ontdekken en of evaluatie aantoont dat de instrumenten positieve effecten sorteren.

Concretisering van de functie van controle en toezicht:
- Controle en toezicht zo dicht mogelijk bij de burger en/of de bron van de persoonsgegevens organiseren.
- Het gaat niet enkel om privacytoezicht. Minstens zo belangrijk is het toezicht op het gebruik van informatie.
- De Persoonlijke Internet Pagina als een mogelijke invulling van een controle- en toezichtsfunctie. Dit door via de PIP mogelijkheden tot het melden van onjuistheden in gegevens te organiseren.
- Burgers en bedrijven in staat stellen niet begrepen gebruik van persoonsgegevens te kunnen melden.

Concretisering van procesbegeleiding:
Het perspectief van de burger hanteren omdat de burger een integraal perspectief biedt: bij de burger komen wet- en regelgeving samen.

Concretisering van optimale transparantie:
- Het realiseren van een Persoonlijke Internet Pagina
- Persoonsgegevens die worden verzameld en gebruikt ter accordering voorleggen aan de persoon die het betreft (bijvoorbeeld de burger), in ieder geval ter kennisgeving
- Uniforme modellen opstellen ten aanzien van wat, hoe en wanneer dient te worden gecommuniceerd naar burgers en bedrijven
- Zorgen dat algemene informatie, bijvoorbeeld wet- en regelgeving, gegroepeerd wordt naar individuele behoeften. Ter illustratie: ik ben een tuinder; welke regels zijn op mij van toepassing?
- Inzicht in specifieke informatie met voldoende waarborgen (EPD, EMD, ELD, EKD, etc.)

Concretisering evaluatieonderzoeken en effectrapportages:
- Effectrapportages hoeven niet zozeer periodiek te worden gepubliceerd, maar kunnen ook worden gekoppeld aan specifieke wet- en regelgevingen. Dit betekent dat het idee van effectrapportages zou kunnen worden geïntegreerd in het wetgevingstraject. In wetgeving wordt dan een effectrapportage verplicht gesteld.
- Organisaties moeten zelf (intern) Privacy Effect Rapportages opleveren, hetgeen gevalideerd kan worden door een externe partij, bijvoorbeeld het College Bescherming Persoonsgegevens.

Vraag 4

Welke instrumenten passen binnen het persoonsinformatiebeleid en/of welke zijn meer “des CBP’s”?

Antwoorden op vraag 4
Onderstaande tabel geeft weer hoeveel personen een instrument als de taak van ofwel het persoonsinformatiebeleid ofwel het College Bescherming Persoonsgegevens zien. Het kan hierbij gebeuren dat een persoon vindt dat de uitvoering van een instrument voor beide partijen is weggelegd.

	PIB	CBP	Beiden
1. Procesbegeleiding	6	1	
2. Optimale transparantie	5	2	
3. Evaluatieonderzoeken en effectrapportages	2	3	2
4. Controle en toezicht	2	4	1
5. Relevante ontwikkelingen	5		2
6. Communicatiegerichtheid	5		2
7. Stimuleren van benutten ICT	6		1

Zoals uit de tabel blijkt zijn de leden van de commissie het grotendeels eens over de verantwoordelijkheid voor de instrumenten 1,2 en 5 t/m 7: zij zien hier een belangrijke rol voor het persoonsinformatiebeleid weggelegd. De leden die aangeven dat optimale transparantie een taak is voor het CBP merken daarbij op dat het persoonsinformatiebeleid daaromtrent het beleid en de kaders moet ontwikkelen.
Over het uitvoeren van evaluatieonderzoeken, het publiceren van effectrapportages en het vormgeven van controle en toezicht zijn de meningen iets minder eensluidend. Dit wordt deels ingegeven door (de meningen over) de huidige taakverdelingen tussen BZK en het CBP.

Bijlage 11: Privacy en ICT in Noorwegen

In december 2006 verscheen in Noorwegen “Eit informasjonssanfunn for alle,” waarvan ook een Engelse versie beschikbaar is, getiteld “An Information Society For All”. In het rapport wijdt de Noorse overheid een hoofdstuk aan privacy, waarin zij ingaat op de maatregelen die op dit gebied zullen worden genomen, gegeven de ontwikkelingen op digitaal gebied. Alvorens de belangrijkste maatregelen te vermelden, is het handig eerst wat meer inzicht te verschaffen in de Noorse privacywetgeving en uitvoering.

