Hoe gaan organisaties die zich inzetten voor privacy om met een veranderende omgeving?

Bachelorscriptie:
Judith van Luijk
280705
Juli 2007
Erasmus Universiteit Rotterdam; Faculteit der Sociale Wetenschappen; Sociologie

Begeleiding: Peter Mascini

Voorwoord

Deze scriptie vormt de afsluiting van mijn bachelor programma sociologie. Na een aantal wisselingen van onderwerp en een scriptiegenoot die besloot te stoppen na een aantal maanden, was het begin verre van ideaal. Ik heb de draad echter weer weten op te pakken en dit heeft geleid tot het eindresultaat wat u nu voor u heeft.

Er zijn een aantal mensen die ik een dankwoord schuldig ben. Ten eerste uiteraard mijn scriptiebegeleider Peter Mascini, die mij keer op keer met nuttige tips en opbouwende kritiek de juiste richting opduwde.
Ook wil ik alle respondenten bedanken die vol enthousiasme tijd voor mij wilden vrijmaken om mij te woord te staan. Het waren keer op keer leuke gesprekken met enthousiaste mensen die zich vol passie op hun manier inzetten voor privacybescherming. In het bijzonder wil ik Geert Klei van Stichting Privacyloket.nl noemen, die altijd erg heeft meegedacht over hoe ik mijn onderzoek zo interessant mogelijk kon maken. Ik heb ook dankbaar gebruik mogen maken van zijn brede netwerk om respondenten aan te schrijven.
Tot slot wil ik mijn vrienden en familie bedanken voor de steun op momenten dat ik vastliep of deadlines moest halen. In het bijzonder wil ik Yannis bedanken voor de tijd en energie die hij gestopt heeft in het kritisch doorlezen van mijn scriptie. Bedankt voor alle nuttige tips!

Rotterdam, juli 2007.

Inhoudsopgave

Hoofdstuk 1; Inleiding

1.1 Inleiding

Organisaties worden vanuit verschillende disciplines bestudeerd. Binnen het sociologische perspectief wordt een organisatie niet als een aparte entiteit gezien, maar in samenhang met de omgeving bestudeerd. Binnen een technische omgeving wordt de nadruk op de markt gelegd, binnen een institutionele omgeving zijn normen en waarden het belangrijkste. Organisaties die in een institutionele omgeving opereren, vertegenwoordigen een bepaalde waarde en proberen deze waarde in stand te houden. Voor dit type organisatie is het van belang dat zij opereert in een omgeving waarin het belang van deze waarde ook wordt erkend. Zij is afhankelijk van de normatieve consensus dat de waarde die zij vertegenwoordigt belangrijk is. Deze normatieve consensus is echter onderhevig aan veranderingen. Legitimiteit van een organisatie kan toe- of afnemen als er veranderingen in de omgeving plaatsvinden. Het is dan ook interessant te onderzoeken wat organisaties doen wanneer zij (als gevolg van maatschappelijke veranderingen) legitimiteit verliezen. Gaan deze organisaties zich aanpassen aan hun omgeving? Proberen deze organisaties zelf de omgeving te beïnvloeden?

Om een antwoord te vinden op deze vragen kan men organisaties bekijken die binnen een context van een veranderende omgeving opereren. Als organisaties afhankelijk zijn van hun omgeving werken zij binnen een institutionele context (Selznick, 1957). Juist bij deze organisaties is het winnen van legitimiteit erg belangrijk. Een voorbeeld van zo'n organisatie die opereert in een institutionele context is een organisatie die zich inzet voor privacybescherming. Privacybescherming is een waarde die op het eerste gezicht onder vuur lijkt te liggen. Veiligheidsmaatregelen en technologische ontwikkelingen winnen aan populariteit en privacybescherming lijkt minder belangrijk te zijn. Er zijn verschillende organisaties die zich inzetten voor de bescherming van privacy. Hoe reageren deze organisaties op een omgeving waarin de steun voor de bescherming van privacy is of lijkt te zijn afgenomen? Wanneer de opinie over privacy verandert, is het aannemelijk dat de legitimering vanuit de omgeving voor de organisatie die zich hiervoor inzet ook verandert. Voelen deze partijen zich genoodzaakt zich aan te passen aan de omgeving om hun boodschap nog te kunnen verkondigen? Deze vraag leidt tot de volgende probleemstelling met bijbehorende onderzoeksvragen:

Probleemstelling:

Hoe reageren organisaties die te kampen krijgen met afnemende legitimiteit vanuit hun omgeving en welke strategieën gebruiken zij om (meer) legitimiteit te verkrijgen?

Onderzoeksvragen:

1. Is er sprake van onderschikking van privacybescherming ten opzichte van andere doelen?
2. Hebben partijen die zich inzetten voor de privacybescherming ervaren dat er maatschappelijke veranderingen hebben plaatsgevonden die van invloed zijn op hun functioneren en/of legitimiteit en aan welke oorzaken schrijven zij dit toe?
3. Hoe hebben partijen die zich inzetten voor de privacybescherming gereageerd op deze maatschappelijke veranderingen? Specifieker: Welke strategieën hebben zij gebruikt om te kunnen blijven functioneren en/of hun legitimiteit te kunnen blijven garanderen?

In deze scriptie zal ik antwoord geven op deze vragen door middel van een kwalitatief onderzoek. Ik zal trachten een beeld te schetsen van wat organisaties doen om legitimiteit vanuit hun sociale omgeving te vergroten en wat voor strategieën zij hiervoor gebruiken.

1.2 De onderzoeksvragen

De probleemstelling bestaat uit drie onderdelen. Om tot een antwoord op deze drie onderzoeksvragen te komen en dus de probleemstelling te kunnen beantwoorden worden verschillende onderzoeksmethoden gebruikt en bronnen geraadpleegd. In het eerste onderdeel (eerste onderzoeksvraag) ga ik de veronderstelling dat privacybescherming de afgelopen tijd onder druk is komen te staan toetsen. Hebben deze veranderingen daadwerkelijk plaatsgevonden en in welke mate? Ik richt me hierbij op een veranderende publieke opinie over privacy, maar ook over veiligheidsmaatregelen en technologie, aangezien deze veranderingen ook gevolgen kunnen hebben voor de mening over privacy. Ter beantwoording van deze vraag zal ik in eerste instantie proberen weer te geven of en hoe de publieke opinie veranderd is.

Het tweede onderdeel (tweede onderzoeksvraag) richt zich op de door organisaties ervaren veranderingen binnen de maatschappij en oorzaken die zij daaraan toeschrijven. Deze veranderingen verwijzen naar ontwikkelingen zoals in de eerste onderzoeksvraag aangegeven.

Het gaat hierbij dus niet zozeer om objectieve veranderingen, maar om de ervaren veranderingen door organisaties. De maatschappelijke veranderingen kunnen zorgen voor verminderde ervaren steun of legitimiteit vanuit de samenleving. Het is immers aannemelijk dat de partijen die zich inzetten voor privacybehoud minder steun ervaren wanneer de samenleving minder waarde hecht aan privacy.

Het derde onderdeel (derde onderzoeksvraag) richt zich op de strategieën die de organisaties gebruiken als reactie op deze maatschappelijke veranderingen. Dit gaat over de vraag hoe de organisaties hebben gereageerd op deze veranderingen.

Ter beantwoording van deze vraag zullen interviews een belangrijke rol spelen. Via de medewerkers is het mogelijk te achterhalen hoe partijen hebben ingespeeld op de maatschappelijke veranderingen. Ook kunnen websites van deze partijen een rol spelen. Hier is veel informatie over een organisatie te vinden en zijn wellicht al veranderingen waar te nemen. Hierbij valt te denken aan bijvoorbeeld een verandering van het takenpakket of de aandachtspunten van een organisatie.

Hoofdstuk 2; Theorie en concepten

In dit hoofdstuk wordt aandacht besteed aan het theoretisch kader van dit onderzoek. In hoofdstuk een gaf ik al aan dat de organisaties die ik zal bespreken in een institutionele omgeving opereren, daarom zal ik in paragraaf 2.1 bespreken wat een institutionele omgeving nu precies inhoudt. In diezelfde paragraaf zal ik daartoe eerst ingaan op wat een institutie is. In paragraaf 2.2 benoem ik een aantal theorieën die zijn gebaseerd op instituties. Uiteindelijk bespreek ik in paragraaf 2.3 een aantal verschillende strategieën die een organisatie opererend binnen een institutionele omgeving, kan toepassen om haar omgeving te beïnvloeden.

2.1 Instituties

Durkheim verstaat onder het begrip institutie:

‘*Het geheel van overtuigingen en praktijken, van opvattingen en manieren van doen, die in het sociale verkeer een verplichtend karakter hebben gekregen, en die betrekking hebben op voortdurend aanwezige of telkens terugkerende sociale aangelegenheden’* (De Jong, 1997: 72).

Hij stelt dus dat instituties het denken, voelen en handelen beïnvloeden. Sociale instituties zijn op de achtergrond aanwezig en zijn dwingende sociale factoren die gedrag bepalen. Voorbeelden van instituties zijn taal, onderwijs, het huwelijk, religie, wetten en fatsoensnormen. Deze definitie geeft een algemene betekenis aan een institutie.

Binnen de organisatiesociologie zijn er definities van instituties die meer de nadruk leggen op organisaties. Wanneer een organisatie impliciet of expliciet over bepaalde waarden beschikt die zij vertegenwoordigt spreken we ook van een institutie. Zo stelt Scott (1995:33) dat:

“*Institutions consist of cognitive, normative, and regulative structures and activities that provide stability and meaning to social behavior”.*

Deze definitie komt voor een deel overeen met die van Durkheim. Ook Scott wijst op het sturende karakter van een institutie. Hij past het begrip echter ook toe op organisaties. Instituties sturen dus het gedrag van individuen en organisaties en oefenen grote invloed uit op de strategische keuzes van een organisatie. De structuren waar Scott het over heeft zijn waarden die geïnternaliseerd zijn door de leden van de organisatie en door hen worden vertegenwoordigd. Hierdoor wordt de organisatie meer dan 'gewoon' een organisatie, zij wordt een boegbeeld voor die waarde.

Selznick besteedt in zijn definitie van een institutie aandacht aan het verschil tussen een institutie en een organisatie. Hij spreekt van een karakter of unieke identiteit van een organisatie. Dit karakter bepaalt in grote mate het gedrag van een organisatie. Hierbij kun je denken aan gedeelde doelen, werkmethoden, vaardigheden en hulpbronnen die gebruikt worden. Het vormen van zo'n karakter gebeurt niet zomaar, maar is een proces; dit noemt Selznick een institutionaliseringproces (Selznick, 1992. Uit Lammers e.a 1983). Het karakter van een organisatie bepaalt in belangrijke mate hoe formele doelstellingen in de praktijk gestalte krijgen. En juist hierin maakt Selznick een onderscheid tussen een organisatie en een institutie. Bij een organisatie is er sprake van een doelgericht verband. Wanneer de organisatie dit doel heeft bereikt, of wanneer blijkt dat zij het doel onmogelijk op deze manier kan bereiken, kan de organisatie direct worden beëindigd of opgeheven. Met andere woorden: een organisatie is niets meer dan een (technisch) instrument om een doel te bereiken. Een institutie kan niet zomaar worden opgeheven, omdat er binnen de organisatie en haar omgeving waarde wordt gehecht aan het bestaan van de waarden en het karakter dat een institutie vertegenwoordigt. Selznick wijst er ook op dat organisaties wel instituties kunnen worden wanneer waarden en ideeën worden ontwikkeld en de organisatie op deze manier wordt 'infused with value' (Selznick, 1957). Hierbij kun je bijvoorbeeld denken aan het Internationaal Olympisch Comité (IOC), in 1894 opgericht door de Fransman Pierre de Coubertin samen met de Griek Demetrius Vikelas. Deze organisatie is in eerste instantie opgericht met als doel het organiseren van de Spelen, maar heeft in de loop van de tijd waarden geïnternaliseerd, zoals verbroedering en wereldvrede.

Een institutie zal altijd de neiging hebben geïnstitutionaliseerde waarden en ideeën in stand te houden en te beschermen tegen inmenging van buitenaf. Institutionalisten zijn van mening dat deze waarden voor een groot deel worden bepaald door de institutionele omgeving en dus niet zozeer vanuit de institutie zelf (Scott, 1987). Het is niet geheel duidelijk of de institutie moet

worden gezien als een 'ontworpen' sociaal verband (Hesse en Benz, 1990), of als een onbewust en ongepland proces (Meyer en Rowan, 1977, uit Lammers e.a. 1983).
In dit onderzoek hanteer ik het begrip institutie zoals gegeven door Scott en Selznick, een definitie met een meer specifiek karakter. Instituties worden immers gezien binnen de context van organisaties en dit sluit beter aan bij mijn onderzoek, waarin ik heb gekozen voor organisaties die zich inzetten voor de bescherming van privacy.

De omgeving van een organisatie speelt een belangrijke rol. Een organisatie is immers voor haar overleven afhankelijk van goederen en diensten van externe partijen zoals concurrenten, vakbewegingen en de media. Deze omgeving kan zowel institutioneel als technisch zijn. Binnen de institutionele omgeving wordt meer waarde gehecht aan normatieve aspecten. Om steun te krijgen zal een organisatie die binnen een institutionele context opereert, moeten voldoen aan normen en waarden vanuit de omgeving. Het is voor een organisatie dus belangrijk dat zij zowel intern als extern partijen vindt die de waarden die zij vertegenwoordigt, ondersteunen.

Een organisatie hoeft echter niet per se te opereren in een institutionele omgeving (Scott en Meyer, 1991), maar kan ook in een technische omgeving opereren of in beide. Binnen een technische omgeving wordt prioriteit gegeven aan economische motieven en neemt de markt een belangrijke positie in. De organisatie wordt beoordeeld op economische prestaties en zal effectief en efficiënt moeten opereren. Wanneer een institutie in beide omgevingen opereert, heeft zij te maken met zowel de legitimiteit en acceptabele vorm van de organisatie als met het effectief en efficiënt produceren van een product of dienst.

Organisaties die afhankelijk zijn van steun vanuit de omgeving opereren in een institutionele omgeving en werken binnen een institutionele context. Deze afhankelijkheid zorgt ervoor dat de organisatie een passief aspect wordt binnen een omgeving die de regels en waarden bepaalt. De omgeving is dominant ten opzichte van de organisatie (Zucker, 1987). Om haar eigen overlevingskansen te vergroten is het dus van belang de institutionele omgeving tevreden te stellen en aan haar verwachtingen tegemoet te komen. Een organisatie zal echter ook altijd proberen zo min mogelijk afhankelijk te zijn van haar omgeving, zodat ze niet altijd hoeft toe te geven aan druk vanuit die omgeving (Hasenfeld, 1983). Wanneer de waarden van de organisatie onderhevig zijn aan maatschappelijke veranderingen kan het voor de organisatie moeilijk zijn autonomie te bewaren. Publiek dienstverlenende organisaties werken binnen een institutionele

context en zijn dus extra gevoelig voor invloeden uit hun omgeving (Selznick, 1957). Wanneer de maatschappij verandert, kunnen immers ook de waarden binnen de maatschappij veranderen die zo kenmerkend zijn voor de organisatie. Om te kunnen blijven overleven zal de organisatie haar waarden moeten aanpassen om binnen haar institutionele omgeving haar plaats te behouden (Lammers, 1983).

2.2 Theorieën

De *institutionele theorie* beschrijft hoe normen en waarden in een organisatie geïnternaliseerd worden. Binnen de sociologie kun je stellen dat het institutionalisme gezien kan worden binnen de stroming van het functionalisme (Suurs, 2005). Binnen dit paradigma is weinig ruimte voor individuen; gedrag wordt bepaald door regels, normen en waarden. Selznick noemt institutionalisering het internaliseren van waarden. Institutionalisering zorgt uiteindelijk voor stabiliteit en legitimiteit, wat de levensvatbaarheid van een organisatie vergroot. Als een organisatie de verwachtingen van de omgeving schendt, zal er verminderde steun zijn vanuit de institutionele omgeving. Het ontwikkelen van een eigen ideologie zorgt voor een zekere duurzaamheid van een organisatie (Selznick, 1957). Maar ook economische bronnen kunnen zorgen voor verhoogde legitimiteit. Een gebrek hieraan kan funest zijn voor een organisatie. Meer economische bronnen zorgen voor een verhoogde autonomie van een organisatie en minder afhankelijkheid van haar omgeving.

Een tweede theorie is de *resource dependency theorie*. Deze theorie gaat ervan uit dat een organisatie afhankelijk is van haar omgeving. Zij is kwetsbaar, omdat ze afhankelijk is van verschillende bronnen uit haar omgeving zoals geld, kennis, arbeid en materiaal. Hoe meer van deze bronnen een organisatie heeft, des te meer macht zij heeft over haar omgeving. Bij deze theorie is er dus sprake van machtsstrijd. Deze machtsstrijd vindt zowel plaats tussen de organisatie en haar omgeving als tussen organisaties onderling. Wil de organisatie overleven, dan moet ze op een succesvolle en verstandige manier omgaan met haar bronnen. De mate van autonomie van een organisatie hangt dan ook af van haar afhankelijkheid van bronnen binnen haar omgeving en het bezit van bronnen waar anderen binnen de omgeving gebruik van willen maken. Er is dus sprake van een interorganisationele afhankelijkheid.

Er zijn twee doelstellingen die verondersteld worden bij de resource dependency theorie; ten eerste streeft een organisatie ernaar zoveel mogelijk controle te krijgen over middelen die hun afhankelijkheid van hun institutionele omgeving verkleinen. Ten tweede probeert een organisatie ook middelen te krijgen die ervoor zorgen dat de afhankelijkheid van andere organisaties van hun organisatie maximaal wordt. Door het streven naar het bereiken van één van deze doelstellingen is er sprake van maximale uitwisseling van bronnen of middelen tussen de organisatie en haar institutionele omgeving. Maar ook het opbouwen van een soort coalitie tussen organisaties kan zorgen voor meer stabiliteit (Pfeffer en Salancik, 1978). Het komt immers nauwelijks voor dat een organisatie compleet autonoom is of juist compleet afhankelijk van haar omgeving.

Een derde theorie is de *ecology population theorie*. Deze theorie gaat uit van een proces van natuurlijke selectie, waarin een organisatie probeert te overleven binnen haar omgeving. Zij zal in haar overleven moeten concurreren met anderen, en in dit streven past zij zich aan haar omgeving aan (Hannan en Freeman, 1984). Binnen deze traditie onderzoekt men het faillissement en de oprichting van nieuwe organisaties, evenals de organisatorische groei. Om binnen haar populatie te kunnen overleven zal een organisatie zich aanpassen of ‘evolueren’. Hierdoor zal een organisatie via druk van buitenaf uiteindelijk een vorm aannemen die het beste past binnen haar omgeving. De theorie stelt dat organisaties die het beste aansluiten bij de verwachtingen van de omgeving degenen zijn die overleven, zij zijn dan geëvolueerd door middel van natuurlijke selectie en hebben het vertrouwen van de omgeving gewonnen. Organisaties die sterk moeten veranderen om aan de verwachtingen van de omgeving te kunnen te voldoen, hebben een grotere kans dat zij niet zullen overleven. De ecology population theorie stelt dat het proces van verandering zelf voor vernietiging van de organisatie zal zorgen. Wanneer een organisatie zich meer en meer aanpast aan haar omgeving verliest ze haar betrouwbaarheid en legitimiteit en wordt ze door middel van natuurlijke selectie ernstig aangetast in haar overlevingskansen. Binnen de ecologische economie wordt de instabiliteit en complexiteit van natuurlijke en sociale systemen zoals het milieu, technologie, bevolking en cultuur erkend. Ondanks de erkenning hiervan is er bij de ecology population theorie weinig aandacht voor institutionele variabelen, zoals regelgeving of het politieke klimaat (Zucker, 1987).

De ecology population theorie gaat er dus vanuit dat organisaties die bij voorbaat voldoen aan de verwachtingen en eisen van de omgeving betere overlevingskansen hebben dan organisaties die sterk moeten veranderen. Sterke veranderingen tasten de legitimiteit en

betrouwbaarheid van een organisatie aan. Dit staat in contrast met zowel de institutionele als de resource dependency theorie. Volgens deze theorieën zullen organisaties die zich sterk aanpassen juist grotere overlevingskansen hebben. Bij de institutionele theorie gaat men ervan uit dat een organisatie juist goede overlevingskansen heeft wanneer zij zich aanpast aan haar omgeving en er sprake is van isomorfisme. Dit verwijst naar een proces waarin organisaties steeds meer op elkaar gaan lijken en dezelfde vorm aannemen. Organisaties die zich goed kunnen aanpassen aan hun omgeving, hebben grotere overlevingskansen. Het verschil tussen resource dependency en institutionalisme is lastig aan te geven. Bij institutionalisme gaat men er immers ook vanuit dat een organisatie afhankelijk is van haar omgeving. Bij de resource dependency theorie is het echter van belang dat de afhankelijkheid van de organisatie van haar omgeving een niet institutionele is. Dit houdt in dat de afhankelijkheid alleen kan bestaan uit afhankelijkheid van bronnen en middelen uit de private sfeer en niet van de overheid (Zucker, 1987). Bij het institutionalisme is een organisatie afhankelijk van de steun van haar omgeving. Economische bronnen en middelen kunnen haar autonomie wel vergroten, maar zullen de afhankelijkheid van een organisatie niet wegnemen.

De noodzaak rekening te houden met de institutionele omgeving kan voor een organisatie grote gevolgen hebben. Het kan immers grote veranderingen binnen de aard en de doelstellingen van de organisatie met zich mee brengen en deze veranderingen kunnen de effectiviteit van de organisatie ondermijnen. Wanneer organisaties niet reageren op druk vanuit de omgeving, overleven zij niet. Er zijn verschillende strategieën die een organisatie, al dan niet bewust gebruikt om met de (veranderende) omgeving om te kunnen gaan. In paragraaf 2.3 ga ik hier verder op in en bespreek ik verschillende typologieën van strategieën.

2.3 Strategieën

Er is een aantal aanpassingsstrategieën die organisaties kunnen gebruiken om hun legitimiteit te bewaren. Deze zijn onder te brengen in een aantal verschillende typologieën die ik hieronder zal behandelen.

Proactieve versus reactieve strategieën

De proactieve strategieën worden beschreven door Hasenfeld (1983). Volgens Hasenfeld proberen organisaties hun afhankelijkheid van de omgeving te verminderen en de greep op andere organisaties te vergroten. De manier waarop ze dit doen hangt af van de positie die zij vervullen in de omgeving. Hasenfeld onderscheidt vier verschillende strategieën om de greep op de omgeving zoveel mogelijk te vergroten. Deze strategieën zijn eenzijdig, omdat de organisatie probeert haar omgeving te beïnvloeden. De omgeving zelf heeft volgens Hasenfeld geen invloed op het handelen van de organisatie (Hasenfeld, 1983). Hieronder staan de vier eenzijdige strategieën zoals door Hasenfeld omschreven.

De eerste strategie is het gebruik van *autoriteit*. Zodra een organisatie autonomie heeft over haar financiën en een dominante positie inneemt in haar sociale netwerk, kan ze zelf eisen gaan stellen aan haar omgeving. Deze strategie brengt weinig kosten met zich mee en de voordelen kunnen zeer groot zijn. Het kan echter ook symbolisch isomorfisme of openlijk verzet van andere partijen uitlokken. Wanneer een partij immers autoriteit heeft, kunnen andere partijen ervoor kiezen dezelfde vorm aan te nemen (isomorfisme) of juist in verzet komen tegen deze autoriteit. Zoals gezegd is een dominante positie een voorwaarde voor het gebruik van autoriteit.

Een tweede strategie is die van *competitie.* Deze strategie vindt plaats tussen meerdere min of meer gelijkwaardige partijen. Door competitie aan te gaan kan een organisatie haar macht vergroten, omdat de service aantrekkelijker wordt. Wanneer prijs en kwaliteit verbeteren en een organisatie anderen kan wegconcurreren, wordt haar invloed alsmaar groter. Echter, niet bij alle organisaties is de prijs en de kwaliteit zo expliciet te meten. Hierbij draait concurrentie meer om het imago dat gecreëerd wordt. Competitie zorgt hiernaast ook voor het scherp houden van organisaties; het moedigt innovaties aan en geeft klanten meer opties. Een organisatie zal competitie aangaan wanneer zij denkt een sterke positie te hebben en dus een grote kans heeft door competitie een nog sterkere positie te krijgen. Een organisatie met een zwakke positie zal niet snel kiezen voor de strategie van competitie. Wanneer een organisatie een machtspositie weet in te nemen, heeft zij een sterke positie en kan deze strategie positief zijn voor een nog sterkere positie.

De derde strategie is die van *coöperatie*. Door met andere organisaties samen te werken kan de organisatie delen in de kennis en expertise die de andere organisaties te bieden hebben. Er

zijn drie verschillende manieren om coöperatie uit te voeren, namelijk via contracten, coalities of coöptatie. Wanneer een organisatie een sterke positie heeft binnen haar institutionele omgeving zal de strategie van coöperatie niet vaak gebruikt worden. Zij is immers weinig afhankelijk van andere organisaties en ziet dus geen voordelen in een samenwerking, omdat dit de autonomie van de organisatie aantast.

Met een *contract* zorgen beide organisaties voor minder afhankelijkheid van hun omgeving; dit is de meest voorkomende vorm van coöperatie. Deze vorm reduceert onzekerheid, omdat een contract verplichtingen voor alle partijen vastlegt.

Bij een *coalitie* worden hulpbronnen van verschillende organisaties samengebracht in een joint venture. Coalities zijn moeilijk te vormen, het is een kostbare manier van samenwerken (denk aan bijvoorbeeld de kosten voor communicatie tussen de organisaties).

Bij *coöptatie* worden elementen van een organisatie gecoöpteerd door een andere organisatie, zodat de organisatie haar legitimiteit kan behouden. Er wordt een stukje autonomie ingeleverd in ruil voor steun van de organisatie. De andere organisatie ruilt haar legitimiteit, geld en kennis in voor invloed op de organisatie. Maar coöptatie kan ook voorkomen wanneer een organisatie haar legitimiteit ziet verdwijnen. In dit geval is het niet zo dat een organisatie zelf haar greep op de omgeving wil vergroten. Zij moet zich aanpassen door middel van coöptatie om haar legitimiteit te behouden. Een voorbeeld hiervan wordt gegeven door Pruijt (2004) wanneer hij schrijft over de krakerbeweging. Een vorm van aanpassing is coöptatie, waarbij een organisatie of beweging bepaalde heersende ideeën zal moeten internaliseren om steun vanuit de institutionele omgeving te behouden en de overlevingskansen te vergroten. Wanneer de woningnood wordt opgelost, zullen krakers altijd bereid moeten zijn te onderhandelen met de overheid, omdat dit de enige manier is om te kunnen behouden wat bereikt is. Zonder woningnood is er immers weinig reden voor de overheid om krakerbewegingen te gedogen en komt de overleving van deze organisaties in gevaar. Een goed voorbeeld van coöptatie is te zien in de geschiedenis van de krakerbewegingen in Groot Brittannië. Daar werd de krakerbeweging getransformeerd in een beweging die voor korte periodes accommodatie verhuurde; hierdoor werd het kraken deels legaal gemaakt. Vanwege de samenwerking van krakers met de lokale autoriteiten kregen zij medeverantwoordelijkheid en verdween de identiteit van de krakerbeweging. In dit geval is dus sprake van coöptatie van de krakers door de lokale autoriteiten.

De vierde en laatste strategie is de *disruptieve* strategie. Deze strategie houdt in dat een

organisatie andere organisaties in haar omgeving aanvalt. De organisatie kan deze strategie gebruiken om voldoende macht te verkrijgen bij onderhandelingen, haar geloofwaardigheid te vergroten, meer bekendheid te verwerven om zodoende steun te krijgen of om derden bij de organisatie te betrekken. Om deze strategie succesvol te maken is een aantal aspecten van belang. Zo moet de organisatie bijvoorbeeld wel over voldoende middelen beschikken om de aanval lang genoeg te kunnen volhouden, zodat deze ook daadwerkelijk effectief is. Wanneer een organisatie een sterke machtspositie heeft binnen haar institutionele omgeving zal ze deze strategie niet snel gebruiken, omdat ze weinig afhankelijk is van de druk van haar omgeving. Het is een riskante strategie, dus een organisatie die een sterke positie inneemt hoeft en zal geen risico's nemen.

De proactieve strategieën zijn nu besproken. Hier tegenover staat een aantal reactieve strategieën die hieronder besproken zullen worden.

De reactieve typologie heeft betrekking op de theorie van Janet Gilboy (1995). Gilboy maakt een onderscheid tussen directe en indirecte strategieën, of openlijke en verborgen strategieën. Deze strategieën zijn reactief, omdat organisaties die gebruik maken van deze strategieën, reageren op druk vanuit de omgeving. Gilboy beschrijft drie ideaaltypen die gebruikt kunnen worden door organisaties om zich aan te passen. De eerste is *accomodation*. Bij accomodation laten beleidsmakers binnen organisaties zich direct en openlijk beïnvloeden door druk vanuit de omgeving van partijen die daar niet toe gerechtigd zijn. Reden hiervoor is dat organisaties afhankelijk zijn van hun omgeving en er dus baat bij hebben deze omgeving tevreden te stellen. Deels zullen leden van organisaties toegeven aan externe druk, omdat ze verwachten hier in de toekomst iets voor terug te zullen krijgen, of ze geloven dat hun eigen positie binnen de organisatie hierdoor verbeterd zal worden (Gilboy, 1995). Maar ook politieke macht speelt hierbij een rol. Vooral organisaties die gecontroleerd worden door de overheid gebruiken vaak de strategie van accomodation. Zij zullen eerder toegeven aan bijvoorbeeld politieke druk. Een goed voorbeeld van accomodation is druk vanuit de media. Wanneer de media bepaalde, naar hun mening, misstanden aan de kaak stelt kunnen organisaties zich genoodzaakt voelen aandacht te besteden aan dit onderwerp. Dit zag je bijvoorbeeld bij de media aandacht voor Stichting Jeugdzorg, toen er grootschalig intern onderzoek naar jeugdvoogden werd verricht na berichten in de media over het tekortschieten van de voogden.

Er zijn verschillende studies die zowel beïnvloeding als het niet beïnvloed worden van organisaties van buitenaf proberen aan te tonen. De conclusies hebben deels te maken met de afhankelijkheid van de organisatie; wanneer steun vanuit de omgeving van cruciaal belang is zal een organisatie ook eerder zwichten voor accomodation (Gilboy, 1995). Maar Gilboy geeft ook aan dat niet alleen de afhankelijkheid hierbij een rol speelt. Het ligt deels ook aan de structuur van een organisatie, bijvoorbeeld de mate van transparantie en samenwerking met andere organisaties. Wanneer deze samenwerking bijvoorbeeld vrijwillig is, is er een grotere kans dat de organisatie zich laat beïnvloeden, omdat de samenwerkende organisatie de samenwerking kan stopzetten wanneer het voor hen geen vruchtbare samenwerking meer is. Ook komt accommodation minder vaak voor in organisaties waar beslissingen zichtbaar en transparant zijn naar de omgeving toe (Gray, 1969). Dit is nog meer het geval wanneer er sprake is van een tegenpartij die kritiek levert. Wanneer een organisatie toegeeft aan druk van partijen die hier niet toe gerechtigd zijn, kan deze tegenpartij immers schade aanbrengen door kritiek te leveren. Een goed voorbeeld hier van is de paspoortaffaire waarbij toenmalig minister van Vreemdelingenzaken, Rita Verdonk, weigerde om voetballer Salomon Kalou versneld een paspoort te geven zodat hij uit zou kunnen komen voor het Nederlandse elftal tijdens het WK 2006. Er was sprake van druk vanuit de media en de voetbalwereld om aan Kalou's verzoek te voldoen. Verdonk kon echter niet toegeven aan deze druk, omdat haar politieke tegenstanders haar beleid als inconsistent hadden kunnen bestempelen als zij Kalou versneld een paspoort zou hebben gegeven. Verdonk stond immers bekend om haar rechtlijnigheid. Het feit dat haar beslissing transparant was, zorgde ervoor dat het voor haar moeilijk werd om accomodation als strategie te gebruiken.

Een tweede strategie is *amplification*. Deze strategie is minder direct en opvallend, reacties volgen niet direct op druk van buitenaf. Beslissingen worden genomen met inachtneming van reacties van derden en de eventuele consequenties voor de organisatie nu of in de toekomst (Gilboy, 1995). Door hierop te anticiperen worden acties en beslissingen beïnvloed, zonder dat zeker is dat deze invloed er ook daadwerkelijk zal zijn. Er zijn verschillende manieren waarop een organisatie dit kan doen. Zo kunnen werknemers besluiten bepaalde acties niet uit te voeren uit angst geen steun te krijgen van hun superieuren. De superieuren hoeven dus geen druk uit te oefenen, omdat de werknemers zelf de consequenties van bepaalde acties voorzien. Gilboy geeft een voorbeeld van de vleesverwerkende industrie. Inspecteurs treden niet op tegen overtredingen,

omdat ze denken hier niet voldoende steun voor te krijgen van hun superieuren. De industrie of de bedrijven hoeven zelf geen invloed uit te oefenen, de inspecteurs handelen zelf al met positief resultaat voor de bedrijven (Gilboy, 1995). Een andere manier is het negeren van bepaalde onderwerpen, omdat de praktijk soms andere dingen vereist dan de wet voorschrijft. Bij een dienstverlenende organisatie kan dit zich uiten in het mijden van bepaalde onderwerpen die gevoelig liggen bij de personen waarvan de organisatie van afhankelijk is. Gilboy geeft een voorbeeld over grensbewaking tussen de Verenigde Staten en Mexico. De immigratiedienst moet een verplicht percentage mensen bij binnenkomst in de Verenigde Staten controleren, maar de meerderheid wordt gewoon doorgelaten. De grensbewakers voelen enerzijds druk om de immigratiewetgeving te handhaven, maar anderzijds vereist in dit geval de praktijk andere dingen dan de wet voorschrijft. De druk om de doorstroom van binnenkomers niet te vertragen is groter dan het bewaken van veiligheid. Deze veiligheid wordt in dit geval genegeerd. Het negeren van bepaalde onderwerpen kan ook zorgen voor een beter imago van de dienstverlenende organisatie, ook dit is een voorbeeld van amplificatie (Gilboy, 1995). Deze strategie zorgt niet direct en per se voor beïnvloeding, maar moet altijd worden gezien in de context van de situatie waarin een organisatie zich bevindt. Amplificatie is duidelijk een indirecte, minder openlijk strategie.

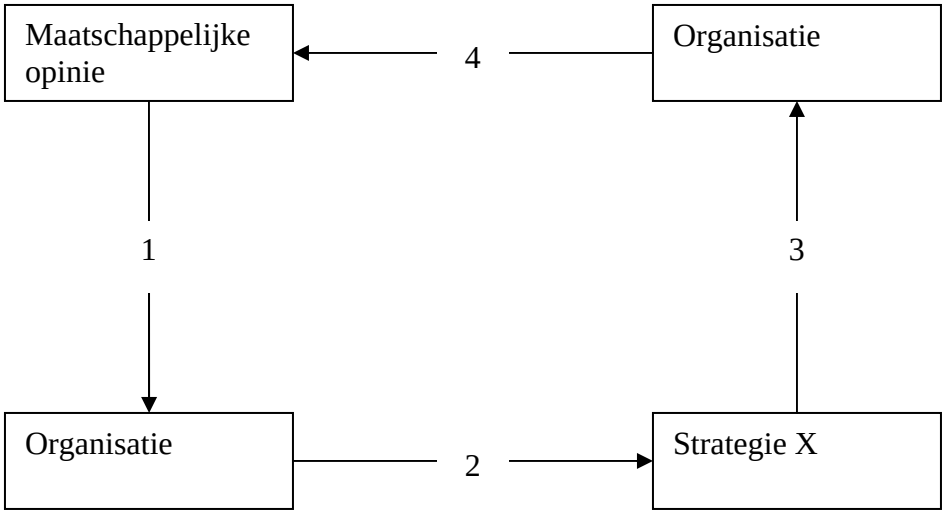
De derde strategie die Gilboy beschrijft is *assimilation*. Deze vorm is nog indirecter dan amplificatie. Bij assimilatie worden beslissingen en acties afgestemd op de mening van de sociale omgeving. Zo spelen professionals in op het ritme van de activiteiten van de organisatie (Gilboy, 1995). Een voorbeeld hiervan is de inspectie van horeca, die plaatsvindt buiten de drukke uren om de productie niet in de weg te zitten. Ook deze strategie valt onder de verborgen strategieën en is, nog meer dan amplificatie, moeilijk te herkennen (Gilboy, 1995).

