



Fraude



Andere landen doen het beter
de casestudies

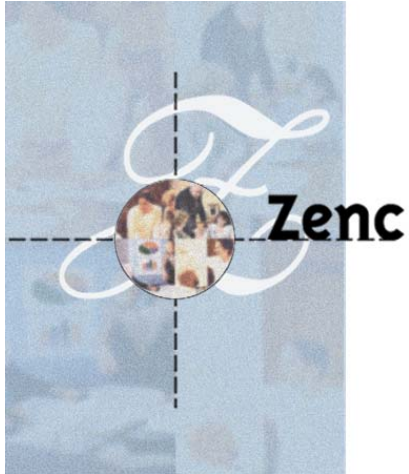
Noor Huijboom en Marco Meesters



Terrorisme



Voedselveiligheid



Definitief

Andere landen doen het beter

Drie vergelijkende casestudies

© Zenc, februari 2003

Auteurs:
drs N.M. Huijboom
M. Meesters
drs R. Titulaer

Inhoudsopgave

1. Inleiding.....	2
1.1. Achtergrond	2
1.2. Probleemstelling	2
1.3. Methoden van onderzoek	3
1.4. Leeswijzer.....	3
2. Sociale zekerheid.....	4
2.1. DIMONA-aangifte	4
2.1.1. Achtergrond	4
2.1.2. Werkwijze.....	5
2.1.3. Verbeteringen	7
2.1.4. Barrières	8
2.2. De Nederlandse Sociale Zekerheid.....	8
2.2.1. Situatieschets.....	8
2.2.2. Wat kan Nederland leren van België?	10
2.2.3. Vernieuwingsagenda	12
3. Terrorismebestrijding	13
3.1. Data matching in de Verenigde Staten.....	13
3.1.1. Achtergrond	13
3.1.2. Fundamentele veranderingen	14
3.1.3. Werkwijze.....	15
3.1.4. Verbeteringen	17
3.1.5. Barrières	17
3.2. Informatie-uitwisseling in de Nederlandse veiligheidssector	17
3.2.1. Situatieschets.....	17
3.2.2. Wat kan Nederland leren van de Verenigde Staten?.....	19
3.2.3. Vernieuwingsagenda	20
4. Voedselveiligheid	22
4.1. Duitse elektronische database en dierpas.....	22
4.1.1. Achtergrond	22
4.1.2. Werkwijze.....	23
4.1.3. Verbeteringen	25
4.1.4. Barrières	25
4.2. De Nederlandse runderadministratie.....	26
4.2.1. Situatieschets.....	26
4.2.2. Wat kan Nederland leren van Duitsland?	28
4.2.3. Vernieuwingsagenda	28
5. Conclusie	30

1. Inleiding

1.1. Achtergrond

Uit onderzoek blijkt dat de Nederlandse overheid op een aantal punten verbeteringen kan doorvoeren met behulp van informatievoorziening en daarbij kan leren van initiatieven in andere landen¹. Er zijn goede voorbeelden te vinden van situaties waarin overheden (van andere landen) met behulp van een adequate informatievoorziening beter in staat zijn om maatschappelijke problemen aan te pakken. Deze voorbeelden kunnen interessant zijn voor de Nederlandse situatie.

Tijdens het exploratieve onderzoek 'Andere landen doen het beter' zijn drie casestudies uitgevoerd naar landen die door een goede informatievoorziening in een bepaalde sector beter presteren dan de Nederlandse overheid. De drie onderzochte cases zijn:

- sociale zekerheidssector in België
- terrorismebestrijding in de Verenigde Staten
- voedselveiligheid in Duitsland

De bevindingen van het onderzoek hebben hun neerslag gevonden in deze rapportage.

1.2. Probleemstelling

De probleemstelling van het verkennende onderzoek naar de drie buitenlandse cases is als volgt:

Welke maatschappelijke en bestuurlijke verbeteringen (bijvoorbeeld op het gebied van efficiëntie en effectiviteit) zijn behaald met toepassing van informatievoorziening² en wat zijn de lessen die hieruit te halen zijn voor Nederland?

Om bovenstaande probleemstelling te kunnen beantwoorden, zijn de volgende deelvragen verkend:

1. Wat is de context van de onderzochte cases (wat zijn bijvoorbeeld politieke issues)?
2. Welke oplossingen hebben de bestudeerde landen gevonden voor problemen en wat is de rol van informatievoorziening in de oplossingen?
3. Op welke barrières is men gestuit men bij de realisatie van de oplossingen?
4. Tot welke maatschappelijke en bestuurlijke verbeteringen hebben de oplossingen geleid?
5. Wat zijn verschillen en overeenkomsten met de situatie in Nederland en hoe worden de verschillen verklaard?
6. Wat kan Nederland leren van de buitenlandse cases?
7. Wat zijn de stappen die Nederland zou moeten nemen en wat zijn de kosten en de baten daarvan?

¹ Zie onder andere: Ministerie van Economische Zaken, ICT-toets 2002.

² Onder componenten van informatievoorziening verstaan we: authentieke registraties, unieke nummers, uitwisselingsprotocollen (XML, EDI), digitale handtekening, verwijzindexen, standaard datadefinities en beheerorganisaties.

1.3. Methoden van onderzoek

De gegevensverzameling van dit onderzoek heeft plaatsgevonden middels deskresearch (literatuurstudie) en Internetresearch. Op grond van de bevindingen uit het desk- en Internetresearch zijn interviews gehouden met Nederlandse experts op de verschillende gebieden (sociale zekerheid, terrorisme en voedselveiligheid). Verschillende buitenlandse experts hebben via e-mail en telefonisch vragen beantwoord. De resultaten van het deskresearch, de interviews en de antwoorden op telefonische vragen en vragen via e-mail zijn geanalyseerd en verwerkt in deze rapportage.

1.4. Leeswijzer

In hoofdstuk 2 zal ingegaan worden op de verbeteringen die in de Belgische sociale zekerheid zijn behaald met de invoering van de DIMONA-aangifte en zal gezien worden welke lessen Nederland hieruit kan leren. Hoofdstuk 3 zal inzicht geven in de successen die met behulp van informatievoorziening zijn behaald bij de bestrijding van terrorisme in de Verenigde Staten. Aangegeven wordt wat Nederland hiervan kan leren. De verbeteringen in de Duitse voedselketen door gebruikmaking van een centrale elektronische runderadministratie en de dierpas zullen in hoofdstuk 4 worden besproken. Naar aanleiding van de Duitse case zal ook hier ingegaan worden op de mogelijkheden die hieruit voortvloeien voor de Nederlandse situatie.

2. Sociale zekerheid

In de Nederlandse sociale zekerheid is fraude een belangrijk probleem. Deze fraude kan verschillende vormen aannemen; van het illegaal tewerkstellen van werknemers ('zwart werk') tot het ten onrechte verkrijgen van uitkeringen. Aan het begin van de kabinetsperiode van het tweede kabinet Kok (1998-2002) is een intensiveringsprogramma voor de bestrijding van dit soort fraude opgestart. Dit programma had als doel een forse extra impuls te geven aan de bestrijding van fraude, onder andere in de sociale zekerheid³.

In de notitie 'Bestrijding fraude en financieel-economische criminaliteit 2002-2006' worden de maatregelen van het intensiveringprogramma geëvalueerd. Een belangrijke conclusie uit deze evaluatie is dat fraudebestrijding meer oplevert dan dat het kost⁴. Een andere, minstens net zo belangrijke conclusie is dat de fraudebestrijding verbetert, maar nog veel beter kan en moet. Zo kan op het gebied van de bestrijding van zwart werk nog veel winst geboekt worden. De handhaving van werkgeversverplichtingen met betrekking tot werknemersadministratie en tewerkstellingsvergunningen blijkt hier een probleem.

In dit kader is het interessant om te zien hoe andere landen omgaan met soortgelijke vraagstukken. In België heeft men op 1 januari 2003 de onmiddellijke aangifte van tewerkstelling ingevoerd, waarbij indienst- en uitdiensttreders direct door werkgevers worden aangegeven. Door de invoering van de onmiddellijke aangifte wordt zwart werk bemoeilijkt en wordt tevens een grote besparing op administratieve lasten gemaakt. In dit hoofdstuk zal de Belgische case beschreven worden (paragraaf 2.1), alsmede de lessen die Nederland hieruit kan halen (paragraaf 2.2).

2.1. DIMONA-aangifte

In de Belgische sociale zekerheid maakt men gebruik van het systeem van de DIMONA-aangifte (**D**éclaration **IM**médiate - **ON**middellijke **A**angifte)⁵, oftewel de onmiddellijke aangifte van nieuwe werknemers en uitdiensttreders. Het systeem is in 1999 ingevoerd in de bouw, uitzend- en transportsector en sinds 1 januari 2003 is het systeem van toepassing op alle sectoren in België.

2.1.1. Achtergrond

Halverwege de jaren '80 worstelde de Belgische sociale zekerheid met organisatorische en informatiekundige vraagstukken. De coördinatie tussen de meer dan 2000 instanties van de sociale zekerheid liet, procesmatig en informatietechnisch gezien, te wensen over. De gebrekkige coördinatie leidde tot een aantal problemen, waaronder⁶:

- Efficiëntie- en tijdverlies bij instellingen. Processen van de afzonderlijke instanties overlaptten elkaar.

³ Notitie 'bestrijding fraude en financieel-economische criminaliteit 2002-2006', Directoraat-Generaal Rechtshandhaving,

⁴ Zie ook: 'Financiële verantwoording SZW (1999, 2000, 2001)'.

⁵ https://www.socialsecurity.be/site_nl/Applics/dimona/infos_home.htm.

⁶ Presentatie Peter Maes, 5-9-2001.

- Overbelasting van informanten. Aan cliënten werd door verschillende instanties meerdere malen gevraagd dezelfde informatie op te geven.
- Verhoogde kans op fraude. Doordat de verplichting van aanmelding niet duidelijk genoeg werd gesteld en de termijn waarop aanmelding kon plaatsvinden ruim was, was het voor werkgevers relatief makkelijk om te frauderen.
- Suboptimale ondersteuning van sociaal beleid. Doordat gegevens niet up-to-date waren en de juistheid van gegevens niet goed gecontroleerd kon worden, was het moeilijk om beleid op deze gegevens te baseren.

Op het hoogste politieke niveau werd voor een stelselherziening gekozen⁷. Het kabinet van de minister-president stelde een administrateur-generaal, de heer F. Robben, aan en gaf hem financieel en politiek mandaat om de organisatie- en informatieprocessen binnen de sociale zekerheid te stroomlijnen. Gekozen werd om een sectorbreed elektronisch netwerk te ontwikkelen voor gegevensuitwisseling: de Kruispuntbank. De Kruispuntbank is een verwijzingsbank voor informatie-uitwisseling tussen verschillende instanties van de sociale zekerheid. De Kruispuntbank slaat zelf geen gegevens op, maar bevat verwijzingen naar lokale databases van instanties. Opslag en beheer van gegevens blijft decentraal (bij de lokale instanties) plaatsvinden. De Kruispuntbank weet van elke persoon welke instantie een dossier over de betreffende persoon heeft, welke gegevens bij deze instantie bekend zijn en wie toegang heeft tot welke gegevens. Er is een Toezichtcomité ingesteld dat toezicht houdt op de gegevensverstrekking. Alle instanties in de sociale zekerheid, ruim 2000 in België, zijn op het netwerk aangesloten.

Ten tijde van de ontwikkeling van de Kruispuntbank waren er in België problemen met betrekking tot zwart werk. In de bouw-, uitzend- en transportsector hadden legale bedrijven, die geen zwart werkers in dienst hadden, last van oneerlijke concurrentie van bedrijven die het met de regels niet zo nauw namen. De problemen werden zo groot ervaren dat er binnen deze sectoren bij werkgeversorganisaties initiatieven ontstonden om de problemen op te lossen. In de sectoren werd, los van elkaar, gewerkt aan een oplossing met een pas voor 'legale' werknemers. Bij de Kruispuntbank was men op dat moment net bezig met het ontwikkelen van toepassingen van het netwerk voor klanten van de sociale zekerheid, zoals de werkgevers. Toen men bij de Kruispuntbank hoorde van de oplossingen die de werkgeversorganisaties in genoemde sectoren aan het ontwikkelen waren, heeft men besloten in samenwerking met de sectoren de DIMONA-aangifte te ontwikkelen. Zo was een breed draagvlak voor de DIMONA-aangifte verzekerd onder werkgevers die zich wel aan de regels hielden.