De inrichting van de Noorse privacywetgeving en de uitvoering daarvan is qua opzet op veel punten vergelijkbaar met de Nederlandse situatie. Privacywetgeving is vastgelegd in de Personal Data Act en de Health Act. Er zijn enkele instanties die zich met privacy bezig houden. Het ministerie van Justitie is verantwoordelijk voor de Personal Data Act en het ministerie van Health and Care Services is verantwoordelijk voor de Health Act. Het Ministry of Government Administration and Reform is verantwoordelijk voor regelgeving op het gebied van persoonsinformatie, voor toezicht op het Data Inspectorate en zij heeft de bestuurlijke verantwoordelijkheid voor het “Privacy Appeals Tribunal”. Het Data Inspectorate is een orgaan voor bescherming van persoonlijke gegevens met sector-overstijgende verantwoordelijkheden. Het Privacy Appeals Tribunal is een onafhankelijk orgaan dat ontstaan is naar aanleiding van de Personal Data Act, de Health Act en een aantal andere wetten. Het Privacy Appeals Tribunal behandelt klachten tegen beslissingen die door het Data Inspectorate gemaakt zijn. Het Data Inspectorate is zowel toezichthouder als ombudsman.

In “An information society for all” kondigt de overheid aan de volgende maatregelen te nemen op het gebied van privacy:

- Measure 8.1: het aanwijzen van een “personal privacy commission”, die technische ontwikkelingen in de gaten houdt en voorstellen doet voor het implementeren van privacymaatregelen
- Measure 8.2: De overheid staat een situatie voor waarin het mogelijk moet zijn om anoniem te blijven in een context waarbij identificatie niet noodzakelijk is, bijvoorbeeld door anonieme bankkaarten of het gebruik van pseudoniemen.
- Measure 8.3: De overheid zal maatregelen implementeren om gebruik van PETs (Privacy Enhancing Technologies) te ondersteunen.
- Measure 8.4: De overheid zal maatregelen implementeren om ervoor te zorgen dat ondernemingen meer compliant zijn met de Personal Data Act, waaronder:
  - het voorbereiden van sectorale best practices met adviezen voor solide technische oplossingen
  - het voorbereiden van een “competency programme”, waarin kennis van privacy en privacymaatregelen wordt gestimuleerd
- Measure 8.5: De overheid zal onderzoeken hoe wettelijke bescherming gewaarborgd kan worden bij geheel of gedeeltelijk geautomatiseerde beslissingssystemen.
- Measure 8.6: De overheid gaat onderzoek doen naar:
  - hoe wetgeving kan worden ontworpen om het gebruik van Privacy Enhancing Technologies te ondersteunen
  - het ontwikkelen van tools om compliancy te kunnen monitoren met de Personal Data Act
  - het ontwikkelen van tools om de veiligheid van informatie te kunnen waarborgen

  - hoe de Personal Data Act effectiever kan worden gemaakt door hem te versimpelen en moeilijke terminologie te vermijden
  - de behoefte om verschillende wetten in het privacy-domein te harmoniseren
- Measure 8.7: De overheid zal de takenscheiding tussen het Data Inspectorate en andere toezichthoudende instanties onder de loep nemen, waarbij sterkere samenwerking en coördinatie wordt beoogd.
- Measure 8.8: Maatregelen zullen worden genomen zodat in opleidingen doelstellingen worden meegenomen om kinderen en jonge volwassenen op de hoogte te stellen van privacy (door informatie over technische ontwikkelingen en uitdagingen op het gebied van privacy)
- Measure 8.10: De overheid zal maatregelen implementeren om ervoor te zorgen dat er genoeg competenties, begrip en interne methodologieën zijn zodat in een vroegtijdig stadium privacy issues kunnen worden betrokken bij nieuwe wetgeving
- Measure 8.11: De overheid zal maatregelen nemen om onderzoek naar privacy te bevorderen en structureren.