Wederzijdse aanpassing; zowel proactief als reactief

De hiervoor besproken strategieën zijn eenzijdige strategieën. Mohr en Guerra-Pearson (2005) stellen echter dat organisaties geen eenzijdige beïnvloeding kennen, omdat zijzelf deel uitmaken van de institutionele omgeving. Zij spreken dan ook over wederkerige strategieën, waarbij de omgeving en de organisatie elkaar beïnvloeden.

Mohr en Guerra-Pearson stellen dat sociale structuren organisatorische vormen produceren, maar ook de vorm produceert structuur. Binnen de organisatiesociologie werd eerst

alleen gekeken naar hoe een organisatie haar omgeving beïnvloedde, maar later in de tijd kwam er meer aandacht voor hoe een institutionele omgeving het karakter van een organisatie beïnvloedt (Mohr en Guerra-Pearson, 2005). Er is geen sprake van een discussie of de organisatie haar omgeving beïnvloedt of andersom, beide theorieën zijn waar.
Verschillende organisaties kunnen in dezelfde institutionele omgeving opereren, maar toch een andere vorm hebben. Dit leidt tot sterke concurrentie. De vorm die een organisatie aanneemt zegt iets over de waarde die zij vertegenwoordigt. Een voorbeeld hiervan is armoedebestrijding. Er zijn verschillende vormen van armoedebestrijding en uit de vorm kun je opmaken welke waarden de organisatie uitdraagt. Zo waren er tot in de 19e eeuw armenhuizen waar mensen terecht konden. Deze armenhuizen waren in beginsel christelijke instanties. In de opvanghuizen diende men zich aan te passen aan de normen en waarden die daarbinnen golden. De christelijke waarde van naastenliefde kreeg vorm in de verschijning van armenhuizen. Deze concrete vorm verspreidt op haar beurt ook weer de waarde die vertegenwoordigd wordt. De armenhuizen zelf zorgden weer de verspreiding van christelijke waarden. Op deze manier is er dus sprake van een wederzijdse beïnvloeding. Tot in de negentiende eeuw waren armenhuizen de manier om christelijke waarden in een organisatie te uiten. Wanneer het ideologische beginsel verandert, verandert de organisatorische vorm daarin mee. Armenhuizen bestaan allang niet meer, de collectieve verantwoordelijkheid van de samenleving heeft dit overgenomen en dit zien we terug bij de huidige bijstandsverlening.
Centraal in dit artikel van Mohr en Guerra-Pearson staat dat sommige instanties zijn gevormd door waarden uit de samenleving (zoals christendom of socialisme), terwijl de instanties tegelijkertijd ook deze waarden proberen te verspreiden in de vorm van opvanghuizen (christendom) en politieke bewegingen (socialisme). Ze streven echter elk op hun eigen manier dezelfde waarde van armoedebestrijding na. Belangrijk is het feit dat er verschillende instanties zijn die op verschillende manieren dezelfde waarden willen verspreiden of beschermen.
Wederzijdse beïnvloeding kun je op de volgende manier schematisch weergeven:



Bovenstaande is een conceptueel model dat grofweg beschrijft hoe maatschappij en organisatie elkaar beïnvloeden. Wanneer de maatschappelijke opinie verandert, kan dit zijn doorwerking hebben op de organisatie. (punt 1). Zij kan bijvoorbeeld door het actief leveren van kritiek druk uitoefenen op deze organisatie. Maar ook door juist passief een organisatie te negeren of geen beroep hierop te doen kan een organisatie door de maatschappij geraakt worden. In het voorbeeld van armoedebestrijding kun je stellen dat de maatschappelijke opinie is dat armoedebestrijding gewenst is. Wanneer deze druk groot genoeg is, zal de organisatie actie moeten ondernemen om hier iets aan te doen. Dit leidt tot handelen volgens strategie X (punt 2). Zo kan een organisatie bijvoorbeeld proberen haar takenpakket uit te breiden of via de media een ander beeld neer te zetten om haar imago te verbeteren. Een christelijke organisatie kan bijvoorbeeld kiezen voor armenhuizen als gevolg van de waarde van naastenliefde. Een socialistische organisatie die meer gericht is op collectieve verantwoordelijkheid kan kiezen voor de invoering van bijstand. Deze strategie wordt eigen gemaakt door de organisatie, waardoor zij in meer of mindere mate verandert (punt 3). Soms zijn deze veranderingen amper zichtbaar of is er zelfs geen sprake van verandering, maar is alleen de beeldvorming van de samenleving over de organisatie veranderd. Maar het kan ook zijn dat de organisatie bijvoorbeeld haar takenpakket heeft uitgebreid of op een andere manier omgaat met burgers, politici of de media. De christelijke of socialistische organisaties hebben zich op een eigen manier hun strategie teneinde armoede tegen te gaan eigen gemaakt. De christelijke organisatie door het opzetten van armenhuizen en de socialistische organisatie door de invoering van bijstand. Deze verandering in de organisatie kan er vervolgens

voor zorgen dat het beeld van de samenleving over de organisatie verandert (punt 4). Op deze manier oefent de organisatie weer invloed uit op de maatschappelijk opinie. Zo kan de samenleving herwaardering krijgen voor de waarde die een organisatie uitdraagt. De armenhuizen dragen de christelijke waarde van naastenliefde uit en hier kan waardering voor komen vanuit de samenleving. Ditzelfde geldt voor de socialistische organisatie; invoering van bijstand kan bijdragen aan meer steun voor het gevoel van armoedebestrijding met collectieve verantwoordelijkheid. Wanneer deze opinie wederom bijgesteld wordt, begint de cyclus weer bij punt 1. Op deze manier blijven organisaties zich aanpassen om te kunnen inspelen op veranderende maatschappelijke aspecten. Het is ook mogelijk dat organisaties juist preventief proberen de maatschappelijke opinie te beïnvloeden. In dit geval begint de cirkel niet bij 1, maar bij het handelen volgens strategie X (punt 2).

Symbolische aanpassing

Een derde typologie van strategieën is feitelijke versus symbolische aanpassing, zoals beschreven door Meyer en Rowan (Meyer en Rowan, 1977. Uit Lammers e.a. 1983). Bij feitelijke aanpassing kan men stellen dat een organisatie van binnenuit beleidsmatig daadwerkelijk veranderd is en zich aangepast heeft. De aanpassing heeft in dit geval feitelijke consequenties voor het werk van de organisatie. Een symbolische aanpassing daarentegen vindt alleen plaats aan de buitenkant van de organisatie, maar verandert niets binnen de organisatie zelf. Meyer en Rowan betogen dat uiterlijke organisatiekenmerken, zoals procedures en regelingen slechts ‘gerationaliseerde mythen’ zijn. Ze lijken rationeel binnen hun institutionele omgeving, maar gelden eigenlijk als een soort keurmerk voor een betrouwbare organisatie. De organisatie probeert de schijn te wekken van betrouwbaarheid. Door het in stand houden van deze mythen vergroten de organisaties hun legitimiteit en daarmee hun overlevingskansen (Meyer en Rowan, 1977. Uit Lammers e.a. 1983). Hier is duidelijk sprake van een symbolische aanpassing en geen feitelijke. Een organisatie die gebruik maakt van standaardprocedures en gestructureerde regelgeving kan door de omgeving als legitiem worden geacht. Het feit dat zij deze structuur of juridisering hanteert hoeft echter niet te betekenen dat de structuur van de organisatie zelf ook daadwerkelijk veranderd is. Bij symbolische aanpassing ontstaat er een scheiding tussen het primaire proces van het uitgeoefende werk en de formele structuur van uitoefening van het werk. Hierdoor komen de

beleidsplannen en de feitelijke praktijk niet met elkaar overeen. Een voorbeeld van symbolische aanpassing kun je zien in het kader van discriminatie op de arbeidsmarkt. Uit onderzoek van Veld en Kruisbergen ‘Een gekleurd beeld’ uit 2002 blijkt dat een kwart van de werkgevers liever geen allochtone werknemer in dienst neemt (Veld en Kruisbergen, 2002). Vanuit sociaal wenselijk en wettelijk oogpunt zal een werkgever dit echter niet openlijk uiten in de vacature of tijdens de sollicitatie. In plaats daarvan kan hij allochtone werknemers afwijzen op basis van irrelevante eigenschappen (indirecte discriminatie), zoals de eis de Nederlandse taal foutloos te kunnen spreken voor functies waarvoor dit niet noodzakelijk is. De werkgever lijkt zich naar buiten toe te conformeren aan de wet waarin discriminatie op basis van etniciteit verboden is, maar dit is slechts schijn.

Voornamelijk non-profit organisaties kunnen op deze manier handelen, omdat hun verdiensten vaak moeilijk meetbaar zijn en zij geen concurrentie ondervinden van de markt. Meyer en Rowan komen er alleen niet uit in hoeverre dit een bewuste of onbewuste strategie is die wordt gehandhaafd (Meyer en Rowan, 1977. Uit Lammers e.a. 1983).

Een verdere uitwerking van het werk van Meyer en Rowan is geschreven door DiMaggio en Powell. Zij richten zich op het isomorfisme, wat ze beschrijven als een proces waarbij organisaties steeds meer op elkaar gaan lijken (iso = hetzelfde, morf = vorm). Ze onderscheiden twee soorten isomorfisme (DiMaggio en Powell, 1983. Uit Lammers e.a, 1983). De eerste vorm is competitief isomorfisme. In een samenleving van vrije concurrentie overleeft alleen de sterkste organisatie. De structuur van die organisatie wordt overgenomen door anderen, omdat de ‘zwakke’ structuren niet kunnen blijven voortbestaan.

Het institutionele isomorfisme is een proces waarbij organisaties zich conformeren aan hun institutionele omgeving en zo steeds meer op elkaar gaan lijken. De eisen en verwachtingen van de omgeving kunnen helemaal los staan van de eigen doelmatigheid van de organisatie. Er zijn drie mechanismen die institutioneel isomorfisme kunnen veroorzaken:

- Afgedwongen isomorfisme. Een organisatie of de maatschappij kan druk uitoefenen op andere organisaties om zo op een doelbewuste manier invloed uit te oefenen. Dit kan bijvoorbeeld gebeuren wanneer een organisatie financieel afhankelijk is van anderen. Door subsidievoorwaarden te veranderen kan invloed worden uitgeoefend.
- Isomorfisme door imitatie. Wanneer organisaties twijfelen over de effectiviteit van hun eigen structuur kunnen ze kijken naar succesvolle soortgelijke organisaties en deze

structuur overnemen. Deze aanpassing gebeurt soms zeer bewust, maar soms ook onbewust.

- Normatief isomorfisme. Door een sterke toename van deskundigen en hoogopgeleiden is er ook sprake van meer homogeniteit van organisaties. Al deze hoogopgeleiden hebben immers eenzelfde studie genoten met soortgelijke organisatietheorieën. Doordat dezelfde kennis wordt gedeeld door de deskundigen, gaan organisaties intern steeds meer op elkaar lijken.

Isomorfisme kan een symbolisch karakter hebben. Organisaties kunnen zich aanpassen aan anderen, zodat ze een goede indruk kunnen maken. DiMaggio en Powell geven een voorbeeld over onderwijs. Zij geven aan dat de meeste scholen bij het bepalen van beleid in eerste instantie kijken naar andere scholen die succesvol zijn. Zij nemen deze werkwijze over, niet zozeer omdat deze effectief lijkt, maar omdat deze werkwijze een goed imago heeft. Hier is dus sprake van isomorfisme met een symbolisch karakter, wat uiteindelijk tot verbetering van het onderwijs leidde.

2.4 Conclusie

Een organisatie is afhankelijk van steun vanuit de omgeving van die organisatie. Voor een organisatie die opereert in een institutionele omgeving houdt dit net name in dat de omgeving belang hecht aan de waarde die de organisatie vertegenwoordigt. Op die manier behoudt een organisatie haar legitimiteit. De strategieën die organisaties toepassen om hun legitimiteit te bewaren, kunnen variëren. Zo is er het onderscheid tussen proactieve en reactieve strategieën, waarbij proactieve strategieën erop gericht zijn de greep op de omgeving zo groot mogelijk te maken en zijn reactieve strategieën een reactie op druk vanuit de omgeving. Daarnaast is er de wederkerige beïnvloeding, waarbij beïnvloeding zowel door de organisatie als door de omgeving plaatsvindt. Dit is dus een combinatie van proactieve en reactieve strategieën. Ten slotte, kan onderscheid worden gemaakt tussen feitelijke aanpassing, waarbij de organisatie van binnenuit beleidsmatig daadwerkelijk verandert, en symbolische aanpassing, die alleen aan de buitenkant van de organisatie plaatsvindt en niets binnen de organisatie zelf verandert. Voordat we verder

gaan met de strategieën die gebruikt zijn door de door mij geselecteerde organisaties, zal ik in het volgende hoofdstuk mijn caseselectie uiteenzetten.

Hoofdstuk 3; Cases en Dataverzameling

Voor de caseselectie heb ik organisaties geselecteerd die zich allemaal op hun eigen manier bezighouden met privacybescherming. Het zijn organisaties die binnen een institutionele context werken en dus afhankelijk zijn van hun omgeving. In mijn caseselectie zijn twee dimensies te onderscheiden die zorgen voor vier typen organisaties. Door de organisaties op deze manier te onderscheiden kan men beter bekijken hoe verschillende organisaties reageren op maatschappelijke veranderingen. Het is immers goed mogelijk dat niet ieder type organisatie op dezelfde manier reageert op veranderingen. De eerste dimensie betreft de omgeving waarin de organisaties zich bevinden, namelijk een institutionele of een technische omgeving. Binnen een institutionele omgeving wordt legitimiteit niet zozeer verworven dankzij technische resultaten van een organisatie (input en output), maar is zij meer het resultaat van bepaalde symbolische activiteiten. Het is, zoals eerder gezegd, voor een organisatie ook mogelijk in zowel een institutionele als een technische omgeving te opereren. Vanuit deze dimensie kun je enerzijds organisaties die geheel in een institutionele omgeving werken, onderscheiden; anderzijds zijn er organisaties die naast de institutionele omgeving ook in een technische omgeving opereren. De tweede dimensie betreft de doelgroep die de organisaties hebben, namelijk een specifieke of een algemene doelgroep. Hieronder heb ik de indeling schematisch weergegeven.

Institutioneel

Specifiek	1) DeVrijePsych	2) CBP Stichting Privacyloket.nl
	3) NIVRA NOREA	4) OBA Privacy Management Groep

Algemeen

Zowel institutioneel als technisch

De cellen 1) en 2) zijn organisaties die zich inzetten voor het behoud van privacy en hiermee een maatschappelijke rol vervullen, namelijk het bijstaan van burgers. Zij vertegenwoordigen de waarde van privacybescherming en proberen deze waarde te verdedigen. Omdat deze organisaties een waarde verdedigen en een maatschappelijke rol vervullen, zijn zij gevoelig voor veranderingen. Deze organisaties zien veranderingen in de maatschappij waarschijnlijk als bedreigend. De doelgroep die zij willen bereiken kan zowel algemeen als specifiek zijn. DeVrijePsych heeft in eerste instantie een specifieke doelgroep, namelijk psychotherapeuten en psychiaters. Het CBP en Stichting Privacyloket.nl richten zich op de hele samenleving en hebben dus een algemene doelgroep.

De cellen 3) en 4) zijn organisaties die andere organisaties ondersteunen en wijzen op hun plicht te voldoen aan de wettelijke bepalingen van de privacywetgeving. Zij vervullen geen maatschappelijke rol waarin ze burgers bij willen staan en doen ook geen pogingen de waarde van privacybescherming te verdedigen. De organisaties bestaan omdat wettelijke verplichtingen hen een markt bieden om winst te maken. Wanneer organisaties en bedrijven weinig aandacht hebben voor privacy, kunnen zij hierop inspelen. Het NIVRA en de NOREA zijn beroepsorganisaties en richten zich op hun specifieke achterban. OBA Privacy Management Groep heeft een algemene doelgroep, zij kunnen iedere denkbare organisatie benaderen.

Hieronder worden de zes geïnterviewde organisaties besproken. Bij het CBP wordt iets uitgebreider stilgestaan. Het CBP is namelijk de belangrijkste speler bij privacybescherming. Alle vijf andere organisaties hebben in meer of mindere mate te maken met het CBP. Dit zal ook blijken uit de interviews, het CBP kwam bij ieder interview ter sprake en eenieder heeft ook een mening over het CBP.

3.1 Het College Bescherming Persoonsgegevens

Het CBP is een organisatie die binnen een institutionele context opereert. In het vorige hoofdstuk is gebleken dat een organisatie die opereert in een institutionele omgeving afhankelijk is van deze omgeving. Om haar legitimiteit te kunnen blijven garanderen zal een organisatie strategieën moeten gebruiken, zodat ze met haar omgeving mee kan gaan of haar omgeving zelf kan beïnvloeden. Het CBP is inmiddels een boegbeeld geworden voor de bescherming van privacy.

Zij heeft als belangrijkste taak het toezicht houden op naleving van de wetten met betrekking tot bescherming van persoonsgegevens (de Wet bescherming persoonsgegevens (WBP), de Wet politieregisters (Wpolr) en de Wet gemeentelijke basisadministratie (Wet GBA)). Daarnaast houdt deze instantie zich bezig met het geven van advies met betrekking tot wetgeving en beleidsvorming, het doen van onderzoek naar nieuwe ontwikkelingen, het toetsen van gedragscodes, klachtenbehandeling en internationale zaken. Het College dient zich te houden aan normen die worden gesteld in de Algemene wet bestuursrecht. Op deze manier worden de taken en bevoegdheden van het CBP op een legitieme manier afgebakend.

De afhankelijkheid van het CBP van haar omgeving kan in eerste instantie discutabel lijken; het bestaansrecht van het CBP is vastgelegd in de wet. Het is een instantie die door de overheid is ingesteld en moet voldoen aan een aantal Europese richtlijnen. Desondanks dit is het wel degelijk van groot belang voor het CBP om legitimiteit vanuit de samenleving te krijgen. Het CBP heeft immers de taak de privacy van de burgers te beschermen en zonder de steun van deze burgers wordt het moeilijk voor het CBP haar taken te kunnen blijven uitoefenen. Naast de morele afhankelijkheid van de sociale omgeving is het CBP financieel afhankelijk van de overheid. Dit kan zorgen voor druk op het CBP voor het uitoefenen van haar taken. Wanneer privacy binnen de politiek op een lager plan wordt gezet, kan dit gevolgen hebben voor de financiële middelen die beschikbaar worden gesteld aan het CBP. Met een krap budget is het vaak lastiger om alle taken goed te kunnen blijven uitoefenen. Wanneer blijkt dat het CBP haar taken niet goed uitoefent, kan ook dit een deuk in haar legitimiteit veroorzaken.

Uit het voorgaande blijkt dat het CBP afhankelijk is van de heersende moraal over privacy binnen de samenleving. In periodes van een veranderende opinie over privacy heeft dit invloed op de rol van het CBP. Het CBP geeft zelf aan zich zorgen te maken over de waarborging van privacy in de toekomst. Het komt steeds vaker voor dat bestuurders, politici en belangengroepen privacybescherming zien als iets wat alleen maar een obstakel is (Kohnstamm, 2004). Het lijkt erop dat de dreiging van terrorisme en een toenemende (aandacht voor) onveiligheid op straat de overhand krijgen en privacy hiervoor moet wijken. Maar ook de koppeling van bestanden van organisaties en het toenemende gebruik van Internet doen de privacy geen goed. Het gebruik van Internet is razend populair en een kritische blik van het CBP wordt vaker als obstakel dan als positief gezien (CBP, 2004). Dit heeft negatieve gevolgen voor het CBP; wanneer privacybescherming gezien wordt als obstakel, kan het voor een instantie die opkomt voor deze

privacy moeilijk zijn steun te vinden binnen de samenleving. Ook in dit geval zal het CBP strategieën moeten toepassen om toch steun te krijgen. Het CBP is dan ook een geschikte case voor dit onderzoek. Het is een organisatie die een bepaalde waarde vertegenwoordigt en een maatschappelijke taak vervult. Het is dan ook interessant te onderzoeken wat deze organisatie doet wanneer deze waarde onder druk komt te staan.

3.2 Stichting Privacyloket.nl

Stichting Privacyloket.nl heeft als doel privacy van burgers te garanderen bij het verwerken van persoonsgegevens. Zo ondersteunt het Privacyloket burgers bij hun recht op verzet en hun recht op privacybescherming. Zij dient daarnaast als vraagbaak voor individuele burgers die vragen hebben over privacy. Een andere doelstelling is organisaties die een probleem hebben, voor te lichten over hoe ze dit het beste kunnen oplossen en. Verder houdt Stichting Privacyloket.nl zich bezig met de bewustwording en informatieoverdracht van privacy naar de burgers en werknemers toe. Tevens treedt zij op als mediator tussen de burger en bedrijven. Ze probeert in kaart te brengen waar zich problemen voordoen en probeert rechtzaken en boetes te voorkomen en met name juist oplossingen te zoeken voor deze problemen (Bron: www.privacyloket.nl). Stichtingsbestuurder Geert Klei zegt over de Stichting Privacyloket.nl:

> *'We zijn een instantie die als een soort ombudsman mogelijke vragen op het gebied van privacy accepteert en daarin op anonieme wijze namens een burger kan optreden richting een partij die zwaar doelbewust is om mensen op afstand te houden, of mensen in het gareel te houden. Wanneer bepaalde instanties meerdere malen over de schreef gaan, kun je dus namens het collectief van klachten naar die instantie lopen en zeggen: we hebben honderd klachten over jullie functioneren. En dan ben je een evenwichtige partij naar elkaar toe. En dat is wat wij nastreven.'*

Stichting Privacyloket.nl is in 2006 ontstaan vanuit het gevoel dat het CBP haar taken niet goed uitvoert en burgers niet (op de juiste manier) bijstaat. Het Privacyloket heeft als taak burgers bij te staan en heeft dus een brede en algemene doelgroep. Wanneer burgers de bescherming van

privacy als weinig belangrijk achten kan deze organisatie ernstig in het nauw komen. Ik heb deze case gekozen omdat ook deze organisatie waardegericht is en afhankelijk van haar institutionele omgeving. Door deze afhankelijkheid is de case erg geschikt voor dit onderzoek.

3.3 DeVrijePsych

DeVrijePsych is een website opgezet door dhr. Mengelberg in samenwerking met een groep psychiaters en psychotherapeuten. Op deze site wordt informatie verstrekt over een aantal bezwaren die zij hebben ten aanzien van nieuwe methodes en regels. De hoofdpunten van deze bezwaren zijn:

- Bemoeienis van politici en ICT managers en verzekeraars met het inhoudelijke werk wat de psychiaters en psychotherapeuten verrichten.
- Beperking op het recht van vrije keuze van behandelaar en behandeling.
- Aantasting van het recht op bescherming van de private levenssfeer.

Door digitalisering en automatisering van de geestelijke gezondheidszorg ontstaat een sfeer waarin het gevaar dreigt dat de patiënt in zijn privacy wordt aangetast (Bron: www.devrijepsych.nl). De heer Mengelberg licht het probleem toe:

> '*Sinds 2006 zijn de Diagnose Behandel Combinaties ingevoerd [DBC]. ... Hierin worden diagnoses en behandelingen aan elkaar gekoppeld. ... In praktijk betekent dit dat je in de computer veel informatie kan vinden wat terug te leiden is naar een patiënt.'*
> *'Vanaf 2008 worden deze DBC's ook gebruikt voor de rekeningen naar de ziektekostenverzekeraar. Dit is met goedkeuring van het College Bescherming Persoonsgegevens. Maar op een rekening staat wat er met een patiënt aan de hand is. Dat impliceert dat iedere werknemer van een ziektekostenverzekeraar kan zien wat er met een persoon aan de hand is. Deze informatie komt ook nog eens in databases terecht, waardoor informatie nog toegankelijker wordt. ... Dit tast de privacy van patiënten in hoge mate aan.'*

Deze website probeert, net als de andere cases, privacybescherming onder de aandacht te brengen. Ook zij vervult hiermee een maatschappelijke rol en komt op voor patiënten. Wat deze

organisatie onderscheidt van de andere organisaties die in een institutionele omgeving opereren is dat zij een specifieke organisatie vormt met een specifieke doelgroep. Dit neemt niet weg dat ook deze case geschikt is voor mijn onderzoek. Ook DeVrijePsych komt op voor privacybescherming en probeert haar doelgroep te wijzen op het belang dat zij hierin ziet. Wanneer er binnen de medische wereld een klimaat ontstaat waarbij efficiëntie en het gebruik van technologie belangrijker worden geacht dan privacybescherming van de patiënt, kan de DeVrijePsych steeds minder steun verwachten vanuit haar omgeving.

3.4 OBA Privacy Management Groep

OBA Privacy Management Groep adviseert en ondersteunt verschillende organisaties bij het voldoen aan de wet- en regelgeving van de Wet Bescherming Persoonsgegevens. Zij probeert deze organisaties te helpen volledig te voldoet aan de eisen die de WBP stelt. Hiervoor heeft zij een eigen methode ontwikkeld; de privacy management methode. OBA Privacy Management Groep is werkzaam voor (semi)overheidsinstellingen en bedrijven. Ook kunnen bedrijven gebruik maken van de expertise van de Functionaris Gegevensbescherming. (Bron: www.privacymanagementgroep.nl). Het is een organisatie die grotendeels in een technische omgeving opereert, maar een zeer algemene doelgroep heeft. OBA Privacy Management Groep kan vrijwel iedere organisatie of instelling benaderen. Deze organisatie ziet kansen in veranderingen omtrent de aandacht voor privacybescherming. Wanneer een organisatie niet goed op de hoogte is van de wettelijke bepalingen die hiervoor gelden, kan OBA Privacy Management Groep hierop inspelen en de organisatie wijzen op de methode die zij hiervoor ontwikkeld heeft. Ook voor OBA Privacy Management Groep is de heersende opinie over privacy belangrijk. Wanneer privacy als onbelangrijk wordt geacht zal de organisatie meer moeite moeten doen klanten te bereiken. Ze zullen zich immers minder bewust zijn van de wettelijke bepalingen die voor privacybescherming gelden. Deze case is geschikt voor mijn onderzoek, omdat ze afhankelijk is van haar omgeving.

3.5 Koninklijk NIVRA

Het NIVRA staat voor Koninklijk Nederlands Instituut van Registeraccountants. Het is de beroepsorganisatie van registeraccountants. Zij streven naar waarborging van integriteit, objectiviteit en deskundigheid van de beroepsgroep. Dit is zowel in het belang van de beroepsgroep als van de maatschappij. Het is belangrijk dat er goed wordt omgegaan met privacy. Zo heeft het NIVRA in samenwerking met de NOREA een richtlijn ontworpen waaraan een privacy audit proof keurmerk is verbonden. Een privacy audit is een opdracht die nagaat of de procedure wel aan alle eisen voldoet die de Wet Bescherming Persoonsgegevens voorschrijft. Het keurmerk laat dus zien wanneer de uitvoering van assurance-opdrachten voldoen aan alle eisen met betrekking tot de bescherming van persoonsgegevens (Bron: www.nivra.nl). Dhr. Plasmooij, ICT manager bij het NIVRA vertelt:

> *'Als beroepsorganisatie zetten wij de standards van de audits, ... Het betekent dat wij de standaard zetten die aansluit bij internationale standaarden, ... Het beoordelen van privacy voor bedrijven en het afgeven van een oordeel, en mogelijk zelfs van een zegel.'*

Ook deze organisatie opereert in een technische omgeving. Het NIVRA heeft een specifieke doelgroep, namelijk de registeraccountants. Zij beoordeelt hoe bedrijven omgaan met privacy en kan hierover een oordeel afgeven. Bij verminderde aandacht voor privacy zal zij mogelijk meer moeite moeten doen bedrijven te wijzen op de wettelijke bepalingen die hiervoor gelden. Zij kan dan ook kansen zien in een veranderende moraal over privacy. Als er minder aandacht is voor privacy kan het NIVRA haar privacy audit aanbieden aan bedrijven. Bedrijven zullen immers minder aandacht willen besteden aan privacy en dit liever uitbesteden. Omdat het NIVRA afhankelijk is van haar omgeving is deze case geschikt voor mijn onderzoek.

3.6 NOREA

De NOREA (Nederlandse Orde van Registerauditors) is de beroepsorganisatie van de IT-auditors. Deze IT-auditors beoordelen de informatiehuishouding van bedrijven. Om dit te

verduidelijken legt dhr. Olthof, directeur van NOREA, uit:

> *'Ik zeg altijd maar gewoon dat de IT-auditor de accountant van de elektronische snelweg is. Auditors die bij uitstek in staat zijn om technologische infrastructuur te beoordelen op voldoende beveiliging en of het beantwoordt aan de wettelijke bepalingen omtrent de privacy. We zijn ook bevoegd om daar een oordeel over af te geven, wat niet alleen voor het bedrijfsleven van belang is, maar ook voor het maatschappelijk verkeer. ... Het kan ook voor de samenleving als geheel van belang zijn. Het is belangrijk dat de samenleving weet dat je op een oordeel van een accountant kunt vertrouwen. Dat dat een oordeel is dat onafhankelijk en onpartijdig is.*'

En, zoals eerder gezegd, heeft de NOREA meegewerkt aan het privacy audit proof keurmerk. Deze case is vergelijkbaar met het NIVRA en is om dezelfde redenen geschikt voor dit onderzoek. Ook zij kan privacy zien als een kans in plaats van een bedreiging. Verandering in de heersende moraal over privacy kan veranderingen binnen de organisatie en hoe zij met haar omgeving omgaat vereisen.

3.7 Dataverzameling en operationalisering

Na het verduidelijken van mijn case selectie zal ik nu uitleggen hoe ik te werk ben gegaan bij de dataverzameling. De dataverzameling heeft deels plaatsgevonden door middel van documentanaylse. Hierbij betrof het studie van (wetenschappelijke) literatuur, van publicaties van de organisaties zelf (bijvoorbeeld jaarverslagen) en van de publieke opinie (bijvoorbeeld internetfora en kranten). Tevens heb ik half gestructureerde interviews afgenomen met leden van organisaties. Hieronder wordt per onderzoeksvraag aangegeven hoe de operationalisering heeft plaatsgevonden.

Zoals eerder gezegd neemt het CBP een dominante rol bij privacybescherming en dus ook in mijn onderzoek. Via de website van het CBP (www.cbpweb.nl) is veel informatie te vinden over het werk van het CBP via jaarverslagen, rapporten en onderzoeken. Dit was erg zinvol voor het creëren van een aantal verwachtingen en veronderstellingen. Ter beantwoording van de eerste

onderzoeksvraag heb ik verschillende onderzoeken over privacy, veiligheid en technologische ontwikkelingen geraadpleegd om erachter te komen wat de ontwikkelingen van de afgelopen jaren zijn en hoe de opinie van burgers zich hiertoe verhoudt.

Voor de tweede onderzoeksvraag waren de jaarverslagen van het CBP erg zinvol bij het vinden van informatie hoe het CBP in de loop van de tijd veranderd is en hoe zij zelf veranderingen in de samenleving ervaren hebben. Uit deze verslagen is echter niet alle nodige informatie te halen en bij de andere vijf organisaties was een antwoord op de tweede onderzoeksvraag niet te vinden via documentenonderzoek. Ik heb er dan ook voor gekozen half gestructureerde interviews af te nemen met leden van de organisaties. Ik heb bij iedere organisatie één interview afgenomen. Bij het CBP was dit het hoofd van de afdeling Beleid, iemand die veel weet over het gevoerde beleid van het CBP, waar aanpassingsstrategieën deel van uitmaken. Bij de andere organisaties waren de respondenten leden die mij veel konden vertellen over de organisatie, namelijk de oprichter van DeVrijePsych, privacydeskundige bij OBA Privacy Management Groep, algemeen directeur van Stichting Privacyloket.nl, ICT manager bij het NIVRA en directeur van de NOREA. De interviews waren tevens voor de derde onderzoeksvraag van belang. De interviews waren half gestructureerd, omdat ik van tevoren nog weinig informatie had over de strategieën die mijn gekozen organisaties toepassen. Ik had een aantal verwachtingen en veronderstellingen, gebaseerd op de gelezen literatuur en data, maar had nog geen compleet beeld. Van het CBP was dit beeld wel iets duidelijker en meer gestructureerd en was ik in staat meer gerichte vragen te stellen dan bij de andere organisaties. De interviews namen tussen drie kwartier tot anderhalf uur in beslag.
Een aantal vragen dat ik gesteld heb ter beantwoording van de tweede onderzoeksvraag zijn:

Ik heb zelf wat onderzoeken gevonden waaruit is gebleken dat niet zozeer de aandacht voor privacy verslapt is, maar vooral de aandacht voor veiligheid/technologie zo is toegenomen. Door het spanningsveld hiertussen is de bescherming van privacy onder druk komen te staan. Zijn die veranderingen hier opgemerkt?

Is het door deze veranderingen en het beeld wat hierover wordt neergezet ook moeilijker geworden voor jullie?

Vervolgens kon ik hierop doorgaan en een antwoord krijgen op de derde onderzoeksvraag:

Wat is jullie reactie hierop geweest, om de legitimiteit van privacywetgeving te behouden?

Los van deze vragen om antwoord te krijgen op de deelvragen, heb ik alle leden van de organisaties (uitgezonderd het CBP) gevraagd naar hun samenwerking met en mening over het CBP. De meeste leden van de organisaties noemden uit zichzelf al het CBP, dus dit was een goede mogelijkheid hier op in te gaan.

3.8 Conclusie

In dit hoofdstuk is de caseselectie behandeld. Er zijn zes organisaties geselecteerd die zich allemaal inzetten voor privacybescherming. Deze organisaties zijn onder te brengen in vier verschillende typen, zoals in het schema op pagina 24 is aangegeven. Dit maakt het mogelijk een vergelijking te maken tussen de verschillende organisaties. Het zijn organisaties die in meer of mindere mate afhankelijk zijn van hun omgeving. Deze afhankelijkheid is voor iedere organisatie anders, zo kunnen sommige organisaties een veranderende omgeving als bedreigend ervaren en anderen hierin juist kansen zien. Tevens heb ik in paragraaf 3.7 uiteengezet hoe ik mijn dataverzameling heb uitgevoerd. In hoofdstuk 4 zal ik antwoord geven op de probleemstelling en onderzoeksvragen.

Hoofdstuk 4; Resultaten

In hoofdstuk 4 worden de drie onderzoeksvragen beantwoord met behulp van de verzamelde data. Paragraaf 4.1 zal antwoord geven op de eerste onderzoeksvraag waarbij maatschappelijke veranderingen zullen worden behandeld. Paragraaf 4.2 zal antwoord geven op de tweede onderzoeksvraag waarbij de door organisaties *ervaren* maatschappelijke veranderingen worden behandeld. Paragraaf 4.3, tenslotte, beantwoordt de derde onderzoeksvraag waarbij de gebruikte strategieën zullen worden behandeld. Bij beantwoording van de probleemstelling zullen vooral de interviews een grote rol spelen, maar ook bronnen als jaarverslagen, artikelen en rapporten kunnen hierbij helpen. Paragraaf 4.4 geeft een samenvatting van alle gevonden resultaten. Er wordt in dit hoofdstuk zo nu en dan verwezen naar krantenartikelen of jaarverslagen. Deze (of een samenvatting van deze) zijn terug te vinden in de bijlagen.

4.1 De eerste onderzoeksvraag

Zoals eerder vermeld, ga ik uit van de veronderstelling dat bescherming van privacy de afgelopen tijd onder druk is komen te staan. Voordat we verder kunnen met het bespreken van strategieën die organisaties gebruiken om hiermee om te gaan, is het noodzakelijk te kijken naar een aantal maatschappelijke veranderingen van de afgelopen jaren. Is de veronderstelling dat privacybescherming minder steun krijgt juist?

In de eerste subparagraaf bespreek ik een opinieonderzoek over privacy. Hieruit kan opgemaakt worden hoe burgers denken over privacy en privacybescherming. Los van dit opinieonderzoek over privacy zijn er andere aspecten die indirect verband kunnen houden met privacybescherming. Zo kun je stellen dat privacy in het geding is wanneer er steeds meer maatregelen worden genomen die de persoonlijke levenssfeer aantasten, zoals het plaatsen van camera's op straat. Hier ligt de toenemende angst en intensivering van de bestrijding van criminaliteit en terrorisme aan ten grondslag (CBP, 2004). Een toenemende aandacht voor veiligheid kan direct of indirect negatief uitpakken voor privacybescherming. Ik zal in de tweede subparagraaf 4.1.2 dan ook een aantal onderzoeken over veiligheid bespreken om aan te tonen dat deze veranderingen negatieve gevolgen hebben voor privacybescherming. Een ander aspect dat

samenhangt met de (verminderde) privacybescherming is de komst van het ICT tijdperk. Toenemend gebruik van Internet, telecommunicatiediensten en identificatie op afstand via bijvoorbeeld een chip bieden enorme voordelen, maar ook gevaren dat de persoonlijke levenssfeer van burgers wordt aangetast. Tegelijkertijd kan dit ook juist meer mogelijkheden bieden voor privacybescherming (CBP, 2004). Het is dan ook belangrijk hier bij stil te staan. Wanneer technologie als belangrijker wordt gezien dan andere zaken als privacybescherming, kan het gevaar van aantasting van privacy als minder belangrijk worden geacht. Dit wordt besproken in paragraaf 4.1.3. Paragraaf 4.1 wordt afgesloten met een korte samenvatting van de gevonden resultaten.