2.1.2. Werkwijze

Het DIMONA-systeem is een systeem waardoor werkgevers het in en uit diensttreden van werknemers direct kunnen en moeten melden. Als een werkgever een nieuwe werknemer in dienst neemt, is hij verplicht dit uiterlijk op het moment van in diensttreden van de werknemer te melden bij de Rijksdienst voor de Sociale Zekerheid (RSZ). Als een werknemer vertrekt, is de werkgever verplicht dit uiterlijk de dag na het vertrek door te geven. De aangifte geschiedt op een elektronische manier; papieren formulieren zijn niet beschikbaar. Er zijn drie methoden van aangifte doen:

⁷ Rob, 'Preadvies Dienstverlening centraal, de uitdaging van ICT voor de publieke dienstverlening', 2000.

- Vocale server. Hier kan de werkgever de aangifte telefonisch doen. Hij wordt dan verbonden met een computer van de RSZ, waarna hij door cijfers in te toetsen de aangifte kan doen.
- Internetapplicatie. In België is er een portaal voor de sociale zekerheid. Hierop staan alle gegevens en alle mogelijke aangiften inzake de sociale zekerheid. Op dit portaal staat ook een applicatie waarmee de werkgever door het invoeren van een aantal gegevens de aangifte kan doen.
- Gestructureerde berichten. Dit is een systeem voor werkgevers die veel aangiften moeten doen (enkele tientallen per week). Dit systeem maakt gebruik van bestandsoverdracht, wat inhoudt dat de werkgever een bestand aanmaakt met aangiften dat automatisch wordt doorgegeven aan de RSZ (een gestructureerd bericht, gestructureerd volgens standaarden gemaakt door de RSZ).

Als de aangifte is gedaan, ontvangt de werkgever een elektronisch bericht van de aangifte. De werkgever kan de status van zijn aangifte aan de hand van het nummer uit dit bericht controleren. De aangifte zal binnen 10 werkdagen worden verwerkt door de sociale zekerheid. Hierna ontvangt de werkgever een bericht met daarin een DIMONA-nummer van de aangifte, alsmede de opgegeven gegevens, waardoor de werkgever kan controleren of de aangifte goed verwerkt is. Dit bericht geldt tevens als wettelijk bewijsmateriaal dat de werkgever de aangifte correct heeft uitgevoerd.

Een belangrijk onderdeel van de aanmelding is de identificatie van de werkgever en de werknemer. De identificatie van de werkgever gebeurt door middel van het inschrijvingsnummer van de werkgever bij de RSZ. De identificatie van de werknemer gebeurt met behulp van het zogenaamde Identificatie Nummer Sociale Zekerheid (INSZ). In 1998 heeft elke Belg een INSZ gekregen; een uniek persoonsnummer voor de sociale zekerheid. Dit nummer wordt door alle instanties van de sociale zekerheid gebruikt. Het nummer staat op de SIS-Kaart (SIS staat voor: Sociaal Informatie Systeem), die iedere Belg gratis heeft ontvangen. De SIS-kaart kan, met behulp van het unieke nummer, toegang geven tot gegevens over de kaarthouder in het netwerk van de Kruispuntbank. De kaart vormt zo de basis voor vermindering van administratieve formaliteiten voor sociaal verzekerden en werkgevers⁸. Het unieke nummer en de SIS-kaart zorgen ervoor dat de identificatie van de werkgever en werknemer goed verloopt.

Als een werknemer geen INSZ heeft, zal hij deze bij de DIMONA-aangifte toegewezen krijgen. De gegevens die de werkgever opgeeft worden automatisch gecontroleerd door een koppeling met het Rijksregister (de Belgische GBA). In de systemen rond de aangifte is ook rekening gehouden met de invoering van een uniek ondernemingsnummer. Dit nummer zal medio 2003 worden ingevoerd, en zal de identificatie van de onderneming nog eenduidiger maken.

Bij de aansluiting van de organisaties op het DIMONA-systeem moesten de werkgevers de werknemers opgeven die zij op dat moment in dienst hadden. Hierdoor is een elektronisch personeelsregister ontstaan dat door verschillende instanties en werkgevers wordt gebruikt.

⁸ Presentatie Peter Maes, 5-9-2001.

2.1.3. Verbeteringen

Verbeterde informatie-uitwisseling

De DIMONA-aangifte draagt bij aan het bestrijden van fraude door ondernemingen en personen. De gegevens die gegenereerd worden door de aangiftes worden doorgestuurd naar de datawarehouse OASIS. Hier worden de gegevens gecombineerd en vergeleken met gegevens uit enkele andere databanken, zoals bijvoorbeeld het werkgeversrepertorium en de LATG (Loon- en Arbeidstijds Gegevens). Het doel van de datawarehouse is om fraudescenario's te detecteren en analyseren. In principe wordt gebruik gemaakt van geanonimiseerde gegevensuitwisseling. Als er een ernstig vermoeden van fraude bestaat tegen een bepaalde werkgever kan de sociale inspectie echter wel toegang krijgen tot de persoonsgegevens. Zo ontstaat een krachtig middel voor de sociale inspectie om fraude op te sporen.

Efficiëntie en effectiviteit

De effectiviteit van inspecties van de sociale dienst is door de invoering van de DIMONA-aangifte sterk verbeterd. Voor de invoering van het systeem hadden werkgevers een bepaalde periode de tijd om een nieuwe werknemer aan te geven bij de sociale zekerheid. Op het moment dat de inspecteur van de sociale dienst langs kwam, kon de werkgever dus altijd beweren dat hij de werknemers die de inspecteurs niet op hun lijst hadden staan, nog moest aangeven. Met de invoering van de DIMONA-aangifte is deze mogelijkheid voor de werkgever verdwenen, aangezien alle werknemers op de dag dat ze beginnen, opgegeven moeten zijn. Inspecteurs van de sociale zekerheid hebben een laptop met mobiele telefoon bij zich, waardoor ze op de werkplaats het personeelsbestand van de werkgever uit de database van de RSZ kunnen raadplegen. Hierdoor kunnen ze direct zien welke werknemers wel en welke niet in het bedrijf horen te zijn. Het resultaat is dat de inspecteurs hun werk effectiever en efficiënter kunnen uitvoeren en fraude door werkgevers makkelijker aan te pakken is. De effectievere en efficiëntere bestrijding van fraude leidt tot grote opbrengsten. Geschat wordt dat door het DIMONA-systeem elk jaar circa 2 miljard euro aan extra opbrengsten worden opgehaald in de sociale zekerheid. De extra opbrengsten in de sociale zekerheid zijn een belangrijke factor in het begrotingsoverschot van de Belgische overheid⁹.

Vermindering van de administratieve lasten van de werkgever.

Door de invoer van de werknemersgegevens door de werkgevers bij de DIMONA-aangifte ontstaat er een elektronisch personeelsregister, waarvan niet alleen de instanties van de sociale zekerheid, maar ook de werkgevers gebruik kunnen maken. Aan de kant van de werkgever verdwijnt een aantal administratieve lasten:

- 4 verschillende sociale documenten vervallen of worden sterk vereenvoudigd;
 - het verplichte papieren personeelsregister vervalt; dit wordt elektronisch bijgehouden en beheerd door de RSZ.
 - het personeelsregister dat werkgevers die personeel op meer dan één vaste plaats tewerkstellen moeten bijhouden, wordt sterk vereenvoudigd.
 - Werkgevers hoeven geen individueel document van iedere werknemer meer af te leveren.
 - Als een werkgever een student aanneemt, hoeft hij geen kopie van het contract meer op te sturen.
- Doordat de werkgever online toegang heeft tot zijn personeelsregister bij de sociale zekerheid, kan deze zijn werknemers tijd- en plaatsonafhankelijk identificeren. Dit

⁹ 'Weer overschot op de Belgische begroting', Volkskrant 7-1-03.

vergemakkelijkt enerzijds de communicatie tussen werkgever en sociale zekerheid en anderzijds de communicatie tussen werknemer en sociale zekerheid.

- De werkgever kan het personeelsregister dat opgebouwd wordt bij de sociale zekerheid gebruiken voor eigen registraties.

Bovenstaande besparingen leiden tot een sterke administratieve vereenvoudiging. Zo zijn 50 formulieren, die voorheen door werkgevers moesten worden ingevuld, verdwenen. Op jaarbasis betekent dit dat de RSZ 1.112.085 formulieren minder hoeft te verwerken. Op 27 formulieren is daarnaast tweederde van de rubrieken verdwenen. Deze formulieren worden 4,6 miljoen keer per jaar gebruikt. De DIMONA-aangifte maakt het mogelijk dat twee andere aangiftes (de driemaandelijke aangifte en de aangifte van sociale risico's) makkelijker kunnen verlopen:

- Bij de kwartaalaangifte (voor de betaling van sociale premies e.d.) via Internet kan de werkgever gebruik maken van zijn elektronische personeelsregister.
- Als de werkgever in een kwartaal geen werknemer in dienst heeft, hoeft hij geen nihil-aangifte te doen.
- De aangifte van sociaal risico kan via Internet worden gedaan.

2.1.4. Barrières

Het proces van vernieuwing in organisaties wordt veelal vertraagd of belemmerd, doordat mensen van de organisaties niet mee willen of kunnen gaan in de verandering. Er ontstaat dan weerstand wat er toe kan leiden dat de vernieuwing niet of niet geheel tot stand komt. In het geval van de DIMONA-aangifte heeft zich deze situatie niet voorgedaan. De problemen met zwart werk in de sectoren waar het als eerst is ingevoerd (de bouw-, uitzend- en transportsector) waren zo groot dat werkgevers blij waren dat hier een oplossing voor kwam. Nu het systeem in deze sectoren duidelijk positieve resultaten laat zien, is het draagvlak in andere sectoren voor invoering van het systeem groot. Ook heeft het feit dat de Kruispuntbank de werkgevers in een vroeg stadium heeft betrokken bij de ontwikkeling van het systeem geleid tot een groter draagvlak bij de werkgevers voor de DIMONA-aangifte.

Om een verandering adequaat uit te kunnen voeren, moet er ook politiek draagvlak zijn. Toen de Kruispuntbank in 1996 besloot dat het tijd was om het netwerk te gebruiken om meer interactie met werkgevers te bewerkstelligen, is er een werkgroep 'modernisering van de sociale zekerheid' opgericht. In deze werkgroep zaten vertegenwoordigers van de premier, de vice-premier, de sociale ministeries en van de instanties van de sociale zekerheid. Zo was de politieke top sterk betrokken bij de invoering van de DIMONA-aangifte. Een ander belangrijk voordeel waar de Belgen gebruik van hebben gemaakt, was het besluit van de Europese Unie in 1996 dat het mogelijk maakte om de wijzigingen in de sociale wetgeving bij Koninklijk Besluit door te voeren. Hierdoor hoefden alleen de hoofdlijnen door het parlement goedgekeurd te worden en hoefde men niet voor allerlei uitvoeringsaspecten het parlement te raadplegen. De implementatie van het systeem kon daardoor veel sneller gebeuren dan anders het geval was geweest.

2.2. De Nederlandse Sociale Zekerheid

2.2.1. Situatieschets

Uit verschillende onderzoeken en rapportages blijkt dat in Nederland veelvuldig werkgeversfraude plaatsvindt bij de tewerkstelling van personeel in de zin van zwart

werken¹⁰. In verschillende bedrijfssectoren, met name land- en tuinbouw, horeca en bouw, wordt al jarenlang stelselmatig verzuimd in de afdracht van premies en belastingen¹¹. In het onderzoek van de Europese Unie van 2000 naar zwart werk in de lidstaten wordt het zwart werk in Nederland op 10 tot 20% van het bruto nationaal product geschat¹². Geconstateerd kan worden dat zwart werken in Nederland al geruime tijd een aanzienlijk probleem vormt.