Eindnoten

[1] Zuurmond, A., Mulder, B. en Bullinga, M. (2005). *De overheid als infrastructuur: concept-studies*. Den Haag: Drukkerij Moretus B.V.

[2] S.D. Warren en L.D. Brandeis (1980). The right to privacy, In: *Harvard Law Review*, no.5, p. 195. Zij spraken in navolging van Judge Cooley over 'the right to be let alone'.

[3] A.F. Westin (1967). *Privacy and Freedom*. New York, p. 7.

[4] Zo is in Duitsland in de periode 1969 tot 1983 het op de Federale Grondwet gebaseerde recht op informationele zelfbeschikking tot ontwikkeling gekomen. Zie: T. Koopmans (1995). Privacy and the dilemma's of human rights' protection. In: P. Ippel e.a., *Privacy disputed*, pp. 45-46. SDU: Den Haag.

[5] Zie: J.L. Johnson (1989). Privacy and the Judgements of others. In: *The Journal of Value Inquiry*, p. 157.

[6] Johnson spreekt er in dit verband over dat privacy 'socially or culturally' gedefinieerd is en van context tot context verschilt en derhalve dynamisch is. Zie: J.L. Johnson (1989). Privacy and the Judgements of others. In: *The Journal of Value Inquiry*, p. 157. Zie ook: A.H. Vedder (1996). Privacy en woorden die tekort schieten, In: Nouwt, S. en W. Voermans (red.), *Privacy in het informatietijdperk*, p.22. SDU: Den Haag.

[7] Omdat de precieze afbakening en betekenis van privacy keer op keer bepaald wordt door uiteenlopende factoren zoals bijvoorbeeld maatschappelijke omstandigheden, beperken wij ons tot de Nederlandse situatie met de eigen Nederlandse maatschappelijke opvattingen. Onderzoeken in en uit andere landen zouden wellicht een 'verkeerd' beeld van de maatschappelijke opvattingen over individuen kunnen geven. Dit nog geheel los van het feit dat ook internationaal bezien wij geen onderzoeken hebben kunnen vinden die expliciet ingaan op de waarden, normen en overtuigingen die achter het begrip privacy liggen. De onderzoeken betreffen de vraag of personen een bepaald verschijnsel al dan niet als een privacyissue of een privacygevaar beschouwen en in feite niet wat zij zelf onder privacy verstaan.

[8] Deze (andere) onderzoeken betreffen, voor zover daarin opvattingen van individuen zijn onderzocht, (enkel) de vraag of zij een bepaald verschijnsel al dan niet als een privacyissue of een privacygevaar beschouwen. Genoemd kunnen worden: Bureau Veldkamp (1988). *Nulmeting ten behoeve van voorlichtingscampagne Wet persoonsregistraties, onderzoek i.o.v. de Rijksvoorlichtingsdienst*; J. Holvast, H. van Dijk, G.J. Schep (1989) *Privacy doorgelicht*. SWOKA onderzoeksrapport nr. 71; Bureau Veldkamp, *Eenmeting ten behoeve van voorlichtingscampagne Wet persoonsregistraties*, 1990, onderzoek i.o.v. de Rijksvoorlichtingsdienst; Bureau Veldkamp, *Onderzoek onder registratiehouders*, 1990, onderzoek i.o.v. de Rijksvoorlichtingsdienst; Bureau Veldkamp, *Evaluatie-onderzoek onder registratiehouders voorlichtingsmiddelen Wpr*, 1992, onderzoek i.o.v. de Rijskvoorlichtingsdienst; Intomart Kwalitatief, *De Wet persoonsregistraties, een kwalitatief onderzoek*, 1994, onderzoek i.o.v. de Registratiekamer; Interview, *Publieksonderoek uitwisseling justitiële gegevens*, 18 mei, 1994, onderzoek i.o.v. de voorlopige raad voor de justitiële informatievoorziening; J.E.J. Prins, W.B.H.J. van de Donk e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster?*, Alphen a/d Rijn/Diegem, Samson, 1995, (ITeR reeks nr. 1); Intomart, *Opinie ten aanzien van chipkaart*, 1996, onderzoek i.o.v. de Evangelische Omroep; Consumentenbond, *Privacy*, 1997; M. van Leeuwen en P. Meijer (NIPO), *Registreren en communiceren, koepelorganisaties over Privacy en de Registratiekamer*, 1997, onderzoek i.o.v. de Registratiekamer.