4.1.1 Privacy

Een recent opinieonderzoek over privacy is *'Burgers en hun privacy'* uit 2004, uitgevoerd in opdracht van het CBP. Het onderzoek vond plaats in de tweede helft van 2004, een onrustige periode na de moord op Theo van Gogh en een antiterreuractie in het Laakkwartier in Den Haag. Er was in deze periode veel media-aandacht en dit kan de houding van burgers ten opzichte van privacy beïnvloed hebben (CBP, 2004).
Het onderzoek '*Burgers en hun privacy'* werd in 2004 voor het eerst uitgevoerd. Het is de bedoeling om dit onderzoek in de toekomst te herhalen. Opinieonderzoeken over privacy in het verleden zijn echter niet eerder gedaan door het CBP of de Registratiekamer. Ook bij andere onderzoekbureaus heb ik geen gegevens over de publieke opinie met betrekking tot de waardering van privacybescherming kunnen vinden. Of er een verandering heeft plaatsgevonden is dan ook moeilijk te zeggen. Wel kan dit onderzoek inzicht bieden in de hedendaagse houding van burgers ten opzichte van privacy.

Uit het onderzoek kan geconcludeerd worden dat burgers nogal tegenstrijdig zijn wanneer het gaat om privacy. Veel respondenten zeggen toch niets te verbergen te hebben. En de overheid weet toch al alles van hen, dus wat valt er nog te verbergen of te beschermen? Hier tegenover staat dat burgers met negatieve ervaringen met persoonsgegevens bewuster en kritischer zijn dan burgers die geen ervaringen hebben met persoonsgegevens. Bij negatieve ervaringen kun je bijvoorbeeld denken aan het ongevraagd krijgen van geadresseerde reclamepost. Er is bij sommigen dus wel een bewustzijn over privacy. De Nederlandse burgers zijn zich ervan bewust

dat overheid en bedrijven beschikken over veel persoonsgegevens. Er is echter een gering bewustzijn onder burgers over de risico's met betrekking tot het gebruik van deze gegevens. Weinigen (5%) denken vaak na over de risico's.

Ongeveer de helft van de Nederlanders hecht veel vertrouwen tot zeer veel vertrouwen in organisaties en hun (correcte) omgang met persoonsgegevens. Er is maar een kleine groep van 5% die zegt weinig of zeer weinig vertrouwen te hebben. Er is wel een onderscheid in de mate van vertrouwen wanneer we kijken naar overheidsinstanties en commerciële organisaties. Het vertrouwen in overheidsinstanties is aanzienlijk hoger dan het vertrouwen in commerciële organisaties. Marktonderzoeksbureaus of de organisaties die persoonsgegevens gebruiken voor marketingdoeleinden (zoals goede doelen, postorderbedrijven en winkels) worden als minst betrouwbaar gezien door burgers.

Over het algemeen kan gesteld worden dat burgers meer vertrouwen hebben in dié organisaties, waarvan zij ook het belangrijk vinden dat deze goed omgaan met hun gegevens. Overheidsorganisaties zijn een goed voorbeeld van organisaties waarvan burgers het belangrijk vinden dat deze goed omgaan met gegevens. Zeventig procent van de burgers verwacht ook dat overheidsorganisaties zorgvuldiger omgaan met gegevens dan het bedrijfsleven. Een kwart (25%) verwacht dat er geen verschil is tussen beide. Een klein gedeelte (2%) verwacht dat bedrijven zorgvuldiger omgaan met persoonsgegevens.

Burgers denken vrij genuanceerd over privacybescherming: de meerderheid wil wel ruimte bieden aan andere waarden zoals terrorismebestrijding, maar stelt daar ook grenzen aan. Dit is gemeten aan de hand van een aantal stellingen waar de respondenten cijfers aan moesten toekennen. Er is bijvoorbeeld gevraagd naar zwarte lijsten van frauderend personeel; de grootste groep van 51% is van mening dat een zwarte lijst van frauderend personeel acceptabel is, maar wel onder bepaalde voorwaarden om de privacy van frauderend personeel enigszins te beschermen. Zo moet men er wel heel zeker van zijn dat deze persoon ook daadwerkelijk gefraudeerd heeft. Ook geeft 48% van de respondenten aan dat het hier ook om zware incidenten moet gaan.

Er kan gezegd worden dat burgers de bescherming van privacy en persoonsgegevens wel belangrijk vinden, maar het mag er niet toe leiden dat terroristen of criminelen vrij spel krijgen.

Verder komt uit het onderzoek duidelijk naar voren dat de meeste burgers geen goed beeld hebben over de inhoud van de Wet Bescherming Persoonsgegevens of de taken van het CBP. Ze geven aan bescherming van persoonsgegevens belangrijk te vinden, maar weten het CBP meestal niet te vinden bij geschillen over privacy en zien het CBP ook niet als een heel belangrijke institutie. In het onderzoek is aan burgers gevraagd tot welke organisatie zij zich zouden wenden als ze problemen hebben met de bescherming van persoonsgegevens. Een grote groep burgers (circa 16%) antwoordt dat zij zich in eerste instantie wendt tot het bedrijf of de instantie waar de problemen zich mee voordoen.

Geconcludeerd kan worden dat de meeste burgers niet erg bezig zijn met privacybescherming. Slechts vijf procent van de burgers denkt vaak na over de risico's van privacy. Wanneer ze er echter goed over nadenken, vinden ze dit vaak toch wel belangrijk.
De meeste mensen zich niet erg bewust van hun rechten en plichten omtrent privacy. Wanneer ze te maken krijgen met privacyschending of geattendeerd worden op privacy gaan ze hier over nadenken. Dit gegeven kan op zichzelf al betekenen dat het voor organisaties die zich inzetten voor privacy soms moeilijk kan zijn, omdat privacy dus niet als vanzelfsprekende waarde wordt gezien. Als privacy niet als vanzelfsprekend wordt gezien zal een organisatie die zich hiervoor inzet veel moeite moeten doen om aandacht te krijgen voor privacybescherming. Mensen zijn immers niet erg geïnteresseerd in privacybescherming.

Of de aandacht voor privacy verminderd of verslapt is, is niet duidelijk. Wat wel duidelijk is, is dat op dit moment de aandacht voor privacybescherming niet groot is. Mensen zijn zich maar weinig bewust van de risico's van privacy en denken pas na over privacybescherming wanneer zij hier negatieve ervaringen mee hebben.
Wat we echter willen weten ter beantwoording van de eerste onderzoeksvraag, is of de aandacht voor privacy in de loop van de tijd veranderd is. Om hier achter te komen zal ik twee andere maatschappelijke aspecten bekijken die een spanningsveld vormen met privacy. Dit is enerzijds de aandacht voor veiligheid en anderzijds de aandacht voor technologische ontwikkelingen.

4.1.2 Veiligheid

Het Nationaal Comité 4 en 5 mei heeft in 2007 onderzoek verricht naar de publieke opinie over vrijheid en veiligheid (Nationaal Vrijheidsonderzoek 2007).
Bij een afweging van vrijheid tegenover veiligheid, kiest het merendeel van de bevolking voor veiligheid. Uit het onderzoek blijkt dat de meeste ondervraagden veiligheidsmaatregelen effectief, maar ook een inbreuk op de privacy achten. Desondanks geeft een meerderheid aan dat deze maatregelen acceptabel zijn. Maar liefst 47% geeft aan dat leven in een veilig land de belangrijkste waarde is (tegenover godsdienstvrijheid, vrijheid van meningsuiting en het genereren van een inkomen). Zelfs wanneer we kijken naar de maatregel die de minste steun krijgt (het afluisteren van alle telefoonverkeer) is er geen meerderheid die dit onacceptabel vindt. Wanneer de respondenten kunnen kiezen tussen privacy of veiligheid, kiest 71% voor veiligheid tegenover 25% voor privacy.
Ook blijkt dat het vertrouwen van burgers in de overheid groot is. De helft van de ondervraagden geeft aan dat de overheid sommige zaken geheim mag houden om de veiligheid te waarborgen. Tevens denkt de helft van de ondervraagden dat de maatschappij veiliger wordt wanneer de overheid meer informatie over burgers heeft. Dit is een goede verklaring voor de steun van burgers voor veiligheidsmaatregelen.
Hieruit blijkt dat het draagvlak voor veiligheidsmaatregelen groot is, zelfs als dat ten koste gaat van privacybescherming. Ook het SCP heeft in ‘De Sociale Staat van Nederland’ veiligheidsgevoelens onderzocht. Deze rapporten worden herhaald, zodat vergelijkingen in de tijd gemaakt kunnen worden. In 2003 wordt bestrijding van misdaad door 67% tot de hoogste prioriteit gesteld, terwijl de prioriteit hiervan tussen 1992 en 2002 door 58% van de respondenten werd geplaatst bij de vijf belangrijkste doelen (maar dus niet als hoogste prioriteit werd gezien). Het SCP stelt dat het maatschappelijk klimaat de afgelopen jaren is veranderd. De tolerantie ten opzichte van criminaliteit is afgenomen. Dit is zichtbaar in de steun van burgers voor repressieve maatregelen, zoals het verhogen van straffen en het uitbreiden van mogelijkheden van DNA onderzoek (SCP, 2003). Ook uit het rapport uit 2005 blijkt dat de steun voor hogere straffen weer is gegroeid; van 40% dat kiest voor bestraffing boven genezing in 1994 tot ongeveer de helft in 2004.

Het SCP heeft in 2004 het rapport ‘In het zicht van de toekomst’ geschreven, waarin een

hoofdstuk wordt besteed aan veiligheid, politie en justitie. In dit rapport beschrijft het SCP een toekomstvisie gebaseerd op trends uit het verleden. Het SCP stelt dat (on)veiligheid al langere tijd als belangrijk maatschappelijk probleem wordt gezien door burgers. Het SCP verwijst naar Boutellier (2002), die zegt dat de utopie van veiligheid niet bereikt kan worden zonder dat burgers hun vrijheden moeten inleveren.

De wens naar veiligheid is een gevoelsmatige kwestie (SCP, 2004). Burgers hebben hoge verwachtingen van de overheid wanneer het gaat om criminaliteitsbestrijding. Ze stellen de overheid verantwoordelijk voor het verminderen van criminaliteit, terwijl is gebleken dat de overheid hier weinig invloed op heeft (SCP, 2004). Ondanks het belang dat wordt gehecht aan veiligheid, komt uit het onderzoek naar voren dat burgers zich steeds minder vaak onveilig voelen. In de Politiemonitor van 1993 gaf 6,3% van de respondenten aan zich vaak onveilig te voelen, dit tegenover 4,4% in 2004 (SCP, 2004). Toch blijkt dat de verwachtingen van burgers over veiligheid in de toekomst weinig rooskleurig zijn. Bijna driekwart van de respondenten is van mening dat problemen rond criminaliteit en onveiligheid in 2020 groter zullen zijn dan nu. Maar liefst 70% van de ondervraagden verwacht een grotere terreurdreiging en 60% verwacht grotere problemen met georganiseerde criminaliteit (SCP, 2004). Er worden dan ook meer veiligheidsmaatregelen verwacht en dit wordt ook als wenselijk bestempeld. Maar liefst 94% verwacht dat cameratoezicht meer toegepast wordt in de toekomst en een grote meerderheid van 86% bestempelt dit als zeer wenselijk of wenselijk. Het lijkt er dus op dat de wens naar meer veiligheid niet geheel te herleiden is tot de feitelijke criminaliteitscijfers. Het SCP stelt dat wellicht het groeiend aantal ouderen gezien kan worden als oorzaak voor een toenemende vraag naar veiligheid (SCP, 2004). Bovendien is er sprake van een trend van afkeer van geweld (SCP, 2004), dat waarschijnlijk de komende jaren nog voort zal zetten.

Uit deze gegevens blijkt dat de vraag naar veiligheid steeds meer toeneemt. Ondanks het feit dat onveiligheidsgevoelens afnemen, wordt veiligheid steeds belangrijk geacht. De vraag naar hogere straffen is gegroeid bij een constante prioriteit van misdaadbestrijding. Bij meer opsporingsbevoegdheden om (het gevoel van) veiligheid te vergroten worden de grenzen van privacy steeds meer opgezocht. Het spanningsveld dat bestaat tussen veiligheid en privacy wordt hierdoor groter. Wanneer de keuze gemaakt moet worden tussen privacy en veiligheid, wordt prioriteit gegeven aan veiligheid.

4.1.3 Technologische ontwikkelingen

De ontwikkeling van technologie en het gebruik hiervan is in sneltreinvaart ontwikkeld en heeft, zoals hieronder zal blijken, gevolgen voor de privacybescherming. Ook zal blijken dat de burger deze ontwikkelingen steunt.

Technologie biedt nieuwe mogelijkheden voor de preventie en bestrijding van criminaliteit (SCP, 2004). Overtredingen kunnen door sensoren makkelijker worden waargenomen en het gebruik hiervan kan op afstand plaatsvinden. Dit soort ontwikkelingen kunnen leiden tot een compleet nieuwe wijze van analyseren en opsporen van veiligheid. De optelsom van een groeiende vraag naar veiligheid plus een grotere terreurdreiging lijken ertoe te leiden dat burgers gemakkelijk aspecten van privacy inleveren in ruil voor veiligheid. Dit kun je concluderen aan de hand van de brede acceptatie van cameratoezicht en de identificatieplicht.

Voor de komst van de ongekende mogelijkheden van informatie- en communicatietechnologie, was de identiteit van een persoon en het proces van identificeren een redelijk beheersbaar proces. (Prins, 2004: 34). Identificatie speelt een belangrijke rol bij de politieke tendens om meer opsporingsbevoegdheden toe te kennen aan politie en justitie (Prins, 2004). De overheid is bereid hiervoor nieuwe technieken en vormen van dataverzameling toe te staan. Prins noemt een aantal nieuwe technieken die het mogelijk maken gegevens tot een persoon te herleiden. Dit biedt uiteraard een scala aan nieuwe mogelijkheden mensen te identificeren op basis van elektronische gegevens. Dit is niet alleen gunstig voor de handhaving van veiligheid, maar kan ook gebruikt worden voor commerciële doeleinden. Klanten worden ongemerkt ‘gevolgd’ en krijgen ongevraagd email of post van bedrijven. De anonimiteit staat volgens Prins behoorlijk onder druk. Identificatie heeft hoge prioriteit bij bedrijven en overheid. Door de mogelijkheden die er op technologisch gebied zijn, wordt dit ook makkelijker gemaakt. Prins stelt dat de wettelijke bepalingen voor privacy niet meer voldoende zijn om deze inbreuk op de privacybescherming tegen te kunnen gaan (Prins, 2004). De WBP (Wet Bescherming Persoonsgegevens) spitst zich alleen toe op gegevensbescherming en dit is niet hetzelfde als privacybescherming. Privacy heeft veel meer te maken met de persoonlijke levenssfeer dan de WBP voorschrijft. ICT maakt het mogelijk veel informatie vast te leggen, te bewerken en uit te wisselen. Uit een onderzoek onder ICT-ers blijkt dat driekwart van hen ervan uit gaat dat dit gevolgen heeft voor privacybescherming (Telecombrief, p.89)

Steunen de burgers technologische ontwikkelingen ook? Het CBP heeft in december 2004 een artikel gepubliceerd, '*Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde'*. Hieruit blijkt dat de belangstelling voor cameratoezicht in de loop van de tijd, vooral na 2000, alleen maar is toegenomen. Volgens het CBP zijn camera's min of meer vanzelfsprekend geworden in het straatbeeld vanuit de veronderstelling dat de effectiviteit van camera's ook daadwerkelijk aanwezig is. Uit het jaarverslag van het CBP uit 2003 blijkt in de meeste gemeenten in Nederland het cameratoezicht niet geëvalueerd op effectiviteit, terwijl het CBP dit wel degelijk noodzakelijk acht.

Uit dit artikel uit 2004 blijkt dat Nederlanders de wenselijkheid van cameratoezicht op straat groot achten. Het SCP heeft in haar rapport 'In het zicht van de toekomst' uit 2004 onderzoek verricht naar de toekomstverwachtingen en wenselijkheid van veiligheidsmaatregelen. De toekomstverwachtingen laten zien dat de meeste mensen weinig positief zijn. Een grote meerderheid van de ondervraagden is van mening dat de problemen rond veiligheid en criminaliteit in 2020 groter of veel groter zullen zijn dan nu (SCP, 2004). Meer dan 90% denkt dat toepassingen als verruiming van cameratoezicht en het inzetten van andere technologische hulpmiddelen zoals DNA-technieken meer en ruimer zullen worden gebruikt. Het merendeel van de ondervraagden vindt dit ook wenselijk; 97% vindt dit voor het toepassen van technologische middelen, zoals DNA-technieken. (SCP, 2004).

4.1.4 Samenvatting

Uit deze verschillende onderzoeken over privacy, veiligheid en technologie kan geconcludeerd worden dat privacy een niet zo belangrijke rol inneemt. Burgers lijken zich niet bewust te zijn van privacybescherming in de samenleving. Ook kan gesteld worden dat de visie en mate van aandacht over veiligheid verandert. Veiligheid staat bij een groot deel van de burgers voorop en meer veiligheidsmaatregelen hebben directe gevolgen voor privacybescherming. Door aanvullende maatregelen en/of bevoegdheden door te voeren, komt privacy in het nauw. Er mogen immers gegevens van burgers verzameld en opgevraagd worden. De identificatieplicht is hier een goed voorbeeld van. Mensen zijn verplicht zich te identificeren wanneer politie daarom vraagt. Burgers steunen deze ontwikkeling ook (CBP, 2004).
Hierbij komt dat de technologische ontwikkelingen elkaar in snel tempo opvolgen en dit ervoor

zorgt dat er steeds meer elektronische gegevens over individuen traceerbaar zijn. De grote steun voor cameratoezicht, het toenemende gebruik van Internet en de vraag naar meer veiligheid wijzen erop dat burgers deze technologische ontwikkelingen steunen (CBP, 2004).
De vraag is dan ook of partijen die zich inzetten voor deze privacy dit zelf ook ervaren en hoe zij hierop reageren? In het volgende hoofdstuk zal ik een antwoord te geven op de tweede onderzoeksvraag.

4.2 De tweede onderzoeksvraag

De resultaten uit paragraaf 4.1 geven aan dat de kennis over privacyregels en rechten en plichten bij burgers erg gering is. Wanneer je dit optelt bij de groeiende aandacht voor veiligheid en technologie kun je veronderstellen dat organisaties die zich inzetten voor privacybescherming moeite hebben legitimiteit te vinden binnen hun omgeving. In deze paragraaf wordt van de verschillende geïnterviewde organisaties bekeken of zij zelf ook daadwerkelijk de besproken maatschappelijke veranderingen als zodanig hebben ervaren. Ook wordt antwoord gegeven op de vraag hoe de tweedeling tussen organisaties die in een institutionele omgeving werken en organisaties die in een technische omgeving werken, zich verhoudt tot de ervaren veranderingen. In paragraaf 4.2.1 wordt dan ook antwoord gegeven op de tweede onderzoeksvraag. Paragraaf 4.2.2 vormt een korte samenvatting van de gevonden resultaten.

4.2.1 Tweede onderzoeksvraag

In het jaarverslag van het CBP uit 2004 komt duidelijk naar voren dat het CBP ervaart dat er minder waarde wordt gehecht aan privacy en zelfs als belemmering wordt gezien. Zo staat in de inleiding beschreven:

‘Sinds enkele jaren is ‘privacy’ voor velen [..]een politieke steen des aanstoots geworden: een niet concreet gedefinieerd belang dat bestuurders en professionals ervan zou weerhouden om politiek en maatschappelijk gewenste doelen te realiseren.’

Ook in 2005 wordt in het jaarverslag aandacht besteed aan de verminderde prioriteit van privacy:

'In de afgelopen jaren heeft de bescherming van de persoonlijke levenssfeer in de publieke opinie haar vanzelfsprekendheid verloren. Zorgen om terrorisme, onveiligheid en maatschappelijke misstanden bij burgers, bestuurders, politici en beleidsmakers hebben ertoe geleid dat de regels voor de bescherming van persoonsgegevens in het publieke debat als zondebok of als obstakel worden afgedaan.'

In het gesprek met mevrouw Schaafsma, die werkzaam is als hoofd van de afdeling beleid bij het CBP, vertelt zij dat het CBP inderdaad veranderingen heeft waargenomen en ervaren:

> *'We hebben gemerkt, zowel op persoonlijk niveau van medewerkers als op professioneel niveau, dat het moeilijk is om ons verhaal [onder de aandacht] te brengen. Het [uitdragen van de boodschap over privacy] is een genuanceerd verhaal en dit bekt nu eenmaal minder lekker dan een kreet als: terrorisme moet bestreden worden, dus er moeten maar camera's daar en daar komen.'*

Zij legt een verband tussen de aanslagen van 2001 en de waarde die gehecht wordt aan privacy. Schaafsma zegt hierover:

> *'Sinds 2001 is er bij de overheid sprake van dat zij acties wil ondernemen om risico's in te dammen, waar wij op zich erg achter staan.'*

Het CBP erkent de invloed van de aanslagen, maar doordat zij zegt achter bestrijding van terrorisme te staan, lijkt zij hier zelf geen probleem mee te ervaren. Echter, in het jaarverslag van 2004 staat beschreven dat het CBP haar uiterste best doet de verruiming van opsporingsbevoegdheden tegen te gaan:

'Daartoe [het voorkomen van terrorisme] achtte het kabinet uitbreiding van opsporingsbevoegdheden noodzakelijk. [..]. in een publieke reactie op de voorstellen

constateerde het CBP dat de noodzaak van uitbreiding van bevoegdheden tot het verzamelen van informatie niet was aangetoond.'

Het CBP is van mening dat de noodzakelijkheid van dit soort maatregelen eerst goed bekeken dient te worden, voordat er tot actie wordt overgegaan.

Schaafsma vertelt:

> *'We hebben geprobeerd erop te wijzen, van, ga nou uit bij alles wat je wil regelen, wat is er nu mogelijk en wordt dit optimaal benut? Als je die analyse hebt gemaakt en daar komt een uitkomst uit van alles wat we kunnen is benut, dan kun je bedenken; wat zijn er voor aanvullende maatregelen nodig?[..] Wij vinden dat een onderdeel van veiligheid ook juist de bescherming van persoonsgegevens is'.*

Hier kun je uit opmaken dat het CBP erkent dat er in de samenleving een spanningsveld zichtbaar is tussen privacy en veiligheid. Het CBP zelf is het hier echter niet mee eens, maar constateert dat de bescherming van persoonsgegevens juist een onderdeel vormt van veiligheid.
Dhr. Klei (Stichting Privacyloket.nl) wijst eveneens op de maatschappelijke tegenstelling tussen veiligheid en privacy. Wel legt ook hij een verband tussen de aanslagen van 2001 en de waarde die gehecht wordt aan privacy vanuit de overheid en de politiek. Hij is echter niet van mening dat de aanslagen in 2001 de aandacht van burgers voor privacy veranderd hebben. In plaats daarvan stelt hij dat de aanslagen van 2001 de politiek hebben beïnvloed en dat de politiek op haar beurt de samenleving weer beïnvloed heeft. Het is dus de politiek die de toon heeft gezet:

> *'Je ziet dat er na 2001 een soort spanningsveld is ontstaan tussen privacy en veiligheid, omdat juist op het gebied van privacy veel aandacht besteed is aan hoe dat vorm gegeven moet worden. Je ziet ook dat er allerlei niet voorziene zaken op het gebied van veiligheid gebeuren, waar de overheidsinspectie de burger dient te beschermen. Daar zit een soort spanningsveld tussen.*
> *Het [privacy en veiligheid] hangt wel samen, maar het werkt niet samen. Maar de grens wordt natuurlijk politiek bepaald, wat wel en niet voor de maatschappij zinvol is. Op*

basis daarvan worden wetten gemaakt, en dan zie je dat er binnen die wetten ook weer spanningsvelden zijn'.

Van belang is dat de aanpak ten behoeve van veiligheid volgens hem een korte termijn doelstelling is. Privacy gaat volgens Klei over een lange termijn gedachte, die niet gemakkelijk beïnvloedbaar is. Hij stelt dat de korte termijn doelstelling altijd boven de lange termijn gedachte wordt geplaatst. Hij vertelt:

'Het is altijd de waan van de dag die bepaalt wat op korte termijn gebeuren moet op het gebied van veiligheid. Dit zijn impulsen. Allerlei bestuurders zullen maatregelen nemen, waar veiligheid overtreden wordt. Dat kun je niet voorkomen, de maatschappij is nu eenmaal zo. Maar privacy is een soort lange termijn aanpak, waarbij we iedereen bewust moeten houden dat wat je doet vastgelegd kan worden en traceerbaar is, zodat hij op een bepaalde manier kan handelen'.

Dhr. Klei stelt dat na 2001 bestuurders vaker maatregelen nemen waar veiligheid overtreden wordt. Doordat de lange termijndoelstelling van privacy niet beïnvloedbaar is, is zij onderhevig aan maatschappelijke veranderingen. Klei stelt dat er een spanningsveld bestaat tussen veiligheid en privacy; wanneer er aan veiligheid meer impuls gegeven wordt, verslapt de aandacht voor privacy.

De heer Mengelberg, oprichter van DeVrijePsych noemt eveneens de aanslagen van 2001:

'We leven een paar jaar na 11 september en niemand weet hoe onze samenleving er over tien jaar uitziet. ... De democratie is helemaal niet zo vanzelfsprekend, en het kan zomaar zijn dat machthebbers over een aantal jaren databases gebruiken voor doeleinden waar ze niet voor bedoeld zijn. ... Elektronische gegevensbestanden kunnen een groot gevaar zijn, omdat ze makkelijk in te zien zijn, en zelfs het Pentagon is gekraakt, dus er kan altijd gelekt worden of ingebroken worden'.

DeVrijePsych is een website die opgezet is door een groep psychiaters en psychotherapeuten uit

onvrede met onder andere de aantasting van de privacy van patiënten in de geestelijke gezondheidszorg. Deze website is drie jaar geleden opgericht, waaruit blijkt dat drie jaar geleden (of korte tijd daarvoor) de maatschappelijke verandering van verminderde aandacht voor privacy is opgemerkt. De website is immers opgericht uit onvrede over afnemende aandacht voor privacybescherming. Hieruit blijkt dat afnemende legitimiteit is opgemerkt bij de psychiaters en psychotherapeuten. In augustus 2006 is de website openbaar en voor iedereen zichtbaar gemaakt. De leden van DeVrijePsych vonden de veranderingen binnen de geestelijke gezondheidszorg zo belangrijk dat zij dit openbaar wilden maken voor een breed publiek. Het bestaan van DeVrijePsych is op zichzelf dus al een teken dat verminderde aandacht voor privacy door deze groep artsen is opgemerkt en ervaren. Zij maken zich echter nog meer zorgen over de toekomst, waarin koppeling van bestanden steeds vaker zullen voorkomen. In de nieuwsbrief van maart 2007 staat hierover het volgende:

'Op termijn zal een zeer groot databestand worden opgebouwd voor allen die met de somatische en geestelijke gezondheidszorg in aanraking zijn gekomen. Dit kan ongekende negatieve gevolgen hebben. De verplichte vermelding van alle burgerservicenummers (BSN) op alle medische gegevensuitwisselingen zal datakoppeling vergemakkelijken.'

DeVrijePsych merkt op dat privacy binnen de politiek een minder belangrijke rol inneemt. Met hun website proberen zij burgers bewust te maken van de risico's van privacyschending.

Alle drie organisaties die zich inzetten voor privacybescherming en hiermee een maatschappelijke taak vervullen ervaren een afnemende steun voor privacybescherming. Er is consensus dat de aanslagen van 2001 verband houden met de gedachtegang van mensen over privacy. Al deze organisaties hebben veranderingen opgemerkt na de aanslagen van 2001. Zij zien deze veranderingen als een bedreiging, omdat ze de prioriteit van privacy aantasten. Aangezien zij zich inzetten voor deze privacy verliezen zij legitimiteit.
Binnen deze drie organisaties kan onderscheid worden gemaakt in de doelgroep die zij hebben, namelijk een specifieke of een algemene. Opvallend is dat er op dit punt weinig verschil lijkt te zijn in de manier waarop ze maatschappelijke veranderingen ervaren. Ze ervaren alle drie een bedreiging van hun legitimiteit. DeVrijePsych, die een specifieke doelgroep heeft, probeert haar

doelgroep wel zo veel mogelijk uit te breiden en iedere geïnteresseerde aan te trekken. Dit kan wellicht als verklaring worden gegeven dat er weinig onderlinge verschillen zichtbaar zijn.
Wel zichtbaar is dat het CBP zich duidelijk probeert te verdedigen door te zeggen dat veiligheid en privacy geen tegenstelling vormt. De andere twee organisaties delen deze visie niet. De reden hiervoor is wellicht dat deze twee organisaties zijn opgericht uit onvrede over privacybescherming, terwijl het CBP een overheidsinstantie is die als waakhond van de privacy dient te werken. Zij behoort een dominante positie in te nemen, wat betekent dat wanneer privacybescherming onder druk komt te staan, zij hiervoor verantwoordelijk voor wordt gehouden.

Dan bespreek ik nu de drie organisaties, die deels in een institutionele en deels in een technische omgeving werken. Om te beginnen de OBA Privacy Management Groep. Dhr. Fernald, privacydeskundige, wijst op de ondergeschiktheid van privacy aan veiligheid. Veiligheid heeft altijd prioriteit, dit terwijl op het gebied van technologie privacy een belangrijk punt is voor veiligheid en beveiliging van systemen. Hij zegt:

> *'Er komen drie gebieden bij elkaar; privacy, bewaking en het recht van de werknemer op privacy. En daar prefereert altijd de beveiliging. Maar de beveiliging is ook een integraal onderdeel van privacybescherming, en die link heeft men nog steeds niet gelegd. Als je goede richtlijnen hebt, heb je adequate beveiliging. Maar het is ook mijn gevoel dat degenen die het moeten controleren en het moeten handhaven ook te weinig kennis hebben van de toepassing van de wet'*.

Er is hier een verschil in beveiliging en veiligheid. Bij beveiliging in technologie is privacy een belangrijke voorwaarde om systemen goed te beveiligen. Er worden immers gegevens verwerkt en de wijze waarop dit gebeurt, dient in overeenstemming te zijn met de WBP.
Veiligheid duidt op de uitbreiding van meer bevoegdheden voor overheidsinstanties om meer informatie te kunnen verkrijgen over burgers. Hierbij worden de grenzen van privacybescherming opgerekt.
Fernald ziet bij een groei van technologische ontwikkelingen een negatief aspect voor de aandacht voor privacy. Juist doordat er zoveel mogelijk is op technologisch gebied wordt het

steeds lastiger gegevens op de juiste manier te verwerken. Volgens Fernald ontbreekt het vaak aan kennis:

> *'Een van de eisen om persoonsgegevens te verwerken, is dat men duidelijk weet van welke doelbinding er sprake is. . . . Maar die logica ontbreekt nog steeds bij veel bedrijven, die gebruiken veel gegevens en halen allerlei technologieën in huis, maar verzuimen de betrokkenen en medewerkers hierover te informeren en bij te scholen over het toepassen van hun taken. De beveiliging heeft een hoge prioriteit, maar de middelen die men gebruikt, daar heeft men geen enkel idee van hoe men dit op een juiste manier kan gebruiken. . . . Bijvoorbeeld videobewaking in de openbare ruimte. Je mag niet een camera over iedere werknemer z'n schouder zetten, want daarmee krijg je volgsystemen.'*

Er wordt eveneens bij de NOREA, de beroepsorganisatie van IT-auditeurs, onderkend dat technologie een positief ding kan zijn, maar ook zeker een gevaar oplevert voor de bescherming van privacy. Dhr. Olthof, directeur van de NOREA, vertelt:

> *'Je moet er dus op kunnen vertrouwen dat uit die computersystemen elk moment de juiste gegevens komen. ... Dit is natuurlijk ten aanzien van de privacy een heel belangrijk aandachtspunt. De technologie is zo geperfectioneerd dat je van mensen alles kunt weten en kunt zien. ... Zo moeten telecombedrijven en internetbedrijven hun gegevens anderhalf jaar bewaren, en dit is iets wat op gespannen voet staat met de privacy. Het duurt geen twee jaar meer voordat er een chip in auto's komt, waardoor je overal ter wereld kunt zien waar die auto zich begeeft. ... Als je dit soort gegevens gaat opslaan en bewaren, kun je van burgers heel nauwgezet bijhouden wat ze doen.'*

Wanneer ik vraag naar veranderingen in de maatschappij, merkt Olthof op dat deze inderdaad opgemerkt zijn in het werk. Zo vertelt hij:

> *'Je ziet dat we midden in de technologische innovaties staan. We hebben ook de taak om, zodra nieuwe technologie beschikbaar is, deze ook gelijk te gebruiken. Er komen steeds allerlei nieuwe systemen.'*

Het lijkt erop dat de NOREA uitdaging ziet in technologische ontwikkelingen die zich voordoen. Door deze ontwikkelingen wordt het voor bedrijven steeds moeilijker de ontwikkelingen bij te houden en zullen zij dus vaker een beroep doen op de audits van de NOREA. Volgens Olthof wordt de rol van auditors dus alleen maar belangrijker naarmate er meer mogelijk is met technologie. Hij zegt hierover:

> *'Er zit een voortdurend spanningsveld van wat aan de ene kant met technologie kan, en aan de andere kant, wat je toch als auditor nodig hebt om goed een beeld te kunnen vormen van wat er precies is gebeurd. En daarom wordt de rol van auditors wel steeds belangrijker, omdat die bedrijfsprocessen en informatie in feite in systemen zitten die volkomen zijn gedigitaliseerd. Je moet er dus op kunnen vertrouwen dat er uit die computersystemen elk moment de juiste gegevens komen.'*

Ook het NIVRA, de beroepsorganisatie van registeraccountants, stelt dat er bij hen een maatschappelijke vraag opgemerkt is. De heer Plasmooij (ICT manager bij het NIVRA) wijdt dit aan de tijdgeest. Hij stelt:

> *'Ons oordeel is vrijwillig, dus de druk komt niet vanuit de wet. Er ontstaat een maatschappelijke behoefte. Er zijn een aantal overheidsinstellingen die zich via onze wijze kunnen verantwoorden, en de verwachting is dat dat er meer zullen worden, en de maatschappelijke ontwikkeling die kant op gaat. ... Zij zien dit op vrijwillige basis, omdat ze er een voordeel in zien. Als er bij bedrijven die met privacy-gevoelige informatie omgaan, twijfel ontstaat, kan dat commercieel schaden.'*

> *'De vereiste om te rapporteren wordt alsmaar groter. Ik kan me voorstellen dat een aantal ondernemingen privacy nog steeds niet als heel strategisch zien, maar dat kan heel snel veranderen. Op het moment dat bedrijven in de publiciteit komen, dat ze hun privacy niet op orde hebben, kan dat enorm schaden, zowel het imago als het financieel deel.'*

Uit voorgaande blijkt dat het NIVRA juist kansen ziet in maatschappelijke veranderingen. Het

NIVRA heeft immers te maken met een toegenomen vraag naar een privacy-oordeel. Door de steeds verdergaande ontwikkelingen op technologisch gebied komt privacy onder druk te staan. Bedrijven weten vaak zelf niet wat wel of niet mag en wanneer zij 'privacy-proof' zijn. Het NIVRA ervaart dat bedrijven steeds vaker verantwoordelijkheid nemen door zelf te vragen om een privacy keurmerk, zodat ze er zeker van zijn dat ze aan alle privacy wetgeving voldoen.

De drie organisaties die in een technische omgeving opereren hebben ontwikkelingen op technologisch gebied opgemerkt en geven aan dat deze invloed hebben op het functioneren van de organisatie. Het is immers noodzakelijk bij te blijven en bij te scholen op het gebied van technologie en wat er wel en niet mag volgens de privacy-wetgeving. Een groot verschil tussen deze drie organisaties en de vorige drie organisaties is dat deze voornamelijk kansen zien in de maatschappelijke veranderingen, waar de vorige drie juist een bedreiging zien. Ook de oorzaken die ten grondslag liggen aan deze veranderingen zijn verschillend. Waar bij de eerste drie organisaties de aanslagen van 2001 genoemd werden, is dit bij deze drie organisaties niet het geval. Technologische ontwikkelingen die elkaar in rap tempo opvolgen worden als oorzaak gezien. Dit tempo ligt steeds hoger en het wordt lastiger voor organisaties om dit bij te houden. De heer Plasmooij zegt over zijn werk als ICT-manager het volgende:

> *'Je zal je continu moeten blijven ontwikkelen. Als je dit niet doet dan ben je volgens mij na 2 of 3 jaar niet meer in staat om je cliënten te helpen. Dat heeft te maken met de snelheid van de ontwikkeling.'*

Door verkeerd gebruik van deze technologieën wordt privacybescherming aangetast.