In Nederland moeten werkgevers bij de indiensttreding van nieuwe werknemers deze aanmelden bij het UWV, bij een arbo-dienst en (indien van toepassing) bij een ziekenfonds. Daarnaast zal de werknemer een loonbelastingverklaring in moeten vullen. Identificatie kan plaatsvinden op het moment van indiensttreding, doordat de werkgever de identiteit van de nieuwe werknemer vaststelt middels een geldig legitimatiebewijs. Controle kan plaatsvinden doordat een werkgever verplicht is om een kopie van een geldig legitimatiebewijs van de werknemer bij de loonadministratie te bewaren. Gemiddeld komt eens in de 7 jaar een controleur langs bij een onderneming voor een standaardcontrole. Deze controle richt zich op de loonadministratie en niet op de aanwezigheid van zwart werkers. Controle op zwart werk gebeurt wanneer er aanwijzingen zijn dat er binnen een bedrijf sprake is van fraude. Bij zwarte fraude bestaat een lage pakkans¹³. Uit het periodiek onderzoek regelovertreding sociale zekerheid blijkt dat de regels door werkgevers worden overtreden, omdat ze geen fysieke repressiedruk ervaren¹⁴. De kans is groter dat er een inspecteur van de Arbeidsinspectie, Belastingdienst of UWV bij een bedrijf over de vloer komt dan een inspecteur van de sociale recherche.

In 1999 is er door het kabinet een programma gestart voor de bestrijding van fraude¹⁵. Dit programma had als doel het intensiveren van de bestrijding van fraude door middel van slimmer handhaven, breder handhaven en meer handhaven. Uit evaluatie van dit programma in 2002 blijkt dat de fraudebestrijding verbetert, maar dat er nog verbetering mogelijk is¹⁶. Zo blijkt dat de werkgeversverplichtingen omtrent werknemersadministratie en tewerkstellingsvergunningen moeilijk te handhaven zijn. De werkgever heeft nu 6 weken de tijd om een nieuwe werknemer aan te melden. Indien de inspecteur van de sociale dienst komt controleren, kan de werkgever altijd volhouden dat een werknemer die niet op de lijst van de inspecteur staat, pas net is begonnen en dus nog aangemeld moet worden.

In het handhavingprogramma 2003-2006 (november 2002) zijn de volgende concrete acties genoemd om zwart werk tegen te gaan:

- Uitbreiding van het bestuurlijke boete-instrumentarium. Om een beter lik-op-stuk-beleid te voeren kan een groot deel van de overtredingen van de Wav (illegale

¹⁰ Zie bijvoorbeeld: 'Jaarverslag 2001 Westlands Interventie Team'.

¹¹ Zie ook: http://home.szw.nl/actueel/dsp_publicatiesindex.cfm?set_id=122.

¹² Europese Commissie, Ontwerpverslag over de mededeling van de commissie betreffende zwart werk, 2000.

¹³ Ministerie van Sociale Zaken en Werkgelegenheid, 'Het opsporingsbeleidsplan van het Ministerie van Sociale Zaken en Werkgelegenheid voor 2002, 2002.

¹⁴ Ministerie van Sociale Zaken en Werkgelegenheid, 'Randomized response-onderzoek, periodiek onderzoek regelovertreding sociale zekerheid', 2001.

¹⁵ Notitie 'bestrijding fraude en financieel-economische criminaliteit 2002-2006', Directoraat-Generaal Rechtshandhaving.

¹⁶ zie Notitie 'bestrijding fraude en financieel-economische criminaliteit 2002-2006', Directoraat-Generaal Rechtshandhaving.

tewerkstelling) met hoge boeten bestuurlijk afgedaan worden. Hiervoor wordt een wetswijziging voorbereid. Toepassingen van de bestuurlijke boete moet in het jaar 2004 leiden tot 400 opgelegde boeten; in 2005 moeten dat 800 boeten zijn.

- Aanpak identiteitsfraude. Verbetering van de samenwerking en het delen van informatie over reis- en brondocumenten bij CWI, UWV, SVB en de Belastingdienst. Samenwerking met politie en justitie in de melding en afhandeling van valse en vervalste identiteitspapieren. Extra aandacht van de Belastingdienst en UWV in voorlichting aan werkgevers over een goede verificatie van de identiteit van nieuwe werknemers en het voeren van een complete administratie door de werkgever.
- Er is afgelopen jaar een reeks van maatregelen door het ministerie van SZW en het ministerie van Financiën gezamenlijk opgesteld om het beheer (en de controle op juistheid) van het sofi-nummer bij verificatie van identiteit praktisch te verbeteren.
- In het kader van de handhaving is een start gemaakt met de uniformering van methoden van legitimatie en identificatie. Dit met als doel dat werkgevers en uitvoeringsinstellingen op termijn identiteitsdocumenten automatisch kunnen uitlezen, de geldigheid van het identiteitsbewijs met behulp van documentherkenning en een koppelingen naar controlebestanden kunnen controleren en foutloos de gegevens kunnen inlezen.
- Intensivering van de controle, opsporing en afdoening. Dichten van het verschil tussen de verschijning op de werkplek en de registratie van dienstverbanden. Afronden van het onderzoek naar de mogelijkheden van een eerstedagmelding. Start van een beperkte pilot van de eerstedagmelding onder enkele werkgevers op basis van vrijwilligheid door UWV en Belastingdienst.

Een belangrijk project in dit kader is de verbetering van de samenwerking tussen UWV en Belastingdienst¹⁷. Het doel is om door herinrichting van de processen te komen tot een verdere administratieve lastenverlichting voor werkgevers en besparing op uitvoeringskosten. Daartoe zal één loket worden gecreëerd voor de werkgever waar deze terecht kan voor de aangifte en afdracht van alle loongerelateerde heffingen. Dit loket zal bij de belastingdienst ondergebracht worden. Er zal een transactiepoort op het Internet komen, waar de werkgever zijn aangiftes kan doen. Daarnaast komt er de mogelijkheid om via een gestructureerd bestand de aangiftes te doen.

De samenwerking tussen UWV en de Belastingdienst zal ondersteund worden door authentieke registraties. De belangrijkste twee zijn de BBR (Basis Bedrijven Register) en de LRD (Landelijke Raadpleegbare Directory van de GBA). Deze registraties worden gebruikt voor de identificatiegegevens van bedrijven en personen. Tevens wordt er een polisadministratie bijgehouden. Dit is een authentieke registratie van alle nominatieve loon- en dienstverbandgegevens en uitkeringsverhoudingen, voor uitkeringen, premie- en loonheffing¹⁸. De UWV is verantwoordelijk voor deze registratie.

2.2.2. Wat kan Nederland leren van België?

In België is men er in geslaagd om de problemen rond zwart werken aanzienlijk te beperken en jaarlijks 2 miljard euro aan extra premies te innen. In Nederland tracht men sinds de jaren '90 om meer grip te krijgen op deze problematiek, maar tot structurele verbeteringen heeft dit voorsnog niet geleid. Nederland heeft te maken met een situatie waarin veelvuldig wordt gefraudeerd door werkgevers, de pakkans van

¹⁷ Rapport 'Samenwerking UWV en Belastingdienst', oktober 2002.

¹⁸ Rapport 'Samenwerking UWV en Belastingdienst', oktober 2002.

werkgeversfraude laag is en geen plannen zijn geformuleerd om deze problemen sectorbreed aan te pakken. Waarom heeft België wel verbeteringen gerealiseerd en Nederland nog niet en wat kan Nederland hiervan leren? Een aantal factoren heeft bijgedragen aan het succes van de Belgen.

Verankering op hoog politiek niveau en middelen

De crisis in de sector van de sociale zekerheid in België was zo groot dat op het hoogste politieke niveau werd gekozen voor stelselherziening. Het kabinet van de minister-president stelde een administrateur-generaal aan die de stelselherziening als primus inter pares leidde. De grote politieke prioriteit, het mandaat, voldoende middelen (financiering uit algemene middelen) en de directe lijnen met het kabinet leidden er in de Belgische situatie toe dat de administrateur-generaal op voortvarende en doelmatige wijze de stelselherziening kon doorvoeren.

Ketenprocessen als basis

De Belgen hebben de problematiek vanuit de sectorbrede processen benaderd. De processen vormden de basis van de inrichting van de informatiearchitectuur. Omdat ketenprocessen en beleid leidend waren en de informatietechnologie volgend, ontstond er een integrale aanpak waarbij ICT werd gezien als middel en niet als doel op zich.

Respecteren van de autonomie van de participerende instanties

In België is niet gestreefd naar centralisatie van gegevensopslag en het integreren van lokale instanties. De Kruispuntbank koppelt decentraal opgeslagen elektronische gegevens. Hierdoor blijven de gegevens dicht bij de bronnen en wordt de autonomie van de betrokken partijen - tot op zekere hoogte - gerespecteerd. Deze, voor betrokken partijen minder bedreigende opzet heeft veel strijd en weerstand voorkomen.

Authentieke registraties als fundament

De authentieke registraties vormen het fundament voor de technologische vernieuwingen (zoals de DIMONA-aangifte) die - doordat gebruik wordt gemaakt van authentieke registraties - vrij eenvoudig kunnen worden doorgevoerd. De Belgen maken gebruik van authentieke registraties, unieke nummering, chipcard en andere componenten die een optimale informatievoorziening mogelijk maken. De basisregistraties betreffen bedrijven, werknemers en Loon- en Arbeidstijdsgegevens (LATG) deze registraties tezamen vormen een relationele database, wat leidt tot voordelen in de zin dat:

- De administratieve lasten van de werkgever worden verlaagd, omdat de werkgever zijn nieuwe werknemer eenmalig kan aanmelden.
- Processen van de deelnemende instanties worden vereenvoudigd, doordat gezamenlijk gebruik kan worden gemaakt van één registratie.
- Gegevens worden hergebruikt en de juistheid van gegevens effectiever kan worden gecontroleerd (bestanden worden automatisch met andere bestanden vergeleken om de juistheid van de opgegeven gegevens te controleren).
- Diensten geïntegreerd en vraaggericht kunnen worden aangeboden. In België is werkelijk sprake van één-loket voor de sociale zekerheid.

Gebruik van nieuwe media

De mogelijkheid van online mutatie en raadpleging levert aan de kant van de werkgever lastenverlichting en aan de kant van de handhaving efficiëntievoordelen op. De werkgever hoeft minder papieren formulieren in te vullen. Zeker in het geval van een automatische mutatie (wanneer de werkgever in zijn eigen systeem een nieuwe medewerker ingeeft, wordt deze informatie automatisch aangepast in het centrale

werknemersbestand). De handhaver kan bij een inspectie ter plaatse online nagaan of er sprake is van een illegale situatie. Deze online dienstverlening is echter alleen mogelijk doordat de informatiearchitectuur eenduidig en adequaat is opgezet.

De vraag die uit het voorgaande voortvloeit, is: waarom hebben verbeteringen op deze schaalgrootte in Nederland nog niet plaatsgevonden en hoe zou Nederland kunnen komen tot deze verbeteringen? De belangrijkste oorzaak is gelegen in het feit dat de informatievoorziening van de sector als geheel vooralsnog te weinig aandacht krijgt. Er zijn en worden allerlei innovatieve deeloplossingen gerealiseerd, maar een herbezinning op de informatievoorziening van de totale sector is nog niet tot stand gekomen. Zolang er geen expliciete uitspraak van de minister van Sociale Zaken is dat hij wil komen tot een integrale verbetering van de informatievoorziening van de sociale zekerheid en zolang daar de benodigde middelen niet voor worden vrijgemaakt, zullen integrale oplossingen niet tot stand komen. Wanneer die uitspraak wel is gedaan kan een ambtelijk projectleider mandaat krijgen om sectorbreed vernieuwingen te gaan doorvoeren.

2.2.3. Vernieuwingsagenda

Verbeteringen in de sociale zekerheid in Nederland zouden plaats moeten vinden door de processen en de informatievoorziening binnen de sector te stroomlijnen. Door gebruik te maken van onder andere authentieke gegevens, uitwisselingsprotocollen, unieke persoonsnummers en adequate identificatiemechanieken, kan de gegevenshuishouding in de sociale zekerheid efficiënter worden ingericht. Hierdoor kan controle en handhaving effectiever plaatsvinden, maar kan ook lastenverlichting voor de klant worden bereikt. Wanneer er een stevig fundament is gerealiseerd in de vorm van een adequate informatiearchitectuur, zullen vernieuwingen, zoals een eerstedagmelding relatief eenvoudig kunnen worden ingevoerd.