[9] G.C.J. Smink, A.M. Hamstra en H.M.L. van Dijk (1999). *Privacybeleving van burgers in de informatiemaatschappij*, (Werkdocument 68 Rathenau Instituut). Den Haag: Rathenau Instituut.

[10] De waarde *zelfstandigheid* heeft betrekking op het zelf kunnen besluiten, zelf verantwoordelijkheid kunnen nemen en de mogelijkheid om gegevens voor zich te houden. *Bewegingsvrijheid* betreft het doen en laten wat je wilt, anoniem kunnen zijn, en niet gecontroleerd worden. *Gelijkheid* speelt bij situaties waarin mensen op basis van ongelijke of beperkte gronden geselecteerd worden. *Vrij blijven van stigmatisering* betekent geen etiket opgeplakt krijgen en niet onderworpen worden aan oordelen, bijvoorbeeld over kredietwaardigheid, van anderen zonder daar zelf op te kunnen reageren. *Ongestoord leven*

betreft het niet gedwongen worden actie te ondernemen, bijvoorbeeld bij ongevraagd gebeld worden. De waarde *eigenwaarde* wordt geschonden als burgers het idee hebben dat ze een deel van hun identiteit weggeven. *Vrij blijven van manipulatie* ziet op het niet onbewust aangezet worden tot bepaald handelen of denken. De *integriteit* wordt geschonden als gegevens zonder toestemming gekoppeld worden. Tot slot de waarde *autonomie*, die betrekking heeft op het zelf normen kunnen stellen en vrij zijn te handelen. Zie pagina 50-52 van *Privacybeleving van burgers in de informatiemaatschappij*.

[11] Zie pagina 101-103 van: G.C.J. Smink, A.M. Hamstra en H.M.L. van Dijk (1999). *Privacybeleving van burgers in de informatiemaatschappij*, (Werkdocument 68 Rathenau Instituut). Den Haag: Rathenau Instituut.

[12] Deze situationele invulling van privacy komt ook naar voor uit de beschrijving van A. F. Westin van drie groepen burgers in de Equifax-Harris onderzoeken. Hij spreekt daarin over de 'Privacy Fundamentalists' (25%), de 'Unconcerned' (18%) en de 'Pragmatic Majority (57%). Zie voor een eerste introductie de *Harris-Equifax Consumer Privacy Survey 1991*, 1991, Uitgevoerd in opdracht van Equifax, Georgia, USA, p. 6-7.

[13] Hieronder valt bijvoorbeeld het recht om anderen uit je huis te weren (het huisrecht).

[14] Hieronder valt bijvoorbeeld het briefgeheim en het telefoongeheim, maar ook het recht om niet opgebeld te worden of geen ongevraagde post te krijgen.

[15] Trb. 1951, 154 en 1990, 156.

[16] Stb. 1978, 177.

[17] Organisatie voor Economische Samenwerking en Ontwikkeling.

[18] OECD recommendation concerning and guidelines governing the protection of privacy and transborder flows of personal data, October 1, 1980.

[19] Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, European Treaty Series No. 108.

[20] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsinformatie en betreffende het vrije verkeer van die gegevens, Pb EG, nr. L 281/31-50 (de algemene EG-Privacyrichtlijn) en Richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsinformatie en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (de Telecom EG-Privacyrichtlijn).

[21] De naam van de nieuwe wet, de Wet bescherming persoonsinformatie, is in dit opzichte dan ook een juistere dan die van de Wet persoonsregistraties.

[22] Het ontwerp (oktober 2000) is te vinden op http://www.consilium.eu.int of op http://www.consilium.eu.int/df/docs/nl/CharteNL.pdf De bescherming van privé-leven is vervat in artikel 8. Artikel 9 regelt de bescherming van persoonsinformatie.