Ook bij deze drie organisaties is er een onderscheid te maken in de doelgroep die zij hebben. Wat je kunt zien is dat de organisaties met een specifieke doelgroep (het NIVRA en de NOREA) positiever zijn over hun kansen dan de organisatie met de algemene doelgroep (OBA Privacy Management Groep). Reden hiervoor is dat de specifieke organisaties waarmee het NIVRA en de NOREA samenwerken, zelf actie ondernemen om aan de privacywetgeving te voldoen. Het NIVRA en de NOREA informeren bedrijven over mogelijkheden, maar hoeven niet actief te werven. OBA Privacy Management Groep probeert zich op zoveel mogelijk bedrijven te richten. Dit zijn bedrijven die zelf (nog) niet bewust met privacy bezig zijn en het belang hiervan zal door

OBA Privacy Management Groep zelf duidelijk gemaakt moeten worden.

4.2.2 Samenvatting

Alle bestudeerde organisaties ervaren een spanningsveld tussen veiligheid en privacy in de maatschappij. Afhankelijk van de omgeving waarin zij opereren, interpreteren zij dit anders. Organisaties die in een institutionele omgeving opereren, ervaren de maatschappelijke ontwikkelingen als bedreigend. Zij zien een sterk afbrokkelend draagvlak voor privacybescherming. De belangrijkste oorzaak zijn volgens hen de terroristische aanslagen in 2001. Voor hen betekent het verminderde draagvlak tevens verminderde legitimiteit. Daar tegenover staat het beeld dat de organisaties, die in een technische omgeving opereren, hebben. Volgens deze organisaties is er eveneens sprake van een spanning tussen privacy en veiligheid. Als oorzaak wijzen zij echter op technologische ontwikkelingen die, bij onjuist gebruik, tot aantasting van privacy kunnen leiden. De oplossing wordt dan ook gezocht in het correcter toepassen van technologieën en gegevens. Deze organisaties zien dan ook juist kansen liggen in de huidige ontwikkelingen, aangezien zij specialisten zijn op het gebied van privacy en technologie.

4.3 De derde onderzoeksvraag

In deze paragraaf wordt antwoord gegeven op de derde onderzoeksvraag, namelijk hoe de besproken organisaties hebben gereageerd op de veranderingen zoals deze in paragraaf 4.1 besproken zijn. Paragraaf 4.3 is onderverdeeld is zes subparagrafen. De eerste vijf subparagrafen geven vijf strategieën weer die gebruikt worden door organisaties. De laatste subparagraaf geeft een samenvatting van de gevonden resultaten op de derde onderzoeksvraag.

4.3.1 Strategie 1 – Draagvlak creëren

Strategie 1a – Consensus building

De eerste strategie die toegepast wordt, is consensus building. Organisaties proberen door middel van coöperatie steun te vinden bij andere organisaties. Deze strategie valt onder de proactieve strategieën. Hasenfeld (1983) spreekt over coöperatie als een eenzijdige strategie om de grip op de omgeving te vergroten. Deze strategie werkt proactief op de omgeving in. Het CBP zoekt samenwerking met een partij met veel macht en legitimiteit. Door haar eigen ideeën in te passen in de visie van deze partij, kan zij proberen samenwerking te krijgen en legitimiteit te vergroten. De politiek besteedt veel aandacht aan veiligheid. Het CBP wil deze partij overtuigen van haar standpunt dat privacy en veiligheid geen tegenstelling is, maar dat deze juist samenwerken. Door de politiek aan haar kant te krijgen, kan het CBP meer legitimiteit verkrijgen.

Schaafsma wil duidelijk maken dat er volgens het CBP geen spanningsveld bestaat tussen privacy en veiligheid. Het CBP is van mening dat privacy een onderdeel is van veiligheid en deze twee niet tegenover elkaar staan, maar juist samenwerken. Dit is een van de belangrijkste boodschappen die het CBP uit wil dragen. Schaafsma vertelt:

> *'Onze voorzitter heeft via de media ook laten weten dat wij absoluut voor veiligheid zijn. Maar je moet je ook afvragen of aanvullende maatregelen ook nodig zijn in situaties. Wij hebben in het afgelopen jaar het idee gehad dat er een tegenstelling werd neergezet waar die tegenstelling in de praktijk niet echt bestaat. Het probleem in de praktijk is soms veel meer dat het soms lastig is dat er veel verschillende diensten zijn, zodat de bestaande bevoegdheden niet optimaal benut worden. Het is dus vaak niet strikt noodzakelijk nieuwe maatregelen te nemen.'*

Hiermee probeert het CBP tegenstanders te betrekken bij haar standpunt, zodat er een debat kan ontstaan. Wanneer het CBP voorstanders van veiligheid kan overtuigen dat veiligheid en privacy samengaan en geen tegenstelling hoeven te zijn, krijgt ze deze tegenstanders uiteindelijk ook aan haar kant.

Ook de voorzitter van het CBP doet een poging steun te krijgen van andere partijen, in dit geval de politiek. Naar aanleiding van de media-aandacht na het bekend worden van het feit dat

Nederlandse banken meewerking verlenen aan Amerikaanse geheime diensten die informatie over financiën opvragen, stelt Kohnstamm, voorzitter van het CBP:

> *'De complexiteit van de transatlantische gegevensverstrekking is te groot om aan de toezichthouders alleen over te laten. We zijn een kleine club en er zijn beperkingen aan hoeveel we kunnen onderzoeken.' De politiek moet de regie nemen en met ons optrekken. Hier staan Europese normen en waarden op het spel.' (NRC Handelsblad, 10 maart 2007).*

Strategie 1b – Informatievoorziening

Een tweede vorm van draagvlak creëren is het bieden van informatie. Bij alle organisaties is hier sprake van, al gaan ze hier allen op een andere manier mee om. Er zijn verschillende manieren om invulling te geven aan informatievoorziening. Bij alle organisaties is informatie te vinden via de website, al zijn sommige websites uitgebreider en duidelijker dan andere. Zo zijn de websites van het CBP en DeVrijePsych erg uitgebreid. Iedere organisatie noemt ook andere aspecten van informatievoorziening.
Het CBP gaat voornamelijk het gesprek aan:

> *'Met alle gezelschappen die hierbij betrokken zijn, alle partijen die hierbij betrokken zijn, probeer je in gesprek te raken en aandacht te vragen voor die noodzakelijkheidstoets [waarbij de noodzakelijkheid van aanvullende maatregelen ten behoeve van veiligheid worden bekeken].'*

Dhr. Fernald van OBA Privacy Management Groep vertelt:

> *'Wij hebben workshops ontwikkeld en we geven masterclasses. Die zijn voor een ieder, dat hangt af van het onderwerp. Het kan zijn voor interne functionarissen gegevensbescherming, het kan zijn voor een directie of bestuur.*
> *We hebben samen met Lemniscaat een FG-opleiding ontwikkeld die is gebaseerd op onze filosofie en daar kan men dus opgeleid worden van gecertificeerd FG-er tot master in de privacy. Ook dat gedeelte heb ik ontwikkeld. Maar ook via mailings en gesprekken overal.*

Ik lul me een slag in de rondte.
Wij zijn nog een jonge organisatie en proberen nu zoveel mogelijk onze filosofie onder de aandacht te brengen. Wij doen dit op dit moment niet via de media, maar hier zitten wellicht in de toekomst wel mogelijkheden.'

Ook hier is sprake van een proactieve aanpak en ligt de nadruk erop zoveel mogelijk bekendheid met de WBP en de privacyeisen te bereiken. Deze aanpak wordt gedeeld door Stichting Privacyloket.nl. Dhr. Klei vertelt:

'We hebben een internetsite waar elke burger vragen kan stellen. We zoeken ambassadeurs over heel Nederland die presentaties kunnen geven, daar hebben we de middelen voor. We zoeken gewoon binding met lokale punten die de aandacht kunnen schenken, zoals gemeentehuizen. We zijn bezig met brochures voor scholen [..].
Ik denk dat het hard nodig is om veel aandacht te geven aan privacyvraagstukken, omdat daarmee eigen gedrag gereguleerd kan worden door zelfregulering, zowel bij bedrijven als bij individuele personen.
Het gaat vooral om bewustwording. Veel mensen hebben wel een gevoel over privacy, maar geen denkwijze over privacy. Op het moment dat ze geconfronteerd worden met taken die daarop slaan gaan ze zich verzetten. Maar er wordt niet vooruit over nagedacht, er is geen gedachtegang van; als dit gebeurt moet ik zo en zo handelen.'

Bij het NIVRA is deze proactieve aanpak wat minder aanwezig. Plasmooij zegt hierover:

'Ons oordeel is vrijwillig, dus de druk komt niet vanuit de wet. Er ontstaat een maatschappelijke behoefte. Er zijn een aantal overheidsinstellingen die zich via onze wijze kunnen verantwoorden, en de verwachting is dat dat er meer zullen worden, en de maatschappelijke ontwikkeling die kant op gaat. [..] Zij zien dit op vrijwillige basis, omdat ze er een voordeel in zien. Als er bij bedrijven die met privacy-gevoelige informatie omgaan, twijfel ontstaat, kan dat commercieel schaden.'

Toch zorgt het NIVRA er ook voor dat ze af en toe bewust naar buiten treden:

‘Wij kunnen ook een stukje voorlichting geven, neutrale voorlichting over de diensten die beschikbaar zijn. Wat wij regelmatig doen, is zorgen dat er gepubliceerd wordt.’

Ook bij de NOREA ligt de nadruk op informatie. Olthof vertelt:

‘Onze voornaamste functie is het zijn van een doorgeefluik van nieuwe regels en richtlijnen en bijbehorende uitleg hoe dit in de praktijk moet worden toegepast. Dat is in feite onze belangrijkste taak. [..] We moeten de informatievoorziening op peil houden om te kunnen onderbouwen en ondersteunen hoe dit in de praktijk vorm moet krijgen. Onze voornaamste taak is het hele circus van educatie en regelgeving.’

Bij DeVrijePsych is ook de informatievoorziening belangrijk, al werken zij in tegenstelling tot de andere organisaties, meer reactief in plaats van proactief. Mengelberg legt uit:

‘Ze komen niet wanneer je wilt dat ze komen, ze werken volgens het systeem: don’t call us, we call you. De media komen naar jou.’

Al komt later in het gesprek toch ook naar voren dat ook zij wel actief mensen benaderen om hun boodschap uit te dragen:

‘We hebben wel beschikking over emailadressen van leden van verenigingen binnen de beroepstak, en dit zijn er duizenden. Via mailings proberen we iedereen te betrekken bij DeVrijePsych.’
‘In eerste instantie wil ik mijn collega’s erbij betrekken. En voor de rest wil ik iedereen erbij betrekken die geïnteresseerd is, het maakt niet uit wie of wat je bent. De manier waarop we dit doen, is een op een. Zoals op de besloten discussiesite, het persoonlijk contact is het meest interessant, omdat we dan intensiever en uitvoerig contact hebben en dieper op een onderwerp in kunnen gaan.’

Uit deze voorgaande stukken blijkt dat het creëren van draagvlak door alle partijen wordt

gebruikt als strategie. Consensus building wordt alleen toegepast door het CBP. Zij zoekt steun bij andere partijen. Doordat het CBP een dominante positie inneemt kan zij gemakkelijker gebruik maken van deze strategie. De strategie van informatievoorziening wordt echter wel door alle partijen toegepast. In ieder gesprek kwam het geven van informatie vrij snel naar voren en dit blijkt dan ook een belangrijke strategie te zijn voor de geïnterviewde partijen. Iedere organisatie heeft eigen kanalen om informatie naar buiten te brengen. Niet iedere organisatie heeft dezelfde mogelijkheden, en er zitten altijd restricties aan deze mogelijkheden. Het is niet altijd mogelijk de media te bereiken, grote organisaties zijn niet altijd benaderbaar en veel burgers zijn niet geïnteresseerd en geïnformeerd genoeg om als doelgroep te dienen. Het is dan ook vaak de vraag op welke partijen ze zich *kunnen* richten en wie ze kunnen bereiken met hun boodschap Alleen het CBP heeft hierin meer macht, zij is immers toezichthouder en kan invloed uitoefenen op partijen die zij zelf uitkiest, zoals politie en justitie. Dit doet zij dan ook op strategische wijze. Zo kiest zij er heel bewust voor hoofd commissarissen bij de politie te benaderen om ervoor te zorgen dat de boodschap van het CBP bij een grote groep mensen terecht komt.

4.3.2 Strategie 2 - Mediamanipulatie

De samenleving komt het meest in aanraking met het CBP via de media, en de media zorgen dan ook voor een belangrijk deel voor de beeldvorming van de burgers over het CBP. Het eerste wat opvalt wanneer we kijken naar het CBP en haar relatie tot de media is de explosieve stijging van artikelen in kranten waar het CBP in voorkomt. Van 1998 tot 2002 zijn er 75 artikelen verschenen waar het CBP (of de Registratiekamer) in voorkwam, tegenover 182 artikelen in alleen 2006. Dit kan verschillende oorzaken hebben. Ten eerste kan dit betekenen dat het CBP de media beter weet te bereiken (en bespelen). Het kan natuurlijk ook andersom werken; de media weten het CBP steeds meer te vinden bij onderwerpen over waarborging van privacy.
Wanneer ik Schaafsma hiernaar vraag zegt ze:

> *'Ja ik denk dat dat wel kan kloppen. Het is een bewuste keuze, maar ook gedeeltelijk een antwoord op de vragen die van buitenaf komen. Het is belangrijk ons verhaal te laten horen. De pers houdt er ook van iets uit een verdomhoekje te halen en juist die partij uit*

te nodigen om zijn verhaal te vertellen, dus het is van twee kanten gekomen.'

Er is dus sprake van een wisselwerking; Het CBP zoekt de pers steeds vaker bewust op om haar verhaal te kunnen vertellen, maar wordt door de media zelf ook benaderd.
Klaarblijkelijk heeft het CBP veel aan aandacht gewonnen in de afgelopen jaren, en dit is niet alleen zichtbaar in het aantal krantenartikelen. Ook de jaarverslagen van het CBP worden steeds langer en uitgebreider en het aantal bezoekers van de website is ook gestegen:

'*Het aantal telefoontjes is de afgelopen jaren gestaag gestegen en lijkt nu stabiel te zijn geworden. De email die wij krijgen stijgt ieder jaar enorm. Wat nog wel het meeste stijgt is het website bezoek.'*

Een strategie van mediamanipulatie lijkt dan ook een voor de hand liggende strategie waar deze instantie mogelijk gebruik van maakt. Het CBP probeert ook via de politiek ruimte te creëren om haar verhaal te kunnen doen en de aandacht op privacy te kunnen vestigen. Om dit te kunnen doen, wil het CBP echter wel neutraal blijven en niet via een bepaalde politieke partij willen spelen of inspelen op het politieke klimaat van het moment. Dit was zichtbaar in de tijd dat het CBP stelde dat Rita Verdonk zich schuldig had gemaakt aan privacyschending in de zaak van Taida Pasic. Op 30 mei 2006 verscheen hierover een artikel in het AD, waarin het CBP stelde dat Minister Verdonk de persoonlijke gegevens van Pasic niet openbaar had mogen maken. Het tijdstip van het naar buiten brengen van dit artikel was erg belangrijk. Schaafsma vertelt hierover:

'We hebben toen in de zaak van Taida enorm goed opgelet wanneer we dit naar buiten gebracht hebben. We wilden namelijk geen rol spelen in het politieke spel dat gaande was. Dit was volgens mij precies in de periode waarin de VVD haar nieuw politiek leider koos, en wij wilden ons hier absoluut niet mee bemoeien. De mededeling over Taida hebben wij wel gedaan, omdat er ook veel vraag van de pers was naar aanleiding van ons onderzoek. Maar dat hebben we volgens mij gedaan precies in de week dat de stemming bij de VVD was gesloten, maar dat uitslag nog niet bekend was gemaakt. Daar is echt over nagedacht.'

'Wat we wel hebben gedaan sinds de afgelopen twee jaar is dat we iets meer richting de Eerste Kamer of Tweede Kamer onze standpunten verduidelijkt hebben. We hebben een officiële taak om informatie over de WBP bekend te maken en advies te geven. Als ons punt onder de aandacht komt is het wel zaak om dit geen ondergesneeuwd kindje te laten worden. Daar proberen we wel heel hard aan te werken.'

'Nee dat zou hier niet geëigend zijn geweest, want het leiderschap bij de VVD heeft niets te maken met een zaak als Taida. Dus je wil een uitspraak doen over die kwestie, maar je wil niet dat dat een politieke lading krijgt, want daar zijn wij niet voor.'

Het CBP heeft in deze situatie rekening gehouden met de media. Zij hebben bewust gewacht met het naar buiten brengen van het artikel. Wanneer ze dit niet gedaan hadden, hadden de media wellicht discussie geopend over de neutraliteit van het CBP. Dit terwijl de media zelf niets te maken hebben met de zaak Taida Pasic. Het CBP houdt rekening met de media om haar positie als onafhankelijk en neutrale partij te behouden. Deze strategie houdt het midden tussen twee door Gilboy beschreven strategieën: amplification en assimilation. Beide vormen zijn terug te vinden in deze strategie. Amplification betekent het nemen van beslissingen met inachtneming van reacties van derden en eventuele consequenties voor de organisatie nu en in de toekomst. In dit geval is dit zichtbaar in het wachten met het naar buiten brengen van het artikel, vanwege de mogelijke discussie over de neutraliteit van het CBP. Assimilation is het afstemmen van beslissingen en acties op het ritme van de organisatie, in dit geval het wachten tot de stemming bij de VVD was gesloten.

4.3.3 Strategie 3 – Uitbreiding van taken en bevoegdheden

Een derde manier van aanpassing aan de sociale omgeving is de uitbreiding van de taken en bevoegdheden. Hierdoor kan een organisatie meer invloed uitoefenen, omdat zij meer bevoegdheden heeft om dit te doen. De uitbreiding van taken en bevoegdheden is een feitelijke strategie. Meyer en Rowan (1977) maken onderscheid tussen een symbolische en een feitelijke strategie. Bij een symbolische strategie verandert een organisatie niet echt, zij verandert alleen haar imago. Bij de uitbreiding van de taken en bevoegdheden is er echter een feitelijke

verandering zichtbaar binnen een organisatie.

We zien deze strategie terug bij het CBP. Het CBP had een voorganger; de Registratiekamer. Taak van de Registratiekamer was het toezicht houden op persoonsregistraties. Met de invoering van de nieuwe Wet Bescherming Persoonsgegevens (WBP) is de Registratiekamer omgevormd naar het CBP. Het CBP heeft meer taken en bevoegdheden dan de Registratiekamer had. Zo is adviesvorming een belangrijke taak geworden van het CBP. Hierdoor lijkt het CBP een andere rol te hebben gekregen; ze kunnen nu onderzoeken doen en met de uitslagen hiervan ook daadwerkelijk een analyse maken en zo bijdragen aan een verbetering van omgang met persoonsgegevens. Het CBP heeft de vrijheid zelf haar taken af te bakenen, uiteraard met inachtneming van de wet en het oordeel van de rechter. Wel was de beslissing om van Registratiekamer naar CBP te gaan Europees vastgelegd. Toch was volgens Schaafsma de Nederlandse overheid helemaal klaar voor uitgebreidere bevoegdheden voor het CBP:

> *'De nieuwe wet [WBP] is een implementatie van een Europese richtlijn, waardoor ieder Europees land dezelfde taken bij een privacybeschermende organisatie moest leggen. [En] ik geloof wel dat Nederland dat wel graag wilde.'*

Het CBP is content met deze verandering in de taakuitbreiding, zij eigent zich deze rol graag toe. Deze verandering is een feitelijke verandering binnen de organisatie. Er zijn nieuwe taken bijgekomen en dit heeft direct invloed gehad op de organisatie.

Stichting Privacyloket.nl legt ook nadruk op de taken die zij hebben. Een feitelijke strategie van Stichting Privacyloket.nl is het opleggen van sancties aan bedrijven. Zij hebben niet de bevoegdheden om boetes uit te delen, maar hebben wel een andere troef in handen. Dhr. Klei vertelt:

> *'De sanctie is dat wij het kunnen publiceren op het Internet, dat een bedrijf over de schreef gaat. En daar zijn bedrijven vaak gevoelig voor.'*

Dit is een van de taken die Stichting Privacyloket.nl heeft en zij kan zodoende druk uitoefenen op bedrijven die niet voldoen aan de privacywetgeving. Op deze manier verhoogt ze haar

legitimiteit.

4.3.4 Strategie 4 - Objectivering

Een vierde strategie omvat een symbolische strategie. Bij deze strategie verandert er binnen een organisatie niets, maar verandert het imago wat deze organisatie heeft. Organisatiekenmerken veranderen niet, terwijl de legitimiteit wel verhoogd wordt (Meyer en Rowan, 1977). In het geval van het CBP probeert zij een imago neer te zetten van objectiviteit en neutraliteit. Er zijn een aantal voorbeelden te noemen waaruit dit blijkt.

Het belang van juridische verantwoording is groot. Op de site van het CBP worden veel wetten en regelingen genoemd waar de meeste burgers niet in geïnteresseerd zijn en begrijpen. Om een voorbeeld te noemen: bij de klachtenbehandeling wordt verteld dat het CBP handelt in overeenstemming met hoofdstuk 9 van de Algemene wet bestuursrecht. Het is niet erg aannemelijk dat mensen bij het indienen van een klacht ook daadwerkelijk weten of opzoeken wat deze wet precies inhoudt en voorschrijft. Logischerwijs dient het CBP zich te houden aan de wetten die voor zoiets als klachtenbehandeling staan. De symboliek werkt dan ook twee kanten op, deze wetten zorgen voor de symbolische waarde van betrouwbaarheid en voor de symbolische waarde van transparantie en controleerbaarheid. Schaafsma vertelt hierover:

> *'Wat altijd wel een dilemma is, is de leesbaarheid van onze uitspraken versus de juridische houdbaarheid en kwaliteit. Het laatste is erg belangrijk voor ons, omdat we moeten kunnen laten zien waar we onze uitspraken nu eigenlijk op baseren. Heel vaak is dat ingewikkeld.*
> *Bij sommige juridische stukken schieten we ons doel een beetje voorbij, omdat het voor professionals goed leesbaar is, maar voor de gewone mensen niet. Je moet niet te technisch over artikelen spreken, omdat je dan niet goed helder maakt wat precies het probleem is.'*

Ook geeft het CBP aan dat zij meer tijd zou willen besteden aan het doen van onderzoeken. Schaafsma zegt hierover:

'Het is natuurlijk wel zo dat je op het moment dat je taken moet invullen [..] je moet kijken hoe je dat moet doen. Ieder jaar bekijken we dit ook opnieuw en groeien we hierin. We vinden dat we nog meer naar onderzoeken moeten, dit gebruik blijkt ook nodig te zijn. En wat we ook willen, daar komt de aandacht in de pers ook weer bij kijken, dat a) de wet bekend is en b) ook bekend is dat er een toezichthouder is die ervoor zorgt dat deze wet wordt nageleefd. Dit maakt dat je ook graag naar buiten wilt treden.'

Door het doen van veel onderzoeken wordt de nadruk gelegd op de objectiviteit en onafhankelijkheid van het CBP.
Ook politieke neutraliteit is, zoals beschreven bij de tweede strategie, belangrijk voor het CBP.

4.3.5 Strategie 5 – Samenwerking met het CBP

De vijfde strategie heeft te maken met samenwerking tussen de partijen onderling. Het NIVRA en de NOREA werken samen door de privacy audits die zij hebben ontwikkeld. Ook Stichting Privacyloket.nl en OBA Privacy Management Groep werken samen. Wat echter interessant is om te bekijken, is hoe het CBP zich verhoudt tot deze partijen? Het CBP is immers een autoriteit op het gebied van privacybescherming, zij neemt een dominante positie in. Alle partijen zijn in meer of mindere mate afhankelijk van de regelgeving die het CBP stelt.
Deze strategie is een symbolische strategie die valt onder de typering van isomorfisme. Wanneer we kijken naar samenwerking zijn er twee groepen te onderscheiden, namelijk de organisaties die zich associëren met het CBP en de organisaties die zich distantiëren van het CBP. De associatie met het CBP kan worden ondergebracht in de strategie van isomorfisme, waarbij organisaties samenwerken en meer op elkaar gaan lijken om een sterkere positie te verkrijgen. De distantiatie van het CBP kan worden ondergebracht in de strategie van xenomorfisme (xeno = vreemd), waarbij partijen juist in protest komen en zich afzetten tegen een andere partij.
Hieronder is te zien dat OBA Privacy Management Groep, Stichting Privacyloket.nl en DeVrijePsych kritisch zijn ten opzichte van het CBP.

Zo zegt dhr. Fernald (OBA Privacy Management Groep):

'Het is belangrijk te kijken hoe het gesteld is met de rechtsgelijkheid in de afhandeling van klachten van burgers waarbij de burger geen ondersteuning heeft gehad van deskundigen en bedrijven wel. Dat is mijn gevoel over het CBP; dat zij aan de kant van de bedrijven staan, maar niet bij de individuele burger. Hierdoor zijn de uitslagen en uitspraken van het CBP altijd ten gunste van de bedrijven.'

'Het CBP pakt dingen naar mijn mening vooral theoretisch aan. Als je de opdracht hebt om de belangen van de burger die gebaseerd zijn op de grondwet te controleren, dan moet je veel voortvarender en actief aan de slag gaan. Je moet niet wachten tot de burger het bewustzijn heeft een klacht in te dienen om het dan schriftelijk af te handelen.'

'En de controleurs van het geheel, het CBP, daar ontbreekt die deskundigheid, die technische kennis. Daar zit volgens mij wrijving, omdat je een puur theoretische afhandeling krijgt van situaties. Vandaar dat wij Stichting Privacyloket ondersteunen, omdat zij intermediating aanbiedt. Zij heeft deskundigheid in huis om te kunnen zeggen: Oh is dat een klacht, wij kunnen via intermediating kijken of de situatie voldoet aan de criteria van de wet en moet dat eventueel aangepast worden.'

'Er ontstaat een gigantische barrière, ze zitten in een hoge toren ver van de burger af, zijn bijna niet benaderbaar en handelen alles zeer theoretisch af. Terwijl de burger het recht heeft op basis van de Europese richtlijn dat de overheid garandeert dat je recht op privacy wordt gerespecteerd.'

Dhr. Klei van Stichting Privacyloket.nl is eveneens van mening dat het CBP haar taken niet op de juiste manier uitvoert. Hij zegt over de eigen taken van Stichting Privacyloket.nl:

'En dit gaat dus allemaal buiten het CBP om. Het is een reguleringsmechanisme wat het CBP eigenlijk laat liggen.
Het CBP gaat in op individuele vragen van burgers en is veel drukker met regelgeving en onderzoeken naar hoe het in Nederland goed vormgegeven kan worden. Dat is op zich natuurlijk ook gedreven door tekorten op het gebied van mensen en middelen die het CBP

zelf heeft.'

Ook dhr. Mengelberg (DeVrijePsych) is niet erg te spreken over de beslissingen van het CBP. Hij vertelt hierover:

> *'Er zijn aardige stukken geschreven door het CBP over het beroepsgeheim. Dit hebben we op de DeVrijePsych ook geciteerd. Maar ik heb het idee dat ze zich gewoon hebben laten omlullen door de staat, en met name in de brief van 6 december, waar ze in feite het beroepsgeheim hebben vrijgegeven. [hierin stond onder andere: "...Daarmee [is] naar het oordeel van CBP voldoende aannemelijk gemaakt dat ...diagnose-informatie op de declaratie ten behoeve van de zorgverzekeraar noodzakelijk moet worden geacht...".[bron:www.devrijepsych.nl]]. Dat is zeer teleurstellend ... . Het CBP heeft sinds kort ook een popi jopi site gemaakt, ik weet niet of je dat hebt gezien [mijnprivay.nl], met een cartoonachtig idee.'*
>
> *'Ik heb de indruk dat hun positie ... niet helemaal optimaal is. Ze hebben best hele goede stukken op die site staan, maar ik heb de indruk dat ze behoorlijk in het nauw zitten.'*

Ook in een reactie van Mengelberg op een brief die hij van het CBP toegestuurd kreeg naar aanleiding van een opmerking van zijn kant over de privacyschending bij zorgverzekeraars, blijkt dat hij niet erg te spreken is over het CBP:

'De stellingname van het CBP is teleurstellend. Het CBP erkent weliswaar het medische beroepsgeheim als uitgangspunt, maar verklaart dit vervolgens tot (relatief) inhoudsloos door haar verwijzing naar een opsomming van omstandigheden waarin dit geschonden moet of kan worden. Het CBP concludeert dat "een patiënt kan er niet vanuit gaan dat het medisch beroepsgeheim boven alles moet kunnen gaan".
Het is spijtig te moeten vaststellen dat het CBP haar tot voor kort kritische houding inzake de bescherming van het medische beroepsgeheim binnen de context van actuele wet- en regelgeving heeft opgegeven'. (DeVrijePsych; Kaspar Mengelberg, 22 februari 2007).

Deze drie organisaties distantiëren zich duidelijk van het CBP en uiten expliciet kritiek. Alledrie verwijten zij het CBP coöptatie. Dit vindt plaats wanneer een organisatie haar legitimiteit ziet verdwijnen. Om dit tegen te gaan kiest de organisatie ervoor een deel autonomie in te leveren voor steun en legitimiteit. OBA Privacy Management Groep en Stichting Privacyloket.nl verwijten het CBP coöptatie aan bedrijven. Het CBP staat volgens deze organisaties altijd aan de kant van de bedrijven. Mengelberg van DeVrijePsych verwijt het CBP coöptatie aan de staat, het CBP heeft haar oorspronkelijke kritische houding laten varen om zich te conformeren aan de overheid.

Bij het NIVRA en de NOREA zien we dat zij juist zeer te spreken zijn over het CBP. Bij het ontwerpen van een raamwerk voor privacy hebben zij de goedkeuring en steun gehad van het CBP, waardoor deze privacy audits snel konden worden verwezenlijkt. Plasmooij (NIVRA) vertelt hierover:

> *'We hebben toen een aantal jaren samengewerkt om het raamwerk te maken. ... We waren toen heel snel klaar, omdat we dit zelf konden doen, en het College heeft dit altijd gesteund.'*

Dit zelfde punt wordt ook door de NOREA genoemd wanneer we praten over het CBP. Olthof zegt hierover:

> *'Zij onderkennen dat het belangrijk is dat organisaties op de hoogte zijn van de WBP en de eisen die deze wet stelt, en het belang dat een derde onafhankelijke partij daar een oordeel over kan vellen. In dit opzicht zagen ze ons ... als een partner om deze taak te vervullen.* [..] *Als er een commercieel belang is bij het afgeven van privacy oordelen kunnen ze zich daar als toezichthouder niet mee bemoeien. Dan moeten ze hun onafhankelijkheid niet in de strijd gooien, ze moeten afstand bewaren van de markt van de privacy.'*

Het NIVRA en de NOREA zijn partijen die wel graag samenwerken en zich positief uitlaten over het CBP. Zij opereren in een technische omgeving en dienen, aldus de theorie, te voldoen aan de eisen die de markt stelt. Zij opereren, als privacy auditeurs, echter ook in een institutionele

omgeving. Het ‘keurmerk’ dat het CBP als het ware aan deze bedrijven verschafte door mee te werken aan de totstandkoming van de privacy audits, verschaft het NIVRA en de NOREA legitimiteit in de ogen van hun klanten. Om efficiënt in een technische omgeving, het bedrijfsleven, te kunnen functioneren, dienen zij dus te voldoen aan de normatieve eisen zoals die in een institutionele omgeving gelden. Het gevolg is dat zij zich vrijwillig conformeren aan hun omgeving. Dit is wat DiMaggio en Powell institutioneel isomorfisme: organisaties die zich conformeren aan hun institutionele omgeving en zo steeds meer op elkaar gaan lijken. Door zich vrijwillig aan (de kwaliteitsnormen van) het CBP te conformeren, hun institutionele omgeving, gaan het NIVRA en de NOREA steeds meer op het CBP lijken en krijgen zij meer aanzien in de ogen van hun technische omgeving (met name hun klanten). Deze vorm van institutioneel isomorfisme wordt door DiMaggio en Powell isomorfisme door imitatie genoemd.

Volgens DiMaggio en Powell kunnen organisaties zich aanpassen aan andere organisaties, om zodoende een goede indruk te maken. Zij noemen dit isomorfisme. Deze strategie is duidelijk zichtbaar bij het NIVRA en de NOREA, die zich associëren met het CBP om zo meer legitimiteit te verkrijgen. DeVrijePsych, het Privacyloket.nl en de OBA Privacy Management Groep hanteren een tegenovergestelde strategie: zij zetten zich juist af tegen het CBP. Zij leggen niet de nadruk op de overeenkomsten met het CBP, maar benadrukken juist de verschillen. Deze strategie van distantiëren kan xenomorfisme genoemd worden en wordt dus ten onrechte over het hoofd gezien door DiMaggio en Powell.

4.3.6 Samenvatting

Ik heb ter beantwoording van de derde onderzoeksvraag vijf strategieën onderscheiden, namelijk het creëren van draagvlak, mediamanipulatie, uitbreiding van taken en bevoegdheden, objectivering en samenwerking.

Tot slot kun je je afvragen waarom een organisatie voor een bepaalde strategie kiest. Zoals beschreven bij de strategie van consensus building heeft dit te maken met de mogelijkheden die organisaties hebben.
Het is dhr. Mengelberg, oprichter van DeVrijePsych die wijst op de grenzen die zitten aan de keuze van de partijen waar een organisatie zich op kan richten. Hij zegt hierover:

‘Wanneer mensen geconfronteerd worden met teksten die totaal onbegrijpelijk zijn kiezen de meeste mensen ervoor om het er maar gewoon bij te laten.’

De geïnterviewde organisaties proberen allen te kijken naar partijen die veel gevoelige informatie bezitten, zoals ziekenhuizen of verzekeraars, of naar partijen die bevoegdheden hebben die de privacy aan kunnen tasten, zoals politie en justitie. Niet iedere organisatie kan deze partij echter bereiken. Om zoveel mogelijk invloed te hebben, trachten zij zoveel mogelijk mensen te bereiken. Aangezien het CBP een dominante positie inneemt en een autoriteit is op het gebied van privacy, kan zij bewuster voor een bepaalde strategie kiezen dan de andere organisaties. Zij heeft de legitimiteit voor de organisatie voor een groter deel zelf in de hand dan de andere vijf organisaties uit het onderzoek.

Hoofdstuk 5; Samenvatting en Conclusies

5.1 Inleiding op de probleemstelling

Organisaties zijn afhankelijk van hun omgeving voor bepaalde bronnen. In deze scriptie heb ik onderzoek gedaan naar organisaties die voornamelijk in een institutionele omgeving opereren. Dat wil zeggen dat zij een bepaalde waarde vertegenwoordigen en proberen deze waarde in stand te houden. Dit type organisatie is afhankelijk van de normatieve consensus vanuit de omgeving, dat de waarde die zij vertegenwoordigt belangrijk is. Deze normatieve consensus is echter onderhevig aan veranderingen. Het is dan ook interessant om te bezien hoe organisaties omgaan met veranderingen in hun omgeving die hun legitimiteit bedreigen. De probleemstelling van deze scriptie luidt dan ook:

Hoe reageren organisaties die te kampen krijgen met afnemende legitimiteit vanuit hun omgeving en welke strategieën gebruiken zij om (meer) legitimiteit te verkrijgen?

Organisaties beschikken over verschillende aanpassingsstrategieën om hun legitimiteit te vergroten of behouden. Zo is er het onderscheid tussen proactieve en reactieve strategieën, waarbij een organisatie haar greep op de omgeving probeert te vergroten (proactief) en waarbij zij reageert op druk vanuit de omgeving (reactief). Daarnaast is er nog de strategie van wederkerige beïnvloeding, een combinatie van de proactieve en reactieve strategieën, waarbij beïnvloeding zowel door de organisatie als door de omgeving plaatsvindt. Ten slotte, kan onderscheid worden gemaakt tussen feitelijke aanpassing, waarbij de organisatie van binnenuit beleidsmatig daadwerkelijk verandert, en symbolische aanpassing, wat alleen aan de buitenkant van de organisatie plaatsvindt en niets binnen de organisatie zelf verandert.

Een voorbeeld van een waarde die recentelijk onder vuur is komen te liggen, is privacybescherming. Voor deze scriptie heb ik onderzoek gedaan naar organisaties die te maken krijgen met afnemende legitimiteit vanuit hun omgeving. Ik heb kwalitatief onderzoek verricht onder zes organisaties, die zich op de een of andere manier bezig houden met privacybescherming: het CBP, DeVrijePsych, Stichting Privacyloket.nl, NIVRA, NOREA en OBA Privacy Management Groep.