Deze verbeteringen kunnen echter alleen worden bereikt wanneer op het hoogste politiek niveau wordt besloten tot het verbeteren van de sociale zekerheid door de processen en de informatievoorziening binnen de sector te stroomlijnen. De minister van Sociale Zaken en Werkgelegenheid zou daarbij expliciet verantwoordelijk moeten zijn voor vernieuwingen in de totale sector van de sociale zekerheid en zou daarop afgerekend moeten kunnen worden. Door de minister wordt dan een ambtelijk projectleider aangesteld die met voldoende middelen en op projectmatige wijze veranderingen kan doorvoeren. De ambtelijk projectleider krijgt vergaande eigen verantwoordelijkheid ziet zich gesteund door een interdepartementaal en interdisciplinair kernteam.

Hoewel een stroomlijning van de processen en informatievoorziening binnen de gehele sector noodzakelijk is, wordt momenteel gewerkt aan een aantal projecten om te komen tot verbeteringen op deelgebieden. Een voorbeeld hiervan is de samenwerking tussen UWV en de Belastingdienst en een experiment met een eerstedagmelding. Deze verbeteringen zouden doorgang moeten vinden, maar zouden tevens moeten worden gezien in het licht van een bredere stroomlijning van de sectorale processen en informatievoorziening. In een vervolgonderzoek zou de toepasselijkheid van de DIMONA-aangifte in de Nederlandse situatie verder kunnen worden uitgewerkt.

3. Terrorismebestrijding

De terroristische aanslagen van 11 september 2001 hebben niet alleen in de Verenigde Staten sterk de aandacht gevestigd op de bestrijding van terrorisme. Ook in Nederland kwam de bestrijding van terrorisme hoog op de politieke agenda. Er rezen twee vragen. Allereerst moest worden onderzocht of er in Nederland personen of organisaties waren die connecties hadden met de terroristen van de aanslag. Daarnaast moest worden voorkomen dat dergelijke aanslagen in Nederland en Europa zouden plaatsvinden. Op deze vraagstukken kan alleen goed worden ingespeeld wanneer de informatievoorziening omtrent het veiligheidsvraagstuk goed geregeld is. Uit verschillende onderzoeken blijkt dat deze informatievoorziening in Nederland beter kan¹⁹.

De aanslag van 11 september heeft in de Verenigde Staten vanzelfsprekend geleid tot een enorme topprioriteit voor het bestrijden van terrorisme. Een van de belangrijkste conclusies die naar aanleiding van de aanslag werd getrokken, was dat de gegevensuitwisseling tussen veiligheidsinstanties aanzienlijk verbeterd moest worden, wil men terroristische aanslagen op effectieve manier kunnen bestrijden. In de Verenigde Staten zijn allerlei stappen genomen om de informatiehuishouding in de veiligheidssector te verbeteren. Het is voor Nederland interessant om te bezien welke lessen zij kan leren van de vernieuwingen in de Verenigde Staten. In dit hoofdstuk zal de case van terrorismebestrijding in de Verenigde Staten beschreven worden (paragraaf 3.1), alsmede de lessen die Nederland hieruit kan halen (paragraaf 3.2).

3.1. Data matching in de Verenigde Staten

3.1.1. Achtergrond

De centrale vraag in de Verenigde Staten naar aanleiding van de aanslag van 11 september was hoe een aanslag van deze grote onopgemerkt kon blijven door de FBI en andere verantwoordelijke organisaties. De FBI, CIA en andere diensten hadden informatie over het mogelijk gebruik van vliegtuigen als wapens, er stond een aantal terroristen op watchlists, er waren verdenkingen tegen buitenlandse studenten op Amerikaanse vliegscholen en er waren gegevens van verdachte financiële transacties. Deze gegevens op zich vormen geen duidelijke aanwijzing voor een aanslag, de combinatie van deze gegevens wel. Ten tijde van de aanslag konden de systemen van de verschillende instanties niet met elkaar communiceren, omdat elke organisatie een eigen systeem met eigen standaarden had. Integrale veiligheidsinformatie ontbrak hierdoor. Een belangrijke conclusie naar aanleiding van de aanslag was dan ook dat de gegevensuitwisseling tussen deze organisaties niet goed georganiseerd was en verbeterd moest worden²⁰.

¹⁹ Verschillende onderzoeken naar aanleiding van rampen wezen uit dat de informatievoorziening omtrent veiligheid in Nederland beter kan. Zie bijvoorbeeld onderzoeken naar aanleiding van Enschede, Volendam en de aanslag op Pim Fortuyn.

²⁰ Statement of Robert J. Jordan of the FBI on 'Information Sharing Initiatives', 17 april 2002.

3.1.2. Fundamentele veranderingen

Oprichting van het Ministerie van Binnenlandse Veiligheid

In de Verenigde Staten houden 22 organisaties zich bezig met binnenlandse veiligheid. De verantwoordelijkheid voor het functioneren van deze organisaties lag voorheen bij verschillende ministeries. Dit maakte de coördinatie van beleid in het algemeen en gegevensuitwisseling in het bijzonder, erg lastig. Na 11 september was de noodzaak voor gegevensuitwisseling duidelijk. Daarom is besloten om de verschillende organisaties die zich bezig houden met binnenlandse veiligheid te verenigen in één ministerie, het Ministerie van Binnenlandse Veiligheid²¹. Als voorloper hierop richtte president Bush in oktober 2001 de Office of Homeland Security (OHS) op, dat binnenkort over zal gaan in het ministerie. Dit was het begin van de meest intensieve reorganisatie van de federale overheid sinds de oprichting van het Ministerie van Defensie in 1947. Een van de belangrijke taken van het ministerie is de coördinatie van *terrorism intelligence*; het verzamelen en analyseren van gegevens om terroristische aanslagen te voorkomen en terroristen op te sporen.

Het samengaan van 22 organisaties in één ministerie en het zorgen voor een goede samenwerking tussen de organisaties is een complexe opdracht. Om het ministerie effectief te laten opereren, is een aantal actielijnen geformuleerd²². Allereerst zal er een organisatiearchitectuur worden ontworpen, waarin de processen van de organisaties op elkaar afgestemd worden. In deze architectuur komt ook naar voren welke informatiebehoefte er bij de organisaties zijn. Ten tweede zal de communicatie tussen de technische systemen van de organisaties (22 infrastructuren en rond de 500 applicaties) verbeterd worden, met name de beveiliging en betrouwbaarheid van transacties. Ten derde zal er een werkbaar model voor kennisdeling ontwikkeld worden, waarin gegevens kunnen worden omgezet in informatie. Tenslotte zal getracht worden om de culturen van de organisaties naar elkaar te laten toegroeien.

Verandering van de wetgeving

In de strijd tegen terrorisme is ook de wetgeving aangepast. In het verleden waren wettelijke en bestuurlijke barrières vaak de oorzaak van een gebrekkige uitwisseling van gegevens. Door de invoering van de 'USA Patriot Act' in oktober 2001 en de 'Homeland Security Information Sharing Act' in april 2002 zijn deze barrières voor een groot deel weggenomen. De USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) geeft de regering een aantal nieuwe bevoegdheden tot het observeren van burgers en het aftappen van communicatiemiddelen. De Homeland Security Information Sharing Act geeft organisaties meer mogelijkheden voor de uitwisseling van gegevens ten behoeve van de binnenlandse veiligheid. In deze wet staat bijvoorbeeld:

'het congres vindt dat federale, statelijke en lokale organisaties informatie voor de binnenlandse veiligheid moeten uitwisselen zoveel als praktisch haalbaar is'.

Publieke opinie en wetenschap geven hiertegen echter soms signalen van protest af. De privacy van individuele burgers zou niet worden gerespecteerd door deze wet. Ook wordt de situatie wel vergeleken met de situatie van de 50-er en 60-er jaren, toen er speciale

²¹ 'Department of Homeland Security Reorganization Plan', November 25, 2002.

²² 'Integrating America', CIO Magazine, by Todd Datz, December 1, 2002.

politieteams waren om 'communistische spionnen' te pakken, en er veel onschuldige mensen zijn opgepakt.

3.1.3. Werkwijze

In de informatievoorziening van de veiligheidssector in de Verenigde Staten kunnen twee soorten gegevensuitwisseling worden onderscheiden, namelijk: horizontale en verticale gegevensuitwisseling²³. Horizontale gegevensuitwisseling is gegevensuitwisseling tussen verschillende landelijke inlichtingendiensten zoals de FBI, CIA, Douane, etc. Verticale gegevensuitwisseling is gegevensuitwisseling tussen inlichtingen- en opsporingsdiensten op verschillende niveaus, zoals gegevensuitwisseling tussen lokale, staats- en federale diensten.

Horizontale gegevensuitwisseling

De inlichtingendiensten houden apart van elkaar gegevens bij in hun databases. De koppeling van deze databases kan zeer waardevolle informatie opleveren over verdachte acties van personen en organisaties. Uitwisseling van gegevens is hiervoor echter niet voldoende; er moet ook een analyse van de gegevens plaatsvinden. Hiertoe zijn de Verenigde Staten bezig om een werkbaar model voor kennisdeling te ontwikkelen.

Er is gekozen voor het principe 'capture once, reuse many'²⁴, wat men in Nederland authentieke bronnen noemt. De databases van de inlichtingen- en veiligheidsdiensten (zoals FBI, CIA, Douane) worden toegankelijk gemaakt voor het Ministerie van Binnenlandse Veiligheid. Het ministerie heeft de taak om de gegevens uit de verschillende databases te sorteren, filteren en analyseren. Het ministerie krijgt dus geen analytische rapporten, maar alleen onverwerkte gegevens. De analyses van het ministerie worden weer verspreid over de organisaties. Er komt dus geen grote centrale database in Washington DC, maar de gegevens worden decentraal verzameld en opgeslagen. Om de gegevens te analyseren wordt gebruik gemaakt van bestaande technologieën op het gebied van data mining. Met deze technologie is men in staat om de inhoud van verschillende databases te combineren en te analyseren. Zo kunnen er nieuwe inzichten ontstaan in bewegingen en activiteiten van terroristen.

De databases zullen zo worden opgezet dat er specifieke gegevens uit te genereren zijn en mensen niet overspoeld worden met niet relevante gegevens. Gemeenschappelijke standaarden voor informatie-uitwisseling ontbreken op dit moment. Het ministerie zal deze standaarden ontwikkelen en opleggen aan de inlichtingendiensten. Hiertoe krijgt het ministerie zeggenschap over de aanschaf en ontwikkeling van nieuwe informatiesystemen door de organisaties.

Verticale gegevensuitwisseling

Voor de bestrijding van terrorisme is ook gegevensuitwisseling tussen organisaties op verschillende niveaus, verticale gegevensuitwisseling, essentieel. Verdachte personen houden zich immers niet aan de grenzen van de jurisdictie van opsporings- en inlichtingendiensten. In de Verenigde Staten heeft men een aantal oplossingen om deze gegevensuitwisseling te faciliteren, namelijk het Law Enforcement Online (LEO), het Regional Information Sharing System (RISS), Joint Terrorism Task Forces (JTTF) en een Terrorism Watch List (TWL). Deze oplossingen zullen nu besproken worden.

²³ 'The Enemy is Within', P. Paulson, Director of Homeland Security.

²⁴ 'Integrating America', CIO Magazine, by Todd Datz, December 1, 2002.

Law Enforcement Online (LEO)²⁵

LEO is het nationale intranet van de FBI. Elke handhavingsorganisatie heeft toegang tot dit intranet. Het intranet wordt gebruikt als communicatiekanaal tussen de verschillende organisaties. Zo wordt er bijvoorbeeld kennis uitgewisseld door best practices, staat er algemene informatie over bepaalde onderwerpen die voor veel organisaties van belang zijn en zijn er e-mail- en chat-functies.

Regional Information Sharing Systems (RISS)²⁶

Dit is een systeem dat bestaat uit 6 regionale centra en het LEO die gegevens uitwisselen en de aanpak coördineren van criminele netwerken die over de jurisdictionele grenzen van opsporingsorganisaties heen werken. Het systeem vergroot de mogelijkheden van lokale en statelijke handhavingorganisaties om criminelen te identificeren, te volgen en op te pakken. RISS integreert verschillende netwerken met verschillende technologie. De gegevensuitwisseling verloopt via een beveiligd intranet waar 5700 handhavingsorganisaties in alle 50 staten en de federale inlichtingsdiensten toegang toe hebben.