[23] Bijvoorbeeld het verbod op binnentreden en huiszoeking en de specifieke vereisten wanneer binnentreden of huiszoeking zijn toegestaan en bepalingen over lokaal- en huisvredebreuk.

[24] Bijvoorbeeld anti-martelbepalingen, regels over geneeskundige behandelingen, de strafbaarstelling van mishandeling en van hinderlijk volgen.

[25] Bijvoorbeeld regels over het brief-, telegraaf- en telefoongeheim en regels ten aanzien van monitoring van bijvoorbeeld e-mail en surfgedrag op internet.

[26] Er wordt dus gekozen om naast dataprotectie een bepaald onderdeel van het begrip privacy nader uit te werken, namelijk de informationele privacy. Dit omdat zowel informationele privacy als persoonsinformatiebeleid betrekking hebben op persoonsinformatie (informatie die gekoppeld is aan personen).

[27] S. Luitjens (2002). *Advies van tafel persoonsnummerbeleid in het kader van identiteitsmanagement.* Stroomlijning basisgegevens.

[28] En dat hierbij wordt gestreefd naar optimale transparantie over deze afwegingen.

[29] Bij deze informationele privacy gaat het om het recht op bescherming van personen in verband met informatie die over hen bekend is of die ten aanzien van hen wordt toegepast. We hebben daarbij met name op het oog het respect voor en de bescherming van de waarden genoemd in paragraaf 2.1.1. enerzijds en uitvoering van de beginselen uit de tweede bijlage anderzijds.

[30] Mayer, R., J. Davis, F.Schoorman (1995). An integrative model of organizational trust. *Acad. of Management Rev*. 20.

[31] College Bescherming Persoonsinformatie (2005). *Jaarverslag 2005*. Den Haag.
[32] Privacy Enhancing Technologies (PET). Dit omvat alle technische maatregelen om privacy te waarborgen.
[33] Ronald Koorn, Herman van Gils, Joris ter Hart, Paul Overbeek en Raúl Tellegen (2004). *Privacy Enhancing Technologies: witboek voor beslissers*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
[34] Uit onderzoek van DEMOS in Groot-Brittannië blijkt bijvoorbeeld dat men niet zozeer bang is voor wat een organisatie weet, als wel voor hoe men gegevens interpreteert en de onrechtvaardige behandeling die daar mogelijk uit zou volgen. Vertrouwen in *het gebruik van data* is dus van groot belang.
[35] Staatscourant 1998, nr. 84.
[36] Niet alleen concreet neergelegd in artikel 10 van de grondwet maar ook geïncorporeerd in enkele andere artikelen.
[37] Zie bijvoorbeeld de verschillende bijdragen in: Burkens M.C., Jurgens E.C.M., Koekkoek A.K., Vis J.J. (red.), *Gelet op de Grondwet. 150 jaar Grondwet*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1998.
[38] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2003). *Kabinetsvisie Andere Overheid*. BZK: Den Haag.
[39] Ronald Koorn, Herman van Gils, Joris ter Hart, Paul Overbeek en Raúl Tellegen (2004). *Privacy Enhancing Technologies: witboek voor beslissers*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
[40] Hierbij valt te denken aan:

- *identificatie* en *authenticatie*: met wie ben ik aan het communiceren (identificatie) en kan ik er zeker van zijn dat de andere partij inderdaad is voor wie hij zich uitgeeft (authenticatie)?
- *autorisatie en kwalificatie*: heeft de andere partij wel de juiste rechten (autorisatie) of eigenschappen (kwalificatie) voor een transactie?
- *vertrouwelijkheid*: kan ik ervan op aan dat alleen degene met wie ik wil communiceren kennis kan nemen van de inhoud van mijn boodschap?
- *integriteit*: is wat ik heb ontvangen wel het oorspronkelijke bericht of is het onderweg gewijzigd?
- *onloochenbaarheid*: kan ik voorkomen dat een afzender later kan ontkennen een bericht ooit verstuurd te hebben of dat een geadresseerde kan beweren mijn bericht nooit te hebben ontvangen?
- *tijdstempeling*: wanneer is dit bericht verzonden of wanneer heeft deze transactie plaatsgehad?