5.2 Resultaten

De probleemstelling valt uiteen in de volgende deelvragen:

1. Is er sprake van onderschikking van privacybescherming ten opzichte van andere doelen?

2. Hebben partijen die zich inzetten voor de privacybescherming ervaren dat er maatschappelijke veranderingen hebben plaatsgevonden die van invloed zijn op hun functioneren en/of legitimiteit en aan welke oorzaken schrijven zij dit toe?

3. Hoe hebben partijen die zich inzetten voor de privacybescherming gereageerd op deze maatschappelijke veranderingen? Specifieker: Welke strategieën hebben zij gebruikt om te kunnen blijven functioneren en/of hun legitimiteit te kunnen blijven garanderen?

Ter beantwoording van de *eerste onderzoeksvraag* was het belangrijk af te bakenen wat de maatschappelijke veranderingen zijn die de onderschikking van privacybescherming veroorzaken. Wanneer we kijken naar privacy zijn drie aspecten van belang. De ontwikkeling in de aandacht voor privacy zelf, de ontwikkelingen op het gebied van veiligheid en de ontwikkelingen op het gebied van technologie.
Uit verschillende onderzoeken is gebleken dat de privacy geen prioriteit heeft bij burgers. Pas wanneer mensen zelf te maken krijgen met privacyschending (en dit ook zo ervaren) gaan ze zich meer verdiepen in het onderwerp. Het is een onderwerp dat in het bewustzijn van de mensen wel aanwezig is, maar het neemt geen prominente plaats in. Op het gebied van veiligheid is echter wel veel veranderd. Na de aanslagen is er een sfeer ontstaan waarin veiligheid prioriteit heeft gekregen. De dreiging van terreur wordt als dermate ervaren dat burgers van de overheid bescherming van de veiligheid verwachten. Burgers vinden het dan ook geoorloofd maatregelen te nemen, zoals het plaatsen van camera's of het toezeggen van meer bevoegdheden voor politie. Dat de privacy hierdoor wordt aangetast, wordt bij deze beslissingen op de koop toe genomen. Wanneer burgers moeten kiezen tussen privacy en veiligheid, kiest maar liefst 71% voor veiligheid tegenover 25% voor privacy. Ook op het gebied van technologische ontwikkelingen heeft de wereld niet stilgestaan. Technologische ontwikkelingen volgen elkaar in rap tempo op en

er is op het Internet al zoveel informatie beschikbaar dat dit onherroepelijk leidt tot aantasting in de privacy. Doordat steeds meer mensen in het Internet actief zijn, zijn steeds meer gegevens over mensen traceerbaar, bijvoorbeeld via het programma Google. De brede acceptatie van cameratoezicht geeft aan dat burgers deze ontwikkeling steunen. Deze drie aspecten wijzen erop dat de aandacht voor privacy ondergeschikt is aan aandacht voor veiligheid en technologie.

Ter beantwoording van de *tweede onderzoeksvraag* heb ik gekeken naar de ervaren maatschappelijke veranderingen door organisaties. Alle bestudeerde organisaties ervaren een spanningsveld tussen veiligheid en privacy in de maatschappij. Afhankelijk van de omgeving waarin zij opereren, interpreteren zij dit anders. Organisaties die in een institutionele omgeving opereren, ervaren de maatschappelijke ontwikkelingen als bedreigend. Zij zien een sterk afbrokkelend draagvlak voor privacybescherming. De belangrijkste oorzaak is volgens hen de terrorismedreiging sinds de aanslagen in 2001. Voor hen betekent het verminderde draagvlak tevens verminderde legitimiteit. Daar tegenover staat het beeld van de organisaties die in een technische omgeving werken. Volgens deze organisaties is er eveneens sprake van een spanning tussen privacy en veiligheid. Als oorzaak wijzen zij echter op technologische ontwikkelingen die, bij onjuist gebruik, tot aantasting van privacy kunnen leiden. De oplossing wordt dan ook gezocht in het correcter toepassen van technologieën en gegevens. Deze organisaties zien dan ook juist kansen liggen in de huidige ontwikkelingen, aangezien zij specialisten zijn op het gebied van privacy en technologie.

De *derde onderzoeksvraag* bevatte de vraag hoe deze partijen hierop gereageerd hebben en wat zij precies doen om hun legitimiteit te behouden?
Ik heb vijf strategieën onderscheiden.

1. Creëren van draagvlak - Proactieve strategie
1a. Consensus building. Het CBP zoekt samenwerking met een partij met veel macht, zoals justitie en politie. Door te stellen dat er geen tegenstelling bestaat tussen veiligheid en privacy proberen zij een opening te vinden voor samenwerking.
1b. Informatievoorziening. Het uitdragen van de boodschap van privacy blijkt het belangrijkste doel te zijn bij alle geïnterviewde organisaties. Zij maken gebruik van verschillende voorzieningen om informatie te delen, zoals websites, persoonlijke gesprekken of workshops.

2. Mediamanipulatie - Reactieve strategie

Het CBP bespeelt de media om haar boodschap naar buiten te kunnen brengen. Zij moet echter ook rekening houden met de media, omdat de media ervoor kunnen zorgen dat het CBP haar imago van neutraliteit en objectiviteit verliest. Timing voor het naar buiten treden is dan ook een belangrijke strategie. Het beïnvloeden van de media is een voorbeeld van een reactieve strategie. Het anticiperen op eventuele reacties van derden en het daarom afstemmen van het naar buiten treden op het ritme van een politieke partij, vormen voorbeelden van amplification en assimilation. Dit zijn indirecte strategieën.

3. Uitbreiding van taken en bevoegdheden - Feitelijke strategie

Door uitbreiding van taken bevoegdheden heeft het CBP meer macht en invloed. Dit leidt tot een grotere legitimiteit. Ook Stichting Privacyloket.nl wijst op de bevoegdheden die zij hebben om bedrijven te bewegen hun privacy op orde te maken.

4. Objectivering - Symbolische strategie

Bij deze strategie probeert het CBP een imago van objectiviteit te creëren, zonder dat er feitelijk iets in de organisatie verandert. Zij besteedt bijvoorbeeld veel aandacht aan het belang van onderzoeken en juridische verantwoording, dit verhoogt het beeld van het CBP als onafhankelijke instantie.

5. Samenwerking met CBP - Symbolische strategie

De onderlinge samenwerking van organisaties blijkt onderverdeeld te zijn in twee groepen; de organisaties die zich associëren met het CBP (het NIVRA en de NOREA) en de organisaties die zich distantiëren met het CBP (OBA Privacy Management Groep, Stichting Privacyloket.nl en DeVrijePsych). Dit zegt iets over de wijze waarop ze naar de overheid kijken. Het NIVRA en de NOREA hebben er baat bij positief te zijn over het CBP, omdat het CBP hen meer legitimiteit geeft door mee te werken aan de ontwikkeling van privacy audits. Dat laatste valt aan te merken als institutioneel isomorfisme. De organisaties die zich afzetten tegen het CBP gebruiken een strategie die kan worden aangeduid als xenomorfisme.

Een vraag die voortvloeit uit deze strategieën, is waarom de organisaties kiezen voor de strategie

die zij hanteren. Hier is geen eenduidig antwoord op te geven. Organisaties hebben geen oneindige mogelijkheden. Zo is de media niet altijd bereikbaar, zijn grote organisaties zijn niet altijd makkelijk te benaderen en zijn veel burgers niet geïnteresseerd en geïnformeerd genoeg om als doelgroep te dienen. Het is dan ook vaak de vraag welke strategie partijen *kunnen* gebruiken en wie ze hiervoor kunnen bereiken. Alleen het CBP heeft hierin meer macht, zij is immers toezichthouder en kan invloed uitoefenen op partijen die zij zelf uitkiest, zoals politie en justitie, wat zij dan ook heel bewust doet.

5.3 Conclusies

Er zijn uit dit onderzoek drie hoofdconclusies te trekken, die voortvloeien uit de drie deelvragen.

Ten eerste kun je stellen dat het draagvlak voor privacybescherming verminderd is. De waardering voor privacy van burgers is al niet groot. Dit wordt echter nog versterkt door een bredere acceptatie en steun voor veiligheidsmaatregelen en technologische ontwikkelingen. Privacybescherming wordt gezien als ondergeschikt aan andere waarden zoals veiligheid en technologische ontwikkeling.

Ten tweede is te concluderen dat de mate waarin deze veranderingen worden ervaren, afhangt van het type omgeving dat een organisatie heeft. Er is gebleken dat een veranderende consensus niet per se een negatief gevolg hoeft te hebben voor de legitimiteit van een organisatie. Organisaties die deels in een institutionele en deels in een technische omgeving werken, kunnen kansen zien wanneer er minder waardering is voor privacybescherming. Wanneer bedrijven of andere organisaties zelf geen oog hebben voor privacybescherming, kunnen zij hun diensten aanbieden op de markt en hun voordeel doen met de geringe kennis over privacybescherming.

Ten derde kun je concluderen dat het CBP de organisatie is die het meeste gebruik maakt van aanpassingsstrategieën. Het CBP neemt een dominante positie in binnen het domein van privacybescherming. Door deze sterke positie is zij meer in staat mogelijke strategieën toe te passen. De andere, kleinere, organisaties hebben deze opties niet. Zij zijn vaak beperkt tot het bieden van informatie. Hiernaast kunnen zij er voor kiezen zich af te zetten tegen het CBP of juist samenwerking te zoeken met het CBP. Op deze manier kunnen zij een signaal afgeven met betrekking tot de tevredenheid over het CBP. Tevens worden de strategieën met name toegepast

door de organisaties die geheel in een institutionele omgeving werken. Dit omdat juist zij zich meer bedreigd voelen dan de organisaties die deels in een technische omgeving werken. Het is gebleken dat deze laatste groep juist kansen ziet in de veranderende opinie over privacybescherming.

5.4 Wetenschappelijke bijdrage

Aan het begin van deze scriptie zijn er een aantal organisatietheorieën besproken. Een van deze theorieën was de ecology population theorie. Deze theorie stelt dat een organisatie die zich meer aan moet passen aan de omgeving dan een andere, meer moeite zal hebben te overleven. Organisaties die door de omgeving al gelegitimeerd zijn, hebben meer bestaansrecht opgebouwd. Een organisatie die veel veranderingen moet ondergaan om zich aan te passen, wordt meer bedreigd in haar legitimering.
Uit deze scriptie is gebleken dat deze theorie niet algemeen geldig is. De organisaties die in deze scriptie geïnterviewd zijn voelden wel degelijk druk om de omgeving te overtuigen van het belang van privacy en het bestaan van hun organisatie. Door hierop te anticiperen maken zij zich juist sterker in hun omgeving in plaats van zwakker. Het blijkt dus dat aanpassingen in sommige gevallen wel degelijk nodig zijn om te kunnen blijven bestaan.

Tevens is gebleken dat een organisatie, door zich te distantiëren van een andere partij, verhoogde legitimiteit kan krijgen. DiMaggio en Powell spreken van isomorfisme als strategie om meer legitimiteit te krijgen. Zij zien echter over het hoofd dat juist een tegengestelde strategie, xenomorfisme, eveneens kan zorgen voor verhoogde legitimiteit.

Literatuurlijst

Berger, P. en Luckmann, T.,The Social Construction of Reality: A Treatise in the Sociology of Knowledge. 1967

Egelkamp, M. De Inflatie van het Begrip Geweld. 2002

Gilboy, J.A. Regulatory and Administrative Agency Behavior: Accomodation, Amplification and Assimilation. 1995.

Hannan, M., and Freeman, J. Structural Inertia and Organizational Change. 1984

Hasenfeld, Y. Human Service Organizations. Chapter 3 en 9. 1983.

Jong, de, M.J. Grootmeesters van de Sociologie. Hoofdstuk 3. 1997

Kruisbergen, E.W. en Veld, T. Een gekleurd beeld. Beelden, beoordelingen en selectie van etnische aanbodcategorieën door werkgevers. 2002.

Lammers, C.J., Mijs, A.A., van Noort, W.J. Organisaties vergelijkenderwijs; ontwikkeling en relevantie van het sociologisch denken over organisaties. 1983.

Mohr, J.W. en Guerra-Pearson, F. The Duality of Niche and Form: The Differentiation of Institutional Space in New York City, 1888-1917. 2005.

Pfeffer, J. and Salancik, R. The External Control of Organizations. 1978

Prins, J. Technologie en de Nieuwe Dilemma's Rond Identificatie. 2004

Pruijt, H. Is The Institutionalization of Urban Movements Inevitable? 2003

Sanz-Menéndez, L. en Cruz-Castro, L. Coping With Environmental Pressures: Public Research Organizations Responses to Funding Crisis. 2003.

Scott, W., The Adolescence of Institutional Theory. 1987.

Selznick, P. Leadership in Administration: A Sociological Interpretation. 1957

Zijderveld, A. C. The Institutional Imperative: The Interface of Institutions and Networks. 2000

Zucker, L.G. Institutional Theories of Organization. 1987

Gebruikte Internetbronnen

www.privacyloket.nl
www.privacymanagementgroep.nl
www.nivra.nl
www.norea.nl
www.devrijepsych.nl
www.cbpweb.nl
www.wikipedia.com
www.telegraaf.nl
www.nrc.nl
www.regering.nl
www.wodc.nl
http://nwi.geog.uu.nl/content/files/suurs_1109249525_Roald%20Suurs%202005%20-%20Instituties;%20Individuen%20en%20Verandering%20-%20Eindpaper%20FMO.pdf
http://www.stanford.edu/group/csw/TCU_curricula1.doc
http://www.scp.nl/publicaties/boeken/9037701590/SCR2004_Hoofdstuk10_VeiligheidPolitieJustitie.pdf
www.4en5mei.nl

Bijlage 1; De Interviews

Interview 1: Berna Schaafsma, hoofd afdeling Beleid - College Bescherming Persoonsgegevens

Kunt u iets vertellen over uw functie binnen het CBP?
Ja, ik ben hoofd van de afdeling beleid, het CBP heeft verschillende afdelingen, zoals de afdeling communicatie, juridische zaken, onderzoek en ondersteunende afdelingen en de afdeling beleid. De afdeling beleid is verantwoordelijk voor het uitvoeren van verzoeken van partijen die op ons afkomen voor advies, zowel wetgevingsadviezen als de behandeling van klachten. Dit betekent dat we voor een groot deel reactief werken, op basis van verzoeken doen we ons werk. En een deel van het werk is de uitvoering van ons eigen jaarplan. We stellen ieder jaar doelstellingen en deze willen we verwezenlijken. Hiervan komt een samenvatting te staan in het jaarverslag die ook op de site komt. Binnenkort komen de doelen van 2007 op de site, dat is onze eigen agenda. Een deel hiervan is voor de afdeling beleid, maar het zijn ook juridische zaken of andere dingen. Maar die zitten eigenlijk per definitie na die van beleid en onderzoek, zij werken naar aanleiding van de uitkomsten van het werk van beleid en onderzoek. Juridische zaken is verantwoordelijk voor de uitkomsten van ons, maar ook voor het opleggen van een mogelijke dwangsom. Zij stellen sancties, bijvoorbeeld bij het niet nakomen van een meldingsplicht.

Wat mij opviel via de informatie die ik via de site kreeg was dat het CBP toch vooral een controlerende functie heeft...
Ja wij zijn een toezichthouder. Wij houden toezicht op de naleving van de Wet Bescherming Persoonsgegevens, maar ook op de naleving van de gemeentelijke basisadministratie en de wet politieregisters. . . .

Ik heb zelf wat onderzoeken op internet gevonden waaruit is gebleken dat niet zozeer de aandacht voor privacy verslapt is, maar vooral de aandacht voor veiligheid zo is toegenomen. Door het spanningsveld hiertussen is de bescherming van privacy onder druk komen te staan. Zijn die veranderingen hier opgemerkt?
Jazeker hebben wij dat opgemerkt, dat is natuurlijk al een aantal jaren. Sinds 2001 is er bij de overheid sprake van dat zij acties wil ondernemen om risico's in te dammen, waar wij op zich erg

achter staan. Onze voorzitter heeft via de media ook laten weten dat wij absoluut voor veiligheid zijn. Maar je moet je ook afvragen of aanvullende maatregelen ook nodig zijn in situaties. Wij hebben in het afgelopen jaar het idee gehad dat er een tegenstelling werd neergezet waar die tegenstelling in de praktijk niet echt bestaat. Het probleem in de praktijk is soms veel meer dat het soms lastig is dat er veel verschillende diensten zijn, zodat de bestaande bevoegdheden niet optimaal benut worden. Het is dus vaak niet strikt noodzakelijk nieuwe maatregelen te nemen.

Dus jullie willen eigenlijk de bestaande bevoegdheden wat meer duidelijk maken, zodat deze meer benut kunnen worden, in plaats van naar nieuwe bevoegdheden te kijken?
We hebben geprobeerd erop te wijzen, van, ga nou uit bij alles wat je wil regelen, wat is er nu mogelijk en wordt dit optimaal benut. Als je die analyse hebt gemaakt en daar komt een uitkomst uit van alles wat we kunnen is benut, dan kun je bedenken; wat zijn er voor aanvullende maatregelen nodig. Daarvoor was onze mening over privacy en veiligheid in veel discussies en rondetafelgesprekken dat deze twee tegenover elkaar stonden als tegenstelling waar wij vinden dat onderdeel van veiligheid ook juist de bescherming van persoonsgegevens is. [Er is ook een lezing gegeven door Kohnstamm in Dordrecht hierover eind 2005.]

Is het door deze veranderingen en het beeld wat hierover wordt neergezet ook moeilijker geworden voor jullie?
Ja, dat hebben we zeker gemerkt, zowel op persoonlijk niveau van medewerkers als op professioneel niveau, dat het moeilijk is om ons verhaal aan het voetlicht te brengen. Het is een genuanceerd verhaal en dit bekt nu eenmaal minder lekker dan een kreet als: terrorisme moet bestreden worden en bevoegdheden moeten worden uitgebreid, dus er moeten maar camera's daar en daar komen. We zijn daar op zich niet op tegen, maar de noodzakelijkheid moet vooral goed bekeken worden voordat dit soort maatregelen genomen worden.

Wat is jullie reactie hierop geweest, om de legitimiteit van privacywetgeving te behouden?
Dit is vooral het voortdurend uitdragen van het verhaal wat ik hiervoor verteld heb. Door het steeds opnieuw te vertellen proberen we er steeds weer aandacht voor te vragen. Met alle gezelschappen die hierbij betrokken zijn, alle partijen die hierbij betrokken zijn, probeer je in gesprek te raken en aandacht te vragen voor die noodzakelijkheidstoets. Op zich liep dit samen . .

. met een tijd waarbij de druk op het CBP misschien wel het grootst was, in 2004, een aantal jaren na de aanslagen.

Ja, het viel me op dat er in het jaarverslag van 2001 niets staat over de aanslagen van 9/11.
Ik was zelf nog niet bij het CBP toen, maar ik kan me voorstellen dat er op dat moment hier nog geen effect was. Er was wel een effect op de samenleving en op ieder als persoon natuurlijk. Maar zover kan ik niet terug, want ik ben zelf vanaf maart 2002 in dienst. Het was vanaf dat moment wel echt een issue, de buitenwereld verandert.

Besteden jullie ook extra aandacht aan de pers, want het viel me op dat het aantal krantenberichten behoorlijk is de gestegen de afgelopen jaren.
Ja dat klopt denk ik ook wel . . .. Ik weet wel dat onze voorzitter is aangetreden in 2004 en hij toen kennismakingsrondes heeft gedaan. Juist in die rondes heeft hij ook telkens weer ons verhaal naar buiten gebracht.

Kunt u iets meer vertellen over de personen waar jullie je dan op richten met deze boodschap?
We zijn een vrij kleine organisatie met een heel groot toezichtsveld. . . . Als je kijkt naar het totale pakket van het CBP dan is politie/justitie een belangrijke actor. Zij hebben prioriteit te gekregen, maar we kunnen het ons niet veroorloven om hier alles op te zetten, er zijn genoeg andere dingen. Wat wij normaal gesproken doen, is te bekijken wie zijn de belangrijkste spelers in het veld, wie bepalen, en wie zitten er in de praktijk, deze partijen zoeken wij op. Er is regulier overleg met politie. Die zoeken we bewust op, maar we proberen dit heel gericht te doen. Er zijn bijvoorbeeld in de politiewereld privacyfunctionarissen benoemd, die vragen over privacy kunnen beantwoorden binnen de politiewereld, zodat wij niet al die vragen hoeven te beantwoorden, maar mensen kunnen doorsturen.

Kunt u iets meer vertellen over de selectie van die partijen, waarom kiezen jullie juist voor deze partijen en niet voor andere?
Een partij waar we voor kiezen moet een voldoende relevantie doelgroep vertegenwoordigen. . . . Aan het begin van het jaar houden bij politie de hoofdcommissarissen een nieuwjaarstoespraak waarin dit soort vraagstukken behandeld worden, en ook in de media naar buiten komen. Dan kun

je verhalen krijgen die volgens ons gedeeltelijk mythes zijn. Zo'n hoofdcommissaris is per definitie een relevantie groep. Zij bereiken hier namelijk een grote groep mee, dus is het voor ons belangrijk met politie hierover te praten. Op deze manier zoeken we voor ons relevante groepen op.

Ok, dat is duidelijk, dan wilde ik nu nog even terugkomen op mijn vraag over de media; of het bewust is dat er meer krantenartikelen zijn geplaatst de afgelopen jaren?
Ja ik denk dat dat wel kan kloppen. Het is een bewust keuze, maar ook gedeeltelijk een antwoord op de vragen die van buitenaf komen. Het is belangrijk ons verhaal te laten horen. De pers houdt er ook van iets uit een verdomhoekje te halen en juist die partij uit te nodigen om zijn verhaal te vertellen, dus het is van twee kanten gekomen. En tegelijkertijd heeft het CBP vanaf 2001 meer vragen gekregen, niet alleen met betrekking tot terrorisme, maar in die periode is ook onze nieuwe wet in werking gegaan. Dit hield nieuwe bevoegdheden in, waarin we meer sancties kunnen opleggen. Dit was een periode waarin we moesten kijken hoe we onze taken het beste konden uivoeren, en wat dit voor onze organisatie betekent. Tegelijkertijd werd in de buitenwereld de stemming anders; ook hier in de binnenwereld gebeurde dit. Daarom kan ik niet goed scheiden wat we waarvoor hebben gedaan. . . . De nieuwe wet is een implementatie van een Europese richtlijn, waardoor ieder Europees land dezelfde taken bij een privacybeschermende organisatie moest leggen.

Is het dan ook zo dat deze wet niet per se een vrij keuze is geweest voor jullie of voor de overheid?
Nee maar ik geloof wel dat Nederland dat wel graag wilde. . . .We hadden een wet persoonsregistratie, dus we hadden wel al iets.

Ik vroeg me ook af of de verandering in organisatie op zichzelf ook een strategie zou kunnen zijn om legitimiteit te vergroten, door jezelf 'belangrijker' te maken zegmaar.
Het is natuurlijk wel zo dat je op het moment dat je taken moet invullen dat je moet kijken hoe je dat moet doen. Ieder jaar bekijken we dit ook opnieuw en groeien we hierin. We vinden dat we nog meer naar onderzoeken moeten, dit blijkt ook nodig te zijn. En wat we ook willen, daar komt de aandacht in de pers ook weer bij kijken, dat a) de wet bekend is en b) ook bekend is dat er een

toezichthouder is die ervoor zorgt dat deze wet wordt nageleefd. Dit maakt dat je ook graag naar buiten wilt treden.

Als ik het goed begrepen heb besteden jullie een aantal taken ook uit aan andere organisaties. Het Privacyloket zorgt bijvoorbeeld voor overname van taken met betrekking tot het bedrijfsleven.
We hebben altijd al gezegd dat we ons noodzakelijkerwijs op moeten stellen in een soort tweede lijn. Dit omdat het toezichtdomein heel Nederland is, een zelfs een stukje Nederland die informatie naar het buitenland wil spelen. Wij zijn een kleine toezichthouder met een groot toezichtsveld. Als je kijkt naar andere toezichthouders hebben zij vaak een veel beperkter toezichtsdomein dan wij hebben, of het vraagstuk veel gedefinieerder. Wij hebben een heel groot toezichtdomein, heel Nederland, iedereen verwerkt gegevens. Plus dat de WBP een wet is met redelijk open normen. Voor een leek is niet een-twee-drie duidelijk wat dit allemaal precies inhoudt. Dit kan bijvoorbeeld ook zijn een gerechtvaardigd belang van verantwoordelijken. Daarin moet een verantwoordelijke afwegen of zijn belang opweegt tegen de verwerking van gegevens van anderen. Zij moeten het belang voor henzelf afwegen tegenover de gegevens die zij uitwisselen. Stel dat uw apotheek, die weet welke medicijnen u gebruikt, een verzoek krijgt van een medicijnenfabrikant die de gebruikers van de medicijnen willen weten, want ze willen een groot onderzoek doen en deze mensen aanschrijven; wat voor grondslag voor deze verstrekking heb ik? Is het verstrekken van deze gegevens verenigbaar met het doel waar ik het voor verzameld heb. Met andere woorden; mag u verwachten dat uw gegevens die daar geregistreerd staan bij een ander terechtkomen?
Noot van Schaafsma: (Dit is bij nader inzien een slecht voorbeeld omdat voor medische gegevens het regime van artikel 16 WBP bijzondere gegevens geldt. Het verwerken van medische gegevens mag niet, tenzij.. Het voorbeeld gaat wel op voor andere bedrijven die gegevens van je hebben.)

En dit is dus hun eigen verantwoordelijkheid?
Dat schrijft de WBP voor, dat ze zelf belangen afwegen en hun verantwoordelijkheid nemen. Dat ze zich afvragen of ze hier een gerechtvaardigd belang hebben, mag ik dit doen? Dat ze deze belangen afwegen, of dit verenigbaar is en hier toestemming voor moeten vragen of niet.

Belangrijk hierbij is ook de informatieplicht. Als iemand gegevens verwerkt hoort hij dit u wel te vertellen. Al dat soort vraagstukken kunnen verschillend zijn voor wat voor soort bedrijf je hebt, en om wat voor soort gegevens het gaat. Dat betekent dat je voor iedere verwerking afzonderlijk moet kijken wat dit betekent. Dat maakt dat we hier veel vragen over krijgen. We hebben een eigen front office, en via de email die algemeen voorlichting kan geven, en we gebruiken ook de website hiervoor. We hebben dus echt een taak om voorlichting te geven, maar het echte adviseren daar kunnen we niet elke vraag op maat beantwoorden. Hierbij zullen ze zelf actie moeten ondernemen, dat moeten ze zelf uitzoeken met een jurist om dan de afweging maken. We proberen wat andere organisaties te helpen, en we zitten hierbij zelf in de tweede lijn, sommige organisaties, zoals het Privacyloket zullen we eerder voorrang geven, zodat zij hun leden goed voor kunnen lichten. Zo hoeven wij maar een partij voor te lichten en niet allemaal individuen afzonderlijk.

Merken jullie ook dat vragen van mensen via website in aantal is gestegen?
Het aantal telefoontjes is de afgelopen jaren gestaag gestegen en lijkt nu stabiel te zijn geworden. De email die wij krijgen stijgt ieder jaar enorm. Wat nog wel het meeste stijgt is het website bezoek. Er komt binnenkort ook, maar ik weet niet of ik dat mag zeggen. Nou ja, hou de website maar goed in de gaten. [per 29 januari is op de website van het CBP ’mijn privacy.nl’ gelanceerd]. Wat we nog merken met de website is dat het voor professionals heel prettig is dat er veel informatie opstaat, maar voor de gewone burger die een dingetje op wil zoeken is het wat problematischer.

Wat mij ook opviel aan de website was dat er veel vaktaal wordt gebruikt, wat voor de gewone burger vrij nietszeggend is. Doen jullie dit bewust?
Wat altijd wel een dilemma is, is de leesbaarheid van onze uitspraken versus de juridische houdbaarheid en kwaliteit. Het laatste is erg belangrijk voor ons, omdat we moeten kunnen laten zien waar we onze uitspraken nu eigenlijk op baseren. Heel vaak is dat ingewikkeld. In veel sectoren in de samenleving is naast de WBP andere wetgevingen van kracht die helpen om de WBP in te vullen. . . . Als wij vragen krijgen, beperken we ons niet tot de WBP, maar pakken we ook die andere wetten erbij. Daar kom je niet onderuit, en dat bevordert de leesbaarheid niet altijd.

Welke kant neigen jullie op qua prioriteit? Is dit de leesbaarheid of de juridische kwaliteit?
Ik denk dat we vanuit het tijdperk komen waarin de juridische kwaliteit voorop stond, en die staat nog steeds hoog. Maar de afgelopen jaren proberen we meer aandacht te besteden aan de leesbaarheid.

Er zijn ook strategieën die symbolisch zijn; het taalgebruik zou hier een voorbeeld van kunnen zijn, ik weet niet of hier bewust mee omgegaan wordt of niet? Ik dacht hier namelijk zelf deze strategie in te herkennen.
Ok, dit doet een beetje pijn hoor.

Dit is niet een per se een negatief punt, je ziet dit bijvoorbeeld veel terug in de advocatuur en de politiek, daar worden andere termen gebruikt; gewoon omdat dat bij het vak hoort en het kunst is te laten zien dat je weet waar je het over hebt.
Nee dat is niet een bewuste keuze, zeker in de afgelopen jaren, van de tijd ervoor weet ik dat niet zo goed. We hebben veel meer als doelstelling om beter over te komen qua leesbaarheid. . . . Bij sommige juridische stukken schieten we ons doel een beetje voorbij, omdat het voor professionals goed leesbaar is, maar voor de gewone mensen niet. Je moet niet te technisch over artikelen spreken, omdat je dan niet goed helder maakt wat precies het probleem is. Je maakt ook niet goed helder hoe je ten opzichte van een probleem staat, hoe je dat wil oplossen. Sinds we dat geconstateerd hebben, zo rond 2004, zijn we eigenlijk meer aandacht gaan besteden aan de leesbaarheid. Je moet je kunnen herkennen in een probleem, om een oplossing te kunnen bedenken. Je moet niet heel koud denken in richtlijnen en wetgeving. Je moet creatief meedenken met mensen, om te kijken of er nog andere manieren zijn om een probleem op te lossen. Hier zitten natuurlijk ook beperkingen aan, maar er zijn genoeg dingen waarbij je goed mee kan denken. . . . Vroeger waren we hier minder mee bezig.

Dus daarin hebben jullie wel een beetje in meegegeven?
Nou niet zozeer meegegeven, maar we hebben ons wel meer opgesteld als een meedenkende toezichthouder. Welk probleem wil je nou precies oplossen, en wat je volgens ons zou moeten doen is het volgende. Je moet onderbouwen waarom het probleem zo groot is en je moet aandacht

besteden aan allerlei randvoorwaarden. Het CBP kan op zo'n moment zeggen: het is niet rechtmatig, dus hier kunnen we niet aan beginnen, maar je kunt je ook opstellen; ik snap jullie probleem, maar hiervoor zou je eigenlijk eerst die en die onderdelen in orde moeten maken. We proberen ons meer te verplaatsen in een probleem wat iemand heeft. We merken dat de reactie op die juridische stukken vaak was; het mag niet van de privacy. Dit terwijl het alleen zo is dat niet mag zoals u het nu heeft opgeschreven en nu van plan bent. Maar dit betekent niet dat het niet onder andere omstandigheden mag. Hierin zijn we wel erg veranderd.

Sinds wanneer is die houding ingegaan voor jullie?
Ik denk dat dat een ontwikkeling is geweest van de afgelopen 2 jaar. . . .

Wat ik nog wilde vragen met betrekking tot de media, is of jullie er ook rekening mee houden wanneer jullie een bericht naar buiten brengen? Zo was er in de tijd dat Verdonk erg vaak in de nieuws was, opeens een bericht van het CBP dat zij zich in de zaak van Taida Pasic niet aan de privacyregels heeft gehouden. Dit was toen wel een erg populair onderwerp.
Ja maar tegelijkertijd zit daar een enorm gevaar aan. We hebben toen in de zaak van Taida enorm goed opgelet wanneer we dit naar buiten gebracht hebben. We wilden namelijk geen rol spelen in het politieke spel dat gaande was. Dit was volgens mij precies in de periode waarin de VVD haar nieuw politiek leider koos, en wij wilden ons hier absoluut niet mee bemoeien. De mededeling over Taida hebben wij wel gedaan, omdat er ook veel vraag van de pers was naar aanleiding van ons onderzoek. Maar dat hebben we volgens mij gedaan precies in de week dat de stemming bij de VVD was gesloten, maar dat uitslag nog niet bekend was gemaakt. Daar is echt over nagedacht.

Dus jullie hebben niet geprobeerd hier juist op in te spelen?
Nee dat zou hier niet geëigend zijn geweest, want het leiderschap bij de VVD heeft niets te maken met een zaak als Taida. Dus je wil een uitspraak doen over die kwestie, maar je wil niet dat dat een politieke lading krijgt, want daar zijn wij niet voor. Wat we wel hebben gedaan sinds de afgelopen twee jaar is dat we iets meer richting de Eerste Kamer of Tweede Kamer onze standpunten verduidelijkt hebben. We hebben een officiële taak om informatie over de WBP bekend te maken en advies te geven. Als ons punt onder de aandacht komt is het wel zaak om dit

geen ondergesneeuwd kindje te laten worden. Daar proberen we wel heel hard aan te werken. Tegenwoordig is het wel zo dat we tijdens een hoorzitting in de Eerste of Tweede Kamer een toelichting geven over ons advies bij een bepaalde wet. Dit doen we wanneer we denken dat er nog niet genoeg aandacht aan is besteed. . . . Maar we moeten ons niet politiek opstellen, of via een bepaalde partij willen spelen. We moeten hierin wel neutraal blijven.

Ok, het is voor mij wel een duidelijk verhaal. Misschien zijn er nog dingen die u zelf wilt toevoegen of dingen die nog niet besproken zijn en wel relevant?
Nee eigenlijk niet, ik ben benieuwd welke andere partijen u nog gaat spreken en wat hieruit komt. Ook zou ik graag het verslag van dit gesprek eerst willen lezen als dat mogelijk is.

[Afronding gesprek].

Interview 2: Henk Fernald, privacy deskundige - OBA Privacy Management Groep.

Kun je even in het kort vertellen wat je functie is binnen de organisatie?
Ik ben Henk Fernald. Ik ben privacydeskundige. En ik ben de bedenker en ontwikkelaar van de privacy management method. Dit is een methode die is gebaseerd op de taken en bevoegdheden van een functionaris gegevensbescherming [FG]. Met behulp van het College Bescherming Persoonsgegevens heb ik die functie omgezet tot een dienst waarbij we laagdrempelig dezelfde deskundigheid en kwaliteit kunnen bieden die grote organisaties kunnen bereiken door grote FG-ers erop te zetten.

Hoe is jullie samenwerking met het CBP daarin?
Ik heb vanaf het begin, dat is 5 jaar geleden, toen de wet nog in conceptvorm was, was ik als onderzoeker bezig voor juridisch integere informatielogistiek en toen heb ik van het CBP toegang gekregen tot alle stukken en ontwikkelingen om te kijken of ik laagdrempelig de deskundigheid van een FG-er als dienst kan aanbieden.

Dus je hebt hierbij gebruik gemaakt van informatie van het CBP?
Ja want anders voldoe je niet aan de criteria van de wet. En het CBP is de hoeder, de bewaker van

de wet. Dus die bepaalt het kader waarbinnen wij moeten functioneren. De taken en bevoegdheden van zo'n functionaris gegevensbescherming die bepaalt de dienst zoals ik die ontwikkelt heb, en waarbij ik vanuit een externe situatie met deze methodiek kan werken voor organisaties, en ik me geleidelijk kan terugtrekken uit zo'n organisatie. Zodat zij met onze methodiek verder de continuïteit kan handhaven, en wij op de achtergrond als deskundige kunnen blijven coachen. Dus dat is de essentie van onze dienst.

En wat voor organisaties zijn dit, die jullie hulp inschakelen?
Het klantenbestand is heel breed, we kunnen vanuit de wet iedere organisatie waar persoonsgegevens verwerkt worden onze diensten aanbieden. Omdat het gestandaardiseerd is, een uitgediept karakter heeft en we gefaseerd werken past het als maatpak voor iedere organisatie, naar eigen behoefte.