Joint Terrorism Task Forces (JTTF)²⁷

Om de informatiestromen te stroomlijnen heeft het Ministerie van Binnenlandse Veiligheid Joint Terrorism Task Forces opgericht. Dit zijn teams die toezicht houden op de informatiestromen tussen federale, statelijke en lokale wethandhavers. De teams bestaan uit vertegenwoordigers van het Ministerie van Defensie en andere overheidsorganisaties en zorgen ervoor dat alle organisaties op elk niveau zo goed mogelijk profiteren van de informatie die door andere organisaties gecreëerd wordt. Om de teams in deze taak te ondersteunen, is het Ministerie van Binnenlandse Veiligheid bezig met een project om de gegevens uit de databases van de lokale, statelijke en federale wethandhavers te koppelen en te analyseren. Daartoe wordt een data warehouse gebouwd, waarin de databases van alle participerende organisaties worden gecombineerd. Daarna worden meerdere analyse instrumenten gebruikt om snel informatie uit te wisselen en te vinden.

Terrorism Watch List (TWL)²⁸

De Terrorism Watch List is de unieke, geïntegreerde lijst van de FBI met daarop gegevens over verdachte individuen die in verband worden gebracht met terrorisme. Er worden drie categorieën onderscheiden. De lijst van de eerste categorie bevat namen van mensen die formeel aangeklaagd zijn of die formeel verdacht worden van een terroristische activiteit. Op de lijst van de tweede categorie staan mensen waar de FBI onderzoek naar doet. De lijst van de derde categorie bevat namen van mensen die door de veiligheidsdiensten en buitenlandse regeringen worden aangedragen. De lijst is toegankelijk voor alle handhavingsorganisaties en veiligheidsdiensten. De namen op de lijst zijn gebaseerd op informatie van FBI, JTTF, veiligheidsdiensten, het Ministerie van Defensie en buitenlandse overheden.

²⁵ www.fbi.gov/hq/cjisd/leo.htm, geraadpleegd op 22-1-2003.

²⁶ www.iir.com/riss, geraadpleegd op 22-1-2003.

²⁷ 'The National Strategy for Homeland Security', Office of Homeland Security, July 16, 2002.

²⁸ 'The National Strategy for Homeland Security', Office of Homeland Security, July 16, 2002.

3.1.4. Verbeteringen

Voorgaande beschreven fundamentele veranderingen van de inrichting van de veiligheidssector en informatievoorziening leiden tot de volgende concrete verbeteringen:

- Terrorisme kan effectiever worden bestreden doordat men over meer integrale informatie beschikt. Hierdoor wordt de veiligheid in de Verenigde Staten verhoogd. Doordat men over betere informatie beschikt is men beter in staat risico's in te schatten en terrorisme op te sporen en te bestrijden.
- Een maatschappelijk effect kan op de langere termijn zijn dat er een groter gevoel van veiligheid onder de burgers van de Verenigde Staten ontstaat en men meer vertrouwen krijgt in het functioneren van de veiligheidsdiensten.

3.1.5. Barrières

Opvallend is dat tot 11 september 2001 in de Verenigde Staten weinig vernieuwing ten aanzien van de informatievoorziening in de veiligheidssector plaatsvond. Hoewel bekend was dat de gegevensuitwisseling tussen veiligheidsinstanties niet goed geregeld was, kwamen innovaties op dit vlak niet van de grond. Dergelijke projecten kregen geen prioriteit en er was geen geld voor beschikbaar. Na de aanslagen van 11 september is deze situatie totaal veranderd. President Bush erkende vlak na de aanslagen dat de gebrekkige gegevensuitwisseling tussen betrokken organisaties een reden was dat de aanslagen niet voorzien waren. De president gaf absolute prioriteit aan het oplossen van dit probleem. Ook het congres en de senaat zagen de noodzaak hiervan in. Daarmee werden alle belemmeringen om aan de slag te gaan weggevaagd. Binnen 6 weken na de aanslagen was de 'USA Patriot Act', de wet die opsporingsinstanties veel meer bevoegdheden geeft, aangenomen en ook de oprichting van een nieuw ministerie ging in sneltreinvaart.

De competitieve cultuur van de inlichtingendiensten en andere organisaties vormde voor 11 september ook een barrière voor de verbetering van de informatievoorziening. Organisaties als de FBI en de CIA waren in het recente verleden sterk gericht op de geheimhouding van hun eigen gegevens en op de bescherming van hun jurisdictie. Hierdoor werd de uitwisseling van gegevens bemoeilijkt. De oprichting van het nieuwe ministerie, dat de verzameling en analyse op zich neemt, verhelpt dit probleem. Nu kan van bovenaf aan de inlichtingendiensten worden opgelegd dat deze hun gegevens beschikbaar moeten maken. Ook is de wil om samen te werken en vooral de noodzaak tot samenwerking na de aanslagen van 11 september voor iedereen duidelijk.

3.2. Informatie-uitwisseling in de Nederlandse veiligheidssector

3.2.1. Situatieschets

In Nederland ligt de taak van terrorismebestrijding primair bij de Algemene Inlichtingen- en Veiligheidsdienst, de AIVD. Deze dienst is verantwoordelijk voor de preventie van terroristische aanslagen en voor de vervolging van terroristen. Een belangrijk onderdeel van deze taak is de verzameling van gegevens met betrekking tot 'gevaarlijke' personen en organisaties. Onder gevaarlijke organisaties en personen wordt verstaan: 'organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor

andere gewichtige belangen van de staat²⁹. Hiertoe heeft de AIVD een aantal bevoegdheden gekregen in de 'Wet op de inlichtingen- en veiligheidsdiensten 2002', zoals het observeren van personen, het inzetten van under-cover agenten, het aftappen van communicatiemiddelen (telefoon, e-mail), etc. Ook heeft de AIVD de bevoegdheid om aan andere bestuursorganen en ambtenaren om informatie te vragen.

De AIVD werkt voor de bestrijding van terrorisme samen met andere organisaties. In Nederland zijn dit de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de politie en het Ministerie van Justitie. Vooral de samenwerking tussen AIVD, politie en Justitie is cruciaal voor de bestrijding van terrorisme. De AIVD vormt de voorkant van de terrorismebestrijding. Als er sprake is van 'een redelijk vermoeden van schuld aan de voorbereiding of uitvoering van terroristisch handelen'³⁰, komen politie en Justitie in actie. De politie kent een speciaal team, de Unit Terrorismebestrijding en Bijzondere Taken (UTBT), onderdeel van het Korps Landelijke Politiediensten (KLPD), dat de opsporing en de aanhouding van vermeende terroristen voor zijn rekening neemt. De vervolging ligt in handen van het Openbaar Ministerie. Dit ministerie heeft hiervoor een Landelijke Officier van Justitie voor Terrorismebestrijding (LOvJT) aangesteld. Daarnaast vormen de LOvJT en de AIVD samen met het KLPD het afstemmingsoverleg terrorisme, waarin de activiteiten van de organisaties worden afgestemd.

De informatie-uitwisseling tussen bovengenoemde organisaties is van groot belang voor de bestrijding van terrorisme. Om de gegevensuitwisseling tussen KLPD en AIVD optimaal te laten verlopen, is er een liaison van de KLPD aangesteld bij de AIVD. Verder zijn ook de Regionale Inlichtingendiensten (RID's) van groot belang voor de AIVD. Deze organisaties hebben als taak het signaleren van politieke radicaliseringstendenzen. De AIVD maakt ook gebruik van gegevens van rechtbanken in Nederland. De gegevensverstrekking van de rechtbanken aan de AIVD gaan via de Officier van Justitie.

In het rapport van de Regieraad ICT³¹ uit 2001 wordt de informatiehuishouding van de politie onder de loep genomen. Hieruit blijkt dat het ontbreken van een overkoepelende infrastructuur en de incompatibiliteit van de applicaties een grote belemmering vormden voor een goede informatie-uitwisseling tussen de organisaties. De raad deed dan ook aanbevelingen om deze situatie te verbeteren. Uit het rapport van de Commissie Van den Haak over de beveiliging van Pim Fortuyn blijkt dat er echter nog nauwelijks resultaten zijn behaald, de informatie-uitwisseling tussen de veiligheidsinstanties verloopt nog steeds niet zoals zou moeten. Een belangrijke conclusie van het rapport van de commissie is dat 'zowel de horizontale als de verticale uitwisseling van informatie erg te wensen over laat'³². Hiervoor is volgens het rapport een aantal oorzaken.

Verticale informatie-uitwisseling

Het ontbreken van een overkoepelende nationale informatiehuishouding vormt een groot probleem. In de uitwisseling van informatie tussen regionale korpsen en het landelijke politiekorps en AIVD speelt het landelijke politiebestedel, zoals dat in Nederland bestaat, een grote rol. De politie is opgedeeld in 25 regionale korpsen en een landelijk korps. Deze korpsen beschikken over grote autonomie op bestuurlijk en operationeel niveau en

²⁹ 'Wet op de inlichtingen- en veiligheidsdiensten 2002', art 6.2.a Staatsblad van het Koninkrijk der Nederlanden, jaargang 2002.

³⁰ Jaarverslag BVD 2001.

³¹ 'Bestek 2001-2005', Regieraad ICT van de politie.

³² Rapport 'De Veiligheid en Beveiliging van Pim Fortuyn, Feiten en Verantwoordelijkheden', Commissie Van den Haak, 2002.

mogen hun eigen keuzes maken over informatiesystemen. Ook hebben de regionale korpsen vaak hun eigen databases. Hierdoor vormt de politieke informatiehuishouding geen geïntegreerd geheel en komt de informatieverstrekking neer op eigen initiatief van de betrokken organisaties. Bij de landelijke en regionale korpsen bestaat echter geen cultuur van gegevensuitwisseling; men beperkt men zich liever tot eigen gegevens. Deze culturele barrière leidt ertoe dat belangrijke gegevens niet bij de KLPD en AIVD terechtkomen.

In de gegevensuitwisseling tussen Regionale Inlichtingendiensten (RID's) en AIVD bestaat geen institutionele barrière, zoals het politiebestedel. De AIVD is een gedeconcentreerde rijksdienst, oftewel de regionale korpsen en de AIVD vormen organisatorisch een twee-eenheid. De AIVD-centrale en de RID-en kunnen, zonder tegengehouden te worden door institutionele barrières, vrij informatie uitwisselen. Dit gebeurt in de praktijk echter nauwelijks, aldus de Commissie Van den Haak.

Horizontale informatie-uitwisseling

De genoemde organisaties die zich bezig houden met het bestrijden van terrorisme vallen onder verschillende ministeries. De AIVD en politie vallen onder het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Officier van Justitie valt onder het Ministerie van Justitie. Om de samenwerking tussen deze ministeries vorm te geven bestaan twee interdepartementale adviesorganen, namelijk de Grote Evaluatiedriehoek (GED) en de Technische Evaluatiecommissie (TEC). In de TEC zijn de Ministeries van Binnenlandse Zaken, Justitie en Defensie en de AIVD vertegenwoordigd. De GED bestaat uit vertegenwoordigers van de Ministeries van Binnenlandse Zaken en Justitie. In de praktijk blijkt dat er nauwelijks verschil is tussen deze organen, beide geven advies aan het gezag over beveiligings- en bewakingsmaatregelen. Dit bemoeilijkt de informatie-uitwisseling tussen departementen omdat niet duidelijk is wie zich waarmee bezig zou moeten houden. Bovendien zijn hierdoor verantwoordelijkheden met betrekking tot de informatie-uitwisseling niet helder.

3.2.2. Wat kan Nederland leren van de Verenigde Staten?

Zoals uit de beschrijvingen van de cases blijkt, zijn de problemen met de gegevensuitwisseling in Nederland en de Verenigde Staten vergelijkbaar. Er zijn politieke, culturele en juridische barrières om tot een goede gegevenshuishouding te komen. In de Verenigde Staten is men echter voortvarend van start gegaan om de situatie te verbeteren, aangespoord door de aanslagen van 11 september. In Nederland kan men een aantal lessen leren van de Verenigde Staten.