Zie ook: Versmissen (2001). *Sleutels tot vertrouwen: TTP's, digitale certificaten en privacy*. Den Haag: Registratiekamer.
[41] In deze paragraaf wordt met name ingegaan op *preventieve* bestrijding van criminaliteit ten behoeve van een verhoogde veiligheid of gevoel van veiligheid.
[42] B. Koops e.a. (2001). *Opsporing versus privacy: de beleving van burgers*.
[43] Zie ook: Rathenau Instituut/TILT (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Neder land aan het begin van de 21ste eeuw*. Den Haag: Rathenau Instituut.
[44] Hoe de patiëntgegevens beschermd moeten worden is beschreven in het rapport van de Nederlandse Patiënten Consumenten Federatie (NPCF). Zie hiervoor: Nationaal ICT Instituut in de Zorg (2006). *Specificatie van de Basisinfrastructuur in de Zorg.*
[45] K. Spaink (2006). *Medische geheimen*, Nijgh & Van Ditmar.
[46] K. Spaink (2006). *Medische geheimen*, Nijgh & Van Ditmar.
[47] In tegenstelling tot paragraaf 3.2.1. betreft het hier *reactieve* criminaliteitsbestrijding.
[48] In tegenstelling tot paragraaf 3.2.1. betreft het hier *reactieve* criminaliteitsbestrijding.
[49] P. Bordewijk (2006). Fraudebestrijding vereist normering. *Overheidsmanagement,* januari 2006.
[50] P. Bordewijk (2006), Fraudebestrijding vereist normering. *Overheidsmanagement,* januari 2006.
[51] P. Bordewijk (2006). Fraudebestrijding vereist normering. *Overheidsmanagement*, januari 2006.
[52] CBP (2006). *Notitie fraudebestrijding door bestandskoppeling.*
[53] M. van Eechoud en J.Kabel (deel 14), Prijsbepaling voor elektronische overheidsinformatie,

ITeR.
[54] M. van Eechoud en J.Kabel (deel 14), Prijsbepaling voor elektronische overheidsinformatie, ITeR.
[55] M. van Eechoud en J.Kabel (deel 14), Prijsbepaling voor elektronische overheidsinformatie, ITeR.
[56] In deze paragraaf staan ontwikkelingen op het gebied van Informatie- en Communicatietechnologie binnen het publieke domein centraal. Hiernaast zijn ook ontwikkelingen op het terrein van de neurowetenschappen relevant. Denk daarbij aan het gebruik van kennis over de werking van het brein en DNA in de veiligheidssector.
[57] Eind 2006 had bijna 29% van de Nederlanders een breedband internetverbinding, hetgeen mede te verklaren is door een daling van de kosten van breedband en draadloos internet.
[58] RFID staat voor Radio Frequency Identification.
[59] Hierbij valt te denken aan GPRS, UMTS, WiFi, WIMAX.
[60] Hiemstra, J. (2003). *Presterende gemeenten*. Kluwer.
[61] L. Assher en A. Ekker (2003) *Anonimiteitswet is hard nodig.* De Volkskrant, 26 augustus 2003.
[62] GBA staat voor Gemeentelijke Basisadministratie.
[63] In Nederland is dat in principe geregeld door middel van de verschillende niveaus van authenticatie (DigiD, DigiD met sms-authenticatie en PKI).
[64] Voor een verdere onderbouwing hiervan, zie paragraaf 4.3.1, waarin nader wordt ingegaan op het spanningsveld tussen privacy, veiligheid en opsporing in de hedendaagse samenleving.
[65] Bovendien beperkt de schets van juridische ontwikkelingen zich tot veranderingen in wet- en regelgeving. Dit betekent dat algehele trends in het juridisch debat over informationele privacy buiten beschouwing worden gelaten.
[66] Rathenau Instituut/TILT (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Neder land aan het begin van de 21ste eeuw*. Den Haag: Rathenau Instituut.
[67] College Bescherming Persoonsinformatie (2006). *Privacy in een controlesamenleving*.
[68] Er zijn diverse vormen van cameratoezicht te onderscheiden. Zo is er cameratoezicht op openbare plaatsen, op de werkplek, in en rond winkels, in en rond woningen en voor de opsporing van strafbare feiten. Zie ook: College Bescherming Persoonsinformatie (2005). *Dossier cameratoezicht*.
[69] De Wet Bijzondere Opsporingsbevoegdheden beoogt normen vast te stellen waaraan opsporingsonderzoeken moeten voldoen, zodat ze ook beter controleerbaar worden.
[70] De Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 regelt bevoegdheden van inlichtingen- en veiligheidsdiensten tot aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht.
[71] Deze bewaarverplichting moet in Nederland echter nog wel door implementatiewetgeving ingevoerd worden. Zie: Europese unie (2006). *Press release 2709th counsil meeting, Justice and Home Affairs*. Brussel.
[72] B. Koops e.d. (2001). *Opsporing versus privacy: de beleving van burgers*.
[73] Rathenau Instituut/TILT (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Neder land aan het begin van de 21ste eeuw*. Den Haag: Rathenau Instituut.
[74] Er wordt hier gegeven de eerdere begripafbakening enkel ingegaan op ontwikkelingen in de zorg die de informationele privacy betreffen. Er zijn ook belangrijke ontwikkelingen gaande die een bedreiging vormen voor de ruimtelijke en relationele privacy. Toegenomen controlemogelijkheden en ‘ambient assisted living’ maken het bijvoorbeeld mogelijk dat mensen meer thuis en minder in het ziekenhuis kunnen verblijven. Daarmee dringen zorgverleners het familieleven en het huisdomein binnen. Burgers staan hier over het algemeen neutraal tegenover. Zie: EPN (2006). *Van wie is mijn gezondheid?.*
[75] T. Hooghiemstra (2002). Privacy bij ICT in de zorg, ZM Magazine.
[76] www.ncpf.nl
[77] Nationaal ICT instituut in de Zorg, MIC 2003. Globaal ontwerp. Zie www.nictiz.nl.
[78] Zie: Koninklijke Nederlandse Maatschappij ter bevordering der Geneeskunst (2004). *Implementatie van de WGBO: van wet naar praktijk; deel 4: toegang tot patiëntengegevens.*