Kun je een aantal concrete organisaties noemen?
Gemeentelijke organisaties, onderzoeksbureau's, bedrijfshulpverleningsbureau's. Ja noem ze maar op, je kan het zo gek niet bedenken of wij kunnen ze hulp aanbieden. En daar is ons Privacy Management Dossier, onze digitale privacy, die is ontwikkeld op basis van die hulpmiddelen van het CBP. Daar hebben we de criteria voor gebruikt van de contouren die door het NIVRA en de NOREA, en dat zijn koepelorganisaties die orders uitvoeren, om de kwaliteitsnorm van ons gestandaardiseerde dossierstructuur vorm te geven. Het bestaat uit vijf fasen, en als je die vijf fasen hebt doorlopen, dan voldoe je volgens onze methodiek volledig aan alle contouren. . . . En daar ben ik dus deskundige in. En wij zijn de enige die niet alleen consultancy aanbieden, maar echt een uitgewerkte dienst met bijbehorende tools die een toegevoegde waarde kunnen hebben voor een organisatie om een transparante structuur te krijgen. Dit maakt het helder en transparant voor alle betrokkenen. . . .
Dan wordt al deze informatie in ons systeem ingevoerd en dan krijg je de inventarisatie en de toetsing van de verwerkingen. Dit is ook iets wat alleen wij doen en anderen niet, en zeker niet het openbaar register wat het CBP gebruikt. Want men gaat er vanuit dat de formeel verantwoordelijke van de organisatie verantwoordelijk is. Wij bieden inzicht in dit register, anders worden de rechten van de betrokkenen volledig uit het oog verloren. Het CBP doet niet haar taak, namelijk het bewaken van de rechten van de burger en dat deze gerespecteerd worden.

Dit is mijn grote discussiepunt met het CBP, het NIVRA en de NOREA; vandaar dat ik zelfstandig ben begonnen. En nu confronteer ik ze vanuit de praktijk met pilotprojecten enzovoorts om ze te laten zien waar er gaten zitten. In dat kader hebben we ontdekt dat we niet alleen maar commercieel aan de slag moeten gaan, maar dat we ook onze deskundigheid beschikbaar hebben gesteld aan het Privacyloket, die namens de belangen van de burger de burger bijstaat als de overheid weer eens te ver gaat, of een bedrijf het niet zo nauw neemt, of het CBP zijn taken niet goed uitvoert. . . . . Dit zijn ondersteuningen die de burger nodig heeft om geen rechtsongelijkheid te krijgen tussen de burger en de overheid. . . . Het is belangrijk te kijken hoe het gesteld is met de rechtsgelijkheid in de afhandeling van klachten van burgers waarbij de burger geen ondersteuning heeft gehad van deskundigen en bedrijven wel. Dat is mijn gevoel over het CBP; dat zij aan de kant van de bedrijven staan, maar niet bij de individuele burger. Hierdoor zijn de uitslagen en uitspraken van het CBP altijd ten gunste van de bedrijven. En dat is volgens mij rechtsongelijkheid. . . .

Wat is de reactie van het CBP hierop geweest?
Het CBP zit tot over hun oren in het werk en het is een nieuwe situatie. Ze moeten voor iedere organisatie structuur bepalen. Het CBP pakt dingen naar mijn mening vooral theoretisch aan. Als je de opdracht hebt om de belangen van de burger die gebaseerd zijn op de grondwet te controleren, dan moet je veel voortvarender en actief aan de slag moet gaan. Je moet niet wachten tot de burger het bewustzijn heeft een klacht in te dienen en het dan schriftelijk af te handelen. . .

Ok, dit is dan even het inhoudelijke verhaal. Uit mijn speurwerk kwam naar voren dat niet zozeer de aandacht voor privacy verslapt is, maar dat vooral de aandacht voor veiligheid steeds groter wordt. Hebben jullie dit ook gemerkt binnen de organisatie?
Ja, als wij privacy aankondigen en aanbieden onder het mom van veiligheid, als je een goede organisatiestructuur hebt en duidelijke afspraken hebt hoe je hulpmiddelen die we ter beschikking stellen gebruiken, is dat een integraal onderdeel van het beveiligen van je bedrijf, inclusief je brandalarm, je videobewaking en al dat soort toestanden. Gezien de hoge mate van digitale gegevensverwerking en hulpmiddelen zitten we in de veiligheid ook in de digitale wereld. . . . Een van de eisen om persoonsgegevens te verwerken, is dat men duidelijk weet van welke doelbinding er sprake is. . . . Maar die logica ontbreekt nog steeds bij veel bedrijven, die

gebruiken veel gegevens en halen allerlei technologieën in huis, maar verzuimen de betrokkenen en medewerkers hierover te informeren en bij te scholen over het toepassen van hun taken. Een van de criteria om aan de privacywetgeving te voldoen is het beveiligingsbewustzijn van de medewerkers en het zorgvuldig omgaan met de hulpmiddelen die zij hebben. We zien in de praktijk heel veel voorbeelden waarin dit fout gaat. . . . Het bewustzijn is laag, terwijl het onderwerp essentieel is. Gevoelige informatie hoort een hogere beveiligingscode te krijgen. Als je dat goed regelt heb je geen enkel last van de privacywetgeving, maar is het eigenlijk een toegevoegde waarde op je organisatiestructuur, omdat je je organisatie helderder en transparanter kan maken. Volgens de privacywetgeving wordt er niets verboden, er wordt alleen maar houvast gegeven op welke manier je persoonsgegevens dient te verwerken in het uitvoeren van je maatschappelijke taken. . . .

Hier heb je het vooral over de beveiliging van het bedrijf, maar merk je ook dat er minder aandacht is voor privacy op zichzelf?
Ja, de beveiliging heeft een hoge prioriteit, maar de middelen die men gebruikt, daar heeft men geen enkel idee van hoe men dit op een juiste manier kan gebruiken. . . . Bijvoorbeeld videobewaking in de openbare ruimte. Je mag niet een camera over iedere werknemer z'n schouder zetten, want daarmee krijg je volgsystemen.

Is het zo dat mensen over het algemeen meer de neiging hebben de aandacht op beveiliging te leggen en hierbij de privacy wegschuiven?
Doordat je meer videocamera's neerzet in bijvoorbeeld een winkel, neem je niet alleen maar de goederen waar, maar je neemt ook de klanten waar. En klanten hebben rechten. Maar je neemt ook je personeel waar. En volgens de CAO mogen volgsystemen alleen maar gebruikt worden bij overeenstemming, dus daar komen drie gebieden bij elkaar; privacy, bewaking en het recht van de werknemer op privacy. En daar prefereert altijd de beveiliging. Maar de beveiliging is ook een integraal onderdeel van privacybescherming, en die link heeft men nog steeds niet gelegd. Als je goede richtlijnen hebt, heb je adequate beveiliging. Maar het is ook mijn gevoel dat degenen die het moeten controleren en het moeten handhaven ook te weinig kennis hebben van de toepassing van de wet.

Wat doen jullie als organisatie om ervoor te zorgen dat die privacy juist wel onder de aandacht komt?
Wij hebben workshops ontwikkeld en we geven masterclasses. We hebben een digitaal privacy management dossier ontwikkeld.

En voor wie zijn die workshops en masterclasses bedoeld?
Die zijn voor een ieder, dat hangt af van het onderwerp. Het kan zijn voor interne functionarissen gegevensbescherming, het kan zijn voor een directie of bestuur. . . . Dus dat is een vrij complex geheel, omdat je dwars door organisaties heengaat. Je hebt niet alleen te maken met de structuur van een afdeling, maar je hebt ook te maken met een infrastructuur van het netwerk, en met digitale berichten, en informatiesystemen. Maar je hebt ook te maken met bedrijven die hun maatschappelijke taak moeten doen en samen met andere bedrijven een gezamenlijke taak moeten uitvoeren, dus moet je ook informatie kunnen delen. Die WBP is een oplossing die tot nu toe bestond in onze samenleving en waar wij in de digitale wereld niet goed wisten hoe je daar integer mee om moet gaan met al die informatiestromen. . . .

En daar proberen jullie via die masterclasses meer duidelijkheid in te geven?
Wij zijn deskundig op dat gebied. En de controleurs van het geheel, het CBP, daar ontbreekt die deskundigheid, die technische kennis. Daar zit volgens mij wrijving, omdat je een puur theoretische afhandeling krijgt van situaties. Vandaar dat wij Stichting Privacyloket ondersteunen, omdat zij intermediating aanbiedt. Zij heeft deskundigheid in huis om te kunnen zeggen: Oh is dat een klacht, wij kunnen via intermediating kijken of de situatie voldoet aan de criteria van de wet en moet dat eventueel aangepast worden.

Zijn er misschien nog andere dingen waardoor jullie proberen de aandacht op de privacy te vestigen?
We hebben samen met Lemniscaat een FG-opleiding ontwikkeld die is gebaseerd op onze filosofie en daar kan men dus opgeleid worden van gecertificeerd FG-er tot master in de privacy. Ook dat gedeelte heb ik ontwikkeld. Maar ook via mailings en gesprekken overal. Ik lul me een slag in de rondte.

Maar doe je dat via bepaalde kanalen, zoals de media, of heb je hierin niet echt structuur?
Wij zijn nog een jonge organisatie en proberen nu zoveel mogelijk onze filosofie onder de aandacht te brengen. Wij doen dit op dit moment niet via de media, maar hier zitten wellicht in de toekomst wel mogelijkheden.

Kun je ook merken dat deze verschuiving in aandacht de afgelopen jaren ook toegenomen is? Dat het meer nodig is voor jullie om dit soort dingen te doen, of is dit altijd al zo geweest?
Het begint iets beter te worden, maar je hebt ten eerste te maken met commerciële organisaties, en ten tweede heb je te maken met een grote onbekendheid . . . En het CBP is heel panisch en wil niets te maken hebben met commercie, terwijl ze de taak hebben de burgers te beschermen. Er ontstaat een gigantische barrière, ze zitten in een hoge toren ver van de burger af, zijn bijna niet benaderbaar en handelen alles zeer theoretisch af. Terwijl de burger het recht heeft op basis van de Europese richtlijn dat de overheid garandeert dat je recht op privacy wordt gerespecteerd. En als ik kijk naar het rapport van de Ombudsman van vorig jaar, 'De maakbare overheid', dan barst je bijna in tranen uit als je dan de conclusie leest. Waarbij de overheid wettelijke richtlijnen formuleert en zelf de overtreder is van zijn eigen wetten en richtlijnen. Dan blijft er voor de burger niet veel meer over dan vertrouwen te hebben in het College Bescherming Persoonsgegevens.

Maar wanneer ik kijk naar jullie functie, dan is dit niet direct gericht op de burger?
Nee, maar de burger is een zeer belangrijk onderdeel van onze dienst. En dat moeten we organisaties juist aan hun bewustzijn peuteren. . . . Daarnaast loop je nog het risico dat op basis van de wijziging in de wet iedere burger nu het recht heeft aan iedere willekeurige organisatie en die moet binnen 4 weken schriftelijk de betrokkene volledig informeren over de persoonsgegevens die van hem worden verwerkt. . . . Alle gegevens die herleidbaar zijn tot een persoon. Dat is het recht van iedere burger. Op basis van zo'n klacht kan het CBP als waakhond een boete opleggen als men die rechten niet respecteert. Maar als het CBP zich zo formeel opstelt en niet actief gaat pushen en het bewustzijn naar een hoger niveau brengen, blijven ze een waakhond en gaan ze alleen maar boetes opleggen en is de burger daar niet mee gediend. Maar het bedrijfsleven ook niet, want als bewaker van de wet moet je ook een vraagbaak zijn, waar we op basis van praktijksituaties kunnen zeggen: hoe zit dit nou precies, hoe moeten we dat doen?

Daarvoor moet je deskundigheid in huis hebben op diverse niveaus. . . . En dat ontbreekt er, naar mijn mening. . . . Daarom heb ik een dienst ontwikkeld en bied ik deze aan als externe functionaris gegevensbescherming voor meer dan een organisatie. . . . Zo kan ik een hele groep aan de criteria laten voldoen en de belangen behartigen bij het CBP, om namens de groep duidelijke afspraken te maken. . . . Mijn mening is dat het CBP puur als waakhond ingezet moet worden bij klachten die binnenkomen bij Stichting Privacloket. . . . Daardoor ondersteunen wij die stichting, want het doel van die stichting is de burgers bij te staan, maar ook de maatschappelijke organisaties die belangen behartigen van burgers, consumentenorganisaties, patiëntenverenigingen, noem ze maar op, laagdrempelig deze deskundigheid ter beschikking te stellen, zodat de leden voor het minimum aan vergoeding deze deskundigheid krijgen en privacy kunnen eisen bij organisaties. . . . Ik hoop dat je wat aan deze informatie hebt om hiermee verder te gaan. . . .

[Afronding gesprek].

Interview 3: Geert Klei, Stichting Privacyloket.nl

Kun je iets vertellen over je functie binnen het Privacyloket, en waar het Privacyloket precies voor staat?
Ik ben stichtingsbestuurder van Stichting Privacyloket.nl. Ik organiseer het stichtingsbestuur, zoals bijeenkomsten. Ik organiseer de raad van advies. Ik organiseer ambassadeurs op het gebied van privacy in Nederland. En het streven is om dat in 2007 allemaal rond te krijgen.

Wat bedoel je daar precies mee, met dit 'rondkrijgen'?
Dat de bezetting van mensen zodanig is dat je de doellijnen van de stichting goed uit kunt voeren. De doellijnen zijn met name als vraagbaak dienen voor individuele burgers die vragen hebben over privacy. En een nevendoellijn is organisaties die een probleem hebben voor te lichten over hoe ze het goed kunnen aanpakken. Daarvoor gebruiken we de Privacy Management Methode. [Deze is ontwikkeld door Henk Fernald]. En de methode brengt in korte tijd alles in kaart wat een organisatie of bedrijf precies moet doen. Dat is in de vorm van een audit.

En hoe lang bestaat het Privacyloket nu, want het is nog een jonge organisatie had ik begrepen?
Ja het is in 2006 gegrondvest. Er is wel al drie jaar over nagedacht. Vanuit het geheel gezien streven we naar een soort mediator functie tussen de burger en bedrijven. We brengen in kaart waar problemen zich opdoen en proberen rechtzaken en boetes te voorkomen en met name juist oplossingen te zoeken.

In mijn onderzoek richt ik me vooral op de maatschappelijke veranderingen met betrekking tot veiligheid en privacy. Is dit voor jullie ook een van de redenen geweest om deze stichting op te zetten? Ik vraag dit omdat jullie er vanaf 2003 mee bezig zijn geweest en dit dus wel samenvalt met de periode na de aanslagen.
Je ziet dat er na 2001 een soort spanningsveld is ontstaan tussen privacy en veiligheid, omdat juist op het gebied van privacy veel aandacht besteed is, hoe dat vorm gegeven moet worden. Je ziet ook dat er allerlei niet voorziene zaken op het gebied van veiligheid gebeuren, waar de overheidsinspectie de burger dient te beschermen. Daar zit een soort spanningsveld tussen.

En dat ervaren jullie ook zo?
Ja. Een heel simpel voorbeeld; cameratoezicht. Elektronica maken het mogelijk om op grote school camera‘s te plaatsen. Ook op plekken waar burgers het juist niet willen, vanwege hun privacy.

Bij het CBP probeerden ze me te overtuigen dat deze twee aspecten samenwerken. Dat veiligheid ook een deel van privacy is. Deel je deze mening ook?
Nee dat spreek ik tegen. Het hangt wel samen, maar het werkt niet samen. Maar de grens wordt natuurlijk politiek bepaald, wat wel en niet voor de maatschappij zinvol is. Op basis daarvan worden wetten gemaakt, en dan zie je dat er binnen die wetten ook weer spanningsvelden zijn. De ene wet werkt de andere wet tegen. Maar dat is een politiek vraagstuk. Omdat het politiek bepaald is, kun je zeggen dat ieder land daarin zijn eigen cultuurkeuze maken. Uit noodzaak gedwongen misschien.

En hebben jullie het idee dat er door dit spanningsveld juist meer vraag is naar een stichting als een Privacyloket, of juist minder?

Het is altijd de waan van de dag die bepaalt wat op korte termijn gebeuren moet op het gebied van veiligheid. Dit zijn impulsen. Allerlei bestuurders zullen maatregelen nemen, waar veiligheid overtreden wordt. Dat kun je niet voorkomen, de maatschappij is nu eenmaal zo. Maar privacy is een soort lange termijn aanpak, waarbij we iedereen bewust moeten houden dat wat je doet vastgelegd kan worden en traceerbaar is, zodat hij op een bepaalde manier kan handelen. Het vervelendste punt op het gebied van privacy is dat je op een gegeven moment geconfronteerd wordt met je eigen uitlatingen, op het Internet bijvoorbeeld. Maar ook uitlatingen voor een camera, zonder dat je weet dat iemand anders dat beheert. En daarmee kun je je eigen zelfstandigheid en zelfauthenticiteit over je eigen uitlatingen. En dan krijg je ook nog vrijheid van meningsuiting, dat is een soort grondrecht. Dat betekent dat je eigenlijk je doelgroep mag kiezen waar je het voor uit. Iemand anders kan jouw uiting in stukjes knippen, waardoor jouw meningsuiting een hele andere betekenis kan krijgen. En dat raakt ook weer privacy. Door de media kan iemand behoorlijk onderuit gehaald worden, door uitingen die hij in een andere context heeft gedaan.

Op wat voor manier reageren jullie daar dan op?
We zijn geen politie-instantie, we zijn een instantie die als een soort ombudsman mogelijke vragen op het gebied van privacy accepteert en daarin op anonieme wijze namens een burger kan optreden richting een partij die zwaar doelbewust is om mensen op afstand te houden, of mensen in het gareel te houden.

En welke partijen doel je dan op?
Het zijn allerlei organisaties in Nederland die sterk georganiseerd zijn. Dit zijn met name commerciële instellingen, maar ook instellingen voor sociale zekerheid die zware middelen kunnen inzetten op het moment dat zij denken dat er misstanden zijn. ...

En dan is het jullie taak om die burger daarin bij te staan?
Wanneer bepaalde instanties meerdere malen over de schreef gaan, kun je dus namens het collectief van klachten naar die instantie lopen en zeggen: we hebben honderd klachten over jullie functioneren. En dan ben je een evenwichtige partij naar elkaar toe en ben je niet alleen een gesprekspartner van een klachtenbureau, maar directie of bestuurder van zo'n instelling. En dat is

wat wij nastreven.

Is dit voor jullie dan vooral een adviesgevende functie, of controlerende functie of en combinatie? Tot hoe ver gaan jullie bevoegdheden hierin?
In wezen zijn dit alleen bevoegdheden die de burger ons wil geven naar aanleiding van zijn klacht.

Maar kunnen bijvoorbeeld ook een sanctie opleggen, of moeten jullie daarvoor bij het CBP aankloppen?
De sanctie is dat wij het kunnen publiceren op het Internet, dat een bedrijf over de schreef gaat. En daar zijn bedrijven vaak gevoelig voor.

Misschien wel gevoeliger dan voor een boete?
Ja, absoluut. Dat zie je ook met ziekenhuizen gebeuren, dat zie je met scholen gebeuren. Het is een maatschappelijk aanvaard iets om te publiceren welke instanties meerdere malen over de schreef bij privacy. Op het moment dat zo'n instantie zegt: daar gaan wij iets aan doen, zijn wij in staat om een audit uit te voeren om te kijken wat ze werkelijk doen en daarmee kun je dus ook weer naar die instantie toe en op Internet publiceren, zodat ze maatregelen nemen. Enerzijds constateren we dus, en anderzijds helpen we ze om maatregelen te nemen die ervoor zorgen dat negatieve PR die ze hebben ook omgezet kan worden in positieve PR. En door die positieve PR zijn ze wat meer geneigd om er meer energie in te stoppen dan ze in eerste instantie zouden willen. En dat is voor de collectiviteit van personen heel positief. En dit gaat dus allemaal buiten het CBP om. Het is een reguleringsmechanisme wat het CBP eigenlijk laat liggen.

Dus hierin onderscheiden jullie je van het CBP?
Ja het CBP gaat in op individuele vragen van burgers en is veel drukker met regelgeving en onderzoeken naar hoe het in Nederland goed vormgegeven kan worden. Dat is op zich natuurlijk ook gedreven door tekorten op het gebied van mensen en middelen die het CBP zelf heeft. Dat is een verschil tussen lange termijn en korte termijn.

Zijn er nog bepaalde aspecten waarbij jullie je specifiek op burgers richten om ze meer bewust te

maken van het belang van privacy en privacybescherming? Of komen ze vanzelf wel naar jullie toe?
We hebben een internetsite waar elke burger vragen kan stellen. We zoeken ambassadeurs over heel Nederland die presentaties kunnen geven, daar hebben we de middelen voor. We zoeken gewoon binding met lokale punten die de aandacht kunnen schenken, zoals gemeentehuizen. We zijn bezig met brochures voor scholen, om kinderen bewust te maken dat hun gedrag op Internet vastgelegd wordt. Zodat ze weten dat ze bijvoorbeeld vijf jaar nadien nog geconfronteerd kunnen worden met hun uitlatingen bij een sollicitatiegesprek. Wat dat betreft is er ook door middel van aandacht op het gebied van privacy help je dus ook weer mee dat veiligheid in Nederland een stukje groter wordt. Door dit vroeg in te dammen dat uitlatingen op Internet boven de normale gesprekstaal uitgaat. Je ziet bijvoorbeeld in spotjes over pesten zie je daar voorbeelden van. Die dingen hangen dus wel samen, die werken in wezen ook samen. De maatregelen op beide gebieden werken samen. Je ziet dat het CBP die maatregelen goed afstemt.

Merk je dat het in de loop van de jaren, voor zover je daar iets over kunt zeggen, het meer nodig is om publiciteit op te zoeken, omdat burgers zich misschien niet altijd bewust zijn van het belang van privacybescherming?
Ja, ik denk dat het hard nodig is om veel aandacht te geven aan privacyvraagstukken, omdat daarmee eigen gedrag gereguleerd kan worden door zelfregulering, zowel bij bedrijven als bij individuele personen.

En zijn er bij die publiciteit ook bepaalde parijen waar jullie je specifiek op richten?
Momenteel zijn we met name bezig met overheidsinstanties voor burgers. Omdat je ook ziet dat overheidsinstanties samenwerken met elektronische data-uitwisseling. Wij adviseren ook grote partijen, zoals gemeenten, UWV, CWI, op welke wijze elektronische data-uitwisseling wel of niet kan. In die zin spelen we zo in op mogelijke misvattingen omtrent het WBP.

Dus in die zin hebben jullie ook een informatieve functie bij grote partijen?
Ja.

En waarom zijn het juist die partijen waar jullie voor kiezen?

Ja daar hebben we een reden voor. Sociale zekerheid zorgt ervoor dat er heel veel aanvragen in Nederland gedaan worden, er worden heel veel formulieren verspreid. Heel veel elektronische data-uitwisseling. En willen die instanties ook efficiënt kunnen werken en niet alles dubbel hoeven te doen, denk bijvoorbeeld aan een zorgloket, waarbij men kijkt naar administratieve lastenverlichting voor de burger. Als dat niet goed wordt uitgevoerd en in strijd is met de privacyrichtlijnen, dan heb je al een conflictbalans tussen administratieve lastenverlichting en privacy. Op het moment dat het niet goed uitgevoerd wordt, kan de burger geconfronteerd worden met dingen die hij niet wil, en de WBP ook voorziet dat dat niet hoeft of mag. Er zijn tientallen voorbeelden van. Die gebeuren vaak niet elektronisch; de ene ambtenaar loopt even naar de andere ambtenaar met de vraag: heb jij informatie over deze klant. Maar met de komst van geavanceerde elektronica gaat dat straks collectief met grote aantallen, burgers worden gescreend als je niet oppast. En dan krijg je het Big Brother effect. De overheid probeert dat juist niet te doen, maar door het streven naar lastenverlichting streven ze er wel naar om alles in een grote databank onder te brengen.

Dit is dus een van de neveneffecten van goed bedoeld beleid?
Ja precies. Dat proces begeleiden wij als objectief buitenstaander namens individuele burgers en zo kunnen misstanden op dat gebied snel opgepikt worden.

Dit zijn vooral dingen die te maken hebben met publicaties in de media. Zijn er nog andere manieren om mensen te beïnvloeden?
Het gaat vooral om bewustwording. Veel mensen hebben wel een gevoel over privacy, maar geen denkwijze over privacy. Op het moment dat ze ermee geconfronteerd worden met taken die daarop slaan gaan ze zich verzetten. Maar er wordt niet vooruit over nagedacht, er is geen gedachtegang van als dit gebeurt moet ik zo en zo handelen. Terwijl er wel heel veel publiciteit is voor rampenbestrijding, je ziet allerlei brieven in de bus over wat te doen bij deze en deze situatie. Dat gaat over grote collectieve rampen. Maar niemand krijgt in de bus informatie over wat te doen als je van een trapje valt. En de privacy is meer in die sfeer, nu nog wel.

En jullie proberen vooral via informatie bewustwording te creëren?
Ja in die zin zijn onze middelen natuurlijk beperkt. In theorie zijn we wel een kanaal die dit goed

zouden kunnen opzetten, maar op dit moment hebben we daar de middelen niet voor.

Maar dit zou in de toekomst misschien nog kunnen veranderen? Of zijn hier geen plannen voor?
Ja dit is wel een punt. We positioneren ons zo dat we in principe via partijen die een belang onderkennen, doordat wij hen attent maken op het gebied van privacy, dat zij ons als beloning een vorm van subsidie kunnen geven.

En wat voor partijen kunnen dit zijn?
Dit kunnen Nutsbedrijven zijn, die ook databases hebben met klanteninformatie. Dit kunnen verzekeringsmaatschappijen zijn, banken, overheidsinstanties, zorginstanties, opleidingsinstanties. Dit is heel breed. Maar alle instanties die bezig zijn met klantgegevens.

[Afronding gesprek].

<u>Interview 4: Kaspar Mengelberg, psychotherapeut en psychiater - oprichter DeVrijePsych</u>

Kunt u iets vertellen over DeVrijePsych?
... Er is nu een stelsel waarin de patiënt in feite onze klant niet meer is. De zorgverzekering is onze klant. Het hele natura stelsel betekent dat de patiënt een dienst in natura krijgt, namelijk de zorg die op de zorgkantoren is ingekocht. Het restitutiestelsel wil zeggen dat de klant, de patiënt in dit geval, betaalt aan de arts, die krijgt daarvoor een kwitantie en kan dan naar de zorgverzekering om dat geld terug te halen op basis van de polis. Het naturastelsel zit anders in elkaar; dan betaalt de patiënt premie aan de zorgverzekeraar en verstrekt vervolgens die dienst in natura. Dit heeft grote consequenties. In die zin dat zij nu de macht bepalen. De zorgverzekeraar kiest ervoor wel of niet een contract met ons aan te gaan. ... Wanneer wij niet doen wat zij willen, gaat het gewoon niet door. En dit heeft gevolgen voor de kwaliteit van de zorg en onze professionele autonomie. Ik beloof als arts dat ik mijn patiënten naar beste weten zal behandelen, en deze belofte kan ik op deze manier niet nakomen. ... Ik sta op mijn professionele autonomie en doe hier dus ook niet aan mee. ... Ik heb gelukkig de positie waarin ik genoeg patiënten heb, maar het is te betreuren dat ik niet iedereen meer kan behandelen, omdat er mensen zijn die het niet zelf kunnen betalen.

En op welke manier verhoudt deze nieuwe manier van verzekeren zich tot de privacy?
In principe is het zo dat datgene wat je aan een dokter verteld, dat een arts een beroepsgeheim heeft. Een arts moet gewoon zijn bek houden over wat er in de spreekkamer besproken wordt. Des te meer geldt dit voor psychiaters of therapeuten, omdat er altijd diepe en soms beschamende zaken worden besproken. ... Sinds 2006 zijn de Diagnose Behandel Combinaties ingevoerd [DBC]. ... Hierin worden diagnoses en behandelingen aan elkaar gekoppeld. ... In praktijk betekent dit dat je in de computer vele informatie kan vinden wat terug te leiden is naar een patiënt. ... Officieel zou dit niet mogen, maar ik geloof daar niet in en vertrouw dit systeem niet. ... Vanaf 2008 worden deze DBC's ook gebruikt voor de rekeningen naar de ziektekostenverzekeraar, dit is met goedkeuring van het College Bescherming Persoonsgegevens. Maar op een rekening staat wat er met een patiënt aan de hand. Dat impliceert dat iedere werknemer van een ziektekostenverzekeraar kan zien wat er met een persoon aan de hand is. Deze informatie komt ook nog eens in databases terecht, waardoor informatie nog toegankelijker wordt. ... Dit tast de privacy van patiënten in hoge mate aan. ... En we leven een paar jaar na 11 september en niemand weet hoe onze samenleving er over tien jaar uitziet. ... De democratie is helemaal niet zo vanzelfsprekend, en het kan zomaar zijn dat machthebbers over een aantal jaren databases gebruiken voor doeleinden waar ze niet voor bedoeld zijn. ... Elektronische gegevensbestanden kunnen een groot gevaar zijn, omdat ze makkelijk in te zien zijn, en zelfs het Pentagon is gekraakt, dus er kan altijd gelekt worden of ingebroken worden. ... Het gaat bij privacy niet om beschamende informatie, het gaat om de belangen die ermee gemoeid zijn. Er zijn verzekeringen die geen arbeidsongeschiktheidsverzekering afsluiten met mensen die in psychotherapie zijn geweest. ... De transparantie waar bureaucraten zo om staan te juichen, is nu een transparantie waarbij verzekeraars kunnen selecteren met wie ze in zee gaan, en dit vind ik kwaadaardig. ... In toenemende maat zijn de verzekeraars en de staat meer en meer de baas. Dit proces is al lange tijd aan de gang. ... Vroeger was het helemaal niet mogelijk in de spreekkamer mee te kijken. Door de moderne technologie kan dat nu wel. ... Om even terug te komen op DeVrijePsych, dat is dus een website. Dat is voortgekomen uit een besloten discussiesite, die heb ik 2,5 jaar geleden opgericht. ... Sinds augustus is de openbare site er, de site die u heeft gezien. Dit is voor mijn collega's, maar ook speciaal voor geïnteresseerde leken. ... Het is een soort openbaar forum. ... We hebben ook wel wat publiciteit van de media gekregen.

En hebben jullie dat bewust opgezocht?
Nee, dat hebben we wel geprobeerd. Maar zo werken de media niet, dat wist ik ook niet. Ze komen niet wanneer je wilt dat ze komen, ze werken volgens het systeem: don't call us, we call you. De media komen naar jou.

Maar ik kan me voorstellen dat wanneer jullie een voor de media toch wel sappig verhaaltje hebben, dat zij hierin geïnteresseerd zijn...
Dat zijn ze ook wel, maar ze komen naar ons. Ze komen dan via via bij ons terecht. We hebben het wel uitvoerig gedaan, via persberichten. Maar ook via vrienden die in die wereld zitten, om ze te benaderen. Maar zo werkt het niet. Ze hebben genoeg om te schrijven, en zij gaan op zoek naar waar ze over kunnen schrijven. We zijn hier wel actief mee bezig geweest. ... We hebben in Trouw gestaan, en zijn op de radio geweest. ... Wij hebben wel enig succes, maar dat neemt niet weg dat we niet op een lijn zitten met de beroepsverenigingen. ... Zij heel braaf conform aan het systeem. ... Wij zijn tot op de dag van vandaag verzwegen door deze verenigingen, zij gaan niet in op onze kritiek en reageren er niet op. DeVrijePsych wordt zelfs niet genoemd. DeVrijePsych is een website, een beweging. Het is geen vereniging, we hebben geen rechtspersoon. Maar het is natuurlijk wel iets ... Over het privacy-aspect hebben ze wel het een en ander geschreven, ze staan wel kritisch tegenover de privacy-aspecten van de DBC's.

En op welke manier probeert u de visie van DeVrijePscych dan uit te dragen?
Via publicaties. Er zijn media waar stukken van ons wel geplaatst worden en daar zijn we dan heel blij mee. Wat we verder doen, is dat we wel proberen handige jongens te zijn. We hebben wel beschikking over emailadressen van leden van verenigingen binnen de beroepstak, en dit zijn er duizenden. Via mailings proberen we iedereen te betrekken bij DeVrijePsych. Daar krijgen we veel reacties op, sommigen zijn heel afwijzend, en sommige reacties zijn heel lovend en instemmend.

Richten jullie je je ook op patiënten, om de burgers zelf bewust te maken van wat er gaande is?
Ja, door de website van DeVrijePsych en door de media proberen we een zo breed mogelijk publiek te trekken.

Maar gebruiken jullie ook een actieve strategie om dit voor elkaar te krijgen?
We proberen ons altijd beschikbaar te stellen en open te zijn naar televisie of radio of kranten toe. Maar echt heel actief gaan we niet te werk nee. Ik zou ook niet weten hoe wij patiënten actief kunnen benaderen. De patiëntenvereniging staat overigens niet aan onze kant, integendeel zelfs. Zij kiezen partij voor de bureaucraten en verzekeraars. Het is zeer te betreuren, maar het is niet anders. Zij krijgen staatssubsidies en zitten daar constant aan tafel. ... Ik ben wel voor technologische vooruitgang overigens. Het is meesterlijk wat er technisch wat en wat er aan informatie te vinden is op bijvoorbeeld Google.

Maar hier is ook een spanningsveld te zien met de privacy. Het kan de privacy beschermen, maar door de vele beschikbare informatie kan het ook zo zijn dat de privacy juist wordt aangetast. Hoe staat u hier tegenover, en is dit in uw werk ook van toepassing?
Ik wil graag de negatieve aspecten bestrijden, en de positieve aspecten houden. Ik denk dat dit ook mogelijk is. Via onze website proberen we de negatieve aspecten tegen te gaan, maar dit betekent niet dat ik tegen technologie ben, helemaal niet zelfs. ... Vrij Internetverkeer past ook bij democratie, in een dictatuur zie je dat Internet maar beperkt gebruikt mag worden, en zelfs Google doet hieraan mee. ... Maar ook onze website van DeVrijePsych, dat kunnen we delen met wie we willen, en dat is prachtig.

Zijn er nog bepaalde groepen of personen waarop je je voornamelijk richten en erbij willen betrekken.
In eerste instantie wil ik mijn collega's erbij betrekken. En voor de rest wil ik iedereen erbij betrekken die geïnteresseerd is, het maakt niet uit wie of wat je bent. De manier waarop we dit doen, is een op een. Zoals op de besloten discussiesite, het persoonlijk contact is het meest interessant, omdat we dan intensiever en uitvoerig contact hebben en dieper op een onderwerp in kunnen gaan. Dit is natuurlijk ook congruent met mijn beroep, om een op een contact te hebben.

Dus jullie gaan liever voor een individueel dieper gesprek dan voor een grotere groep mensen waarbij de aandacht wat aan de oppervlakte blijft?
Nou dat is niet helemaal waar, we treden graag naar buiten in de media om de mensen te

informeren. Maar het is een ongehoord ingewikkeld verhaal, alleen de transactie van geld via de belasting naar zorgkantoren naar ons is al zo moeilijk om uit te leggen. Veel mensen snappen dat systeem al niet, en dat is ook niet gek, want het is van de gekke hoe dit in elkaar zit en uitgelegd wordt op een website van verzekeraars. ... Wanneer mensen geconfronteerd worden met teksten die totaal onbegrijpelijk zijn kiezen de meeste mensen ervoor om het er maar gewoon bij te laten. En dat komt natuurlijk gunstig uit voor de verzekeraars. Er is maar een klein groepje dat denkt: godverdomme, dit gaat mij aan en ik wil dit snappen en ik ga verdere vragen stellen. De meeste kiezen ervoor het er maar gewoon bij te laten. Ik heb hier een stuk over geschreven waarin ik dit murwlullerij noem; murw geluld worden, omdat het onbegrijpelijk is. ... Dit afhaken bij moeilijke taal is een enorm probleem volgens DeVrijePsych. ...

Hoe is jullie verhouding met CBP hier eigenlijk in?
Er zijn aardige stukken geschreven door het CBP over het beroepsgeheim. Dit hebben we op de DeVrijePsych ook geciteerd. Maar ik heb het idee dat ze zich gewoon hebben laten omlullen door de staat, en met name in de brief van 6 december, waar ze in feite het beroepsgeheim hebben vrijgegeven. [hierin stond onder andere: "...Daarmee [is] naar het oordeel van CBP voldoende aannemelijk gemaakt dat ...diagnose-informatie op de declaratie ten behoeve van de zorgverzekeraar noodzakelijk moet worden geacht...".[bron:www.devrijepsych.nl]]. Dat is zeer teleurstellend ... . Het CBP heeft sinds kort ook een popi jopi site gemaakt, ik weet niet of je dat hebt gezien [mijnprivay.nl], met een cartoonachtig idee.