Verankering op hoog politiek niveau en middelen

Een belangrijke les die kan worden geleerd is het feit dat veranderingen alleen dan kunnen worden gerealiseerd, wanneer het probleem op hoog politiek niveau verankerd is en verantwoordelijkheden om te komen tot verbeteringen worden toegewezen aan een politieke probleemhebber die de middelen (waaronder budget) krijgt om verbeteringen door te voeren. In de Verenigde Staten heeft de president opdracht gegeven tot het verbeteren van de informatievoorziening in de veiligheidssector en is de minister van Binnenlandse Veiligheid verantwoordelijk voor de realisatie van verbeteringen. De minister van Binnenlandse Veiligheid beschikt over de middelen om te komen tot verbeteringen. Hierdoor kunnen de Verenigde Staten verbeteringen voortvarend en integraal aanpakken.

Gegevensuitwisseling met een decentrale gegevensopslag

Een andere les betreft de gegevensuitwisseling tussen regionale korpsen en de landelijke organisaties. Deze gebeurt in de Verenigde Staten veelal elektronisch en in twee richtingen. Er is een aantal netwerken opgezet dat de gegevensuitwisseling faciliteert, doordat organisaties gegevens aan anderen kunnen sturen, maar ook doordat organisaties in de databases van anderen kunnen kijken.

Tactisch omgaan met culturele barrières

In de Verenigde Staten verzamelt het ministerie de gegevens uit de databases van FBI, CIA en andere organisaties. De culturele bezwaren van rechtstreekse gegevensuitwisseling worden zo weggenomen.

Een belangrijk verschil tussen de situatie in de Verenigde Staten en de situatie in Nederland is het juridisch kader. In de Verenigde Staten is een aantal juridische bezwaren tegen gegevensuitwisseling verdwenen door de veranderde wetgeving na 11 september. In Nederland is dit niet gebeurd. Binnen de huidige wetgeving blijken echter nog veel verbeteringen op het gebied van gegevensuitwisseling mogelijk.

3.2.3. Vernieuwingsagenda

Uitgaande van een brede interpretatie van het vraagstuk veiligheid kunnen we stellen dat er in Nederland de laatste jaren meerdere explosieve situaties zijn geweest (Enschede³³, Volendam en de aanslag op Fortuyn) waarbij elke keer bleek dat gebrekkige informatievoorziening en een zwakke informatiepositie van de overheid één van de belangrijke oorzaken was van het falende overheidsoptreden. Organisaties blijken keer op keer autonoom wat betreft de inrichting van hun werkprocessen en de daarbij horende informatisering. Resultaat van die autonomie is gebrekkige informatie-uitwisseling die mede de oorzaak is van het falende optreden. Met andere woorden: willen overheden effectief optreden en presteren naar het niveau dat de samenleving eist, dan zullen organisaties beter moeten samenwerken, hetgeen inhoudt dat zij hun werkprocessen op elkaar afstemmen en niet langer meer denken in 'hun' informatie. Zij zullen horizontale en verticale arrangementen moeten ontwikkelen om tot een goede, gemeenschappelijk informatiehuishouding te komen. Dat is een noodzakelijke, maar niet voldoende voorwaarden voor effectief overheidsoptreden. Bestuurlijke autonomie zal, in ieder geval op deelterreinen (inrichting werkprocessen, informatievoorziening) ingeleverd moeten worden.

Om in de Nederlandse situatie te komen tot verbeteringen zal er daarnaast voor gezorgd moeten worden dat er verankering is op hoog politiek niveau. Uit het rapport van de commissie Kraak komt niet het beeld naar voren dat dat inmiddels zo is. Het kabinet moet de noodzaak zien om te komen tot fundamentele verbeteringen van de informatievoorziening in de veiligheidssector. Vervolgens moet een Minister expliciet verantwoordelijk worden gesteld voor de door te voeren verbeteringen. Dan pas is het politieke klimaat geschapen waarbinnen een ambtelijk projectleider, mits deze organisatorische en financiële ruimte krijgt, een gedegen plan kan ontwerpen voor een integrale herziening van de informatieprocessen binnen de veiligheidssector. Op grond van de herziening van de informatieprocessen zou binnen het project een interdisciplinair en interorganisationeel team aan de slag kunnen gaan om te komen tot een concept voor informatie-uitwisseling tussen de instanties. Interdisciplinair omdat vanuit

³³ Rapport van de Commissie Oosting.

verschillende perspectieven, zoals: juridisch, organisatorisch, informatiekundig perspectief gezamenlijk kan worden gezocht naar oplossingen. Interorganisationeel zodat de verschillende belanghebbende instanties vanuit hun specifieke deskundigheid betrokken zijn.

4. Voedselveiligheid

De verschillende voedselcrisissen, zoals de BSE-crisis, de Varkenspest en de MKZ-crisis, hebben ertoe geleid dat voedselveiligheid hoog op de Nederlandse politieke agenda staat. Er wordt intensief gedebatteerd over mogelijke verbeteringen in de voedingssector. De heersende opinie is dat de voedselketen transparanter moet worden gemaakt. Enerzijds moet transparantie bijdragen aan het wegnemen van het vertrouwensprobleem van de consument. De consument moet in de supermarkt kunnen zien hoe het product tot stand is gekomen en wat er precies in het product is verwerkt, zodat hij keuzes kan maken om het product al dan niet te kopen. Anderzijds moet transparantie bijdragen aan het beter kunnen bestrijden van uitbraken van ziekten. Wanneer het besmettingsgebied preciezer kan worden aangewezen, zullen er bijvoorbeeld minder dieren preventief hoeven te worden afgemaakt.

De discussies over voedselveiligheid en maatregelen om de veiligheid te waarborgen, beperken zich niet tot Nederland. In veel (met name westerse) landen wordt door overheden, in samenspraak met bedrijven, gezocht naar oplossingen om meer grip te krijgen op de kwaliteit van voedsel. Veel oplossingen worden gezocht in het verbeteren van de informatievoorziening in de voedselketen. In Duitsland tracht men met behulp van een authentieke registratie en een elektronische dierpas voedingsmiddelen traceerbaar te maken. In dit hoofdstuk zullen we deze Duitse case beschrijven (paragraaf 4.1), alsmede de lessen de Nederland hieruit kan leren (paragraaf 4.2).

4.1. Duitse elektronische database en dierpas

In de Duitse voedselketen maakt men gebruik van een centrale elektronische database voor runderen in combinatie met een etiketteringssysteem, om volledige transparantie in de rundvleesketen - van geboorte tot en met het product in de supermarkt - te kunnen bewerkstelligen³⁴. De elektronische database en het etiketteringssysteem zijn respectievelijk in 1999 en 1998 ingevoerd. Recentelijk is een pilot gestart om met behulp van een dierpas meer gegevens van runderen automatisch te registreren.

4.1.1. Achtergrond

Halverwege de jaren '90 werd Duitsland - net als veel andere Europese landen - geconfronteerd met runderen die geïnfecteerd waren met het BSE-virus. Veel dieren moesten preventief worden afgemaakt en consumenten hadden geen enkel vertrouwen meer in de kwaliteit van rundvlees. Sindsdien staat de voedselveiligheid hoog op de Duitse politieke agenda. Als gevolg van latere crisissen, zoals de MKZ-crisis, heeft de voedselveiligheid nog steeds grote prioriteit binnen het regeringsbeleid in Duitsland³⁵. De regering heeft vanaf de jaren '90 verschillende maatregelen genomen om de veiligheid van voedsel zeker te stellen, 'von Erzeuger bis zum Verbraucher'³⁶.

³⁴ 'Zur Tierkennzeichnung', agrar.de.

³⁵ Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft, 'Zukunft der Tierhaltung', juli 2002.

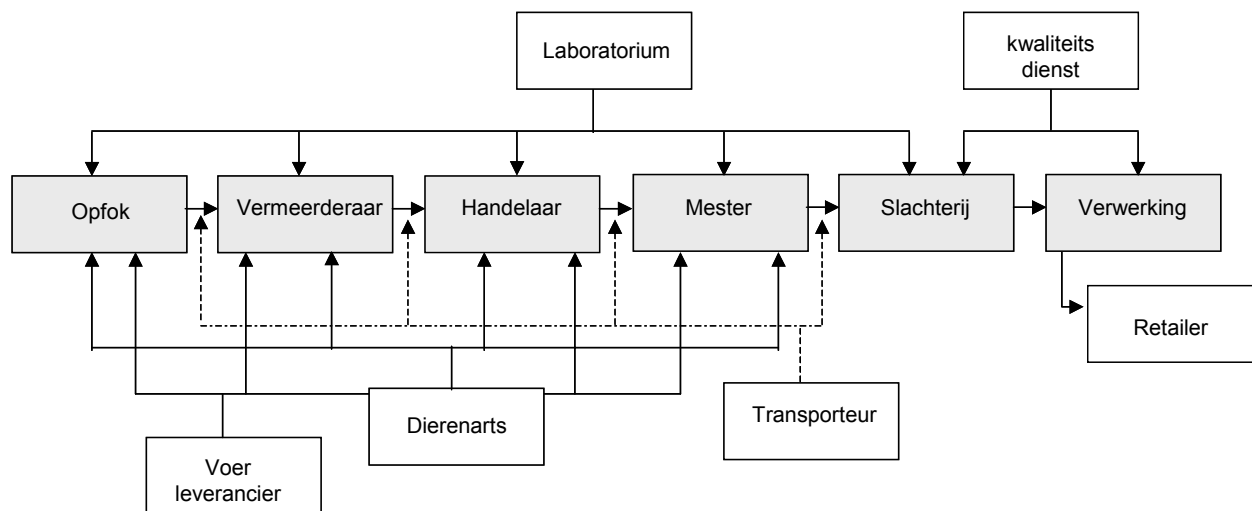
³⁶ Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft, 'Vertrauen durch Veränderung', september 2001.

De belangrijkste maatregelen die in Duitsland op centraal niveau zijn genomen naar aanleiding van de crisissen, zijn de volgende:

- In 1996 is in Duitsland een centraal registratiesysteem voor runderen geïmplementeerd. Elk rund dat wordt aangemeld krijgt een uniek nummer, een 'Kennzeichnung', waaraan verschillende gegevens over het betreffende dier zijn verbonden.
- Sinds 1 juli 1998 moet rundvlees geëtiketteerd worden, waarbij de herkomst van het vlees wordt aangegeven. Het systeem van etikettering sluit aan bij de centrale runderregistratie, waardoor een dier in de hele keten (geboorte, slacht, verwerking, etc.) traceerbaar is.
- In februari 2002 is men gestart met een pilot project met de dierpas, waardoor meer gegevens over dieren beschikbaar zijn voor meer participanten in de voedselketen en op een meer toegankelijke wijze.

4.1.2. Werkwijze

Op 26 september 1999 heeft men in Duitsland een centrale elektronische database voor runderen opgericht. In deze database zijn alle runderen in Duitsland geregistreerd. De database is opgericht om voedselveiligheid te kunnen garanderen, door verbeterde transparantie van de keten. In de database staan alle fases die een rund doorloopt en de betrokkenen zijn verplicht om binnen een bepaalde termijn 'aangifte' te doen wanneer zij eigenaar worden van een dier of een dier verkopen³⁷. Bij de geboorte of aankoop van een rund wordt het rund aangemeld door de boer. Ook als de boer het rund verkoopt of naar de slacht brengt, meldt de boer dit. Het slachthuis meldt het als een rund het slachthuis binnengebracht wordt en als het geslacht wordt. Een handelaar meldt het als hij runderen koopt en verkoopt. De bedrijven van markten, verzamelplaatsen en landbouwtentoonstellingen melden toegang en afgang van runderen. Zo worden alle fases van de rundvleesketen vastgelegd in de database en zijn dus later terug te vinden.



Figuur 2. Ketenweergave runderen³⁸

³⁷ www.hi-tier.de.

³⁸ Ketenweergave door de heer T. van Rheenen.

Runderen kunnen op drie manieren worden aangemeld of afgemeld³⁹.

- Er bestaat de mogelijkheid om met behulp van papieren formulieren aangifte te doen. Van deze mogelijkheid wordt steeds minder gebruik gemaakt, maar de Duitse regering wil deze mogelijkheid blijven bieden voor degenen die - om welke reden dan ook – geen gebruik kunnen of willen maken van andere methoden van aangifte.
- Telefonische aangifte.
- Aangifte via Internet. Deze wijze van aanmelding wordt door het Ministerie van Landbouw sterk aangeprezen en gestimuleerd. Bijna 80 procent van de 120.000 meldingen per dag worden via het Internet gedaan.