Utrecht: KNMG.

[79] EPN (2006). Van wie is mijn gezondheid?

[80] P. Bordewijk (2006). Fraudebestrijding vereist normering, Overheidsmanagement

[81] CBP (2006). *Notitie fraudebestrijding door bestandskoppeling.*

[82] CBP (2006). *Notitie fraudebestrijding door bestandskoppeling.*

[83] Zie: www.szw.nl

[84] J. Prins (2004). *Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy*

[85] Ronald Koorn, Herman van Gils, Joris ter Hart, Paul Overbeek en Raúl Tellegen (2004). *Privacy Enhancing Technologies: witboek voor beslissers*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[86] Rathenau Instituut/TILT (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Neder land aan het begin van de 21ste eeuw*. Den Haag: Rathenau Instituut.

[87] Zie voetnoot 86.

[88] CTIVD (2007). Toezichtsrapport nummer 12. De CT-Infobox is een samenwerkingsverband van de Algemene Inlichtingen en Veiligheidsdienst, de Immigratie- en Naturalisatiedienst, het Korps Landelijke Politiediensten, het Openbaar Ministerie en de MIVD met als doel bij te dragen aan de effectieve bestrijding van terrorisme in Nederland. De bijdrage voorziet in het binnen wettelijke kaders bijeenbrengen en vergelijken van informatie over netwerken en personen die op de één of andere wijze betrokken zijn bij terrorisme, in het bijzonder islamitisch terrorisme en de daaraan gerelateerde radicalisering.

[89] CTIVD (2006). Toezichtsrapport nummer 10.