Nou ja ze krijgen veel kritiek van andere partijen dat ze zich teveel richten op bedrijven en niet op de burgers, terwijl ze zich wel voor deze burgers zouden moeten inzetten. Op deze manier proberen ze dit denk ik recht te zetten.
En dat is ook legitiem dat ze dat doen. Wat ze horen te doen is privacy bescherming en belangenbescherming voor de burgers. Ik heb de indruk dat hun positie ... niet helemaal optimaal is. Ze hebben best hele goede stukken op die site staan, maar ik heb de indruk dat ze behoorlijk in het nauw zitten. ... Maar de beslissing van 6 december is zeer slecht en zeer teleurstellend. Mensen moeten met alles naar hun arts kunnen gaan en daar moet die arts zijn bek over houden.

[Afronding gesprek].

Interview 5: Jan Plasmooij, ICT manager - NIVRA

Kun je iets vertellen over je functie binnen het NIVRA?
Mijn functie? Ik ben werkzaam bij het NIVRA en mijn aandachtspunt is informatietechnologie en alle ontwikkelingen op dit gebied. En ik zorg dat die onder de aandacht wordt gebracht onder de leden, en dat wij als beroepsorganisatie alle IT ontwikkelingen die belangrijk zijn voor accountants, maar ook voor het bedrijfsleven.

En op welke manier heb je in je werk te maken met privacy?
Als beroepsorganisatie zetten wij de standards van de audits, ... en nu wordt het technisch. Het betekent dat wij de standaard zetten die aansluiten bij internationale standaarden, ... Het beoordelen van privacy voor bedrijven en het afgeven van een oordeel, en mogelijk zelfs van een zegel. ... Wij zijn een organisatie die het raamwerk en de voorwaarden bepalen, waaronder die werkzaamheden mogen plaatsvinden.

Wordt dit door steeds verdergaande technologie makkelijker of juist moeilijker om dit werk te blijven doen? Worden jullie tegengewerkt bij het bepalen van zo'n raamwerk door bijvoorbeeld bedrijven?
Nee. Eind 1999 en begin 2000 ben ik betrokken geweest bij de overheid, met het initiatief dat toen nog van de Registratiekamer kwam, om naar een vorm van privacycertificering te gaan. De reden van het College was dat als er een soort privacycertificering beschikbaar komt, hopen zij dat de markt daar gebruik van gaat maken, zodat er dus een soort van regulering in de markt gaat bestaan. ... Dat betekent dat de toezichthouder daar dan weer voordelen mee heeft. Als de markt zichzelf reguleert, ... dan zou de toezichthouder dat kunnen toezien, en dat zou betekenen dat je de toezichtactiviteiten wat anders zou kunnen inrichten. ... Het toenmalig hoofd van de Registratiekamer wilde dat een beetje naar zich toetrekken, en toen Kohnstamm [voorzitter van het CBP] kwam is dat veranderd. Hij vond het idee prima, maar wilde dat de marktpartijen, en dat zijn de beroepsorganisaties daar invulling aan moeten geven. We hebben toen een aantal jaren samengewerkt om het raamwerk te maken. ... We waren toen heel snel klaar, omdat we dit zelf konden doen, en het College heeft dit altijd gesteund. ... Ik denk dat er een goede marktwerking

kan ontstaan, maar ik snap dat jij kan zien dat privacy een minder belangrijk issue wordt, zeker ook in het kader van criminaliteitsbestrijding, maar ook in de misbruik van wetgeving. Persoonlijk heb ik daar geen probleem mee. Bijvoorbeeld bij het rekeningrijden, dan ligt iedereen gelijk weer wakker, dan denk ik van ok als je niet gefotografeerd wil worden moet je niet op de A2 gaan rijden. Maar wat je wel ziet, internationaal, is dat bedrijven zich moeten verantwoorden over beleid en uitvoering daarvan en over wat wij compliance noemen. Dat ze zich dus houden aan de wet en verantwoord omgaan met gegevens. Dat geldt niet alleen voor zakelijke bedrijven, maar ook voor bijvoorbeeld ziekenhuizen. ... Die druk op die verantwoording en de consequenties die eraan hangen wanneer je die niet neemt, daarvan denken we dat dit product [het raamwerk van het NIVRA] daar helemaal in past. Wij kunnen ze laten zien hoe ze binnen de wet kunnen handelen en conform de WBP hun werk kunnen doen. En dat past in de tijdgeest van de maatschappelijke vraag hier meer duidelijkheid over te krijgen.

En zien die bedrijven dat meer als een noodzakelijk aspect, of zien zij ook daadwerkelijk het belang hiervan in?
Ons oordeel is vrijwillig, dus de druk komt niet vanuit de wet. Er ontstaat een maatschappelijke behoefte. Er zijn een aantal overheidsinstellingen die zich via onze wijze kunnen verantwoorden, en de verwachting is dat dat er meer zullen worden, en de maatschappelijke ontwikkeling die kant op gaat. ... Zij zien dit op vrijwillige basis, omdat ze er een voordeel in zien. Als er bij bedrijven die met privacy-gevoelige informatie omgaan, twijfel ontstaat, kan dat commercieel schaden. Wanneer bekend wordt dat een ziekenhuis niet goed met gegevens omgaan, gaan de mensen er niet meer naartoe. Er zijn een aantal bedrijven voor wie het interessant is om zeg maar te demonstreren om de zaak op orde te houden, je kunt het als een plus zien. ...

Maar goed, ik kan me voorstellen dat grote bedrijven sneller zullen zeggen: we schuiven dit even onderin het laatje.
Bij grote ondernemingen komt die compliance vraag ook op tafel. ... De vereiste om te rapporteren wordt alsmaar groter. Ik kan me voorstellen dat een aantal ondernemingen privacy nog steeds niet als heel strategisch zien, maar dat kan heel snel veranderen. Op het moment dat bedrijven in de publiciteit komen, dat ze hun privacy niet op orde hebben, kan dat enorm schaden, zowel het imago als het financieel deel.

Maar zolang de tendens er is dat de privacy niet zo belangrijk is, is die druk ook niet zo groot.
Dat klopt. ... We zijn in Nederland goed in het maken van regels, maar veel minder goed in het handhaven van die regels. We maken regels en vervolgens gedogen we dat mensen er niet goed mee omgaan. ... Als het College wat meer zou handhaven, en met name in sectoren waarvan bekend is dat ze een loopje nemen met de privacyregels, dan zou de druk ... toenemen. Wij zouden erg gebaat zijn bij een wat strakkere handhaving. ... Wanneer bedrijven zich niet aan de regels houden, en dat komt in de krant te staan, is dat ook een manier van reclame maken, alleen is het geen positieve reclame. Als er wat strakker gehandhaafd wordt zou dat heel mooi zijn.

En hoe moet ik dat zien met de bedrijven en organisaties waar jullie mee werken, zoeken jullie die zelf op of komen zij vanzelf naar jullie toe?
Wij zijn een beroepsorganisatie, dus wij reguleren het beroep. In wezen worden de opdrachten gedaan door de accountantskantoren. De meeste bedrijven, zeker grote bedrijven, hebben vaste accountants. Dus wij verwachten dat als er vragen zijn, dat zij contact opnemen. ... Wij zijn niet degenen die de dienstverlening doen. ... Wij kunnen ook een stukje voorlichting geven, neutrale voorlichting over de diensten die beschikbaar zijn.

En op welke manier uit zich dat concreet, het voorlichting geven?
Wat wij regelmatig doen, is zorgen dat er gepubliceerd wordt. Dat kan zijn dat we zelf zorgen dat er artikelen verschijnen. Dat kan in een van onze eigen bladen zijn ..., maar je kunt het ook via interviews doen. Stel dat er morgen in de krant komt dat de ziekenhuizen er een potje van maken, kan ik me voorstellen dat de voorzitter zegt: ik stap naar de pers. ... Er zijn immers mogelijkheden om hier iets aan te doen, en zo kun je indirect weer iets wat gebeurt koppelen aan het reclame maken. ...

En zijn er dan nog specifieke partijen of actoren waar je je op richt?
Er zijn wel sectoren in Nederland waarvan we weten dat de informatie die ze hebben gevoeliger is. Dan kun je denken aan instellingen die met gezondheid te maken hebben, zeker ziekenhuizen. Daar wordt allemaal informatie bewaard van mensen, medische informatie ook en dat is heel gevoelig als dat op straat komt. Er zijn organisaties die informatie hebben over de financiële

situatie van mensen. Dat zouden financiële instellingen kunnen zijn, maar je hebt ook een groep van deurwaarders die geld innen bij mensen die een achterstand hebben van schulden. Niemand wil graag publiekelijk hebben dat hij schulden heeft. Dat is ook een sector waar dat soort gevoelige informatie wordt bewaard. ... Zo zijn er in Nederland een aantal sectoren waarbij de informatie gevoelig is. De overheid heeft een aantal systemen waar verschillend over wordt gedacht, als je het bijvoorbeeld over rekeningrijden hebt, dan registreert dat systeem precies waar je rijdt. ... Ik heb er geen probleem mee, ik kan me voorstellen dat er mensen zijn die er een probleem mee hebben als die informatie ergens anders voor wordt gebruikt dan waar het voor bedoeld is, ... of wordt bewaard. En bij sommige bedrijven gaan ze ook niet zorgvuldig om met gegevens van hun eigen medewerkers. ... Als ik op Google mijn naam intoets bij foto's, komt gewoon mijn foto op het Internet, dat is een foto van het NIVRA, maar hier is nooit toestemming voor gevraagd. ...

Ja en mensen zijn natuurlijk heel erg bang voor volgsystemen...
Ik denk dat wij al op zoveel plaatsen geregistreerd staan dat iedereen in Nederland eigenlijk al gevolgd kan worden. Via de mobiele telefoon kan je al wereldwijd gevolgd worden, en ook creditcards en bankpassen. Zo is er veel informatie over cliënten en klantgedrag. Google is een organisatie die bij uitstek al niets anders doet dan informatie verzamelen. Tot op heden zeggen ze dat ze deze informatie niet zakelijk zullen aanwenden, maar er zijn mensen die huiverig zijn dat dit beleid zal veranderen in de toekomst. ...

Hoe zien jullie dit onder de maatschappelijke veranderingen? De technologische ontwikkelingen gaan maar door. Verandert dit jullie werk ook?
Ja, ... Er is een enorme slag aan de gang. De hele papieren wereld gaat heel snel naar de informatietechnologie. ... Die digitalisering van de hele informatie-uitwisseling, maar ook van alles om ons heen dat dat enorme gevolgen zal hebben. Dat heeft een enorme impact op de maatschappij. ... De vraag waar je tegenaan loopt is of je geen scheiding krijgt in de maatschappij tussen jongen mensen en ouderen die de ontwikkelingen nooit hebben meegemaakt. Al sterven die natuurlijk uit, maar ik word ook ouder en de vraag is of ik het bij zal kunnen houden. ...

Maar wat zou dat voor het NIVRA kunnen betekenen?

Onze leden zitten in de zakelijke dienstverlening. Dat betekent dat zij gewoon moeten zorgen dat ze kunnen blijven omgaan met die technologie en bedrijven en organisaties moet kunnen helpen bij die omslag. Wij kunnen bedrijven helpen om processen anders in te richten. Dus voor ons liggen er alleen maar kansen denk ik.

Zou het niet moeilijk worden om dit bij te houden?
... Mensen die in de zakelijke dienstverlening zitten zullen continu moeten blijven bijleren, dat zit ook in de regelgeving. Dat is de manier om te blijven overleven. Je zal je continu moeten blijven ontwikkelen. Als je dit niet doet dan ben je volgens mij na 2 of 3 jaar niet meer in staat om je cliënten te helpen. Maar dat heeft te maken met de snelheid van de ontwikkeling. Maar ik denk dat het voor ons alleen maar interessant is. ...

[Afronding gesprek].

Interview 6: Wilfried Olthof, directeur NOREA - beroepsorganisatie van IT-auditor

Wat is precies de taak van de NOREA?
Er zijn dus twee beroepsorganisaties, het NIVRA bepaalt of je gekwalificeerd bent als accountant om onderzoek te kunnen gaan uitvoeren. NOREA doet eigenlijk precies hetzelfde, maar dan niet voor registeraccountants. NOREA richt zich op de auditor, wij zijn de beroepsorganisatie van de IT-auditors. Ik zeg altijd maar gewoon dat de IT-auditor de accountant van de elektronische snelweg is. Auditors die bij uitstek in staat zijn om technologische infrastructuur te beoordelen op voldoende beveiliging en of het beantwoord aan de wettelijke bepalingen omtrent de privacy. We zijn ook bevoegd om daar een oordeel over af te geven, wat niet alleen voor het bedrijfsleven van belang is, maar ook voor het maatschappelijk verkeer. ... Het kan ook voor de samenleving als geheel van belang zijn. Het is belangrijk dat de samenleving weet dat je op een oordeel van een accountant kunt vertrouwen. Dat dat een oordeel is dat onafhankelijk en onpartijdig is.

En hoe maken jullie dat dan duidelijk?
Door te wijzen op hoe dat oordeel wordt afgegeven. ... Het is voor iedereen ter inzage, dat is openbaar. ... Daar gelden standaard teksten en formulieren voor. ... Onze auditors zijn op een hele

cruciale plaats in de samenleving werkzaam, onze leden werken bij alle grote bankverzekeraars en accountantskantoren. ... We hebben dus overal vertegenwoordigers in, dus dat oordelen over privacy zou kunnen plaatsvinden op alle cruciale plaatsen in de samenleving. ... We hebben in overleg met het CBP en het NIVRA gezegd dat we de richtlijnen beter en gestructureerde moeten aanpakken. Nu staat voor de beroepsbeoefenaren dat er voor de privacy een oordeel moet worden afgegeven op basis van richtlijnen en regels waar ze zich aan moeten houden. ... Het CBP ondersteunt deze dienst van harte en is ook betrokken geweest bij het ontwikkelen van het hele raamwerk van de privacy-oordeling. ... Dit is dus een beetje de hele context waarbinnen het verhaal zich afspeelt. ... Wij zijn natuurlijk niet helemaal bevooroordeeld, want we hebben er belang bij dat er een markt is voor dit hele privacy aspect. Maar het kan zijn dat een bank het elegant vindt om aan zijn klanten te kunnen laten zien dat ze aan alle eisen voldoen die aan privacy gesteld worden. Maar dit kan ook gewoon voor een postorderbedrijf gelden. ... Onze auditors hopen natuurlijk dat er ook veel vraag zal komen naar deze onderzoeken. ...

En hoe proberen jullie dit in de markt te krijgen?
Door allereerst te wijzen op risico's die er zijn als je niet overeenstemt met de wettelijke eisen die er zijn. Het is niet alleen het risico dat je strafbaar bent, maar ook een risico dat wij dat ontdekken. Wij oordelen niet alleen, maar brengen ook adviezen uit. We komen wel eens ergens binnen en kunnen dan diegene adviseren zus en zo te handelen. ... Je kan iemand erop wijzen dat ze risico lopen op het gebied van privacy en hun gegevens op straat zouden kunnen belanden, zoals bij vertrouwelijke bankgegevens. Dat kan wanneer een bank z'n eigen technologie niet goed genoeg beveiligd heeft. Dat is ook een risico uit het oogpunt van privacy, maar dan is het meer risico van de klant heeft zijn vertrouwelijke gegevens op straat liggen. Op die manier probeer je dus als auditor ... te wijzen op de belangen die ermee gemoeid zijn.

Dus de oordelen hebben meer te maken met wettelijke bepalingen en het doen van adviezen dan met het belang voor de bedrijven zelf?
Ja dat klopt. Wij werken met compliance, dus de vraag of je voldoet aan alle privacy richtlijnen, en dan draait je winkel gewoon goed en is alles goed beveiligd.

En op welke manier komen jullie in contact met potentiële klanten?

Vaak wordt je gewoon gevraagd een oordeel te doen, om een jaarrekening te controleren. Dat is vaak je eerst contactmoment. Vervolgens bouw je een adviesrelatie op. ... Dat kan natuurlijk ook niet zomaar, want als je een controle relatie hebt mag je niet ook adviseren. Dat zou betekenen dat je je eigen controle gaat bekritiseren. En dat staat onze onafhankelijkheid in de weg. Als je een adviesrelatie aangaat moet je andere mensen vragen om de controle voor hun rekening te nemen. ... Hierin moet een scheiding worden gemaakt. ... En bij die adviesrelatie is privacy vaak een heel belangrijk aandachtspunt. En dan ga je kijken wat voor technologie je aantreft. ... Er zijn bedrijven waar dit keurig geregeld is, en er zijn er ook waar dit een ondergeschoven aandachtspunt is. ... En bij ons hebben we ook een register, gewoon een database waar gegevens in staan. Wanneer we pretenderen verstand te hebben van privacy, moeten we zelf de zaken die gaan over onze eigen leden ook goed op orde hebben natuurlijk.

Ik kan me voorstellen dat jullie juist in contact willen komen met bedrijven waar dit dus een ondergeschoven aandachtspunt is. Hoe komen jullie bij deze mensen terecht?
Ja, ... we proberen dat wel te doen. Dat is een kwestie van marketing en verkooptechniek. En daarom ontwikkelen we ook brochures, zodat onze leden dat mee kunnen nemen om aan de klant te geven.

Dus op die manier probeer jullie wel een beetje invloed uit te oefenen op de klanten?
Ja. Via onze bladen en via onze website hebben we aan onze leden kenbaar gemaakt dat we hier normen en handreikingen voor ontwikkeld hebben. ... Wanneer er richtlijnen veranderen of bijkomen sturen we gelijk een brochure naar alle leden, zodat zij hun cliënten op de hoogte kunnen stellen. ... Dit doen we ook via de elektronische nieuwsbrief, op die manier houden we iedereen op de hoogte.

Dus de nadruk ligt wel op het bieden van informatie?
Ja. Onze leden hebben ook een verplichting om 40 uur per jaar te besteden aan nieuwe informatie en hiermee zich dus te ontwikkelen. En we bieden ook cursussen, congressen en seminars aan over verschillende onderwerpen. We hebben ook wel eens een keer een seminar gehad over privacy.

En waren daar genoeg geïnteresseerde mensen voor te vinden?
Ja er waren ik denk zo'n 120 mensen, dus dat is best redelijk. En bij accountants is het vaak zo dat ze specialisten hebben op bepaalde terreinen, vrijwel ieder kantoor heeft iemand in dienst die gespecialiseerd is in privacy. ...

En wanneer we kijken naar maatschappelijke veranderingen, zoals de technologische ontwikkelingen, kun je merken dat dit je werk erg heeft veranderd?
Ja natuurlijk. Je ziet dat we midden in de technologische innovaties staan. We hebben ook de taak om, zodra nieuwe technologie beschikbaar is, deze ook gelijk te gebruiken. Er komen steeds allerlei nieuwe systemen.

.... [Er komt iemand binnen met thee].

Ja dus we hadden het over bedrijfsapplicaties en de omvangrijke systemen, die systemen ontwikkelingen zich nu heel snel. Daar moet je als auditor in het jaar dat dat geïmplementeerd is, moet je daar al mee kunnen werken en een oordeel over kunnen geven. ... Wat je ook ziet is dat tegenwoordig ... bij jaarrekeningen van bedrijven, zij dit eigenlijk zo snel mogelijk na 1 januari af willen zien, zodat ze de boeken kunnen sluiten. Vroeger kwam ergens in maart of april het jaarverslag pas, met de accountantsverklaring erbij. ... Ze willen nu eigenlijk dat op 1 of 2 januari de accountant er al naar gekeken heeft en zijn goedkeuringsverklaring heeft gegeven. Er zit een voortdurend spanningsveld van wat aan de ene kant met technologie kan, en aan de andere kant, wat je toch als auditor nodig hebt om goed een beeld te kunnen vormen van wat precies is gebeurd. En daarom wordt de rol van auditors wel steeds belangrijker, omdat die bedrijfsprocessen en informatie in feite in systemen zit die volkomen in gedigitaliseerd. Je moet er dus op kunnen vertrouwen dat er uit die computersystemen elk moment de juiste gegevens komen. ... Dit is natuurlijk ten aanzien van de privacy een heel belangrijk aandachtspunt. De technologie is zo geperfectioneerd dat je van mensen alles kunt weten en kunt zien. ... Zo moeten telecombedrijven en internetbedrijven hun gegevens anderhalf jaar bewaren, en dit is iets wat op gespannen voet staat met de privacy. Het duurt geen twee jaar meer voordat er een chip in auto's komt, waardoor je overal ter wereld kunt zien waar die auto zich begeeft. ... Als je dit soort gegevens gaat opslaan en bewaren, kun je van burgers heel nauwgezet bijhouden wat ze doen. ...

En wordt jullie werk hierdoor ingewikkelder; jullie moeten tenslotte wel steeds meer je best doen om inderdaad bij te blijven.
Het audit gebied is sowieso heel erg ingewikkeld. Je kunt dit beroep alleen maar goed doen als je je voortdurend blijft ontwikkelen op technologisch gebied.

Ja, maar ik kan me voorstellen dat dat wat druk veroorzaakt.
Ja, maar men onderkent dat dit gewoon een strategische invulling is van je beroep. ... Onze voornaamste functie is het zijn van een doorgeefluik van nieuwe regels en richtlijnen en bijbehorende uitleg hoe dit in de praktijk moet worden toegepast. Dat is in feite onze belangrijkste taak. ... We moeten de informatievoorziening op peil houden om te kunnen onderbouwen en ondersteunen hoe dit in de praktijk vorm moet krijgen. Onze voornaamste taak is het hele circus van educatie en regelgeving.

En is de vraag naar die informatie ook erg toegenomen of niet?
De vraag wordt bepaald door wat de markt dicteert. ...

En hoe is jullie samenwerking met het CBP?
Zij onderkennen dat het belangrijk is dat organisaties op de hoogte zijn van de WBP en de eisen die deze wet stelt, en het belang dat een derde onafhankelijke partij daar een oordeel over kan vellen. In dit opzicht zagen ze ons ... als een partner om deze taak te vervullen.

Maar het CBP zelf neemt niet heel veel initiatieven op dit gebied?
Nou ze vonden het wel belangrijk, maar ze waren ook zo prudent te zeggen dat het niet hun business is, en als dit wel zo is moeten ze daar afstand van nemen. Als er een commercieel belang is bij het afgeven van privacy oordelen kunnen ze zich daar als toezichthouder niet mee bemoeien. Dan moeten ze hun onafhankelijkheid niet in de strijd gooien, ze moeten afstand bewaren van de markt van de privacy. Het CBP kan geen concurrentie zijn wanneer ze een onafhankelijk toezichthouder zijn. ... Dan wordt privacy ook een commercieel product, en dan moet het CBP wel onafhankelijk een oordeel kunnen geven wanneer dit product zorgt voor aspecten die minder wenselijk zijn. ... Er is een concreet belanghebbende. ... Als iemand veel geld

kan verdienen door iedereen maar heel snel certificaten te geven, wordt er alleen maar geld verdiend, zonder dat er gekeken wordt of het inhoudelijk ook klopt. Als je namens de regering verantwoordelijk bent voor het toezicht op de wijze waarop met privacy wordt omgegaan, kun je je niet met marktpartijen inlaten. Dit zou een einde van de onafhankelijkheid van het CBP betekenen. ...
Er komt overigens ook wel eens een vraag van de leden om privacy meer op de kaart te zetten en de compliance in orde te krijgen. Dan pakken we dat op en gaan we kijken hoe wat dat het beste kunnen doen en leggen we contact met de toezichthouder. We zijn nu ook bezig in de sfeer van de gezondheidszorg, hoe een aantal beoordelingsproducten kunnen worden neergezet. ... Daar zijn natuurlijk ook veel partijen bij betrokken, zoals zorgverzekeraars en accountants. ... In overleg worden dan standaarden besproken, maar deze moeten natuurlijk wel binnen de kaders passen, er moet wel enige cohesie zijn. Het is niet zo dat ieder bedrijf zijn eigen standaarden kan zetten. Dat is de rol van de beroepsorganisatie.

[Afronding gesprek].

Bijlage 2; Krantenartikelen

In deze bijlage vindt de lezer een aantal artikelen over privacybescherming die verschenen zijn in verschillende kranten. Er wordt in de scriptie naar sommige artikelen verwezen, anderen zijn meer ter illustratie of als achtergrondinformatie.

AD/Algemeen Dagblad
30 May 2006 Tuesday

DEN HAAG
Verdonk over de schreef met Taïda

Verdonk had de persoonlijke gegevens van Taïda Pasic niet openbaar mogen maken. Die conclusie trekt het **College Bescherming Persoonsgegevens** (CBP). De minister van Vreemdelingenzaken heeft volgens het CBP 'onzorgvuldig en onrechtmatig' gehandeld door toch een boekje over de scholiere open te doen. De oppositiepartijen willen Verdonk nu op het matje roepen. De scholiere Pasic wilde in Nederland haar vwo-examen doen. In de juridische strijd die vooraf ging, bracht het ministerie van Verdonk in februari persoonlijke gegevens naar buiten. Dit was in strijd met de Wet bescherming persoonsgegevens, stelt het CBP.

Leeuwarder Courant
July 12, 2006

Waakhond CBP kan werk niet aan

DEN HAAG[(GPD)[De persoonlijke gegevens van de bevolking worden onvoldoende beschermd. Zorgen over terrorisme en andere vormen van criminaliteit leidden in de afgelopen jaren tot afbrokkeling van de bescherming van privacygevoelige gegevens.

Bovendien kan het **College Bescherming Persoonsgegevens** (CBP) het werk lang niet aan. Dit constateert het CBP, dat toezicht houdt op de naleving van wetten over het gebruik van persoonsgegevens, in het jaarverslag over 2005. Uit onderzoek in 2004 en 2005 bleek dat de burgers maar weinig vertrouwen hebben in de wijze waarop in de samenleving met persoonsgegevens wordt omgesprongen.

"De afgelopen jaren heeft de bescherming van de persoonlijke levenssfeer in de publieke opinie haar vanzelfsprekendheid verloren", concludeert CBP- voorzitter Jacob Kohnstamm. Volgens hem heeft de organisatie te weinig mensen en te weinig geld, en kan zij maar een beperkt aantal van zijn taken uitvoeren."Alleen door alle zeilen bij te zetten, hebben we op enkele grote dossiers kunnen doen wat van ons wordt verwacht", stelt het CBP.

Als voorbeeld van wat wel lukte noemt het CBP de richtlijnen in verband met de stelselwijziging in de gezondheidszorg. Na intensief overleg met het ministerie van volksgezondheid en artsen- en patiëntenorganisaties werden extra gedragsregels opgesteld voor de omgang met persoonsgegevens door ziektekostenverzekeraars. Ook heeft het CBP zich intensief bemoeid met maatregelen voor criminaliteits- en terrorismebestrijding.

Het college betreurt dat het maar mondjesmaat toekomt aan de handhaving van de Wet Bescherming Persoonsgegevens en andere privacyregels. Bovendien lijkt het langzamerhand al gewoon te zijn geworden dat overheidsinstanties en particuliere bedrijven allerlei bestanden en koppelingen hiertussen aanleggen, met het oog op het voorkomen van iedere denkbaar misbruik. Kohnstamm: "In dit maatschappelijk klimaat bestaat het risico van vermindering van de gevoeligheid voor de noodzaak tot bescherming van persoonsgegevens".

AD/Algemeen Dagblad
July 13, 2006

CBP: meer aandacht voor bescherming gegevens nodig
DEN HAAG (ANP)

Het **College Bescherming Persoonsgegevens** (CBP), de waakhond voor de privacywet, pleit daarvoor in zijn jaarverslag over 2005, dat gisteren is gepresenteerd. De belangstelling voor privacyzaken neemt volgens voorzitter Jacob Kohnstamm steeds verder toe, wijzend op het stijgend aantal mensen en instellingen dat zijn college weet te vinden.

Vorig jaar waren er 65.000 bezoekers per maand op de CBP-website, een stijging van 50 procent in vergelijking met 2004. De eerste helft van 2006 gaat het zelfs om 100.000 bezoekers per maand. Het aantal e-mails is verdubbeld en het downloaden van uitspraken van het CBP noemt Kohnstamm 'indrukwekkend'.

De grootste groep mensen maakt zich druk om de verstrekking van hun gegevens aan derden. 'Dan duiken zomaar ergens hun gegevens op, zonder dat ze die zelf hebben verstrekt.' Volgens Kohnstamm zijn mensen daar gevoelig voor, ook al hebben ze niets te verbergen. Hij wijst erop dat burgers alert kunnen en moeten zijn en zelf zaken kunnen veranderen als het hen niet aanstaat.

Het CBP wijst erop dat een deugdelijke en fatsoenlijke bescherming van allerlei gegevens mogelijk is met de nieuwe informatiesystemen en nieuwe technologie. Dat gebeurt nu onvoldoende, vindt het college.

'De techniek lijkt nu de grenzen aan te geven voor privacy in plaats van de normen en waarden in de samenleving', aldus Kohnstamm.

Het CBP verwijst naar het burgerservicenummer, een vervanging van het sofi-nummer, waarmee koppelingen van gegevens mogelijk zijn. Dat dient het gemak van de overheid en van de burger zelf maar er is niet voorzien in goede hulp als er administratieve ongelukken gebeuren. 'Als het eenmaal misgaat met dat nummer, dan gaat het goed fout.' Kohnstamm vertrouwt erop dat de Tweede Kamer dit corrigeert in het wetsvoorstel.

Verder blijft het CBP zich zorgen maken over het gewijzigde krachtenveld rond privacy.

Bestuurders, politici en belangenbehartigers wijzen de laatste jaren de bestaande bescherming van persoonsgegevens ten onrechte aan als een zondebok of een obstakel.

Zij verschuilen zich achter de zorgen om terrorisme, onveiligheid en maatschappelijke misstanden. In dit klimaat wordt de privacy snel terzijde geschoven, stelt het CBP.

NRC Handelsblad

Bos zegt onderzoek toe naar verstrekken bankgegevens

Door een onzer redacteuren

De Kamer had hem vragen gesteld naar aanleiding van een artikel in NRC Handelsblad van afgelopen zaterdag. Advocaten, adviseurs en deskundigen vertelden daarin dat Amerikaanse opsporingsdiensten rechtstreeks bij kantoren van Europese banken in de VS informatie opvragen van Europese klanten. Volgens Europese en ook Nederlandse wetten mag dat niet.

Omdat de belangen groot zijn, sprak een deel van de zegslieden op anonieme basis. Wel erkende een woordvoerder van de Rabobank dat dergelijke verzoeken vanuit de VS worden gehonoreerd.

Bos zei dat hem niets bekend was over deze kwestie, maar dat hij samen met zijn collega Ernst Hirsch Ballin (Justitie, CDA) de zaak gaat uitzoeken. De Kamer krijgt uiterlijk eind april de resultaten van dat onderzoek.

De PvdA-bewindsman houdt het voor mogelijk dat de klantgegevens niet direct zijn verstrekt aan opsporingsdiensten in de VS, maar langs de officiële weg, via rechtshulpverzoeken of via een samenwerking tussen Nederlandse en Amerikaanse toezichthouders. Ook dit laat hij onderzoeken. Als Nederlandse privacywetgeving wordt overtreden is dat „ook mij een zorg”, aldus Bos. Het ministerie heeft opheldering gevraagd bij de Rabobank. Die zegt volgens Bos dat ze niet meewerkt aan verzoeken ‘via de achterdeur’. Tegenover NRC Handelsblad heeft de bank echter bevestigd deze verzoeken wel te honoreren.

Kamerlid Kees Vendrik (GroenLinks) vroeg ook om opheldering over de rol van De Nederlandsche Bank (DNB). DNB en het ministerie van Financiën wisten al in 2002 dat ook Swift, de instantie in Brussel die voor de bankwereld internationale overboekingen verzorgt,

Europese bankgegevens afgeeft aan de Amerikaanse autoriteiten. Ministerie en DNB zwegen hierover tot de kwestie vorig jaar uitlekte.

In de ogen van Bos hoefde DNB de Nederlandse privacytoezichthouder College Bescherming Persoonsgegevens (CBP) niet op de hoogte te stellen van het overhandigen van de gegevens door Swift.

Bos wil nu wel dat de banken hun klanten informeren dat hun betalingsverkeer via Swift bij onder meer de Amerikaanse inlichtingendienst CIA terecht kan komen. Fractievoorzitter Pechtold (D66) wil dat dit „met een goede brief" gebeurt. Volgens Bos is het aan de banken zelf om te bepalen hoe ze hun klanten informeren.

14 maart 2007

NRC Handelsblad

DNB eist uitleg over afgeven van bankgegevens

Door een onzer redacteuren

Rotterdam, 15 maart. Toezichthouder De Nederlandsche Bank (DNB) wil van de banken opheldering over het afgeven van klantgegevens aan de CIA en andere Amerikaanse inlichtingen- en opsporingsdiensten. Dat zeggen bronnen in de bankwereld.

Het initiatief volgt op een toezegging van minister Bos (Financiën, PvdA) aan de Tweede Kamer dat hij het verstrekken van privacygevoelige informatie door banken aan de VS zal onderzoeken. Een woordvoerder van DNB zegt: „Als er signalen binnenkomen, gaan wij daar serieus naar kijken".

Zaterdag verklaarden advocaten, adviseurs en deskundigen in NRC Handelsblad dat Amerikaanse diensten als CIA en FBI rechtstreeks bij Europese banken in de VS informatie van individuele Europese klanten vragen, en krijgen. Volgens Europese en ook Nederlandse wetten mag dat niet. De 'achterdeurverzoeken' zijn een schending van de privacy en in strijd zijn met strafrechtelijke procedures. De Rabobank bevestigde tegenover deze krant dat dergelijke verzoeken gehonoreerd worden. Volgens de Amerikaanse antiterrorismewet zijn banken verplicht mee te werken.

Inmiddels overlegt de Nederlandse Vereniging van Banken (NVB) met het College Bescherming Persoonsgegevens. CBP-voorzitter Jacob Kohnstamm meldde zaterdag dat banken boetes kunnen verwachten als zij hun klanten er niet van op de hoogte stellen dat hun gegevens in handen kunnen komen van de VS.

Belangenbehartiger NVB zegt dat de banken aan de wettelijke eis tot informatie aan klanten zullen voldoen. Het CBP wil dat er een campagne komt om rekeninghouders die internationale betalingen verrichten erop te wijzen dat de Amerikanen kunnen 'meekijken'.

15 maart 2007

NRC Handelsblad

Monetaire autoriteiten zwegen vier jaar lang tegenover Tweede Kamer
CIA kijkt via achterdeur mee bij banken
Banken, ook Nederlandse, werken mee met Amerikaanse geheime diensten. Over privacyschending, boetes en de lange arm van de VS. „Montesquieu is overboord gegooid."

Joep Dohmen en Dimitri Tokmetzis

Halverwege het gesprek maakt Jacob Kohnstamm een vergelijking.

Zomaar even, om het probleem duidelijk op de kaart te zetten.

„Wat zou u ervan vinden als Poetin of de Chinezen hier uw financiële gegevens zouden opvragen? Uw spaartegoeden, hypotheek, bankafschriften. Zouden wij dat accepteren?"

De voorzitter van het College Bescherming Persoonsgegevens (CBP), de privacywaakhond van Nederland, laat even een stilte vallen. Dan gaat hij door: „Precies dát gebeurt nu door de Amerikanen. En die toenemende greep vanuit de VS is niet aanvaardbaar. Het leidt ertoe dat we de normen en waarden van de VS hier opgelegd krijgen. En dat terwijl er geen sprake is van wederkerigheid. Als Europa gegevens zou opeisen van Amerikaanse bedrijven, dan staan de VS op hun kop. Dit rechtvaardigt een sterk optreden."

Het zit de Collegevoorzitter hoog: „In ons rechtstelsel hebben we checks and balances, die met de extraterritoriale werking van de Amerikaanse wetgeving teniet worden gedaan. Die bepalingen brengen het Europese rechtstelsel uit balans en overschaduwen het."

De War on Terror, die na '9/11' losbarstte, wordt door de Amerikanen niet alleen uitgevochten met kruisraketten of bomtapijten op Tora Bora. Sinds 2002 hebben ze hun greep op de wereldwijde informatiestromen verstevigd. Maar waar de veiligheidsmaatregelen op luchthavens vaak nog zichtbaar zijn, is er ondertussen ook een sluipende, maar minstens zo ingrijpende ontwikkeling aan de gang in de financiële wereld. Duizenden accountants en specialisten zijn op zoek naar de financiële sporen van terroristen, in de VS, maar vooral ook daarbuiten. En daarbij gaan de Amerikanen ver.

Een tipje van de sluier is vorig jaar juni opgelicht door The New York Times. De geheime dienst CIA bleek sinds de aanslagen dagelijks de beschikking te hebben over miljoenen bankoverschrijvingen uit de hele wereld, óók van klanten van Nederlandse en andere Europese banken. Dat gebeurde met hulp van de Belgische organisatie SWIFT, die voor 8.100 banken en financiële instellingen in de hele wereld de internationale overboekingen verwerkt.