De database vormt de basisregistratie voor de verschillende betrokkenen in de keten. In de database zijn gegevens opgenomen zoals: het unieke nummer van het betreffende rund, de geboortedatum van het rund, het bedrijf waar het rund geboren is, alle verhandelingsbedrijven en bedrijven waar het rund is gehouden, het slachthuis waar het rund is geslacht⁴⁰. De rundveehouders, slachtbedrijven, veeartsen, etiketteringsinstanties, premie-instanties en andere betrokkenen van de keten hebben toegang tot (delen van) de database. Het tijdig aanmelden en afmelden van runderen is bij wet geregeld⁴¹. Wanneer een bedrijf of instantie een rund niet tijdig of niet correct registreert, wordt de premie voor het betreffende rund geblokkeerd⁴². Dit is de belangrijkste prikkel voor het correct en tijdig aanmelden en afmelden van runderen. Inspectieautoriteiten controleren de juistheid van gegevens bij het bezoeken van bedrijven. Het aantal incorrecte meldingen blijkt erg laag te zijn.

Gegevens omtrent de voeding en medicatie van de runderen zijn tot nog toe niet opgenomen in de centrale elektronische database. Voor de veiligheid van vleesproducten is het niet alleen van belang dat van elk stuk vlees bekend is van welk dier het afkomstig is, maar ook welk voedsel dit dier heeft gekregen en welke medicijnen e.d. het dier heeft gehad. Om ook op dit punt transparantie te kunnen bereiken is men in februari 2002 in de Duitse deelstaat Schleswig-Holstein begonnen met het pilot-project 'Elektronischer Tierpass', oftewel de elektronische dierpas⁴³. Dit is een chip die in het oor van het dier wordt geplaatst, in de plaats van het oormerk. Op deze chip staan, naast een aantal gegevens over het dier (geboortedatum, herkomstsoort, afstamming), ook gegevens over andere belangrijke zaken (voer, inenting en gezondheidsstatus). De gegevens worden opgeslagen in de centrale runderregistratie. De elektronische dierpas onderscheidt zich van het oormerk, doordat de gegevens op de pas kunnen worden aangepast door de boer of dierenarts, in overleg met de gerechtigde veterinaire. Door de toevoeging van de informatie omtrent voer, medicatie, etc. wordt de hele keten transparanter. Zo maakt de dierpas het mogelijk dat in het slachthuis alle gegevens over het dier bekend zijn, zodat kwaliteitscontrole efficiënter en grondiger kan worden uitgevoerd. Ook kunnen consumenten in de winkel zien waar het vlees vandaan komt en welke stoffen er in het product zijn verwerkt.

³⁹ 'Hi-Tier', Herkunftssicherungs- und informationssysteme für Tiere, www.hi-tier.de.

⁴⁰ Gesetz über die Verarbeitung und Nutzung der zur Durchführung der Rechtsakte der Europäischen Gemeinschaft über die Kennzeichnung und Registrierung von Rindern erhobenen Daten (Rinderregistrierungsdurchführungsgesetz - RiRegDG).

⁴¹ Bundesgesetzblatt, 'Bekanntmachung der Neufassung der Viehverkehrsverordnung', Vom 11. April 2001.

⁴² Ministerium für Ernährung und Ländlichen Raum Baden-Württemberg, 'Merkblatt für die Gewährung der Sonderprämie für männliche Rinder und der Allgemeinen Schlachtprämie sowie tierbezogener Ergänzungsbeiträge', 2002.

⁴³ 'Modelproject Elektronischer Tierpass', agrar.de.

4.1.3. Verbeteringen

Transparantie

De centrale elektronische runderregistratie zorgt op een aantal manieren voor meer transparantie en daardoor verbeteringen in de voedselketen. Ten eerste kunnen bedrijven en instellingen op elk moment opvragen bij welke bedrijven het rund is geweest (van geboorte tot slacht). Dit is een groot voordeel indien een bepaalde ziekte (zoals BSE) uitbreekt. Met deze informatie kunnen maatregelen op effectieve wijze genomen worden. Op de tweede plaats kunnen consumenten op het etiket van een product de herkomst van het vlees en de verwerkte stoffen zien. De consument heeft zo goed inzicht waar het vlees vandaan komt, wat de exacte ingrediënten zijn en kan op grond van deze informatie een beslissing nemen tot het al dan niet kopen van het product. Het vertrouwen van de consument in producten neemt door deze transparantie toe.

Lastenverlichting

Doordat gebruik wordt gemaakt van een één authentieke registratie hoeven de verschillende betrokkenen in de keten (voor wat betreft de gegevens in de authentieke registratie) geen eigen registraties meer te voeren. De bedrijven kunnen uitgebreide informatie over hun runderen in de centrale database vinden en kunnen gebruik maken van een register volgens de EU-specificaties, die zij anders zelf zouden hebben moeten opzetten. In de pilot van deelstaat Schleswig-Holstein gaat het delen en hergebruiken van gegevens nog verder. Hier kunnen ook dierenartsen, voerleveranciers en laboratoria gegevens invoeren en gebruik maken van (delen van) de database. Daarbij worden de kosten van het registreren van de runderen gedrukt, doordat de aangifte via Internet direct in de database kan worden geplaatst, zonder dat daar extra werk in zit voor de beheerorganisatie van de database.

Gegevens van de gehele rundvleesketen gestroomlijnd

In de pilot van de deelstaat Schleswig-Holstein worden gegevens gestroomlijnd die betrekking hebben op de gehele keten. Betrokkenen uit het eerste deel van de keten (opfok tot en met mesten, zie figuur 2) zijn voornamelijk geïnteresseerd wanneer een rund zich waar bevond. Deze gegevens zijn van belang bij het bestrijden van besmettelijke ziekten. Belanghebbenden uit het tweede deel van de keten (bijvoorbeeld Unilever en Ahold) zijn juist erg geïnteresseerd in welk voer en welke medicatie dieren hebben gehad. Dit levert hen informatie op over de kwaliteit van het vlees. Bovendien kan de consument gedetailleerdere informatie worden geboden omtrent de stoffen die zijn verwerkt in een product. De Duitsers zijn er in de pilot van Schleswig-Holstein in geslaagd om de gehele keten meer transparant te maken.

Efficiëntie en effectiviteit

Door gebruikmaking van de dierpas zijn in het slachthuis alle gegevens over het te slachten dier bekend, zodat kwaliteitscontrole efficiënter en grondiger kan worden uitgevoerd.

4.1.4. Barrières

Om dit project van de grond te krijgen moest er bij de betrokken partijen (boeren, ondernemers, politici) de wil gekweekt worden om hieraan mee te werken. Deze barrière is door de BSE-crisis geslecht. De minister-president van de deelstaat Schleswig-Holstein zegt hierover: 'De BSE-crisis was een heilzame schok, die van de ene op de andere dag de toekomst van de landbouw en de zekerheid van levensmiddelen op de

politieke agenda heeft geplaatst'⁴⁴. Deze crisis heeft ook de consument wakker geschud. Deze wilde plotseling echt meer weten over de herkomst en bewerking van vleesproducten. Hierdoor is de retail, maar zijn ook boeren (door de retail) gedwongen om aan vernieuwingen te werken om te komen tot meer transparantie.

Een andere belemmering voor een adequate informatievoorziening betrof het feit dat ondernemers runderen niet tijdig of niet correct aanmeldden of afmeldden. Dit is ondervangen doordat het tijdig aanmelden en afmelden van runderen sinds 2001 bij wet is geregeld⁴⁵. Wanneer een bedrijf of instantie een rund niet tijdig of niet correct registreert, wordt de premie voor het betreffende rund geblokkeerd⁴⁶. Dit is de belangrijkste prikkel voor het correct en tijdig aanmelden en afmelden van runderen. Inspectieautoriteiten controleren de juistheid van gegevens bij het bezoeken van bedrijven. Het aantal incorrecte meldingen blijkt erg laag te zijn.

4.2. De Nederlandse runderadministratie

4.2.1. Situatieschets

Zoals in de inleiding al werd aangegeven, staat voedselveiligheid in Nederland hoog op de politieke agenda. Dit is het gevolg van een aantal crisissen (BSE, MKZ, varkenspest, etc.) wat werd versterkt door het feit dat het crisisapparaat van het ministerie van Landbouw Natuur en Visserij (LNV) onvoldoende bleek toegerust om een crisis van een dergelijke omvang in zijn totaliteit te beheersen. De publieke opinie keerde zich tegen het massaal ruimen van dieren. De massale ruiming was nodig, omdat de risicogroep onvoldoende precies aangegeven kon worden doordat de vastlegging van diergegevens niet adequaat genoeg geregeld was.

De landbouwsector in Nederland is georganiseerd in productschappen. Dit zijn corporaties waarin het bedrijfsleven en de overheid samenwerken en waarin de wetten die door de overheid worden opgelegd worden omgezet in meer gedetailleerdere regels en beleid. Ten tijde van de crises waren de productschappen verantwoordelijk voor de registratie van runderen in de zogenaamde I&R-database (Identificatie & Registratie database). In deze database staan alle verplaatsingen die een dier maakt, dus van geboorte tot slacht. Door de samenwerking in de productschappen en het gedeelde rekenschap binnen de productschappen was er geen duidelijke ministeriële verantwoordelijkheid voor de kwaliteit en het beheer van de I&R-database. In het tweede kabinet Kok (1998-2002) is de verantwoordelijkheid voor de I&R-database bij de Dienst Basisregistraties van het Ministerie van LNV neergelegd. In de I&R registratie worden alle verplaatsingen die een dier maakt bijgehouden; wat betekent dat wanneer een dier geboren wordt dit door de boer aangemeld moet worden. Vervolgens moet elk bedrijf waar het dier geweest is het dier aanmelden en afmelden. De bedrijven zijn zelf verantwoordelijk voor de aanmelding en voor de juistheid van de gegevens, het ministerie zorgt voor het beheer en de kwaliteit van de gegevens.

⁴⁴ 'Modellprojekt 'Elektronischer Tierpass' vorgestellt', @grar.de

⁴⁵ Bundesgesetzblatt, 'Bekanntmachung der Neufassung der Viehverkehrsverordnung', Vom 11. April 2001.

⁴⁶ Ministerium für Ernährung und Ländlichen Raum Baden-Württemberg, 'Merkblatt für die Gewährung der Sonderprämie für männliche Rinder und der Allgemeinen Schlachtprämie sowie tierbezogener Ergänzungsbeiträge', 2002.

De informatievoorziening van de keten als geheel laat te wensen over⁴⁷. Een belangrijke oorzaak hiervan is gelegen in het feit dat de informatievoorziening zich niet richt op de hele keten, maar voornamelijk op het eerste deel van de keten (opfok tot en met slacht). Hierdoor zijn onvoldoende gegevens beschikbaar die van belang zijn bij de verwerking van rundvlees door de retail. De informatievoorziening heeft als belangrijkste doel om uitbraken van dierziekten te bestrijden en richt zich daarbij op verplaatsingen van dieren in de voorkant van de keten; het fokken tot en met het slachten. Medicatiegegevens van runderen worden door de individuele veeartsen in eigen databases geregistreerd⁴⁸. Gegevens over voeding van runderen worden door de individuele boeren in eigen registraties bijgehouden⁴⁹. De gegevens over medicatie, voeding en de gezondheid van een rund zijn niet gekoppeld aan de gegevens van de I&R en kunnen niet worden uitgewisseld. Hierdoor is bepaalde informatie omtrent runderen en rundvlees - in vergelijking met de situatie in Schleswig-Holstein - moeilijk te genereren. Wanneer retailbedrijven - of de consument - bijvoorbeeld willen weten welke stoffen precies in een product zijn verwerkt (waaronder stoffen die voortvloeien uit medicatie en voeding), zullen deze gegevens (in vergelijking met de situatie in Schleswig-Holstein) niet eenvoudig te verkrijgen zijn. Bij de verschillende bedrijven die het betreffende rund hebben gehouden en de betrokken veeartsen zal moeten worden nagegaan welke voeding en medicatie het dier heeft gehad⁵⁰. Een ander voorbeeld betreft het geval dat een veevoeder verboden ingrediënten in voer heeft verwerkt. In Schleswig-Holstein is dan exact en op eenvoudige wijze te achterhalen welk rund het betreffende voer heeft gehad. In Nederland zal meer moeite moeten worden gedaan om die gegevens te achterhalen en de juistheid van de gegevens is onzekerder. De rundvleesketen is in Nederland dan ook maar in beperkte mate transparant.