[90] Onder meer de volgende onderzoeken: Commissie Bestuurlijke Evaluatie AIVD (2004). *De AIVD in Verandering.* Den Haag, Clingendael Centrum voor Strategische Studies; TNO (2005). *Democratische Controle Inlichtingen- en Veiligheidsdiensten*. Den Haag; CTIVD (2007). *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de Contra Terrorisme Infobox*. Den Haag

[91] De volgende typen fraude kunnen worden onderscheiden:

- *Identiteitsfraude:* wanneer een persoon door onrechtmatig gebruik van identiteitsdocumenten een uitkering, subsidie of voorziening verkrijgt, die hij bij gebruik van zijn eigen identiteit niet, of niet in die mate, zou hebben gekregen. Het gebruik maken van valse of gestolen paspoorten, verblijfspapieren of sofi-nummers zijn vormen van identiteitsfraude.
- *Inkomensfraude:* hier is sprake van als iemand inkomsten uit arbeid of een andere uitkering niet, niet volledig of onjuist opgeeft, waardoor hij ten onrechte een (te hoge) uitkering ontvangt. Inkomsten spelen bijvoorbeeld een rol bij het bepalen van de hoogte van de uitkering op grond van de WWB, WW, WAO, WIA, Anw of AOW (inkomsten van de partner die jonger is dan 65 jaar).
- *Vermogensfraude:* hiervan is sprake wanneer in de sociale zekerheid een persoon niet opgeeft dat hij over vermogen beschikt. Vermogen speelt vooral in de bijstand een rol. Bekende vormen van vermogensfraude zijn het niet opgeven van een bankrekeningsaldo, auto of onroerend goed.
- *Leefvormfraude* speelt bij uitkeringen waar de woon- en leefsituatie van een (potentiële) uitkeringsgerechtigde medebepalend is voor het recht en/ of de hoogte van de uitkering. Bij een bijstandsuitkering moet men in de gemeente verblijven (daadwerkelijk wonen en ingeschreven staan) waar een uitkering wordt aangevraagd.

[92] Transact (2006). *Huiselijk geweld: feiten en cijfers*.

[93] De conclusies die wij trekken uit de case studies zijn getoetst bij Cees Meesters, voorzitter van de Nederlandse Vereniging van Burgerzaken.

[94] Zie ook: Constantijn van Oranje, *Maarten Botterman,* Lorenzo Valeri (2005*). Persoonsinformatiebeleid van de Openbare sector in Europees perspectief*. Leiden.

[95] Het betreft:

Organisatie	**Naam**	**Functie**
Agentschap Basisregistratie Persoonsgegevens en reisdocumenten	Esther 't Hoen	Beleidsmedewerker
Agentschap Basisregistratie	Sasja van Immerzeel	

Persoonsgegevens en reisdocumenten		
Belastingdienst	W.J. van Duijn	Teamlid Juridische zaken
BKWI	Tonkie Zwaan	
BKWI	Jan Breeman	Voorzitter Domeingroep Privacy & Beveiliging
CIZ (Centrum Indicatiestelling Zorg)	Tineke van EE	Projectleider
CIZ (Centrum Indicatiestelling Zorg)	Arne van Huis	
DIVOSA/ CP-ICT	Ronald de Zwart	Manager Coördinatiepunt ICT gemeenten
Federatie Opvang	Johan Gortworst	Beleidsmedewerker
Gemeente Rotterdam	Sylvia van Gilst	
IBG (Informatie Beheer Groep)	Gineke Kuipers	Decentrale privacyofficier
IBG (Informatie Beheer Groep)	Rian Huiberts	Senior medewerker basisregistraties
Ministerie van Binnenlandse Zaken	Lotte Nijland	Beleidsmedewerker
Ministerie van Justitie	Leon Poffe	Programmamanager EG
Ministerie van Justitie	Maartje Boots	Beleidsmedewerker
Ministerie van VWS	Lenneke Wolswinkel	Beleidsmedewerker
Ministerie van VWS	Myra Klee	Projectleider Bescherming
Nederlandse Verenging van banken	G. Boudewijn	Hoofd afdeling betalingen
NVVB (Nederlandse Verenging voor Burgerzaken)	Ank van Vierzen-Jongman	Directeur NVVB
Politie	Hans van Bentvelzen	
Politie Haaglanden	Daan Driessen	Medew. landelijke uitrol EG
Politie Haaglanden, Unit MEP	Willem Timmer	Hoofd Unit MEP
Vrouwen Opvang Hera in Gelderland	Mariëtte van Dorst	Directeur vrouwenopvang
Zorgverzekeraar Nederland	P.J.H. Jansen	afdeling Informatiebeleid