De onthulling schudde Europa wakker. De Art. 29 Data Protection Working Party, de verzameling van Europese privacytoezichthouders, veroordeelde de „heimelijke, systematische en langdurige overdracht van persoonsgegevens door SWIFT aan het Amerikaanse ministerie van Financiën". Dat gebeurde ook nog eens op „een vertrouwelijke, niet-transparante en systematische manier zonder rechtsgrondslag, en zonder de mogelijkheid van onafhankelijke controle". Het was een schending van „fundamentele Europese principes van dataprotectie en een overtreding van de Belgische en Europese wetten", zeggen de privacytoezichthouders.

De klanten van de banken, wier gegevens naar Amerika zijn doorgespeeld, was nooit verteld wat er gebeurde. De toezichthouders van SWIFT, zoals de Europese Centrale Bank en de Nationale Bank van België wisten ervan, maar zwegen. De meeste centrale banken informeerden zelfs hun eigen overheden niet. Zo kreeg de Belgische regering pas aan de vooravond van de publicatie in de The New York Times te horen wat er aan de hand was. Premier Guy Verhofstadt van België veroordeelde de schending van de privacy.

Hoe zit het eigenlijk in Nederland? Eén ding is zeker: waar in andere EU-landen en het Europees Parlement veel beroering ontstond na de SWIFT-onthulling, ging de affaire in Nederland betrekkelijk geruisloos voorbij. Terwijl ook hier dezelfde patronen zichtbaar waren.

De Nederlandsche Bank (DNB), toezichthouder op de Nederlandse banken en daarnaast medetoezichthouder op de betrouwbaarheid en bedrijfszekerheid van de systemen van SWIFT, is ook in 2002 door SWIFT op de hoogte gesteld. DNB lichtte vervolgens het ministerie van Financiën in, meldde minister Zalm (Financiën, VVD) na de onthulling in antwoord op vragen uit de Tweede Kamer. Vier jaar lang hadden DNB en Financiën aan de Kamer en privacywaakhond CBP niets verteld (zie: Privacybeschermer haalt uit naar DNB).

Wie, negen maanden na de onthulling over SWIFT, denkt dat het illegaal doorsluizen van bankgegevens aan de Amerikanen is gestopt, heeft het mis. Zeker, de Europese Commissie en de VS onderhandelen momenteel over een verdrag: daardoor zou Europa voortaan op de hoogte zijn welke gegevens de Amerikanen precies 'aftappen'. Maar ondertussen laat SWIFT de CIA nog steeds meekijken.

De vraag die opdoemt is of de SWIFT-affaire op zichzelf staat. Gebruiken de Amerikanen misschien nog andere middelen om financiële informatie te vergaren? En wordt die informatie alleen voor terrorismebestrijding gebruikt of misschien ook voor economische spionage? Kortom: hoever reikt de greep van de VS op Europese financiële instellingen?

Bij de officiële instanties blijkt het antwoord op deze vragen niet makkelijk te vinden.

Directeur toezicht Arnold Schilder van DNB verwijst naar de antwoorden van de minister van Financiën aan de Tweede Kamer, en zegt dat hij zich „niet herkent in het beeld dat Nederlandse banken stelselmatig, buiten rechtshulpverzoeken om, informatie verstrekken aan de Amerikaanse autoriteiten."

Ook de Nederlandse Vereniging van Banken (NVB) geeft geen uitsluitsel. De woordvoerder is kort: „Geen commentaar."

Wat de bevoegdheden van Amerikaanse opsporingsdiensten zijn, is wettelijk vastgelegd en wordt ook met enige regelmaat besproken tijdens openbare hoorzittingen van het Congres. Startpunt is de Patriot Act die vlak na 11 september 2001 van kracht werd. Daarmee brachten de Amerikanen met één pennenstreek wereldwijd banken onder hun gezag.

Artikel 319 stelt dat de ministers van Financiën en Justitie financiële informatie mogen opvragen bij alle banken in de VS, óók bij de bijkantoren van buitenlandse banken. Buitenlandse banken die slechts een rekening hebben bij een Amerikaanse bank zijn ook verplicht mee te werken. Iedere financiële instelling die internationale overboekingen in dollars doet, valt hiermee onder deze wet. En dat zijn in de praktijk zo goed als alle banken in de wereld.

Al op 12 februari 2002, kort na de inwerkingtreding van de Patriot Act, werd duidelijk wat dit betekent. Plaatsvervangend onderminister van Financiën Mary Lee Warren zei op een hoorzitting

van het Congres: „Het geeft ons een mechanisme om buitenlandse bankgegevens op te vragen met administratieve dwangbevelen."

Dat was geen loze kreet.

Want in de eerste drie maanden dat de wet van kracht was, waren er meteen 90 buitenlandse bankrekeningen gecontroleerd. Inmiddels zijn we jaren verder en kunnen meer dan 150 Amerikaanse overheidsdiensten, van CIA, FBI, OFAC tot de Amerikaanse postdienst, de bestanden van financiële instellingen laten doorzoeken. Dat gaat allemaal via het Amerikaanse Financial Crimes Enforcement Network.

Als het Financial Crimes Enforcement Network (FinCEN) een verzoek om informatie krijgt, dan wordt dat doorgestuurd naar de 29.000 instellingen waar zij contact mee onderhoudt, waaronder de bijkantoren van de buitenlandse banken en de Amerikaanse banken die de rekening van buitenlandse banken beheren. Binnen twee weken zijn de banken, meldt FinCEN, verplicht aan te geven of de gevraagde informatie aanwezig is. Het antwoord van de banken wordt teruggekoppeld naar de verzoekende dienst. Die kan bij een positief bericht zelf actie ondernemen en de informatie bij de bank opvragen. Om de informatie te krijgen, kunnen de toezichthouders, ministeries en opsporingsdiensten een administratief dwangbevel uitvaardigen. Daar komt geen rechter en officier van justitie aan te pas.

Het tappen van SWIFT past dus volgens de VS binnen de bevoegdheden, die de opsporings- en veiligheidsdiensten in dat land sinds '9/11' hebben. Die bevoegdheden gaan zover dat ze informatie kunnen opeisen over klanten die zich buiten de jurisdictie van de VS bevinden.

Via SWIFT kunnen de Amerikanen een schat aan informatie krijgen: over de omvang van een internationale overboeking, de betrokken banken, het tijdstip, de zender en de ontvanger.

Maar banken hebben natuurlijk veel méér gegevens over hun klanten, zoals andere rekeningen, hypotheken en betalingsgeschiedenissen. En ook die gegevens willen de Amerikanen hebben, zeggen advocaten en adviseurs tegen NRC Handelsblad. Een aantal wil niet met naam in de krant. Daarvoor zijn de zakelijke belangen van hun cliënten, de banken, aan de Amerikaanse kant van de oceaan, te groot.

Europese banken staan, zo wordt duidelijk, voor een dilemma. Aan de ene kant willen ze hun relatie en positie in de VS niet beschadigen. Maar aan de andere kant mogen ze volgens Europese wetten voor strafvordering en voor privacybescherming zulke gegevens niet afstaan zonder dat de vereiste juridische wegen zijn bewandeld.

Volgens de 'koninklijke weg' zouden de Amerikanen eerst een rechtshulpverzoek moeten doen, of een verzoek moeten indienen bij een Nederlandse toezichthouder. Als banken toch rechtstreeks aan de 'achterdeur' informatie afgeven aan de Amerikanen, overtreden ze in Europa de wet.

Die achterdeur staat open, weet Eric Schreuders, partner van privacy-adviesbedrijf Net2Legal in Leiden. „De VS gaan ervan uit dat hun regels van toepassing zijn op alle banken die een kantoor hebben in Amerika. Dat geldt voor de hele bank, dus ook voor het Europese moederbedrijf. Een rechtshulpverzoek vergt al snel maanden. Een officier van justitie toetst de aanvraag en filtert er mogelijk informatie uit. Waarom zou een Amerikaanse opsporingsdienst die moeite nemen, als hij alle informatie veel sneller rechtstreeks bij de bank kan opvragen?"

De Amerikanen hebben een stok achter de deur voor het geval Europese banken niet meewerken, benadrukt Cees Schaap, witwasdeskundige en directeur van SBV-Forensics in Dordrecht. „Banken die de gegevens niet overhandigen, kunnen een boete krijgen die in de miljoenen loopt. In het uiterste geval trekt Amerika de bankvergunning in. Geen zaken doen in of met de VS is geen optie. Als een verzoek binnenkomt, zal een bank loyaal reageren."

Postdoconderzoeker Bart Custers aan de Universiteit van Tilburg, die overheid en banken adviseert in privacykwesties, zegt dat het geen moeilijke keuze is om de gegevens, ondanks alle bezwaren, tóch af te staan. „De grote banken halen een flink deel van hun omzet uit Amerika. Die gaan dat echt niet in gevaar brengen. Bedrijven kijken naar wat het kost. Aan de ene kant heb je de Nederlandse privacytoezichthouder, het CBP, die relatief lage boetes kan opleggen: pakweg de prijs van een business class vliegticket. Aan de andere kant heb je de Amerikanen die boetes opleggen die in de tientallen miljoenen lopen. Aan welke kant van de oceaan ga je dan zitten?"

Daar komt bij, zegt Rogier Raas, partner bij advocatenkantoor Stibbe, dat bestuurders en managers van een bank in de VS in uitzonderlijke gevallen persoonlijk aansprakelijk gesteld kunnen worden als ze niet meewerken. Raas: „Als een organisatie een boete krijgt, dan is daar

nog wel mee te leven. Zodra medewerkers aan vervolging blootstaan of niet meer naar de VS kunnen, dan heeft een bank een groter probleem. De kans op vervolging kan al voldoende reden zijn om mee te werken."

Geconfronteerd met de mogelijkheid dat de banken zelf, naar Europees inzicht op illegale wijze, gegevens aan Amerikaanse autoriteiten verstrekken, zegt directeur toezicht van De Nederlandsche Bank, Arnold Schilder, dat hem zulke feiten „als zodanig" en „stelselmatig" niet bekend zijn.

De feiten die Schilder niet kent zijn wel bekend bij de advocaten en adviseurs met wie deze krant sprak. Zij bevestigen dat de banken zijn bezweken onder druk van de VS. Advocaat Rogier Raas (Stibbe) memoreert een zaak waarbij een bank in Nederland een Amerikaans verzoek kreeg om klantgegevens te overleggen. De bank had niet veel keuze.

De gegevens bevinden zich in een grijze jurisdictie, zegt Raas: „Informatie is tegenwoordig een vloeibaar geheel. Grote banken hebben tentakels over de hele wereld en overal liggen gegevens opgeslagen."

Soms is het voor een bank moeilijk om de rechtmatigheid van een verzoek te bepalen. „Moeten ze iedere keer als een verzoek binnenkomt advocaten inschakelen?", zegt Raas. „Dat gebeurt dus niet altijd. Bij ieder verzoek worden wel vragen gesteld: Is het rechtmatig, dan kun je gegevens verstrekken. Is het niet rechtmatig, dan liever niet, maar hoe hard wil je het spelen?" Meestal zijn Amerikaanse advocatenkantoren bij zulke afwegingen betrokken. „Wij worden doorgaans om algemeen advies gevraagd in de trant van 'wat moeten we doen als'. Dan weet je dat er een verzoek is binnengekomen."

Witwasdeskundige Cees Schaap herinnert zich een zaak waarbij een Amerikaanse toezichthouder een internationale betaling van Nederland naar Panama had onderschept, en daarop actie ondernam.

Hoe vaak zijn banken in Nederland in de afgelopen vijf jaar geconfronteerd met informatieverzoeken uit de VS, buiten de reguliere rechtshulpverzoeken om? Wat voor soort informatie is opgevraagd en is die informatie ook geleverd?

ABN Amro en ING ontkennen noch bevestigen het uitleveren van informatie via de achterdeur. De Rabobank geeft toe de gevraagde informatie in Amerika te overleggen, maar wil geen details geven (zie: ‘We doen precies wat we volgens de Amerikaanse wet moeten doen’).

De Europese Federatie van Banken (EFB) laat weten „zeer bezorgd” te zijn over de straffen en de extraterritoriale werking van de Patriot Act. Ook de EFB wil niet in detail treden, omdat de federatie betrokken is bij het zoeken naar een oplossing.

Dat Amerika zo eenvoudig tot financiële gegevens uit Europa toegang kan krijgen, mag van forensisch accountant Cees Schaap niet lichtvaardig worden opgenomen: „Nederlandse onderdanen worden blootgesteld aan het recht van een andere staat.”

Het raakt de rechtsbescherming van de Europese burger omdat er geen checks and balances meer zijn, aldus Schaap. De VS kunnen bij allerlei financiële gegevens in Europa komen zonder dat een rechter in Europa de rechtmatigheid daarvan kan controleren. Schaap: „Montesquieu is overboord gegooid. Een standaardtoetsing door een onafhankelijke partij is niet meer de norm.”

Uiteindelijk gaat het in deze kwestie om wie de regels bepaalt: Europa of Amerika. Alle conflicten zoals rond de passagiersgegevens in de luchtvaart, rond SWIFT en nu met de banken, draaien om de vraag wie sterker is, vindt de Tilburgse onderzoeker Custers. „De VS zijn daarbij in het voordeel. Die spreken uit één mond. De EU moet er telkens met 27 lidstaten uit zien te komen.”

Maar het houdt niet op bij cliëntgegevens van Europese banken, de Amerikaanse arm reikt verder. Dat vermoedt Willem Debeuckelaere. Hij is ondervoorzitter van de Belgische Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Debeuckelaere vreest dat SWIFT of banken of vliegtuigpassagierslijsten maar stukjes van de puzzel zijn.

Debeuckelaere: „Voor zover wij het nu zien, gaat het niet alleen om banken. We hebben nog geen concrete bewijzen, maar ook andere bedrijven die een band met de VS hebben, kunnen gevraagd worden de meest vertrouwelijke gegevens van hun Europese klanten te leveren. Neem softwarebedrijven die economische, medische of juridische gegevens van klanten uit Europa in

handen hebben. Er zijn nogal wat firma's uit de VS die hier werken. Volgens de Amerikaanse wetgeving kunnen bedrijven als Unisys verplicht worden die informatie door te sturen."

Waar houdt het op? De Amerikaanse wet geldt immers ook voor niet-Amerikaanse bedrijven. Debeuckelaere: „Neem uw KLM of Koninklijke Shell. Ook bij hen kunnen gegevens, van welke aard dan ook, worden opgevraagd. Je moet er niet aan denken wat dat kan betekenen."

De Nederlandse privacycontroleur, het College Bescherming Persoonsgegevens, vindt dat de politiek moet ingrijpen. De complexiteit van de transatlantische gegevensverstrekking is te groot om aan de toezichthouders alleen over te laten. Voorzitter Kohnstamm: „Wij zijn een kleine club en er zijn beperkingen aan hoeveel we kunnen onderzoeken. De politiek moet de regie nemen en met ons optrekken. Hier staan de Europese normen en waarden op het spel."

Aanstoot

Jacob Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens (CBP), houdt zijn irritatie over collega-toezichthouder De Nederlandsche Bank (DNB) niet binnensmonds. „DNB is al sinds 2002 op de hoogte van de gegevensoverdracht door SWIFT. DNB wist dat het politiek gevoelig lag. Anders had ze de minister van financiën niet zelf ingelicht. Als een toezichthouder weet of kan vermoeden dat de Nederlandse wet wordt overtreden, vind ik het merkwaardig en verwijtbaar dat ze haar collega-toezichthouder niet inlicht. Ik heb daar wel aanstoot aan genomen".

DNB zegt dat het toezicht op de privacy niet in haar takenpakket zit. Kohnstamm: „Formeel gezien klopt dat. Maar er staat DNB niets in de weg om ons op de hoogte te stellen. Waarom wel de minister waarschuwen en niet het CBP"?

Het CBP stuurde begin januari een brief naar alle banken met daarin de opdracht hun klanten in te lichten dat de Amerikanen hun gegevens kunnen onderscheppen. In reactie hierop werd Kohnstamm half februari bij de centrale bank voor een gesprek gevraagd. Flip Klopper, directeur betalingsverkeer, kondigde aan binnenkort namens de banken met een antwoordbrief te komen. Een „merkwaardige" opstelling, zegt Kohnstamm. „De gang van zaken verbaast me. Het CBP schrijft een brief aan de banken en dringt aan op naleving van de wet. Als reactie daarop krijgen

wij nu een brief van een collega-toezichthouder die zich in dit geval kennelijk meer als belangenbehartiger opstelt dan als toezichthouder".

Kohnstamm dreigt de banken met een last onder dwangsom in het geval zij hun wettelijke plicht niet nakomen tot het verschaffen van informatie over wat er met de persoonsgegevens van hun klanten via SWIFT gebeurt. „De banken overtreden op dit punt zonder twijfel de wet. Zij dienen hun klanten te informeren. Als toezichthouder kunnen we niet aanvaarden dat de banken er mee weg komen".

De toezichthouder zegt ook te weinig bevoegdheden te hebben. Kohnstamm: „We kunnen pas een 'boete' opleggen nadat we een bank hebben gewaarschuwd dat zij het niet nog een keer moet doen. Het zou wel zo effectief zijn als we stevige boetes zonder waarschuwing vooraf konden uitdelen".

DNB zegt dat zij zelf contact heeft gezocht met het CBP toen deze in januari over de SWIFT-kwestie een brief had gestuurd aan de banken. „Afgesproken is dat wij met de banken overleggen hoe ze met informatie aan hun klanten het CBP tegemoet kunnen komen, in afwachting van een oplossing door de Europese en Amerikaanse politiek", zegt DNB.

De Rabobank laat weten dat haar vestiging in New York inderdaad verzoeken krijgt van Amerikaanse opsporingsdiensten buiten het officiële rechtshulptraject om, gebaseerd op de Patriot Act. „Daar wordt door ons aan meegewerkt, ook als het gaat om bankgegevens die uit Europa komen. Wij doen precies wat we volgens de Amerikaanse wet moeten doen", zegt een woordvoerster. De bank wil niet zeggen niet hoeveel verzoeken jaarlijks binnenkomen. Ook over de inhoud ervan zegt de bank niets.

Volgens de Rabobank komen ook bij het hoofdkantoor in Utrecht „sporadisch" verzoeken vanuit Amerika binnen. In zo'n geval verwijst de bank de vragende instantie door naar de Amerikaanse ambassade in Nederland of naar de Nederlandse politie. De woordvoerster: „Die komen dan met het verzoek terug bij ons, soms door tussenkomst van de Nederlandse geheime dienst, de AIVD." De dienst krijgt de gegevens van de Rabobank en die stuurt hij dan door naar de VS.

ING zegt in een schriftelijke reactie dat het „in strijd is met ons beleid om nadere informatie te verstrekken omtrent gegevens die door de autoriteiten worden opgevraagd en omtrent de vraag in hoeverre ING aan deze verzoeken gevolg heeft gegeven."

Bij ABN Amro is het weinig anders: „ABN Amro respecteert de nationale, Europese en andere relevante internationale wetgeving ten aanzien van het verstrekken van informatie aan autoriteiten. Als er een spanningsveld bestaat tussen de eisen die door autoriteiten [..] aan ons gesteld worden, dan gaan wij daarover – als dat nodig is – in overleg met onze toezichthouders om tot een oplossing te komen."

SWIFT, de Society for Worldwide Interbank Financial Telecommunications in het Belgische Terhulpen verwerkt meer dan tien miljoen internationale transacties per dag voor 8.100 banken en financiële instellingen in de hele wereld. Op twee servers, in Terhulpen en in New York, worden de transacties geregistreerd en 124 dagen bewaard.

Kort na de aanslagen van 11 september 2001 dwong het Amerikaanse ministerie van Financiën toegang tot de gegevens af. De CIA mocht, ten behoeve van terrorismebestrijding, in het geheim in de gegevens grasduinen. In 2003 kreeg SWIFT bedenkingen over het tappen door de CIA. De organisatie wilde er liever vanaf. De Amerikaanse centrale bankier Alan Greenspan en de directeur van de FBI intervenieerden persoonlijk om de medewerking van SWIFT te behouden.

Vanaf die tijd is er enige controle op welke gegevens worden getapt. Een volgens SWIFT „onafhankelijke controleur", adviesbureau Booz Allen Hamilton, ziet toe op de naleving van de Amerikaanse wetten voor privacy en strafvordering. Actiebeweging Privacy International betwist echter dat het adviesbureau onafhankelijk is. De Amerikaanse overheid is een grote klant van Booz Allen Hamilton. In de senior consulting staff van het bureau zitten diverse oud-werknemers van geheime diensten, onder wie een voormalige directeuren van de CIA en de National Security Agency (NSA).

Op 23 juni vorig jaar bracht The New York Times het bestaan van het geheime programma naar buiten. Volgens Europese privacytoezichthouders is de gegevensoverdracht van SWIFT in strijd met de Europese richtlijnen en de nationale wetten van België, waar SWIFT onder valt. Ook de Belgische regering heeft de gegevensoverdracht bestempeld als illegaal.

Desgevraagd zegt Arnold Schilder, directeur toezicht van De Nederlandsche Bank (DNB), dat het toezicht van DNB en haar medetoezichthouders op SWIFT is gericht op de betrouwbaarheid van de technische systemen. DNB heeft een verantwoordelijkheid voor het bevorderen van de goede werking van het betalingsverkeer. Schilder: „DNB werd in 2002 op de hoogte gesteld en heeft dit onmiddellijk gemeld aan de minister van Financiën. Nu eind 2006 is gebleken dat de Europese privacy-autoriteiten bezwaar maken, zal dit op Europees-Amerikaans politiek niveau moeten worden opgelost."

Het Nederlandse ministerie van Financiën zegt desgevraagd geen oordeel te hebben over de legaliteit van de gegevensoverdracht. Een woordvoerder laat weten dat op Europees niveau naar een oplossing wordt gezocht. De Raad van Ministers en de Europese Commissie hebben hiertoe een gezamenlijke werkgroep ingesteld. Het ministerie zegt ook in Nederland naar een oplossing te zoeken. Welke concrete stappen daarvoor worden genomen „kan en wil" de woordvoerder niet vertellen.

Ook SWIFT zelf zegt in een reactie een politieke oplossing toe te juichen: „Het probleem is het verschil in wetgeving. Daardoor is een grijs gebied ontstaan en dat moet politiek opgelost worden."

NRC Handelsblad

Mei 12, 2007

Iedereen verdacht;
Technologie en juridische bevoegdheden zijn een gevaar voor de privacy in Nederland

'Brave burgers hebben niets te verbergen?" Bert-Jaap Koops, hoogleraar Regulering van Technologie aan de Universiteit van Tilburg is aan het woord. "Volgens mij heeft iedereen wel iets te verbergen. Bijna niemand wil een camera in de slaapkamer met een rechtstreekse verbinding naar het politiebureau. Wat mensen eigenlijk bedoelen is: 'Ik doe niets verdachts, dus naar mij zullen ze toch niet kijken'. Maar dat is niet meer zo."

Simon Hania, technisch directeur van internetprovider xs4all zegt het nog wat scherper: "Als je zegt 'ik heb niets te verbergen, dus ook niets te vrezen', zeg je eigenlijk 'ik vertrouw iedereen, onvoorwaardelijk'. Maar wie doet dat nou werkelijk? Iedereen heeft wat te verbergen, om heel valide redenen. Vrouwen mogen bijvoorbeeld om begrijpelijke redenen hun zwangerschap verzwijgen tijdens een sollicitatiegesprek."

Nederlanders hebben groot vertrouwen in de overheid als het gaat om bescherming van de privacy. Uit recent onderzoek, in opdracht van het Nationaal Comité 4 en 5 mei, blijkt dat een meerderheid het goed vindt dat politie en justitie het internetverkeer volgen. Met andere privacybeperkende maatregelen, zoals cameratoezicht, plaatsbepaling via mobiele telefoons en kentekens, preventief fouilleren, hebben Nederlanders al helemaal geen moeite.

Dit vertrouwen staats haaks op de inhoud van het rapport Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Onderzoekers van de Universiteit van Tilburg zijn nagegaan wat het cumulatieve effect is van de technologische ontwikkelingen en privacybeperkende maatregelen van de afgelopen tien jaar. Koops, een van de auteurs, ziet de contouren van een Big Brother-samenleving opdoemen. "De technologie en de juridische bevoegdheden zijn er al. Alleen Big Brother zit zelf nog niet achter de knoppen. Van een centrale aansturing van de versplinterde informatiebestanden is voorlopig nog geen sprake."

In 2007 is het eenvoudig om van iedere Nederlander na te gaan waar die zich wanneer bevindt en wat hij doet (zie kader). Uit DNA kunnen steeds meer kenmerken worden afgeleid van de drager en diens familie. Biometrische paspoorten (identiteitsbewijzen met een radiochip, een digitale foto, een vingerafdruk en mogelijk een gezichtsscan) vervangen de komende jaren het huidige papieren exemplaar. Deze digitale informatie kan worden gebruikt in 'slimme' camera's, die bijvoorbeeld gezichten herkennen. Radio Frequency Identification-chips (RFID) rukken op in alledaagse producten. De informatie op deze superkleine chips, bijvoorbeeld over waar het product is geweest, is op afstand te raadplegen.

De maatschappelijke gevolgen van deze technologieën zijn niet te overzien. Vast staat wel dat ze grote consequenties hebben voor de privacy. Koops: "De Wet bescherming persoonsgegevens, die onze privacy regelt, gaat ervan uit dat niet meer informatie verzameld wordt dan strikt noodzakelijk is. Maar er wordt altijd meer informatie verzameld dan echt nodig is. Informatie is voor bedrijven en ook voor de overheid veel te belangrijk geworden om te laten liggen."

Dat de informatievergaring nauwelijks is in te perken, beaamt Jacob Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens. "Wel kunnen we erop toezien wie onder welke omstandigheden de informatie gebruikt."

Maar zulk toezicht blijkt in de groeiende berg van oude en nieuwe gegevens steeds moeilijker. De gegevens worden steeds toegankelijker gemaakt voor politie en justitie. In het kader van misdaad- en terreurbestrijding krijgen zij meer bevoegdheden om in de informatieberg te speuren naar die ene terrorist of crimineel. Liefst in een zo vroeg mogelijk stadium, nog voordat een misdrijf is gepleegd.

De verruiming van bevoegdheden begon al voordat Bush in 2001 de War on terror afkondigde. De IRT-affaire, waarbij politie en justitie oneigenlijke opsporingsmethoden hadden toegepast, toonde omstreeks 1996 de noodzaak van duidelijke wettelijke regelingen. Kort daarop werden de bevoegdheden van politie en justitie niet alleen vastgelegd, maar ook verruimd.

Daarnaast nam de maatschappelijke druk toe om de veiligheid op straat te verbeteren. In 1997 werd de eerste camera, na lang publiek debat, opgehangen in Ede. Tien jaar later houden in een middelgrote stad als Maastricht bijna tachtig camera's het publiek in de gaten.

Strafrecht

Het gevolg van dit alles, vindt Koops, is dat de maatschappij steeds meer wordt ingericht ten behoeve van het strafrecht. Zo zijn telecomaanbieders nu verplicht langdurig klantgegevens op te slaan, langer dan hun bedrijfsvoering rechtvaardigt. Koops: "Daar lijkt niets op tegen, maar het is een fundamenteel andere rol van het strafrecht. Vroeger kwam het strafrecht pas om de hoek kijken als een strafbaar feit had plaatsgevonden. Het werd gezien als laatste redmiddel. Nu wordt het strafrecht in toenemende mate ingezet ter preventie van strafbare feiten met als gevolg dat iedere Nederlander een potentiële verdachte is."

Bovendien richten justitiële onderzoeken zich steeds vaker op personen op wie geen verdenking rust, maar die zich op enigerlei wijze in de buurt van de verdachte bevinden. Sinds januari 2006 staat het de officier van justitie vrij om allerlei gegevens op te vragen van personen met wie een verdachte toevallig contact heeft gehad. Er hoeft niet altijd een (dreiging van) een misdrijf te zijn om in allerlei bestanden te duiken. Met de aanvulling op de Wet op de Inlichtingen- en Veiligheidsdiensten die eind dit jaar wordt verwacht, kan de AIVD complete bedrijfsbestanden opvragen om die vervolgens met slimme software te doorzoeken op verdachte patronen, zoals bankoverschrijvingen naar de Al-Fourqaan moskee in Eindhoven.

Daarbij komt dat lagere politiefunctionarissen steeds meer verantwoordelijkheid krijgen. Voor het natrekken van telefoonnummers hoeft een politieman niet meer op fiat van een meerdere te wachten. Een officier van justitie mag nu zonder toestemming van een rechter-commissaris bevelen dat iemand langdurig wordt geobserveerd en dat opsporingsambtenaren identificerende gegevens opvragen. Soms kan een officier van justitie zelfs een inval bij iemand thuis gelasten en hiervoor pas achteraf toestemming vragen bij de rechter-commissaris.

Dat is nog niet alles. Allerlei persoonsgegevens, waar politie en veiligheidsdiensten vroeger veel

meer moeite voor moesten doen, zijn nu ruim beschikbaar. Alle overheidsdiensten moeten op bevel van een officier van justitie hun bestanden openstellen. Met de invoering van het burgerservicenummer (zie kader) is het een koud kunstje om deze bestanden, met zeer veel informatie over alle Nederlandse burgers, aan elkaar te koppelen.

Ook bedrijven vallen in toenemende mate onder dit regime. Met de uitbreiding van de vorderingsbevoegdheid van januari vorig jaar en de toevoeging op de Wet Inlichtingen- en Veiligheidsdiensten moeten bedrijven alle identificerende gegevens van hun klanten prijsgeven.

Opsporingsdiensten krijgen bovendien steeds meer zoekinstrumenten door nieuwe technologie. Alle telefoonnummers, adressen en binnenkort ook e-mailadressen en IP-nummers worden bijvoorbeeld iedere 24 uur ververst in het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Hier hebben alle opsporingsambtenaren toegang toe. Zo kan de politie precies achterhalen wie een bepaalde e-mail heeft gestuurd of bericht op een internetforum heeft geplaatst. Kortom, gesprekken en discussies die vroeger niet door derden werden gehoord of gezien, liggen nu vast in databanken voor zolang de wetgever dat wenst.

Afvalligen

Voor 'gevoelige informatie' over politieke, religieuze en seksuele voorkeur, is nog steeds een bevel van de rechter-commissaris nodig. Maar in praktijk is de scheiding tussen gewone en gevoelige informatie vaag. Een officier van justitie kan bijvoorbeeld een bibliotheek sommeren om alle leners op te geven van boeken van Sayyid Qutb, de islamitische prediker die vindt dat alle ongelovigen en afvalligen moeten worden gedood.

De betere informatievoorziening van politie, justitie en veiligheidsdiensten leidt er niet toe dat er minder fouten worden gemaakt. Integendeel, zegt Annelies Röttgering, voorzitter van de Nederlandse Vereniging van Strafrechtadvocaten (NVSA). "Zo zien we keer op keer dat de politie meeluistert in gesprekken tussen advocaten en cliënten. Afluisteren is uitdrukkelijk verboden, maar de rechter treedt er in de praktijk nauwelijks tegen op. Het gebeurt geregeld dat een cliënt voor de deur van de advocaat wordt aangehouden, terwijl die voor een afspraak kwam.

"

Justitieel onderzoek wordt soms begonnen op basis van zachte informatie, afkomstig van kliklijnen, de Criminele Inlichtingen Eenheid (CIE) of de AIVD. Waartoe dit kan leiden, bleek in 2004, toen een arrestatieteam van het korps Amsterdam-Amstelland een huis binnenviel. De Bank of Scotland vermoedde dat iemand vanuit Nederland zijn systemen probeerde te kraken en stuurde twee e-mails met het IP-adres van de vermoedelijke dader naar internetprovider UPC. Die schakelde de politie in, die dezelfde avond nog een inval deed om de boosdoener te betrappen. De e-mails bleken echter twee verschillende IP-nummers te bevatten, waarvan één onjuist was zodat het arrestatieteam de verkeerde woning binnenviel.

Op dit soort fouten moeten Nederlanders vaker rekenen, zegt Röttgering. "Bepaalde groepen worden waarschijnlijk meer getroffen dan andere. Als je een blanke man bent van middelbare leeftijd, heb je minder te vrezen dan wanneer je van Marokkaanse of Turkse komaf bent."

CBP-voorzitter Kohnstamm begrijpt dat in de strijd tegen terreur en zware criminaliteit offers nodig zijn. "We beseffen ook wel dat je soms iets van de privacy moet inleveren om bepaald gevaar te bedwingen." Wat hem stoort is dat de verhoudingen vaak uit het oog worden verloren. "De laatste jaren gebruikt het kabinet meteen grof geschut als het gaat om anti-terreurmaatregelen. Het laat na om te bewijzen dat alle andere middelen zijn uitgeput. Ook gaat het niet na of de nieuwe harde maatregelen wel het gewenste effect sorteren."

Kohnstamm vreest bovendien dat de wetgeving steeds wordt uitgebreid en dat als de kans op terrorisme kleiner wordt de beperkingen van de privacy niet verdwijnen. "De vraag is: wie bepaalt de norm van wat extremistisch of onwenselijk gedrag is? Wie bepaalt welke middelen proportioneel zijn tegen welke vormen van criminaliteit?"

Dat een nette burger niets te verbergen heeft, noemt Kohnstamm "gevaarlijke onzin". "Het zou goed kunnen dat je nooit iets van de afbraak van privacy merkt. Maar het is ook mogelijk dat je toevallig en geheel buiten je schuld in beeld komt bij een onderzoek. En stel dat er dan ook nog fouten worden gemaakt. Geloof me, je leven ligt dan helemaal overhoop. We hebben de checks

and balances niet voor niets. Als je de wettelijke beschermingen van onze vrijheid afbreekt, zet je de deur open naar willekeur."

NRC Handelsblad
Mei 14, 2007

De bespiede mens

De privacywet is niet meer goed te handhaven door de snelle technische ontwikkelingen en het gebrekkige normbesef bij overheden en bedrijven. Deze conclusie is van de voorzitter van het College Bescherming Persoonsgegevens (CBP), Jacob Kohnstamm, en dient te worden begrepen als een alarmkreet die een politiek antwoord behoeft.

Voorlopig vraagt het CBP om de bevoegdheid strengere sancties op te mogen leggen. Maar vooral moet er een debat komen over de razendsnelle veranderingen voor de burger die het gevolg zijn van de opslag, bewerking en het gebruik van persoonsgegevens op steeds meer plaatsen. Het trefwoord daarbij is 'controlestaat', een term die is ontleend aan een recent wetenschappelijk rapport van het Rathenau Instituut. Dat rapport wordt veel geciteerd, maar heeft nog weinig praktische gevolgen gehad.

Ook de strekking van het recente jaarverslag van het CBP doet de haren te berge rijzen. Er rijst een beeld op van de constant bespiede mens, wiens communicatie en verplaatsingen steeds worden bijgehouden en opgeslagen, of het nu om treinvervoer, gsm-gebruik, e-mailverkeer of internetbezoek gaat. Het autokenteken fungeert als visitekaartje dat binnen de overheid van politie naar fiscus naar Rijkswaterstaat naar sociale dienst wordt doorgeseind. De burger is veranderd in een gsm-peilzender, een wandelende OV-chip, een digitaal opgeslagen camerabeeld, wiens persoonlijke levenssfeer ondergeschikt is aan het toevallige doel van de databank. Deels door eigen toedoen, maar merendeels ongevraagd.

Recent voorbeeld was een 'experiment' van het politiekorps Zuid-Holland-Zuid die van de plaatselijke 'hangjeugd' digitale foto's maakte en die opsloeg in een eigen databank. Het past precies in de trends die het Rathenau Instituut signaleerde: een steeds verder oprukken van politieonderzoek in de privésfeer van niet verdachte burgers. De politie maakt daarbij steeds vaker gebruik van databanken bij bedrijven of overheidsdiensten en dwingt dat ook vaker af.

De roep om strengere sancties voor het CBP is begrijpelijk - de toezichthouder komt geloofwaardigheid en gezag tekort. Maar het is ook de omgekeerde weg. Eerst dienen Kamer en kabinet zich te bezinnen op deze ontwikkelingen die breed worden gesignaleerd. De invoering van het biometrische paspoort met bijbehorende centrale databank, het burgerservicenummer en de OV-chipkaart zijn goede aanleidingen. Straks (of nu al?) leeft de burger in een glazen huis en is het strafrecht van uiterst redmiddel in preventief controle-instrument veranderd.

Velen laat de bescherming van de persoonlijke levenssfeer intussen koud als zij 'de veiligheid' ten goede komt. De 'verdachte' is immers altijd de ander. Terwijl er veelal een nogal ruim bemeten vertrouwen bestaat in de goede bedoelingen van de overheid. Privacy is inderdaad geen absolute waarde en ook geen grotere dan individueel welzijn, zelfbeschikking of gezondheid. Tegelijk is het recht om je ongestoord terug te trekken in de eigen levenssfeer wel essentieel voor veel andere burgerrechten. Zorgelijk is vooral de opbloei van al die databestanden met persoonlijke informatie die als paddestoelen in de herfst met onzichtbare draden met elkaar verbonden zijn.