De oorzaak van het feit dat de informatievoorziening omtrent runderen zich slechts richt op een bepaald deel van de keten kan zijn dat er sprake is van een versnippering van beleid over de betrokken departementen (LNV, VWS, EZ en VROM) waar het gaat om voedselveiligheid⁵¹. Waar het Ministerie van LNV de problematiek omtrent runderen benaderd vanuit het perspectief van agrariërs (bestrijden van ziekten - eerste deel van de keten), richt het Ministerie van VWS zich op de volksgezondheid (inspectie omtrent kwaliteit van voedsel - met name het laatste deel van de keten). Het Ministerie van EZ gaat uit van de belangen van de consument (prijs-kwaliteit verhouding - het laatste deel van de keten) en het Ministerie van VROM richt zich op milieuvraagstukken (eerste deel van de keten). Naast versnippering van beleid leidt institutionele fragmentatie ertoe dat

⁴⁷ In deze casestudie hebben wij de rundvleesketen onderzocht, maar ook in andere voedselketens laat de informatievoorziening te wensen over. Zie bijvoorbeeld: Voortgang I&R TRC 2002/1003, waarin het volgende wordt geschreven over de registratie van schapen en geiten: 'In tegenstelling tot runderen is voor schapen en geiten op dit moment geen centraal identificatie en registratiesysteem beschikbaar. Deze situatie is in het kader van de dieziektebestrijding (MKZ, scrapie) onwenselijk en kan niet worden gecontinueerd tot medio 2004'.

⁴⁸ Aldus Gezondheidsdienst voor dieren.

⁴⁹ Aldus Keuringsdienst diervoedersector.

⁵⁰ Het Ministerie van LNV is voornemens een aanbesteding te doen voor het ontwikkelen en invoeren van een nieuw I&R-systeem (zie: Voortgang I&R, TRC 2002/7591). Uit de kamerstukken blijkt niet dat ook voeding en medicatie van runderen in een nieuwe registratie worden meegenomen.

⁵¹ Deze versnippering wordt o.a. geconstateerd in 'het invensteringspakket, innovatienetwerk op het gebied van vertrouwd, lekker, gezond en veilig voedsel' van Food Delta, augustus 2001. Ook wordt versnippering geconstateerd in de nota 'Impuls voor vernieuwing, organisatie-ontwikkeling bij LNV', Ministerie LNV, 2001.

niemand zich verantwoordelijk voelt voor de voedselketen als geheel. Elk ministerie is verantwoordelijk voor en heeft bevoegdheden ten aanzien van een deel van de keten, waardoor geen van de ministeries rekenschap geeft over de hele keten. Om te komen tot een volledige transparantie in de rundvleesketen 'van geboorte tot bord' is een integrale benadering en eenduidige verantwoordelijkheid noodzakelijk. Hiervoor is het niet noodzakelijk dat organisatie of instituten integreren maar dat afstemming wordt gewaarborgd en de verantwoordelijkheid voor de keten als geheel wordt toegewezen.

4.2.2. Wat kan Nederland leren van Duitsland?

In Duitsland loopt men wat betreft voedselveiligheid voor op Nederland. De voedselketens in Nederland kunnen veel transparanter worden, wanneer er een adequate informatievoorziening wordt gerealiseerd. Wat kan Nederland leren van de Duitse situatie?

Verankering op hoog politiek niveau en middelen

De verschillende voedselcrisisen hebben er in Duitsland toe geleid dat hoge prioriteit is gesteld aan het transparant maken van de hele voedselketen. Hierdoor is de informatievoorziening voortvarend verbeterd en worden geëxperimenteerd met innovatieve projecten zoals in Schleswig-Holstein. Institutionele fragmentatie leidt er in de Nederlandse situatie toe dat er geen probleemhebber is voor de voedselketen als geheel: geen ministerie voelt zich voor de hele keten verantwoordelijk.

Stroomlijning basisregistraties

In de pilot Schleswig-Holstein wordt informatie met behulp van authentieke registraties zoveel mogelijk gedeeld en hergebruikt. Bovendien beslaat de informatievoorziening de hele runderketen. Nederland kent momenteel verschillende registraties binnen de voedselketen welke gestroomlijnd zouden moeten worden. Voor de rundvleesketen is het van belang dat belanghebbenden de beschikking hebben over eenduidige en volledige informatie omtrent runderen en rundvlees in de hele keten. Om te komen tot een brede benadering van de informatievoorziening omtrent voedselveiligheid zullen de departementen intensief moeten samenwerken. De rundvleesketen - en ook de ander voedselketens - overstijgen de grenzen van de afzonderlijke departementen en zo ook de processen en informatie die aan de rundvleesketen (of andere voedselketens) ten grondslag ligt.

Lastenverlichting

Verschillende belanghebbenden in de keten hebben in Duitsland toegang tot de elektronische registraties. Omdat men alle gegevens in authentieke registraties ter beschikking heeft en (geautoriseerde) betrokkenen gegevens kunnen invoeren en raadplegen, hoeven afzonderlijke betrokkenen zelf minder te registreren (namelijk: alleen dat deel waar men voor verantwoordelijk is). Dit leidt in de Duitse situatie tot lastenverlichting en zou in de Nederlandse situatie dezelfde effecten kunnen hebben.

4.2.3. Vernieuwingsagenda

Om te komen tot bovenstaande verbeteringen zouden de processen en informatievoorziening van de gehele voedselketen gestroomlijnd moeten worden. Verschillende innovatieve projecten zijn vanuit verschillende departementen gestart. Ministeries gaan echter te geïsoleerd te werk; een brede aanpak van het voedselveiligheidsvraagstuk ontbreekt. Wanneer men wil komen tot een effectieve

uitvoering van beleid omtrent voedselveiligheid (waarvan de rundvleesveiligheid nog maar één onderdeel is), dan zullen betrokken organisaties beter moeten samenwerken.

Zolang er op hoog politiek niveau geen uitspraak is gedaan om te komen tot verbeteringen van de processen en informatievoorziening van de voedselketen in zijn geheel en niemand daarvoor verantwoordelijk is, is de kans groot dat departementen langs elkaar heen blijven werken. Om te komen tot integrale verbeteringen zal hiertoe een beslissing moeten worden genomen op het hoogste politieke niveau en zal een minister verantwoordelijk moeten gesteld voor het bereiken van resultaten.

5. Conclusie

In de voorgaande hoofdstukken is een aantal buitenlandse innovaties in de vorm van cases beschreven. Daarbij is aangegeven wat deze innovaties in de buitenlandse situatie hebben opgeleverd en wat Nederland hiervan kan leren. Wanneer we de verschillende cases in samenhang analyseren, valt het op dat - op alle drie de gebieden (Sociale Zekerheid, Terrorismebestrijding en Voedselveiligheid) - er in de Nederlandse situatie belemmeringen zijn, waardoor sectorbrede innovatie niet van de grond komt. Dit terwijl deze sectorbrede innovaties in het buitenland wel van de grond komen.

In de Verenigde Staten is men er - in tegenstelling tot Nederland - in geslaagd om terrorismebestrijding adequater te laten plaatsvinden met behulp van een slimme manier van gegevensuitwisseling. Zwart werk wordt in België effectiever en efficiënter bestreden dan in Nederland door de invoering DIMONA-aangifte. Deze elektronische aangifte is mogelijk doordat de informatievoorziening in de gehele Sociale Zekerheid in België gestroomlijnd is. De rundvleesketen in Duitsland is transparanter dan die in Nederland. Informatie over runderen en rundvlees is in de hele keten voorhanden, 'von Erzeuger bis zum Verbraucher'. In de Belgische Sociale Zekerheid en de Duitse rundvleesketen worden de administratieve lasten voor de betrokken ondernemers gereduceerd.

Waarom lukt het niet om in Nederland soortgelijke verbeteringen van de grond te krijgen? Er is geen sprake van een technologische barrière; allerlei hoogstaande technologieën zijn op de markt te verkrijgen. In de cases zien we de volgende barrières:

1. Institutionele barrière. Nederland vormt een decentrale eenheidsstaat, waarin taken en verantwoordelijkheden gedecentraliseerd zijn. Dit kan een barrière zijn voor innovatie. Vaak hebben organisaties een verregaande autonomie op het gebied van informatiesystemen. Zo hebben de regionale politiekorpsen, als gevolg van deze autonomie, allemaal verschillende systemen die niet met elkaar kunnen communiceren. Ook blijkt vaak dat innovaties niet van de grond komen als er verschillende ministeries bij betrokken zijn, die moeten samenwerken. Dit kwam bijvoorbeeld naar voren in de case van voedselveiligheid, waar de Ministeries van VWS en LNV moeten samenwerken om een goede registratie te ontwikkelen. Verschil in de belangen bij de departementen blijkt een terugkomende hindernis. Niet alleen bij het bewaken van de voedselveiligheid, maar ook bij de bestrijding van terrorisme blijkt dit een belangrijke barrière.
2. Politieke barrière. In Nederland ontbreekt het vaak aan een probleemhebber en – verantwoordelijke op hoog politiek niveau. De oorzaak hiervan is dat er vaak meerdere ministeries betrokken zijn bij maatschappelijke vraagstukken en waar een aantal organisaties verantwoordelijk is, blijkt niemand zich verantwoordelijk te voelen. Politieke steun is veelal onmisbaar voor het tot stand komen van sectorbrede innovaties. In België was er steun op hoog politiek niveau en ook in de VS was deze steun aanwezig.
3. Financiële barrière. Een factor die de totstandkoming van innovaties blijkt te belemmeren is het feit dat er geen geld voor wordt vrijgemaakt.
4. Culturele barrière. Keer op keer blijkt dat er tussen de betrokken organisaties geen cultuur van gegevensuitwisseling en samenwerking te bestaan. De politie houdt liever haar gegevens voor zichzelf, omdat men niet vertrouwt dat de andere organisaties zorgvuldig met de informatie omgaan. Ook staan (medewerkers van) organisaties er meestal niet om te springen om werkprocessen te laten aansluiten op de

werkprocessen van andere organisaties. Men begeeft zich liever binnen de grenzen van de organisatie dan dat men over de grenzen van de organisatie heen kijkt.

In het buitenland speelden deze barrières vaak ook een rol. Toch is men er daar wel in geslaagd om de innovaties in te voeren. Nederland kan daar een aantal lessen van leren:

1. Verankering op hoog politiek niveau. Zowel in de VS als in België was steun voor de innovaties op hoog politiek niveau. Hierdoor werd het mogelijk om verbeteringen op voortvarende en samenhangende wijze te ontwikkelen en door te voeren.
2. Gebruik authentieke registraties als fundament. In alle drie onderzochte cases wordt gebruik gemaakt van authentieke registraties waarbij gegevensbeheer en opslag decentraal plaatsvinden. Hierdoor blijft de autonomie van participerende organisaties gehandhaafd, en kan ook de privacy beschermd worden.
3. Voldoende financiële middelen. In de buitenlandse cases werd voldoende financiële ruimte gegeven om hoogwaardige oplossingen te ontwikkelen.
4. Wel samenhang geen integratie. In de verschillende buitenlandse cases is gekozen voor een koppeling van (authentieke) gegevens die decentraal opgeslagen en beheerd worden. Hierdoor blijven de gegevens dicht bij de bronnen en wordt de autonomie van de betrokken partijen - tot op zekere hoogte - gerespecteerd. Deze, voor betrokken partijen minder bedreigende opzet kan veel strijd en weerstand voorkomen
5. Draagvlak bij participerende organisaties. Wanneer deelnemende organisaties voordeel hebben van een innovatie zullen ze veel eerder geneigd zijn mee te werken aan de implementatie ervan. In België en Duitsland hebben betrokken organisaties bijvoorbeeld baat bij een goede registratie, omdat hun administratieve lasten verlicht worden. Draagvlak kan ook gekweekt worden door een proef te starten in een probleemsector, zoals in de Belgische sociale zekerheid is gebeurd met de DIMONA-aangifte. Door successen te halen in een probleemsector kan in andere sectoren draagvlak gekweekt worden.